Starke Authentisierung – jetzt!

Detlef Hühnlein[1] · Christine Ziske[2] ·Tina Hühnlein[1]
Tobias Wich[1] · Daniel Nemmert[1] · Sebastian Rohr[3]
Markus Hertlein[4] · Cornelius Kölbel[5]

[1]ecsec GmbH
vorname.nachname@ecsec.de

[2]KikuSema GmbH
christine.ziske@kikusemamail.de

[3]accessec GmbH
rohr@accessec.com

[4]XignSys GmbH
hertlein@xignsys.com

[5]NetKnights GmbH
cornelius.koelbel@netknights.it

Zusammenfassung

Vor dem Hintergrund der zahlreichen Sicherheitsvorfälle bei Anbietern von Online-Diensten und den damit verbundenen, oftmals millionenschweren Fällen von Identitätsdiebstahl im Jahr 2016 hat sich kürzlich eine verbandsübergreifende Arbeitsgruppe "Starke Authentisierung - jetzt!" gegründet, die darauf abzielt, den praktischen Einsatz von starken Authentisierungsmechanismen im Internet durch Sensibilisierung von Nutzern und Anbietern von Online-Diensten zu fördern und den Weg zum Einsatz geeigneter Authentisierungsverfahren im Internet zu ebnen. Der vorliegende Beitrag stellt erste Zwischenergebnisse dieser für alle interessierten Personen und Organisationen offenen und gemeinnützigen Initiative vor und ruft gleichzeitig zur Mitwirkung sowie zur aktiven Nutzung von starken Authentisierungsmechanismen im Internet auf.

1 Einleitung

Obwohl inzwischen viele sichere und benutzerfreundliche Mechanismen zur starken Authentisierung im Internet existieren, werden diese bislang in der Praxis oft noch nicht eingesetzt. Trotz der bekannten Schwächen erfolgt die Anmeldung an Online-Diensten im Regelfall einfach mit Benutzername und Passwort. Auf der anderen Seite belegen die zahlreichen Sicherheitsvorfälle bei Anbietern von Online-Diensten und den damit verbundenen, oftmals millionenschweren Fällen von Identitätsdiebstahl im Jahr 2016[1], dass statische Passwörter im Internet

[1] Siehe z.B. [Yahoo], [LinkedIn], [Twitter], [Dropbox], [Badoo], [DailyMotion], [Rambler] und [VKontakte].

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 444-456.

alleine keinen ausreichenden Schutz mehr bieten und zukünftig im Einklang mit den einschlägigen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik[2] und EU-weit geltenden Regularien[3] stärkere Mechanismen zur Authentisierung eingesetzt werden müssen.

Deshalb hat sich eine verbandsübergreifende Arbeitsgruppe "Starke Authentisierung - jetzt!" gebildet, die darauf abzielt, den praktischen Einsatz von starken Authentisierungsmechanismen im Internet durch Sensibilisierung von **Endnutzern** und **Anbietern von Online-Diensten** zu fördern und den Weg zum Einsatz geeigneter Authentisierungsverfahren im Internet zu ebnen. Der vorliegende Beitrag stellt die für alle interessierten Personen und Organisationen offene, gemeinnützige Initiative vor und ruft gleichzeitig zur Mitwirkung sowie zur aktiven Nutzung von starken Authentisierungsmechanismen im Internet auf.

Der weitere Beitrag ist folgendermaßen gegliedert: Abschnitt 2 erläutert, was unter einer „starken Authentisierung“ zu verstehen ist. Abschnitt 3 liefert einen Überblick über die in der Praxis typischerweise genutzten Verfahren zur starken Authentisierung. Außerdem wird gezeigt, wie die Integration der starken Authentisierung erfolgen kann (Abschnitt 4), welche Open Source Komponenten und zertifizierten Authentisierungsdienste dafür zur Verfügung stehen (Abschnitt 5) und wo heute bereits starke Authentisierung eingesetzt wird (Abschnitt 6). Schließlich findet sich in Abschnitt 7 eine kompakte Zusammenfassung des Beitrags.

2 Was ist eine „starke Authentisierung“?

Wie in [Hühn08] erläutert, ist die *Identität* einer Entität durch die Menge der ihr zugeordneten *Attribute* bestimmt. Dies umfasst bei einer natürlichen Person z.B. Name, Anschrift, Geburtsdatum, Kontonummer, E-Mail-Adresse, Telefonnummer und bei einer juristischen Person neben dem Namen und der Anschrift z.B. eine Registernummer, eine Steuernummer, die Umsatzsteuer-ID und den Verweis auf vertretungsberechtigte natürliche Personen. Aus Gründen der Datensparsamkeit (vgl. § 3a BDSG) wird man nicht in jedem Kontext alle Attribute einer natürlichen Person verwenden, sondern nur die im konkreten Fall notwendige Untermenge (*partielle Identität*)[4], die möglicherweise nur aus einem anwendungsspezifischen *Pseudonym* bestehen kann.

Die *Authentisierung* ist das Aufstellen einer Behauptung über eine solche partielle Identität und die *Authentifizierung* ist die Prüfung dieser Behauptung[5]. Hierfür können unterschiedliche Verfahren sowie *Authentifizierungsfaktoren* aus den Bereichen Besitz, Wissen und Biometrie eingesetzt werden. Bei einer *dynamischen Authentifizierung*[6] werden im Regelfall kryptographische Mechanismen eingesetzt, so dass sich die Daten zum Nachweis der Identität bei jedem Authentifizierungsvorgang ändern. Von einer *starken Authentifizierung*[7] spricht man, wenn zusätzlich mindestens zwei unabhängige Faktoren eingesetzt werden.

---

[2] Siehe z.B. [BSI11a] und [BSI11b].

[3] Siehe z.B. [2014/910/EU], [2015/1502/EU], [2015/2366/EU] und [2016/679/EU].

[4] Siehe [ClKö01]

[5] Siehe z.B. [2015/1502/EU] Anhang (Abschnitt 1 Nr. 2 und Abschnitt 2.3) und [2015/2366/EU] Artikel 4 Nr. 29.

[6] Siehe [2015/1502/EU] Anhang, Abschnitt 1 Nr. 3.

[7] Vgl. [2015/1502/EU] Anhang (Abschnitt 1 Nr. 2 und Abschnitte 2.2.1 und 2.3) und [2015/2366/EU] Artikel 4 Nr. 29 und Artikel 97.

Bei einer ***„starken Authentisierung“*** werden also zwei unabhängige Faktoren in einem dynamischen Protokoll zum Nachweis der Identität oder der Autorisierung einer Transaktion genutzt.

Eine solche starke Authentisierung wird beispielsweise gemäß Artikel 97 [2015/2366/EU] für den Zugriff auf ein Zahlungskonto oder bei einem elektronischen Identifizierungssystem ab dem Sicherheitsniveau „substanziell“ gemäß Artikel 8 [2014/910/EU] gefordert und entspricht dem beim Schutz von personenbezogenen Daten gemäß Artikel 32 [2016/679/EU] zu berücksichtigenden Stand der Technik.

3 Welche Verfahren werden in der Praxis genutzt?

In der wissenschaftlichen Literatur[8] und in internationalen Standards[9] finden sich unzählige unterschiedliche Verfahren für die Authentifizierung, so dass die vollständige Aufzählung aller existierenden Verfahren sicherlich den Rahmen des vorliegenden Beitrags sprengen würde bzw. grundsätzlich unmöglich erscheint. Vielmehr wurde im Rahmen der Diskussion unter den in der verbandsübergreifenden Arbeitsgruppe mitwirkenden Experten ein grobes Klassifizierungsschema entwickelt, in das sich die in der Praxis eingesetzten Verfahren einteilen lassen.

Eine generelle Beobachtung ist, dass von den grundsätzlich möglichen Faktorkombinationen (Besitz + Wissen, Besitz + Biometrie, Wissen + Biometrie) de facto die Kombination aus Besitz und Wissen klar dominiert und biometrische Authentifizierungsmechanismen im Internet bislang[10] kaum in der Praxis eingesetzt werden.

Aktuell werden für die Authentifizierung im Internet insbesondere die nachfolgend aufgeführten Authentisierungstoken, jeweils in Verbindung mit einem zusätzlichen wissensbasierten Faktor (z.B. PIN), eingesetzt. Kriterien für die Vertrauensniveaubewertung von Authentifizierungsverfahren finden sich in [2015/1502/EU] und [TR-03107-1].

3.1 Elektronischer Personalausweis

Elektronische Ausweisdokumente, wie z.B. der elektronische Personalausweis, können zur starken Authentisierung im Internet genutzt werden. Im Fall des Personalausweises wird hierfür ein geeignetes Kartenterminal[11] oder Smartphone[12] benötigt und das so genannte „Extended Access Control“-Protokoll (Version 2) gemäß [TR-03110] ausgeführt. Für den Zugriff auf die im Ausweis gespeicherten Daten wird ein so genanntes Berechtigungszertifikat benötigt, durch das Bürgerinnen und Bürger die Identität des zugreifenden Online-Dienstanbieters und den Zweck des Datenzugriffs erkennen können. Auf dem Personalausweis sind die in § 18 PAuswG aufgeführten Identitätsattribute (d.h. Familienname, Geburtsname, Vornamen, Doktorgrad, Tag der Geburt, Ort der Geburt, Anschrift, Dokumentenart, Ordensname, Künstlername) gespeichert. Außerdem können mit dem so genannten „dienste- und kartenspezifischen Kennzeichen“

[8] Siehe z.B. [ClJa97], [BoMa03], [WJMM05] und [BRAC09].

[9] Siehe z.B. [ISO9798], [ISO24727], [EN419212], [IEEE1363], [ICAO9303] und [RFC5256].

[10] Allerdings ist damit zu rechnen, dass sich dies im Zuge der breiten Verfügbarkeit von Smartphones mit Fingerabdrucksensor [statista] und entsprechender Standards, wie [FIDO-UAF] und [W3C-WA], mittelfristig ändern dürfte.

[11] Siehe https://www.ausweisapp.bund.de/ausweisapp2/voraussetzungen/

[12] Siehe https://www.ausweisapp.bund.de/download/

sehr datenschutzfreundliche, anwendungsspezifische Pseudonyme berechnet werden und es kann darüber hinaus eine datenschutzfreundliche Altersverifikation oder Wohnortbestätigung durchgeführt werden.

3.2 Signaturtoken

Bei einem Signaturtoken wird zur Authentisierung letztlich eine digitale Signatur über eine so genannte „Challenge“ erstellt, in die eine von der prüfenden Instanz gewählte Zufallszahl einfließt. Wie der letztlich zu signierende Wert gebildet wird, ist bei den verschiedenen auf diesem Prinzip basierenden standardisierten Authentisierungsprotokollen[13] geringfügig unterschiedlich. Das Signaturtoken kann als Signaturkarte ausgeprägt sein, so dass man damit auch qualifizierte elektronische Signaturen erstellen oder Banktransaktionen mittels [FinTS] absichern kann. Um eine Chipkarte zur Authentisierung nutzen zu können, ist ein entsprechendes Chipkartenterminal notwendig, das im Regelfall über die USB-Schnittstelle an einen Rechner angeschlossen wird. Um die Benutzerfreundlichkeit zu erhöhen, kann die Chipkarte mit dem Kartenterminal integriert und beispielsweise als USB-Token realisiert sein. Ein technisch sehr einfach gehaltenes, über USB oder per NFC nutzbares Token, das zur Signatur-basierten Authentisierung – und im Regelfall nur dazu – verwendet werden kann, ist das von der FIDO-Alliance spezifizierte „Universal Second Factor“ (U2F) Token[14].

3.3 TAN- und OTP-basierte Verfahren

Sowohl beim elektronischen Personalausweis als auch bei den Signatur-Token, muss für die Realisierung des Protokollablaufs eine technische Kommunikationsschnittstelle zwischen dem Endgerät des Nutzers (PC, Tablet, Smartphone etc.) und dem kryptographischen Authentisierungstoken vorhanden sein. Für Anwendungsbereiche in denen eine derartige Schnittstelle nicht oder nur schwer realisiert werden kann, empfiehlt sich der Einsatz von Einmalpasswörten (One Time Passwords, OTP), bzw. falls auch zusätzlich Transaktionsdaten abgesichert werden sollen, TAN-basierte Verfahren zur starken Authentisierung, da hier die Übertragung der als Authentisierungscode fungierenden TAN/OTP vom Authentisierungstoken zum Endgerät durch den Nutzer selbst erfolgen kann. Hierbei existieren vielfältige Varianten, die insbesondere danach unterschieden werden können, ob die TAN bzw. das OTP beim Benutzer oder auf der Serverseite erzeugt wird.

Beim chipTAN-Verfahren[15] wird zusätzlich zu einer Bankkarte ein mobiler TAN-Generator zur Entgegennahme der zu schützenden Transaktionsdaten und zur *dezentralen* Erzeugung der TAN benötigt.

Beispiele für die *zentrale* Erzeugung von TANs sind das mobileTAN-Verfahren[16] oder die österreichische Handysignatur[16]. Erwähnenswert erscheint, dass die Sicherheit dieser Verfahren von der offenbar nicht immer gegebenen Sicherheit der für die Übertragung der TAN bzw. des OTP genutzten Mobilfunknetze[17] abhängt.

---

[13] Siehe z.B. [ISO9798] (Part 3), [EN419212], [RFC5256], [RFC4252], [FIDO-RMF] und [W3C-WA].

[14] Siehe https://fidoalliance.org/certification/fido-certified-products/

[15] Siehe [DK-Komp].

[16] Siehe https://www.handy-signatur.at

[17] Siehe https://www.heise.de/newsticker/meldung/Deutsche-Bankkonten-ueber-UMTS-Sicherheitsluecken-ausgeraeumt-3702194.html

Bei Einmalpasswort-Verfahren wird in der Regel aus einem symmetrischen, geheimen Schlüssel und einer Sequenznummer, der Zeit und/oder einer Challenge[18] ein zur starken Authentisierung geeigneter Code erzeugt. Dieser wird wie eine TAN vom Benutzer typischerweise auf einem anderen[19], vertrauenswürdigen Endgerät des Benutzers, z.B. zusätzlich zu einer Authentisierung mit Benutzername und Passwort, in einem entsprechenden Anmeldedialog eingegeben.

Der geheime Schlüssel, mit dem der Benutzer das Einmalpasswort erzeugen kann, ist in einem „Einmalpasswort-Generator“ gespeichert. Hier gibt es unterschiedliche Sicherheitsstufen von einer App auf einem Smartphone über vorinitialisierte OTP-Hardware-Token bis hin zu initialisierbaren Hardware-Token. Eine genauere Sicherheitsbetrachtung von OTP-Token findet sich in [OSS2FA].

3.4 Smartphone-basierte Verfahren

Neben den vorher beschriebenen Verfahren zur starken Authentifizierung werden in der Praxis zunehmend auch Smartphone-basierte Verfahren[20] eingesetzt. Hierbei wird das zur Authentisierung genutzte Schlüsselmaterial in einer sicheren Ausführungsumgebung gespeichert und angewandt. Der Authentisierungsvorgang kann über interne Mechanismen der gängigen Smartphone-Betriebssysteme oder extern per NFC oder durch QR-Code gestartet werden.

Ein Beispiel für den breitflächigen Einsatz eines Smartphone-basierten Verfahrens zur starken Authentisierung und Identifizierung ist die schwedische „E-Legitimation“. Hierbei handelt es sich um ein elektronisches Identifizierungsmittel (eID), das von den schwedischen Banken herausgegeben wird und vom schwedischen Staat legitimiert ist. Mit der BankID / Mobilt BankID können sich Privatpersonen im Internet gegenüber Unternehmen, Banken und Behörden identifizieren und mittels fortgeschrittener elektronischer Signaturen Verträge abschließen. Alle Privatpersonen, die über eine schwedische Personennummer verfügen, können sich eine BankID ausstellen lassen. Für die mobile Authentisierung benötigt der Bürger die schwedische Personennummer, die BankID / Mobilt BankID und die BankID Sicherheits-APP. Die BankID / Mobilt BankID nutzt ein Softtoken bzw. auf der SIM-Karte gespeicherte Schlüssel, ist zwei Jahre lang gültig und kann über die Bank gesperrt werden. Falls man das Passwort vergisst, muss man eine neue BankID beantragen.

Die Verwendung ist sehr einfach: Der Anwender öffnet über einen Browser die Internetseite des gewünschten Dienstleistungsanbieters, z.B. seinen digitalen Behördenbriefkasten. Gleichzeitig muss auf dem Handy die BankID Sicherheits-APP gestartet sein und der Anwender bestätigt die Legitimation oder die Signaturerstellung jeweils mit seinem 8-stelligen Sicherheitscode.

Alle wichtigen Lebensbereiche des Bürgers sind bereits abgedeckt. Es kann z.B. der Zugriff auf medizinische Daten, Krankenversicherung, Arbeitsamt, Elektronischer Postkasten für Behördenbriefe, Kreditauskünfte und nicht zuletzt die elektronische Steuererklärung genutzt werden.

---

[18] Siehe [RFC4226], [RFC6238] und [RFC6287].

[19] Sofern keine physikalische Trennung vorhanden ist, müssen anderweitige Sicherheitsmechanismen zur zuverlässigen Separation der Ausführungsumgebungen vorgesehen werden, um die Sicherheit des Verfahrens gewährleisten zu können (vgl. Artikel 9 [EBA-RTS] und [HaMü16]).

[20] Siehe z.B. [AZE09], [SFG09], [WGM04], [DATEV-SL], [HMP15] und [WGM04].

3.5 Sonstige Verfahren

Wie oben erwähnt, sind grundsätzlich weitere Verfahren zur starken Authentisierung denkbar, die andere Authentisierungstoken und -protokolle sowie zusätzlich oder alternativ zum Faktor Wissen biometrische Merkmale nutzen. Darüber hinaus kann in bestimmten Anwendungsszenarien die Auswertung von zusätzlichen Merkmalen, wie z.B. der aktuelle Ort des Zugreifenden und beispielsweise der Zeitpunkt des Zugriffs, sinnvoll sein.

4 Wie kann die Integration erfolgen?

4.1 Direkte Integration

Im einfachsten Fall erfolgt die Integration eines Verfahrens zur starken Authentisierung, wie in Abbildung 1 angedeutet, direkt in dem Online-Dienst, was insbesondere aus Sicherheitsgründen vorteilhaft sein kann. Auf der anderen Seite ist der Aufwand zur Integration unterschiedlicher Authentisierungsmechanismen oftmals proportional zur Anzahl der unterstützten Verfahren und der Online-Dienst muss immer dann angepasst werden, wenn Änderungen an der eingesetzten Authentisierungstechnologie notwendig werden.

Abb. 1: Direkte Integration

4.2 Integration über spezialisierten Authentisierungsdienst

Um den Prozess der starken Authentisierung von den fachlichen Abläufen in Online-Diensten zu entkoppeln, empfiehlt sich der Einsatz eines spezialisierten Authentisierungsdienstes, der über standardisierte Protokolle für das föderierte Identitätsmanagement angesprochen werden kann. Hierdurch können leicht unterschiedliche Mechanismen zur starken Authentisierung unterstützt und notwendige Fortentwicklungen in der Authentisierungstechnologie ohne Auswirkungen auf den Online-Dienst vorgenommen werden.

In diesem Fall erfolgt nach dem Zugriff des Benutzers auf den Online-Dienst (1) eine Umleitung des Benutzers zum Authentisierungsdienst (2), der die starke Authentifizierung des Benutzers im Auftrag des Online-Dienstes mit einem sicherheitstechnisch geeigneten Verfahren durchführt (3) und das Ergebnis der Authentifizierung in einer gesicherten Weise zum Online-Dienst zurückschickt (4), bevor der Benutzer im Erfolgsfall Zugriff erhält.

Damit die ausgelagerte Authentifizierung nicht missbraucht werden kann, müssen geeignete Sicherheitsmaßnahmen implementiert werden, die regelmäßig im Rahmen von geeigneten Zertifizierungsverfahren (z.B. gemäß ISO 27001 auf Basis vom IT-Grundschutz) geprüft und zertifiziert werden. Soweit im Rahmen der starken Authentifizierung auch personenbezogene Daten verarbeitet werden, sind die Anforderungen des Bundesdatenschutzgesetzes zu berücksichtigen, deren Erfüllung beispielsweise im Rahmen einer Zertifizierung gemäß des Trusted-Cloud-Datenschutz-Profils für Cloud-Dienste nachgewiesen werden kann.

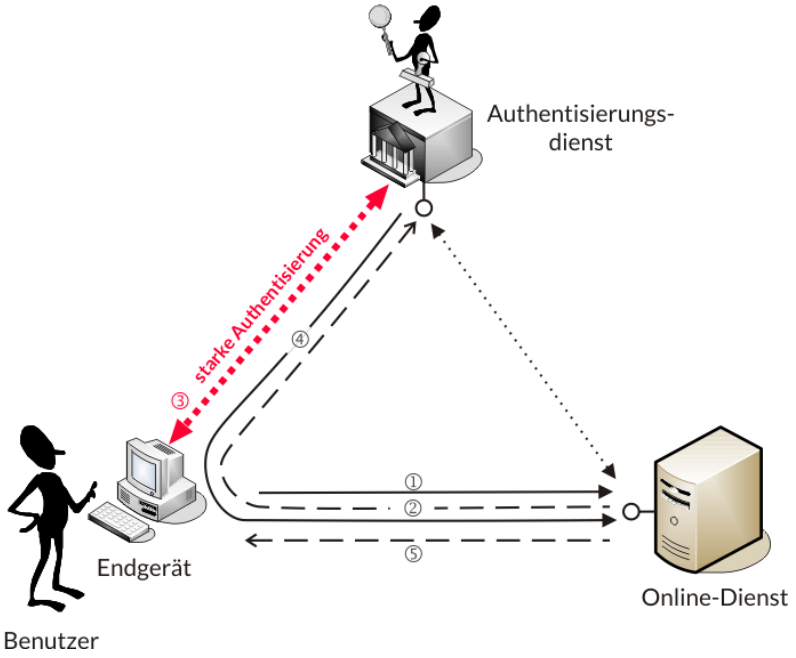

Abb. 2: Integration über spezialisierten Authentisierungsdienst

Das heute am weitesten verbreitete Protokoll für das föderierte Identitätsmanagement und die Auslagerung der starken Authentisierung an einen spezialisierten Authentisierungsdienst ist das im Jahr 2005 vom Security Services Technical Committee der internationalen Standardisierungsorganisation OASIS standardisierte SAML (Security Assertion Markup Language) Protokoll [SAML2], bei dem XML-basierte Nachrichten ausgetauscht werden.

Hierbei wird in Schritt (2) im Zuge der Umleitung an den Authentisierungsdienst ein so genannter `<AuthnRequest>` an den Authentisierungsdienst geschickt und in Schritt (4) das Ergebnis der Authentifizierung in einer `<Response>`-Nachricht an den Online-Dienst zurückgeschickt.

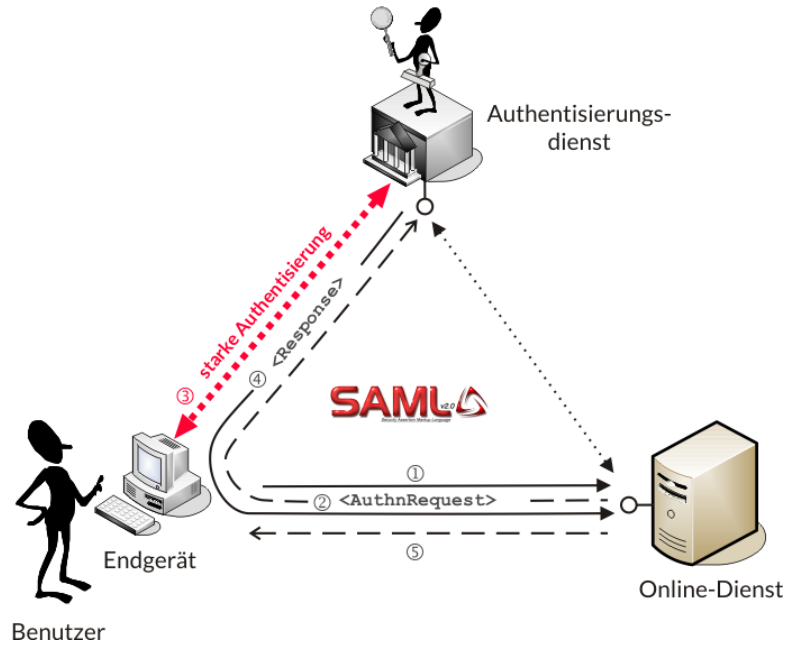

Abb. 3: SAML-basierte Integration

Ein weiteres Protokoll für die Auslagerung der starken Authentisierung ist das auf dem OAuth 2.0 Authorization Framework basierende OpenID Connect Protokoll [OIDC].

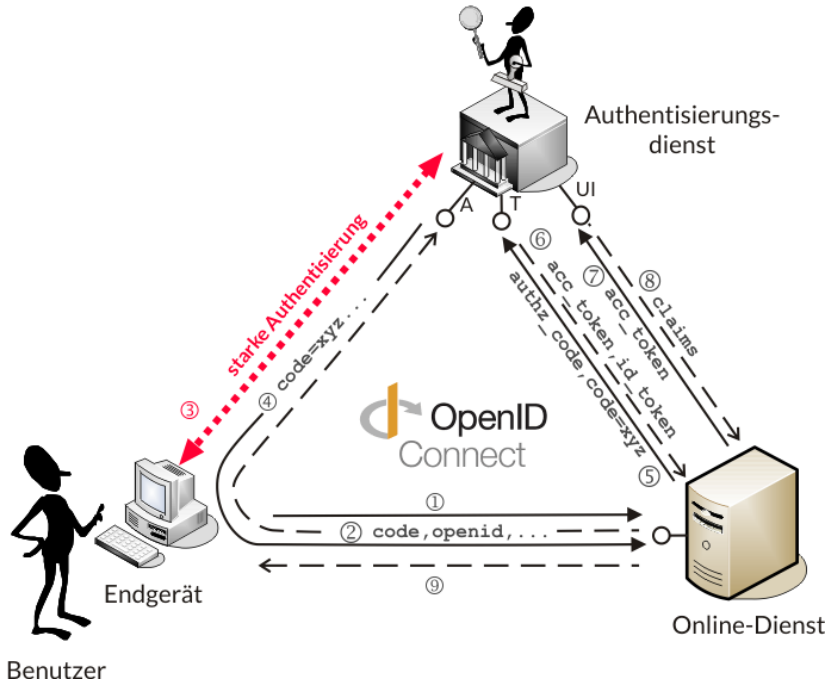

Abb. 4: OpenID Connect-basierte Integration

Anders als bei SAML bietet der Authentisierungsdienst bei OpenID Connect zusätzlich zum Authentisierungsendpunkt weitere Endpunkte (Authorization Endpoint (A), Token Endpoint (T) und UserInfo Endpoint (UI)) an, von den zumindest die ersten beiden im Zuge eines Authentisierungsvorganges vom Online-Dienst angefragt werden müssen, um das Ergebnis der Authentifizierung und möglicherweise weitere Identitätsinformationen (Claims) zu erhalten.

5 Welche Open Source Komponenten und zertifizierte Authentisierungsdienste sind verfügbar?

[OSS2FA] erörtert, dass sowohl der Einsatz offener Standards als auch der Einsatz von Open Source Komponenten für Authentisierungsdienste sinnvoll ist. Für die konkrete Integration der starken Authentisierung stellt sich die Frage, welche **Open Source Software Komponenten**[21] und **zertifizierten Authentisierungsdienste**[22] verfügbar sind. Für diesen Zweck wird in der 2FA.jetzt-Initative aktuell eine entsprechende Übersicht erarbeitet, die längerfristig von der offenen 2FA-Community gepflegt werden soll.

6 Welche Online-Dienste unterstützen bereits 2FA?

Umgekehrt ist es insbesondere für Nutzer interessant, welche Online-Dienste bereits Mechanismen zur starken Authentisierung unterstützen. Auch für diese Zwecke wird aktuell in der

[21] Siehe z.B. [BHH+14], [WPS+13] und [OSS2FA]

[22] Siehe z.B. [HHW+15].

2FA.jetzt-Initiative, gestützt auf Vorarbeiten aus dem US-amerikanisch geprägten „Two Factor Auth (2FA)"-Projekt[23] und dem auf FIDO U2F Token und Einmalpasswort-Generatoren beschränkten „USB-Dongle Authentication“-Projekt[24], eine entsprechende Übersicht erarbeitet, die längerfristig auch von der 2FA-Community gepflegt werden soll.

7 Fazit

Der vorliegende Beitrag hat erste Zwischenergebnisse der verbandsübergreifenden Arbeitsgruppe "Starke Authentisierung - jetzt!" vorgestellt und ruft hiermit zur aktiven Mitwirkung in dieser gemeinnützigen Initiative auf!

Interessierte Personen und Organisationen sind herzlich eingeladen, unter https://2fa.jetzt oder über ask@2fa.jetzt mit der Initiative Kontakt aufzunehmen.

Literatur

[2014/910/EU] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, http://data.europa.eu/eli/reg/2014/910/oj

[2015/1502/EU] Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, http://data.europa.eu/eli/reg_impl/2015/1502/oj

[2015/2366/EU] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, http://data.europa.eu/eli/dir/2015/2366/oj

[2016/679/EU] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, http://data.europa.eu/eli/reg/2016/679/oj

[AZE09] F. Aloul, S. Zahidi, S., W. El-Hajj: *Two factor authentication using mobile phones*, International Conference on Computer Systems and Applications (AICCSA 2009). IEEE/ACS, S. 641-644, (2009)

[Badoo] Heise News: *Dating-Seite Badoo: 127 Millionen Passwort-Hashes im Netz*, 07.06.2016, https://www.heise.de/security/meldung/Dating-Seite-Badoo-127-Millionen-Passwort-Hashes-im-Netz-3228893.html

[23] Siehe http://twofactorauth.org

[24] Siehe http://www.dongleauth.info

[BHH+14] S. Baszanowski, H.-M. Haase, T. Hühnlein, M. Tuengerthal, D. Henze, U. Renz: *Der SkIDentity Cloud Connector*, in: M. Kubach, D. Hühnlein (Hrsg.): Vertrauenswürdige Identitäten für die Cloud: Arbeiten und Ergebnisse des SkIDentity-Projekts, (2014)

[BoMa03] C. Boyd & A. Mathuria: *Protocols for authentication and key establishment*, Springer, (2003)

[BRAC09] D. Bhattacharyya, R. Ranjan, F. Alisherov, M. Choi: *Biometric authentication: A review*. International Journal of u-and e-Service, Science and Technology, 2(3), 13-28, (2009)

[BSI11a] BSI: *Sicherheitsempfehlungen für Cloud Computing Anbieter – Mindestsicherheitsanforderungen in der Informationssicherheit*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile, (2011)

[BSI11b] BSI: *Mindestanforderungen zur Informationssicherheit bei eCommerce-Anbietern*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Mindestanforderungen-eCommerce-Anbieter.pdf?__blob=publicationFile, (2011)

[ClJa97] J. Clark, J. Jacob: *A survey of authentication protocol literature: Version 1.0*, (1997)

[ClKö01] S. Clauß, M. Köhntopp: *Identity management and its support of multilateral security*, Computer Networks, 37(2), S. 205-219, 2001

[DailyMotion] Heise News: *DailyMotion anscheinend gehackt: 87,6 Millionen Nutzer betroffen*, 06.12.2016, https://www.heise.de/security/meldung/Hacker-erbeuten-43-Millionen-Daten-von-Nutzern-des-Web-Baukastens-Weebly-3356684.html

[DATEV-SL] DATEV: *DATEV SmartLogin*, https://www.datev.de/web/de/datev-shop/it-loesungen-und-security/datev-smartlogin/, (2017)

[DK-Komp] Die Deutsche Kreditwirtschaft: *DK-Kompendium Online-Banking-Sicherheit*, Stand: Februar 2014, https://die-dk.de/media/files/DK_Kompendium_Online-Banking-Sicherheit_V1.2.pdf

[Dropbox] Heise News: *Gestohlene Dropbox-Passwörter offenbar echt*, 31.08.2016, https://www.heise.de/security/meldung/Gestohlene-Dropbox-Passwoerter-offenbar-echt-3310017.html

[EBA-RTS] European Banking Authority: Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), 23 February 2017, http://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

[EN419212] EN 419212: *Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services*, Part 1-5, (2017)

[FIDO-RMF] FIDO Alliance: *FIDO U2F Raw Message Formats*, FIDO Alliance Implementation Draft 15 September 2016, https://fidoalliance.org/specs/fido-u2f-v1.1-id-20160915/fido-u2f-raw-message-formats-v1.1-id-20160915.pdf, (2016)

[FIDO-UAF] FIDO Alliance: *FIDO UAF Complete Specifications*, https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202.zip, (2016)

[FinTS] Die Deutsche Kreditwirtschaft: *FinTS – Financial Transaction Services, Schnittstellenspezifikation, Hauptdokument*, Version 4.1, http://www.hbci-zka.de/spec/4_1.htm, (2014)

[HaMü16] V. Haupert, T. Müller: *Auf dem Weg verTAN: Über die Sicherheit App-basierter TAN-Verfahren*, im Tagungsband der „Sicherheit 2016“, Lecture Notes in Informatics (LNI) 256, S. 101-112

[HHW+15] D. Hühnlein, T. Hühnlein, T. Wich, B. Biallowons, M. Tuengerthal, H.-M. Haase, D. Nemmert, S. Baszanowski, C. Bergmann: *SkIDentity – Mobile eID as a Service*, DACH-Security 2015, https://ecsec.de/pub/SkIDentity_DACH2015.pdf, (2015)

[HMP15] M. Hertlein, P. Manaras, N. Pohlmann: *Bring your own device for authentication (BYOD4A). The XignSystem*, In: Pohlmann, N., Reimer, H., Schneider, W. (eds.) Proceedings of the ISSE Securing Electronic Business Processes Highlights of the Information Security Solutions Europe Conference, Springer, (2015)

[HSW+12] D. Hühnlein, J. Schmölz, T. Wich, B. Biallowons, M. Horsch & T. Hühnlein: *Standards und Schnittstellen für das Identitätsmanagement in der Cloud*, DACH Security 2012, http://www.ecsec.de/pub/2012_DACH_IdM.pdf, (2012)

[Hühn08] D. Hühnlein: *Identitätsmanagement – Eine visualisierte Begriffsbestimmung*, Datenschutz und Datensicherheit (DuD), S. 163-165, 2008, http://www.ecsec.de/pub/2008_DuD_Glossar.pdf

[ICAO9303] ICAO: *Doc 9303 – Machine Readable Travel Documents*, Part 1-12

[IEEE1363] IEEE: *IEEE Standard Specifications for Public-Key Cryptography* (2000), *Amendment* (2004), *Password-Based Public-Key Cryptographic Techniques* (2008), *Hard Problems over Lattices* (2009), *Identity-Based Cryptographic Techniques using Pairings* (2013)

[ISO9798] ISO/IEC 9798: *Information technology – Security techniques – Entity authentication*, Part 1-6

[ISO19002] ISO 19092: *Financial services – Biometrics – Security Framework*, (2008)

[ISO24727] ISO/IEC 24727: *Identification cards – Integrated circuit cards programming interfaces, Part 3 – Application interface, Annex A, Authentication Protocols*, 2008

[LinkedIn] Heise News: *LinkedIn-Hack: 117 Millionen Passwort-Hashes zum Download aufgetaucht*, 01.06.2016, https://www.heise.de/security/meldung/LinkedIn-Hack-117-Millionen-Passwort-Hashes-zum-Download-aufgetaucht-3224212.html

[OIDC] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, C. Mortimore: *OpenID Connect Core 1.0*, November 8, 2014, http://openid.net/specs/openid-connect-core-1_0.html

[OSS2FA] K. Cinkler, C. Kölbel: *Zwei-Faktor-Authentifizierung mit Open-Source-Komponenten*, Working Group Security der Open Source Business Alliance, 12.04.2016, http://osb-alliance.de/news/veroeffentlichungen/zwei-faktor-authentifizierung-mit-open-source-komponenten

[Rambler] Heise News: *Fast 100 Millionen Klartextpasswörter von russischem Web-Portal Rambler im Netz*, 07.09.2016, https://www.heise.de/newsticker/meldung/Fast-100-Millionen-Klartextpasswoerter-von-russischem-Web-Portal-Rambler-im-Netz-3315622.html

[RFC4226] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen: *HOTP: An HMAC-Based One-Time Password Algorithm*, RFC 4226, (2005)

[RFC4252] T. Ylonen, C. Lonvick, Ed.: *The Secure Shell (SSH) Authentication Protocol*, RFC 4252, (2006)

[RFC5256] T. Dierks, E. Rescorla: *The Transport Layer Security (TLS) Protocol*, Version 1.2, RFC 5256, (2008)

[RFC6238] D. M'Raihi, S. Machani, M. Pei, J. Rydell: *TOTP: Time-Based One-Time Password Algorithm*, RFC 6238, (2011)

[RFC6287] D. M'Raihi, J. Rydell, S. Bajaj, S. Machani, D. Naccache: *OCRA: OATH Challenge-Response Algorithm*, RFC 6287, (2011)

[RFC6749] D. Hardt: *The OAuth 2.0 Authorization Framework*, RFC 6749, (2012)

[SAML2] S. Cantor, J. Kemp, R. Philpott & E. Maler: *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0.*, https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, (2005)

[SFG09] G. Starnberger, L. Froihofer, K. M. Göschka: *QR-TAN: Secure mobile transaction authentication*, International Conference on Availability, Reliability and Security 2009 (ARES'09). IEEE, 2009

[statista] statista: *Penetration of smartphones with fingerprint sensors worldwide from 2014 to 2018,* https://www.statista.com/statistics/522058/global-smartphone-fingerprint-penetration/

[TR-03110] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token*, BSI TR-03110, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html

[TR-03107-1] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Elektronische Identitäten und Vertrauensdienste im E-Government – Teil 1: Vertrauensniveaus und Mechanismen*, Version 1.1 vom 31.10.2016, 2016, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf?__blob=publicationFile&v=2

[Twitter] Heise News: *33 Millionen Twitter-Passwörter kursieren angeblich im Netz*, 09.06.2016, https://www.heise.de/security/meldung/33-Millionen-Twitter-Passwoerter-kursieren-angeblich-im-Netz-3233021.html

[VKontakte] Heise News: *Nach LinkedIn, Tumblr und MySpace: 171 Millionen VKontakte-Passwörter im Netz*, 06.06.2016, https://www.heise.de/security/meldung/Nach-

LinkedIn-Tumblr-und-MySpace-171-Millionen-VKontakte-Passwoerter-im-Netz-3227916.html

[W3C-WA] V. Bharadwaj, H. Le Van Gong, D. Balfanz, A. Czeskis, A. Birgisson, J. Hodges, M. B. Jones, R. Lindemann, J. C. Jones: *Web Authentication: An API for accessing Scoped Credentials*, W3C Editor's Draft, https://w3c.github.io/webauthn/, (2017)

[Weebly] Heise News: *Hacker erbeuten 43 Millionen Daten von Nutzern des Web-Baukastens Weebly*, 21.10.2016, https://www.heise.de/security/meldung/Hacker-erbeuten-43-Millionen-Daten-von-Nutzern-des-Web-Baukastens-Weebly-3356684.html

[WGM04] M. Wu, S. Garfinkel, R. Miller: *Secure web authentication with mobile phones*, DIMACS workshop on usable privacy and security software, Vol. 2010, (2004)

[WPS+13] T. Wich, D. Petrautzki, J. Schmölz, M. Horsch & D. Hühnlein: *An extensible platform for eID, signatures and more*, Open Identity Summit 2013, LNI 223, S. 55-68, (2013), http://www.ecsec.de/pub/2013_OID_Platform.pdf

[WJMM05] J. Wayman, A. Jain, D. Maltoni, D. Maio: *An introduction to biometric authentication systems*, Springer London, S. 1-20, (2005)

[Yahoo] Heise News: *Yahoo muss erneut Massenhack beichten: Eine Milliarde Opfer*, 15.12.2016, https://www.heise.de/security/meldung/Yahoo-muss-erneut-Massenhack-beichten-Eine-Milliarde-Opfer-3570674.html