Single-Sign-On-Dienste: Überblick und aktuelle Entwicklungen

RTR Fachbereich Telekommunikation und Post (RTR FB TKP)

Stand: 12.07.2021

Management Summary

Single-Sign-On-Dienste (in der Folge: „SSO“) stellen einen wichtigen Dienst in der Wertschöpfungskette des Internets dar. Sie ermöglichen niedrigschwelligen Zugang für Nutzerinnen und Nutzern zu Drittservices durch den Entfall einer nochmaligen Identifikation. Gleichzeitig können diese Dienste aber dazu dienen, die bestehende Marktposition von Unternehmen, die solche Dienste anbieten, weiter zu festigen bzw. auszubauen.

Für die RTR.Telekom.Post ist das Thema aus verschiedenen Gründen von Interesse:

1. Das Ökosystem des Internets besteht neben der Ebene der Datenübertragung, deren Monitoring die EU-Netzneutralitäts-Verordnung durch die Regulierungsbehörde vorsieht,[1] aus zahlreichen weiteren Ebenen, auf denen die Offenheit des Internets (für Verbraucherinnen und Verbraucher sowie für Diensteanbieter) eingeschränkt werden kann. Solche potenziellen Einschränkungen werden von BEREC und den nationalen Regulierungsbehörden laufend beobachtet.[2]

2. Neben etwa den von der RTR.Telekom.Post bereits untersuchten Ebenen der Betriebssysteme und App Stores[3] können auch SSO-Anbieter eine Rolle als digitale Gatekeeper einnehmen. Zudem sind derartige horizontale Dienstleistungen und Angebote (wie etwa auch Sprachsteuerungen, Zahlungssysteme etc.) prädestiniert, Daten aus unterschiedlichen Aktivitäten der Nutzerinnen und Nutzer zu generieren und eine allenfalls gegebene Marktmacht in andere Bereiche zu übertragen.

3. Zusätzlich zu bestehenden SSO-Lösungen von Betriebssystemanbietern und sozialen Netzwerken gibt es auch seitens der österreichischen Mobilnetzbetreiber Pläne, solche Dienste anzubieten[4].

---

1 Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zu Endkundenentgelten für regulierte intra-EU-Kommunikation sowie zur Änderung der Richtlinie 2002/22/EG und der Verordnung (EU) Nr. 531/2012.

2 „Draft BEREC Report on the ex ante regulation of digital gatekeepers“, BoR (21) 34, BEREC, 11.03.2021, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/9880-draft-berec-report-on-the-ex-ante-regulation-of-digital-gatekeepers (zugegriffen am 05.07.2021).

3 „Zur Offenheit des Internets: Betriebssysteme, Apps und App Stores“, RTR Fachbereich Telekom und Post, 06.2019, https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/OffenesInternetApps2019.de.html (zugegriffen am 05.07.2021). Eine Studie zu App Stores wurde auch von der niederländischen Regulierungsbehörde ACM durchgeführt: „Market study into mobile app stores“, ACM/18/032693, ACM, 11.04.2019, https://www.acm.nl/sites/default/files/documents/market-study-into-mobile-app-stores.pdf (zugegriffen am 05.07.2021). Auch die französische Regulierungsbehörde ARCEP widmete sich in einem Bericht dem Einfluss von Endgerätesoftware: „Devices, the weak link in achieving an open internet“, ARCEP, 02.2018, https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf (zugegriffen am 05.07.2021).

4 Siehe Kapitel 2.4.

4. Zudem überschneiden sich SSO-Dienste in ihrer Ausgestaltung in einigen Aspekten mit dem Thema „elektronische Identifizierung“, das seinerseits eine wesentliche Grundlage für die von der TKK beaufsichtigten Vertrauensdienste bildet.[5] Vor diesem Hintergrund ist es aus Sicht der Regulierungsbehörde essentiell, sich mit dem Thema auseinanderzusetzen.

Aktuell ändern sich die rechtlichen und technischen Rahmenbedingungen für solche Single-Sign-On-Lösungen, etwa durch den Entwurf des Digital Markets Acts (DMA),[6] die Bestrebungen oder die Änderungen von Browser-Herstellern in Hinsicht auf Third-Party-Cookies. [7] Die damit einhergehenden Änderungen sind wesentlich für das gesamte Ökosystem des Internets und für viele Wertschöpfungsprozesse.

Nach einer Einleitung in Kapitel 1 gibt Kapitel 2 einen Marktüberblick, welche Akteure Single-Sign-On-Dienste anbieten. Dabei wird auf die Bestrebungen hin zu einer europäischen elektronischen Identität[8] eingegangen. Weiters wird erörtert, welche Marktteilnehmer Single-Sign-On-Dienste nutzen. Dabei wird empirisch erhoben, wie verbreitet SSO-Lösungen durch österreichische Websites eingebunden werden[9]und es wird festgestellt, dass solche Lösungen hierzulande oftmals dazu eingesetzt werden, Nutzerinnen und Nutzern einen Zugang zu Diskussionsforen zu ermöglichen. Von den einbindenden Websites wird meist auf die SSO-Lösungen von Anbietern sozialer Netzwerke und Betriebssysteme zurückgegriffen.

Die technischen Grundlagen dieser Dienste werden in Kapitel 3 erörtert. Es wird festgestellt, dass die Änderungen von Browser-Herstellern, die mit einer Stärkung der Privatsphäre der Nutzerinnen und Nutzer argumentiert werden, Auswirkungen auf die Funktion und potenzielle Datensammlung von SSO-Lösungen von Websites haben. Ein Angebot ist dennoch weiterhin möglich. Insbesondere eine aktuell gebräuchliche technische Lösung des Angebots für Websites – die Nutzung von Software Development Kits (SDKs) – könnte Anpassungen erforderlich machen. Davon nicht unmittelbar betroffen ist die Verwendung von SSO durch Apps.

In Kapitel 4.2 werden die wettbewerblichen Aspekte von SSO-Diensten thematisiert. So wird festgestellt, dass es sich bei Anbietern von SSO-Diensten um Plattformen handelt, die von positiven indirekten Netzwerkeffekten profitieren und SSO-Dienste nutzen können, um die eigene Marktposition zu festigen. Zudem wird auf mögliche Auswirkungen des aktuellen Entwurfs zum Digital Markets Act auf die aktuellen Anbieter von SSO-Diensten eingegangen. Dabei wird festgestellt, dass insbesondere die Geschäftsbedingungen von Apple, die unter bestimmten Bedingungen eine Verpflichtung zum Angebot des Apple-SSO „Sign in with Apple“ in über den App-Store

---

5 https://signatur.rtr.at.
6 Siehe Kapitel 4.2.
7 Siehe Kapitel 3.2.
8 Siehe Kapitel 2.5.
9 Siehe Kapitel 2.6.

vertriebenen Apps vorsieht, nicht mit den im aktuellen Entwurf des DMA getroffenen Zielsetzungen vereinbar scheinen.

Anbieter von SSO-Diensten können als zentrale Instanzen potenzielle digitale Gatekeeper im offenen Internet darstellen. Derzeit ändern sich die technischen Rahmenbedingungen für diese Gatekeeper, eine ex-ante-Regulierung ist im aktuellen Entwurf zum DMA vorgesehen. Ein weiteres Monitoring und das Führen einer politischen Diskussion scheint deshalb sinnvoll, um die Innovationskraft des Ökosystems Internet zu erhalten. Überdies sollte aus Sicht der Regulierungsbehörde wegen der mit den Diensten verbundenen Bedeutung auch der Wettbewerb in diesem Segment unterstützt und gefördert werden.

Inhaltsverzeichnis

Management Summary 2

1 Einleitung 6

2 Marktüberblick 8
2.1 Anbieter von SSO 8
2.2 Anbieter von sozialen Netzwerken 8
2.3 Anbieter von Betriebssystemen und Anbieter von App-Stores 8
2.4 Angebot durch Mobilnetzbetreiber 10
2.5 Öffentliche Stellen 11
2.6 Nutzung von Single-Sign-On 11

3 Technische Aspekte 14
3.1 Aktuelle Vorgangsweise, Anbieter von SSO-Diensten und offene Standards in Browsern 14
3.1.1 Software Development Kits 15
3.1.2 OpenAuth 2 und OpenID Connect 16
3.1.3 WebAuthn 17
3.1.4 Passwort-Manager 18
3.2 Phase-out von Third-Party-Cookies und andere Entwicklungen 19

4 Wettbewerbliche Aspekte 23
4.1 Netzwerkeffekte 23
4.2 Beurteilung nach dem Entwurf zum Digital Markets Act (DMA) 25

5 Fazit 27

1 Einleitung

Im vorliegenden Dokument soll auf die Bedeutung und Entwicklungen von Single-Sign-On (SSO) und Third-Party-Identity-Providern (IDP) für die Nutzung von registrierungspflichtigen Diensten im Internet sowie mögliche wettbewerbliche Implikationen eingegangen werden. Anbieter von SSO-Diensten ermöglichen es, vereinfacht dargestellt, bereits bestehende Benutzerkonten zu nutzen, um Services Dritter ohne erneute Registrierung zu nutzen. Dies hat eine Reihe von Vorteilen für alle Beteiligten:

Für Drittanbieter: Durch das Angebot von SSO-Lösungen können Diensteanbieter ihren Nutzerinnen und Nutzern einen niederschwelligen Zugang anbieten – die Hürde der eigenen Benutzerregistrierung entfällt. Das erhöht die Conversion Rate[10] von Besuchern. Zudem erleichtert es die Datenhaltung und verringert Sicherheitsanforderungen, da Stammdaten wie Namen, E-Mail-Adressen und Passwörter nicht gesondert gespeichert werden müssen, weil diese Aufgabe durch einen Dritten - den SSO-Anbieter – übernommen wird.

Für Nutzerinnen und Nutzer: Für sie bringt die Möglichkeit eines SSO den Vorteil, dass gesonderte Registrierungen bei einzelnen Diensten nicht mehr notwendig sind. Im Idealfall reichen einige Klicks statt eines mühsamen Sign-Up-Prozesses (Suchen von Zugangsdaten, Passwörtern, ggf. Neuregistrierung etc.), um neue Dienste zu nutzen. Durch die zentrale Anmeldung kann zudem die Sicherheit der dortigen Identifizierung erhöht werden, indem etwa ein zweiter Faktor, biometrische Merkmale oder ein besonders starkes Passwort verwendet wird und dadurch mittelbar auch die Sicherheit der Anmeldung bei davon abhängigen Diensten erhöht werden.

Für Anbieter von Identifikationsdiensten (Identity Provider, SSO Diensteanbieter): Für diese Gruppe bietet eine weite Verbreitung den Vorteil, die eigene Marktposition zu stärken, da Nutzerinnen und Nutzer nicht mehr ohne weiteres die Verwendung einstellen können, wenn das Nutzerkonto für die Anmeldung bei Drittdiensten verwendet wird (Lock-in Effekt). Den Anbietern ermöglicht es zusätzlich durch die Kenntnis der verwendeten Drittdienste, bessere Profile der eigenen Nutzerinnen und Nutzer zu erstellen.

Neben einer Vielzahl von unterschiedlichen Akteuren auf dem Markt für Single-Sign-On-Dienste[11] wird in Österreich auch seitens der Telekomindustrie angedacht, eine solche Lösung anzubieten[12]; ebenso durch den Bund und die Europäische Union.[13]

In diesem Dokument wird zuerst ein Überblick über die Angebotsseite und die Nachfrageseite des Marktes geboten, es werden die technischen Grundlagen und Weiterentwicklungen erörtert, anschließend wird eine wettbewerbliche Beurteilung

---

[10] Das ist in diesem Zusammenhang der Anteil der Besucher, die sich registrieren (gemessen an der Anzahl der Besucher insgesamt).

[11] Siehe Kapitel 2.1ff.

[12] Siehe Kapitel 2.4.

[13] Siehe Kapitel 2.5.

vorgenommen und abschließend ein Blick auf die durch den Entwurf des Digital Markets Acts (DMA) zu erwartenden Änderungen geworfen.

Nicht in diesem Dokument behandelt werden Anbieter, deren hauptsächliche Dienstleistung darin besteht, rechtliche Know-Your-Customer (KYC) oder andere Vorschriften abzudecken, indem bspw. die Identität von Nutzerinnen und Nutzern durch einen Abgleich mit Reisepassfotos durchgeführt wird. Im verwandten Themenbereich der Vertrauensdienste bestehen weitreichende Zuständigkeiten der TKK und des Fachbereichs RTR.Telekom.Post [14] Sowohl SSO-Dienste als auch Anbieter von Vertrauensdiensten ermöglichen es in einem bestimmten Ausmaß, eine elektronische Identifizierung von Personen vorzunehmen. Während der Fokus bei den nachfolgend behandelten SSO-Anbietern auf einer möglichst niedrigschwelligen Integrationsmöglichkeit des Authentifizierungsdienstes und damit einhergehend einer starken Verbreitung bei Diensten von Dritten liegt, liegt dieser bei Vertrauensdiensteanbietern auf der Erstellung, Überprüfung und Validierung von elektronischen Signaturen und elektronischen Siegeln, die neben etwa der Signatur von Dokumenten auch zur Identifizierung verwendet werden können. Einhergehend mit der rechtlichen Qualifikation solcher Signaturen müssen Vertrauensdiensteanbieter zahlreiche Kriterien erfüllen, um qualifizierte Vertrauensdienste anbieten zu dürfen. Aufgrund dieser unterschiedlichen Ausrichtung wird im weiteren nicht näher auf qualifizierte Vertrauensdiensteanbieter iSd Art. 3 Z 19 der Verordnung (EU) 910/2014 eingegangen.

[14] https://signatur.rtr.at.

2 Marktüberblick

2.1 Anbieter von SSO

Weltweit angeboten werden SSO-Dienste etwa von Anbietern von Betriebssystemen oder den Betreibern sozialer Netzwerke. Wenngleich die Kerndienste dieser Anbieter anders gelagert sind, verfügen sie idR über eine große Nutzerzahl, Geschäftskunden und externe Entwickler, was einen Eintritt in den Markt für SSO-Dienste erleichtert. Im deutschen Sprachraum bietet eine Reihe deutscher Unternehmen mit *netID*[15] eine angebotsübergreifende SSO-Lösung an. Auch die Austria Presse Agentur (APA) arbeitet an einer SSO-Lösung,[16] die bis Ende des Jahres 2021 starten soll.[17] Ebenfalls angeboten wird ein SSO-Dienste von Amazon.[18]

Seitens der Telekommunikationsindustrie bietet die GSMA mit Mobile Connect ein SSO-System an,[19] das neben der Authentifizierung auch Identitätsdienstleistungen anbietet, da die einzelnen Telekommunikationsbetreiber im Zuge der Kundenbeziehung über qualifizierte Personendaten verfügen.

2.2 Anbieter von sozialen Netzwerken

Eine Vielzahl von sozialen Netzwerken – darunter etwa Facebook, Weibo oder vKontakte – bietet SSO-Lösungen an. Der Authentifizierungssoftware-as-a-Service-Anbieter auth0 etwa bietet allein in seiner Software Log-ins von über 30 Anbietern sozialer Netzwerke und anderer IT-Konzerne an, neben den vorhin genannten etwa auch Google, LinkedIn, Baidu, Yammer oder Soundcloud[20].

2.3 Anbieter von Betriebssystemen und Anbieter von App-Stores

Auch die drei wesentlichen Anbieter von Betriebssystemen – Microsoft, Google und Apple – bieten SSO-Lösungen an. Microsoft brandet sein System mit „Sign in with Microsoft“ und erlaubt die Verwendung persönlicher oder beruflicher Microsoft-

---

15 „European Net ID Foundation – European Net ID Foundation“, ohne Datum, https://enid.foundation/ (zugegriffen am 19.03.2021). Diese Log-In-Lösung soll die Verwendung einer gemeinsamen Registrierung auf den teilnehmenden Websites ermöglichen.

16 „APA setzt im Jubiläumsjahr auf Stärkung der Digital-Strategie“, *DER STANDARD*, 25.03.2021, https://www.derstandard.at/story/2000125345804/apa-setzt-im-jubilaeumsjahr-auf-staerkung-der-digital-strategie (zugegriffen am 23.04.2021).

17 „‚Allianzen sehr mühsam zustande zu bringen‘: Markus Breitenecker sucht Mitspieler in Medienbranche“, *Der Standard*, 24.06.2021, https://www.derstandard.at/story/2000127651163/allianzen-sehr-muehsam-zustande-zu-bringen-markus-breitenecker-sucht-mitspieler (zugegriffen am 24.06.2021).

18 Amazon.de: „Login mit Amazon nutzen“, ohne Datum, https://www.amazon.de/gp/help/customer/display.html?nodeId=G4CY3HAXTSFLGC22 (zugegriffen am 23.06.2021).

19 „Authentication“, *MobileConnect*, ohne Datum, https://mobileconnect.io/authentication/ (zugegriffen am 19.03.2021).

20 „Social Login - Time to implement it in your apps“, *Auth0*, ohne Datum, https://auth0.com/learn/social-login/ (zugegriffen am 19.03.2021).

Konten für Websites und Anwendungen Dritter.[21] Gleiches gilt auch für Google[22] und Apple,[23] die auch SSO-Lösungen anbieten. Gemeinsam ist allen diesen Lösungen, dass für Entwickler keine weiteren Kosten entstehen (siehe 3.1.1).

Besonders hervorzuheben ist an dieser Stelle das Unternehmen Apple, das in seinen App Store-Leitlinien festlegt, dass ein „Sign in with Apple" in Apps, die über den App Store vertrieben werden, nicht nur verwendet werden kann, sondern vielmehr verwendet werden muss, wenn in der App auch ein SSO-Dienst eines anderen Anbieters eingebunden ist.[24] Ausnahmen erlaubt Apple hier nur für Apps anderer sozialer Netzwerke und Apps, die nur ihr eigenes Login anbieten, bestimmten Apps im Bildungswesen, der Nutzung von staatlichen Authentifizierungsdiensten und Apps, die speziell auf bestimmte soziale Netzwerke zugeschnitten sind.[25] Anders als bei anderen Anbietern ermöglicht Apple es seinen Nutzerinnen und Nutzern, dass, bei der Anmeldung mit Apple, keine echten E-Mail-Adressen weitergegeben werden müssen. In diesem Fall erhält die App nach dem Login einer Nutzerin bzw. eines Nutzers lediglich eine von Apple bereitgestellte „Wegwerf"-E-Mail-Adresse.[26] Die Identität der Nutzerinnen und Nutzer wird damit gegenüber Dritten besonders geschützt, eingehende E-Mails werden durch Apple dann an die eigentlichen Nutzerinnen und Nutzer weitergeleitet.

Apps, die gegen die am 30.6.2020 in Kraft getretenen Apple-Richtlinien verstoßen und etwa ein Google oder Facebook-Login, aber kein „Login with Apple" anbieten, werden bei einer Prüfung durch Apple abgelehnt und haben so keine Möglichkeit, auf iOS-Geräten installiert zu werden. Für die Lösung selbst bietet Apple unterschiedliche Implementierungen an, so dass der Dienst auch abseits von iOS-Geräten in Apps unter anderen Betriebssystemen und Websites offensteht.[27]

Bei der Aufnahme des Login-Dienstes in die Nutzungsbedingungen des App Stores hält Apple hier eine Einzelrolle. Weder die Richtlinien von Google Play[28] noch die Richtlinien des Microsoft Stores[29] enthalten vergleichbare Bestimmungen. Anders als beim Apple-Betriebssystem iOS ist sowohl unter Googles Android als auch unter Microsofts Windows ein Sideload von Apps prinzipiell möglich, die Verwendung des jeweiligen

---

[21] „Add sign in with Microsoft - Microsoft identity platform", ohne Datum, https://developer.microsoft.com/en-us/identity/add-sign-in-with-microsoft (zugegriffen am 19.03.2021).

[22] „Use your Google Account to sign in to other apps or services - Computer - Google Account Help", ohne Datum, https://support.google.com/accounts/answer/112802?co=GENIE.Platform%3DDesktop&hl=en (zugegriffen am 19.03.2021).

[23] (Sign in with Apple - Apple Developer, no date)

[24] „New Guidelines for Sign in with Apple - News - Apple Developer", ohne Datum, https://developer.apple.com/news/?id=09122019b (zugegriffen am 19.03.2021).

[25] Ebd.

[26] „Hide My Email for Sign in with Apple", *Apple Support*, ohne Datum, https://support.apple.com/en-gb/HT210425 (zugegriffen am 19.03.2021).

[27] „Getting Started - Sign in with Apple - Apple Developer", ohne Datum, https://developer.apple.com/sign-in-with-apple/get-started/ (zugegriffen am 19.03.2021).

[28] „Richtlinienübersicht für Entwickler", ohne Datum, https://play.google.com/about/developer-content-policy/ (zugegriffen am 19.03.2021).

[29] hickeys: „Microsoft Store-Richtlinien - UWP applications", ohne Datum, https://docs.microsoft.com/de-de/windows/uwp/publish/store-policies (zugegriffen am 19.03.2021).

App Stores ist also nicht verpflichtend notwendig.[30] In Hinsicht auf diese Besonderheit ist etwa bereits ein Verfahren gegen „Login with Apple“ durch das US-Justizministerium anhängig.[31]

2.4 Angebot durch Mobilnetzbetreiber

Im Telekommunikationsmarkt relevant ist das Thema Single-Sign-On auch dadurch, dass ein solches System weltweit durch Mobilnetzbetreiber betrieben wird. Dies erfolgt durch die Industrievereinigung dieser Anbieter – der GSM Association (GSMA) – unter dem Marktnamen „Mobile Connect“. Während dieses System hierzulande noch nicht in Betrieb ist, kommt es in zahlreichen anderen Ländern bereits zur Anwendung.

In Österreich wurde seit 2018 auf Initiative von A1[32] die Implementierung des „Mobile Connect“-Systems verfolgt. An der Diskussion war auch die RTR.Telekom.Post beteiligt, die eine Reihe von Workshops zu diesem Thema organisierte, an denen alle österreichischen MNOs und MVNOs teilnehmen konnten. Besondere Aufmerksamkeit wurde von RTR.Telekom.Post darauf gelegt, dass eine Partizipationsmöglichkeit für MVNOs besteht. Zudem soll sichergestellt werden, dass durch „Mobile Connect“, etwa im Zusammenhang mit der Rufnummernportierung, keine zusätzlichen Barrieren im Wettbewerb entstehen.

Eine Besonderheit von Mobile Connect ist, dass im System, das auf der Mobilfunkrufnummer (MSISDN) der Teilnehmer aufbaut, auf eine bestehende Vertragsbeziehung zwischen dem Endkunden und dem Anbieter des Kommunikationsdienstes aufgesetzt werden kann. Da in Österreich seit September 2019 eine Pflicht zur Erhebung der Identität von Teilnehmern von Kommunikationsdiensten besteht (§ 97 Abs 1a TKG 2003, umgesetzt in der IVO[33]), ist es den teilnehmenden Kommunikationsdiensteanbietern in der Regel möglich, im Zuge der angebotenen SSO-Lösung qualifizierte Aussagen zur Identität von Teilnehmerinnen und Teilnehmern zu treffen.

Hinsichtlich dieser Identitätsfeststellung unterscheidet die GSMA zwischen „Mobile Connect Authenticate“, wo durch den Kommunikationsdiensteanbieter bestätigt wird, dass das anfragende Gerät sich in Besitz des Teilnehmers bzw. der Teilnehmenden befindet und „Mobile Connect Authenticate Plus“, wo durch aktive Aufforderung des Teilnehmers zur Eingabe eines zweiten Faktors wie einer PIN sichergestellt wird, dass eine Authentifizierung nur durch den Teilnehmenden selbst vorgenommen werden kann.

---

30 Mit dem Digital Markets Act könnte künftig auch für Apple eine Verpflichtung einhergehen, alternative App-Stores zuzulassen. Siehe dazu Art. 6 c des Draft DMA; COM(2020) 842 final

31 CPI: „DOJ Looks Into Complaints Regarding The ‚Sign In With Apple‘ Button“, *Competition Policy International*, 24.02.2021, https://www.competitionpolicyinternational.com/doj-looks-into-complaints-regarding-the-sign-in-with-apple-button/ (zugegriffen am 23.04.2021).

32 RTR: „1. Workshop „Mobile Connect Global ID““, *RTR*, 08.10.2018, https://www.rtr.at/TKP/aktuelles/veranstaltungen/veranstaltungen/MobileconnectglobalID/1._Workshop_-Mobile_Connect_Global_ID-.de.html (zugegriffen am 22.03.2021).

33 Verordnung des Bundesministers für Verkehr, Innovation und Technologie über Verfahren zur Identifikation von Teilnehmern (Identifikationsverordnung), BGBl. II Nr. 7/2019.

In Mobile Connect ist je nach Land eine Verrechnung gegenüber den einbindenden Diensten vorgesehen. In den Niederlanden, wo Mobile Connect bereits angeboten wird, werden vom Betreiber KPN 0,05 EUR pro abgeschlossenem Log-in-Vorgang verrechnet.[34]

Eine Besonderheit der Verwendung der MSISDN ist, dass auf bestehende Portierprozesse zurückgegriffen werden kann. Im Gegensatz zu anderen SSO-Anbietern bestehen sohin bei „Mobile Connect" für die Anwender potenziell weniger Gefahren eines Vendor-Lock-ins, denn zwischen Mobilfunkanbietern ist der Wechsel aufgrund Mobilnummernportierung einfach möglich.

Im Juni 2021 wird auf der Website der GSMA eine Unterstützung von Mobile Connect in Österreich von A1 angekündigt.[35]

2.5 Öffentliche Stellen

Auch von staatlichen Stellen und der Europäischen Union gibt es Pläne zur Unterstützung von SSO, wobei die Erbringung des Identitätsnachweises im Vordergrund steht. In Österreich wird dieses Bestreben unter dem Begriff „ID Austria" verfolgt.[36] Auf europäischer Ebene wurde im Juni 2021 von der Europäischen Kommission ein Vorschlag für eine Verordnung betreffend die europäische digitale Identität[37] vorgelegt. Auch dieser sieht eine niedrigschwellige Verwendungsmöglichkeit zum Nachweis bestimmter Daten gegenüber Drittwebsites vor. Bei sehr großen Online-Plattformen[38] sieht der Vorschlag der Kommission weiters eine Pflicht vor, ein Log-in oder den Nachweis bestimmter Attribute wie ein Mindestalter mit der europäischen digitalen Identität zu unterstützen.[39]

2.6 Nutzung von Single-Sign-On

Single-Sign-On-Lösungen werden von zahlreichen Apps und Websites eingebunden. Unter den beliebtesten Websites Österreichs[40] gibt es zahlreiche Anbieter, die ein Single-Sign-On-System eines Drittanbieters, wie etwa von Betriebssystemanbietern oder Betreibern sozialer Netzwerke, ermöglichen.[41] Von den 100 beliebtesten Websites in Österreich bieten insgesamt 89 Websites eine Log-In-Möglichkeit.[42] Von

---

34 „Mobile Connect", *KPN API Store*, 05.04.2019, https://developer.kpn.com/apis/kpn-mobile-connect-api (zugegriffen am 23.06.2021).

35 „Operators | Mobile Connect Developer Portal", ohne Datum, https://developer.mobileconnect.io/operators?title=&name_list=AT&field_mobile_connect_status_value=All (zugegriffen am 22.03.2021).

36 E-Government Innovationszentrum: „ID Austria - Anbindung", ohne Datum, https://eid.egiz.gv.at/anbindung/allgemeines/ (zugegriffen am 11.06.2021).

37 Dokument COM/2021/281 vom 03.06.2021, 52021PC0281.

38 Der Vorschlag verweist für die Einstufung als „sehr große Online-Plattform" auf die Definition des Vorschlags zum DSA (COM/2020/825 vom 15.12.2020), der in Artikel 25 Abs. 1 eine Untergrenze von 45 Millionen Nutzern vorsieht.

39 Artikel 1 Abs 16 des Vorschlags der Europäischen Kommission.

40 Quelle: Reppublika Digital Ratings, Stand: Februar 2021.

41 Quelle: Eigene Erhebung, abgefragt zwischen 01.04.2021 und 08.04.2021. Während SSO nicht nur bei Websites, sondern auch bspw bei Apps verwendet werden kann, wurden hier nur Websites betrachtet.

42 D.h. die Websites bieten eine Möglichkeit für Nutzer an, erweiterte Funktionalitäten nach einer Registrierung zu nutzen. Quelle: Eigene Erhebung.

diesen bieten 24 die Möglichkeit an, sich mit einem Single-Sign-On anzumelden. Unter den Single-Sign-On-Anbietern ist Facebook am beliebtesten mit 21 Websites,[43] gefolgt von Google mit 14 Websites[44] und Apple mit 8 Websites.[45] Bei Nachrichtenseiten werden solche Single-Sign-Ons oft verwendet, um eine Teilnahme am Diskussionsforum zu ermöglichen, aber auch etwa Postdienste bieten, wie in Abbildung 1 sichtbar, SSO-Dienste an.[46]

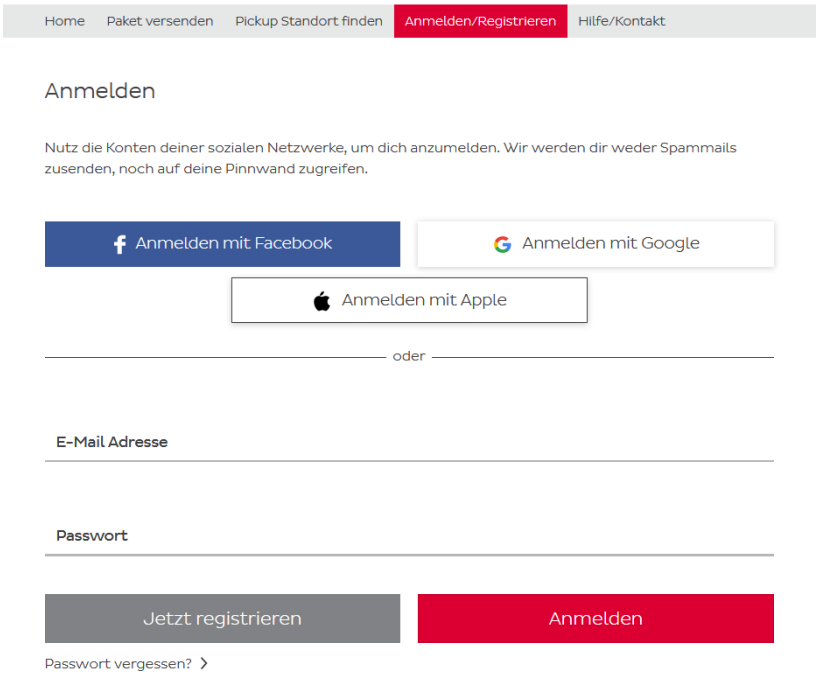

Abbildung 1: Einbindung verschiedener SSO-Dienste durch einen Postdienst.

Konkrete Zahlen zur Nutzung von Single-Sign-On-Diensten durch Verbraucher liegen für Österreich nicht vor.

Für Deutschland wurden solche Nutzungszahlen vom Wissenschaftlichen Institut für Infrastruktur und Kommunikationsdienste (WIK) 2019 erhoben.[47] Bei empirischen Erhebungen in Form einer Online-Umfrage gaben 14 % der befragten Nutzerinnen und Nutzer an, sich innerhalb der letzten 4 Wochen zumindest einmal bei einem Online-

43 AliExpress, Chefkoch.de, Conrad, Die Welt, DPD, Focus Online, Geizhals, GIGA.de, Herold, Heute, Hofer, Ichkoche.at, Idealo, Kronen Zeitung, Meinbezirk.at, Netflix, NÖN, Pinterest, TikTok, Vienna Online, Zoom.

44 AliExpress, Chefkoch.de, Conrad, DPD, Focus Online, GIGA.de, Herold, Idealo, LinkedIn, Pinterest, Reddit, Samsung, TikTok, Zoom.

45 AliExpress, Chefkoch.de, DPD, Focus Online, Hofer, Reddit, Idealo, TikTok.

46 „myDPD - Login“, ohne Datum, https://www.mydpd.at/login (zugegriffen am 25.06.2021).

47 Wiewiorra, Lukas, Andrea Liebe und Serpil Taş: „Die wettbewerbliche Bedeutung von Single-Sign-On- bzw. Login-Diensten und ihre Relevanz für datenbasierte Geschäftsmodelle sowie den Datenschutz“ WIK/462 (06.2020), https://www.wik.org/presse/meldungen/detailansicht?tx_ttnews%5BbackPid%5D=85&tx_ttnews%5Btt_news%5D=2352&cHash=617b726b6deeaa6238797e15c1db8eb5 (zugegriffen am 15.03.2021).

dienst oder einer Webseite mit einer SSO-Lösung eines sozialen Netzwerkes angemeldet zu haben. Im Gegensatz dazu gaben 83 % an, sich im selben Zeitraum bei einer Website mit einer Kombination aus Username bzw. E-Mail-Adresse und Passwort angemeldet zu haben. Einen Passwortmanager nutzten 15 % der Befragten.

3 Technische Aspekte

Im folgenden Kapitel soll darauf eingegangen werden, welche technischen Gesichtspunkte bei der Einbindung von SSO-Diensten in Websites zu berücksichtigen sind. Es wird zudem kurz die fortlaufende technische Standardisierung solcher Einbindungen und Prozesse beleuchtet.

3.1 Aktuelle Vorgangsweise, Anbieter von SSO-Diensten und offene Standards in Browsern

Moderne Webbrowser isolieren Programmcode, Nutzerdaten und Ressourcen von aufgerufenen Websites grundsätzlich voneinander (sog. „Sandboxing"). Dadurch wird verhindert, dass einzelne Websites auf die Daten anderer mit dem Browser besuchter Websites zugreifen können. Technisch wird dieses Verhalten unter anderem durch die *Same-origin-policy* definiert.[48] Diese stellt sicher, dass Websites und Programmcode nur auf Nutzerdaten von Websites zugreifen können, die unter demselben Hostname erreichbar sind. Während somit etwa Programmcode der auf www.rtr.at/TKP eingebunden ist, auf www.rtr.at/medien zugreifen kann (da sich beide Fachbereiche der RTR denselben Hostname www.rtr.at teilen) wäre ein Zugriff auf etwa www.bmlrt.gv.at nicht möglich.

Während ein solches Sandboxing von Websites per se sinnvoll ist, stellt es bei der Nutzung von SSO eine gewisse Herausforderung dar. Das Sandboxing verhindert, dass Websites auf Nutzerdaten Dritter zugreifen können. Das führt dazu, dass zwar eigene Log-in-Informationen verarbeitet werden, aber, ob eine Nutzerin oder ein Nutzer auch auf einer fremden Website – etwa Facebook – eingeloggt ist, ist nicht zugänglich. Eine Website, die einen Facebook-Single-Sign-On-Login nutzen möchte, kann somit aufgrund des eigenen, von „facebook.com" unterschiedlichen Hostnames, nicht feststellen, ob ein Besucher bzw. eine Besucherin einen Facebook-Account besitzt und dort allenfalls eingeloggt ist. Diese Information wäre aber notwendig, um den dortigen Log-in mitzunutzen. Um dieses Problem zu lösen, gibt es in der Praxis unterschiedliche Möglichkeiten, diese Informationen für ein Log-in dennoch zu verwenden.

Das im Internet gebräuchliche *Hypertext transfer protocol* (HTTP)[49] nutzt *Cookies*, um Informationen zu einzelnen Sitzungen zu speichern. Cookies selbst sind kurze Zeichenfolgen, die idR auf Aufforderung des Servers im Browser angelegt werden und bei wiederholten Aufrufen zum Server übertragen werden. Dadurch ist es möglich, Funktionalitäten, die Informationen über längere Zeit benötigen, wie etwa einen Log-in-Bereich, anzubieten. In der Terminologie wird zwischen „First Party"- und „Third Party"-Cookies unterschieden, wobei erstere Cookies beschreiben, die von einer Website selbst gesetzt wurden (etwa: Facebook-Cookie beim Aufruf von facebook.com), und zweitere solche, die von eingebundenen Websites außerhalb der Hauptdomain

[48] „Same-origin policy - Web security | MDN", 19.02.2021, https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy (zugegriffen am 24.03.2021).

[49] Reschke, Julian F. und Roy T. Fielding: „Hypertext Transfer Protocol (HTTP/1.1)", RFC 7230, 06.2014, https://tools.ietf.org/html/rfc7230 (zugegriffen am 30.11.2020). Aktuelle Websites werden üblicherweise über eine sichere Verbindung (eng. „secure") übertragen, erkennbar am „https"-Präfix.

verwendet werden (etwa: Facebook-Cookie beim Aufruf einer Website, die ein Facebook-Login anbietet).

3.1.1 Software Development Kits

Um ein Single-Sign-On anbieten zu können, besteht die technische Möglichkeit für Websites, direkt dynamisch Programmcodes des SSO-Anbieters, sog. „Software Development Kits" („SDK"), einzubinden. Diese Möglichkeit steht neben Apps auch Websites offen. Facebook bietet sein SDK für Websites etwa unter der Adresse https://connect.facebook.net/en_US/sdk.js an, welches durch die Website eingebunden werden kann.[50] Durch eine solche Einbindung wird der Programmcode von Facebook Teil des Codes der einbindenden Website und gemeinsam ausgeführt. Der Zugriff auf nähere Infos, etwa ob ein Nutzer auf Facebook eingeloggt ist und sich somit einfach anmelden kann, erfolgt durch die Verwendung von Third Party-Cookies.

Ebenfalls mit SDKs möglich ist die Einbindung von Single-Sign-On-Lösungen in Apps, wobei hier im Vergleich zu Websites durch die Betriebssysteme technisch weniger Einschränkungen bestehen.

Auf demselben Prinzip basiert auch Googles „One tap sign in with Google"-SDK.[51] Durch die Einbindung einer Javascript-Datei wird der Code von Google nachgeladen. Wird anhand der dortigen Third Party-Cookies erkannt, dass eine Nutzerin bzw. ein Nutzer eingeloggt ist, kann sich der Nutzende mit einem „Klick" registrieren oder anmelden, wie in Abbildung 2 [52] angeführt ist. Bereits einmal für den Dienst registrierte Nutzerinnen und Nutzer können dadurch auch automatisch angemeldet werden.

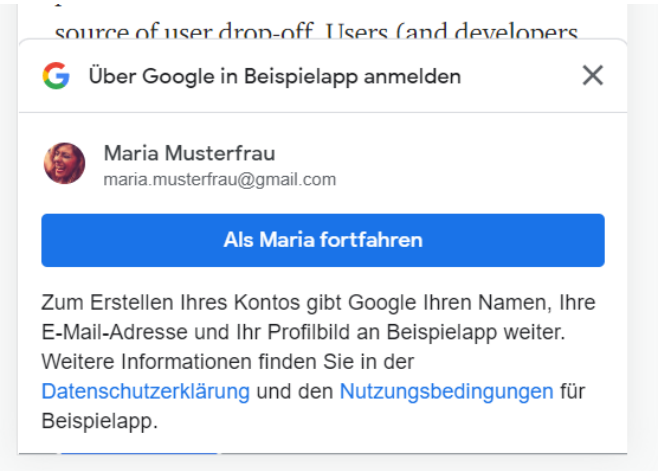

Abbildung 2: Darstellung eines "One tap sign in with Google"

[50] „Web - Facebook Login - Dokumentation", *Facebook for Developers*, ohne Datum, https://developers.facebook.com/docs/facebook-login/web/ (zugegriffen am 24.03.2021).

[51] „Overview | Sign In With Google", *Google Developers*, ohne Datum, https://developers.google.com/identity/gsi/web/guides/overview (zugegriffen am 30.03.2021).

[52] Quelle: „Sign In With Google | Google Developers", ohne Datum, https://developers.google.com/identity/gsi/web (zugegriffen am 30.03.2021).

Aus datenschutzrechtlicher Sicht ist bei einer Einbindung von SDKs in Websites besonders darauf zu achten, dass bei einem reinen Ansurfen einer Website bereits personenbezogene Daten wie IP-Adressen sowie technische Informationen des Browsers an die jeweiligen Authentifizierungsdiensteanbieter übermittelt werden.[53] Zudem wird der Code des SDKs durch den Browser gleich wie der Code der einbindenden Website ausgeführt, rein technisch besteht durch den SDK-Anbieter deshalb im Browser des Nutzers bzw. der Nutzerin Zugriff auf weite Teile der einbindenden Website. Dieser Zugriff ist nicht auf öffentliche Teile beschränkt, sondern besteht auf allen Unterseiten, die das SDK referenzieren, somit auch auf Unterseiten, die erst nach einem Log-in zugänglich sind und benutzerspezifische Informationen enthalten.

3.1.2 OpenAuth 2 und OpenID Connect

Abseits der SDKs, die von den Anbietern von Authentifizierungsdiensten bereitgestellt werden, gibt es insbesondere mit OAuth 2 [54] und OpenID Connect [55] etablierte Standards, die die Nutzung von Authentifizierungsdiensten erleichtern. Da für die Standards Implementierungen in vielen Programmiersprachen und Programmbibliotheken bereitgestellt sind, ist ein einfaches und sicheres Einbinden – auch mehrerer – solcher Authentifizierungsdienste einfach möglich.

In Abbildung 3[56] ist der Authentifizierungsprozess bei OAuth 2 dargestellt. Wie dort ersichtlich ist, wird hier die Nutzerin bzw. der Nutzer eines einbindenden Dienstes bei Verwendung der Log-in-Möglichkeit weg von der Anwendung hin zur Website des Authentifizierungsanbieters geleitet. Auf dieser kann dann der eigentliche Authentifizierungsvorgang durchgeführt werden. War dieser erfolgreich, wird die Nutzerin bzw. der Nutzer zurück zur Anwendung geleitet, wobei gleichzeitig mit der Weiterleitung ein „Code Grant" des Authentifizierungsanbieters der Anwendung übermittelt wird. Dieser „Code Grant" kann dann in weiterer Folge durch die Anwendung verwendet werden, um Daten zum Nutzerkonto vom Authentifizierungsanbieter, etwa Stammdaten wie E-Mail-Adresse oder Namen, zu erlangen.

Dadurch, dass alle relevanten Daten hier durch eigene Endpunkte oder als Bestandteil von Weiterleitungen übermittelt werden, ist zudem keine Verwendung von Third-Party-Cookies notwendig.

---

[53] „Fashion ID GmbH & Co. KG. gegen Verbraucherzentrale NRW e. V.", 29.07.2019, http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=16385238 (zugegriffen am 30.11.2020).

[54] „OAuth 2.0 — OAuth", ohne Datum, https://oauth.net/2/ (zugegriffen am 30.03.2021).

[55] „OpenID Connect | OpenID", 01.08.2011, https://openid.net/connect/ (zugegriffen am 30.03.2021).

[56] Quelle: Ankit Babbar: „Designing OAuth Auth Flow", *DEV Community*, 19.09.2020, https://dev.to/babbarankit/designing-oauth-auth-flow-96i (zugegriffen am 16.06.2021).

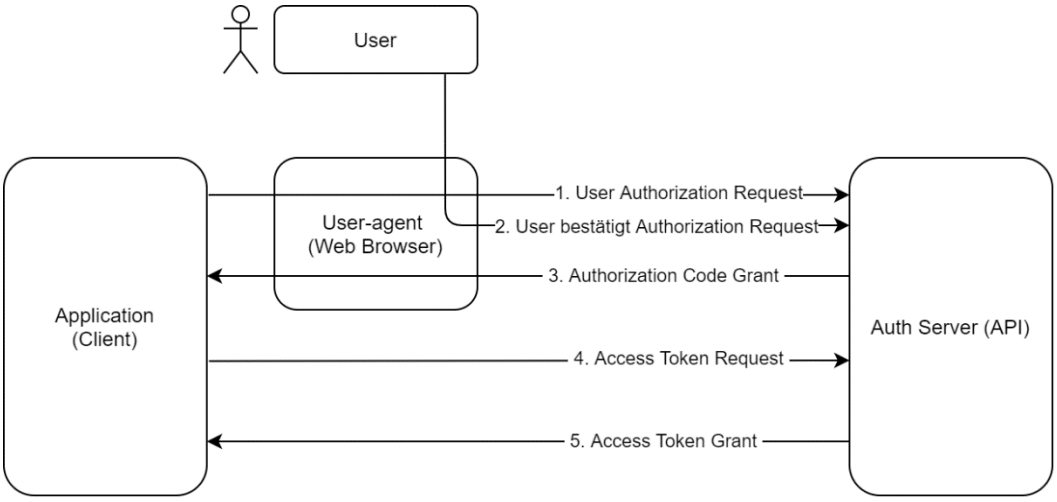

Abbildung 3: Schematischer Prozess bei OAuth 2

OpenID Connect setzt auf dem OAuth 2-Standard auf und erweitert ihn um standardisierte Endpunkte und Datenformate[57] für die Übermittlung von Nutzerdaten. Angeboten werden OAuth 2 und OpenID Connect etwa von Microsoft[58] oder Google.[59] Durch die Standardisierung ist es auch kleineren Anbietern möglich, eine SSO-Lösung anzubieten, die von Dritten unter geringem Aufwand eingebunden werden kann.

3.1.3 WebAuthn

Einen dezentraleren Ansatz, um sichere Log-ins ohne Passwort zu ermöglichen, verfolgt der Standard WebAuth.[60] Alle verbreiteten Browser (Stand 2021: Edge, Safari, Firefox, Chrome[61]) ermöglichen mit diesem Standard, Anbietern von Websites auf Hardware-Security-Token[62] oder vom Betriebssystem bereitgestellte sichere Authentifizierungsmerkmale wie Fingerprint-Reader oder Gesichtserkennung zurückzugreifen und diese anstelle eines herkömmlichen Passworts zu verwenden. Der Abgleich selbst findet nicht durch den Browser, sondern durch den Bereitsteller des zweiten Faktors, also der Hardware Token oder des Betriebssystems, statt. Das Ergebnis wird samt einem kryptographischen Schlüssel durch den Browser der Anwendung übermittelt. Der Ablauf ist in Abbildung 4[63] skizziert. Darin ist ersichtlich, dass der Browser als „Mittler“ zwischen der aufrufenden Website und dem zweiten Faktor des

---

[57] Bradley, John, Nat Sakimura und Michael B. Jones: „JSON Web Token (JWT)“, ohne Datum, https://tools.ietf.org/html/rfc7519 (zugegriffen am 30.03.2021).

[58] hpsin: „Microsoft identity platform and OpenID Connect protocol - Microsoft identity platform“, 22.05.2020, https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-protocols-oidc (zugegriffen am 14.05.2021).

[59] „Verwenden von OAuth 2.0 für den Zugriff auf Google APIs“, *Google Developers*, 15.04.2021, https://developers.google.com/identity/protocols/oauth2?hl=de (zugegriffen am 14.05.2021).

[60] „Web Authentication: An API for accessing Public Key Credentials - Level 2“, ohne Datum, https://www.w3.org/TR/webauthn/ (zugegriffen am 30.03.2021).

[61] „Can I use... WebAuthn“, 12.06.2021, https://caniuse.com/webauthn (zugegriffen am 30.03.2021).

[62] Solche physischen Geräte sind günstig erhältlich und dienen als zweiter Faktor, siehe etwa Schmidt, Jürgen: „Passwortloses Anmelden dank FIDO2“, *c't Magazin*, 19.08.2019, S. 2, https://www.heise.de/ct/artikel/Passwortloses-Anmelden-dank-FIDO2-4494951.html (zugegriffen am 11.06.2021).

[63] „Web Authentication API - Web APIs | MDN“, 16.03.2021, https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API (zugegriffen am 30.03.2021).

Nutzers agiert. Die aufrufende Website selbst erhält somit nie direkten Zugriff auf den verwendeten Faktor und damit potenziell sensible Daten wie biometrischer Information.

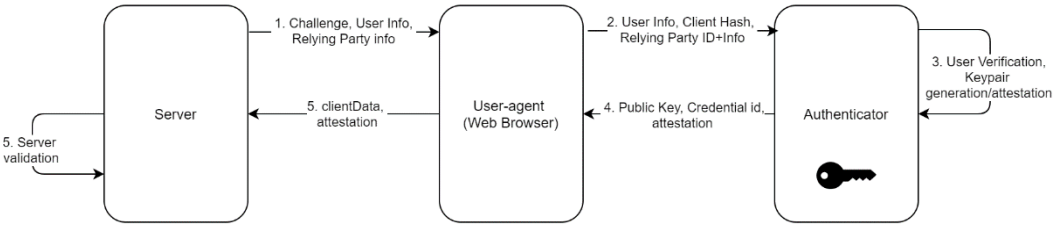

Abbildung 4: Schematischer Prozess bei WebAuthn

Neben einem reinen Ersatz für Passwörter ermöglicht es der Standard auch, den sonst erforderlichen Username automatisch zu vergeben.[64] Dadurch wird Anwendungen eine Schnittstelle bereitgestellt, über die sich Nutzer ohne Bekanntgabe von persönlichen Daten einloggen können. Die Authentifizierung erfolgt ausschließlich clientseitig, eine Registrierung bei einem Authentifizierungsanbieter ist damit nicht erforderlich.

Da die Authentifizierung an einen zweiten Faktor – ein Hardware-Security-Token oder eine biometrische Authentifizierung – gebunden ist, beinhaltet der Standard keine einfache Möglichkeit zur Portabilität der Authentifizierung.[65] Eine Authentifizierung ist damit grundsätzlich abhängig vom verwendeten zweiten Faktor, beispielsweise an ein konkretes Endgerät oder einen konkreten Hardware-Security-Token gebunden. Die Einbindung weiterer Geräte obliegt der Website, die ein WebAuthn-Log-in anbietet.

Aufgrund der Neuheit dieses Standards ist derzeit noch keine starke Verbreitung zu beobachten – wenn, dann eher subsidiär als zweiter Faktor zusätzlich zu einem Passwort.[66] Aufgrund der technischen Ausrichtung, die mehr auf einen Ersatz von Passwörtern abzielt als auf eine seitenübergreifende Identität, und aufgrund der geringen Verbreitung wird auf eine potenzielle wettbewerbliche Rolle von WebAuthn nicht weiter eingegangen.

3.1.4 Passwort-Manager

Eine clientseitige Möglichkeit zur Verwaltung von Nutzer-Accounts und Passwörtern bieten auch ein Passwort-Manager an. Solche sind sowohl als eigenständige Software erhältlich, aber genauso in allen großen Browsern integriert. In der Regel unterstützen

64 „Web Authentication: Resident Credential“, ohne Datum, https://www.w3.org/TR/webauthn/#resident-credential (zugegriffen am 30.03.2021).

65 „Consider allowing RPs to indicate that they want platform authenticators to be synced across devices · Issue #969 · w3c/webauthn“, *GitHub*, 25.06.2018, https://github.com/w3c/webauthn/issues/969 (zugegriffen am 30.03.2021).

66 „WebAuthn Is Great and It Sucks“, *Okta Security*, ohne Datum, https://sec.okta.com/articles/2020/04/webauthn-great-and-it-sucks (zugegriffen am 11.06.2021).

sie auch einen geräteübergreifenden Zugriff auf die gespeicherten Authentifizierungsdaten. So ermöglicht etwa Google eine Synchronisation über das Google-Konto[67] für Chrome und Android-Anwendungen, Mozilla unterstützt unter dem Produktnamen „Firefox Lockwise“ [68] ebenfalls eine geräteübergreifende Passwortsynchronisierung. Während, etwa für eine solche geräteübergreifende Verwendung, ein Account angelegt werden kann, ist ein solcher rein technisch, wie bei WebAuthn auch umgesetzt, nicht zwingend notwendig.

Neben den in Browsern integrierten Passwort-Managern gibt es solche auch als eigenständige Software, die sowohl kostenlos als auch kostenpflichtig erhältlich sind.[69]

Zur Nutzung von Passwort-Managern ist seitens des Dienstanbieters grundsätzlich keine Anpassung des Log-in-Vorgangs erforderlich, da sich Passwort-Manager direkt in die jeweiligen Registrierungsformulare der Websites integrieren. Um die Integration zu verbessern, bestehen Web-Standards, um Nutzer beim Ausfüllen des Formulars zu unterstützen oder ein solches Ausfüllen automatisiert zu ermöglichen[70]. Da die auf Websites zu setzenden Passwörtern durch den Passwortmanager generiert werden, besteht kein Risiko, dass bei Sicherheitsvorfällen des Dienstes bekannt gewordene Zugangsdaten auf anderen Websites verwendet werden können. Zur Absicherung dieser Zugangsdaten bieten Passwortmanager auch die Möglichkeit, ein Master-Passwort zu setzen, oder auch eine Zwei-Faktor-Authentifizierung zu verwenden.[71] Weiters wird in der Regel eine Lösung angeboten, auf die durch den Passwortmanager gespeicherten Zugangsdaten von mehreren Geräten aus zuzugreifen.

3.2 Phase-out von Third-Party-Cookies und andere Entwicklungen

Aktuell gibt es von allen Browserherstellern Bestrebungen, Third-Party-Cookies zu deaktivieren oder zumindest ihre Tauglichkeit für nutzerverfolgende Display-Werbung einzuschränken. Begründet werden diese Bestrebungen damit, dass Third-Party-Cookies häufig für invasive, nutzerverfolgende Werbung verwendet werden, diese Praktiken aus Nutzersicht unerwünscht seien und eine Abstellung dem Datenschutz zweckdienlich sei.

---

67 „Ihre Passwörter auf allen Geräten verwenden - Android-Gerät - Google Chrome-Hilfe“, ohne Datum, https://support.google.com/chrome/answer/6197437?co=GENIE.Platform%3DAndroid&hl=de (zugegriffen am 23.06.2021).

68 „Firefox Lockwise – Passwortmanager — Hab deine Passwörter überall parat.“, *Mozilla*, ohne Datum, https://www.mozilla.org/de/firefox/lockwise/ (zugegriffen am 31.03.2021).

69 „Passwortmanager“, *KONSUMENT* 2018/4 (22.03.2018), https://www.konsument.at/passwortmanager042018.

70 „The HTML autocomplete attribute - HTML: HyperText Markup Language | MDN“, 27.03.2021, https://developer.mozilla.org/en-US/docs/Web/HTML/Attributes/autocomplete (zugegriffen am 31.03.2021).

71 „KONSUMENT.AT - Passwortmanager - Test“.

Unter dem Begriff „Tracking Prevention“ versehen Apple in Webkit/Safari,[72] Mozilla in Firefox[73] und Microsoft in Edge[74] ihre Browser mit Mechanismen, die die Wirksamkeit solcher seitenübergreifender Cookies stark einschränken oder überhaupt blockieren. Google verfolgt für Chrome unter dem Begriff der „Privacy Sandbox“ ein ähnliches Konzept, um seitenübergreifende Nutzerverfolgung zu unterbinden.[75] Die Änderungen betreffen ausschließlich Websites, die über die jeweiligen Browser aufgerufen werden. Installierbare Apps sind davon nicht direkt betroffen, wenngleich es seitens der Betriebssystemhersteller ebenfalls Bestrebungen gibt, App-übergreifendes Tracking einzuschränken.[76]

Insbesondere bei den Bestrebungen von Google herrschen wettbewerbliche Bedenken, da durch eine Verringerung der Effektivität von Display-Werbung durch Dritte Google in der Vormachtstellung als Werbeplattform weiter gestärkt werden könnte.[77] Anders als bestehende Display-Werbung-Anbieter setze Google stärker auf Werbung in den eigenen Suchergebnissen, die sich an der konkreten Suche orientieren, und wäre allein bereits deshalb von dieser Beschränkung weniger stark betroffen. Zudem verfüge Google über eine breite Präsenz mit einer Vielzahl an eigenen Plattformen und Diensten, weshalb für Google auch ohne Nutzerverfolgung auf Websites Dritter zahlreiche Möglichkeiten bestehen, Profile über Nutzer zu bilden und für zielgerichtete Werbung zu verwenden. Zudem festige die von Google vorgeschlagene technische Alternative „FLoC“ die eigene Marktposition weiter, während weiterhin datenschutzrechtliche Bedenken bestehen würden.[78] Gleichzeitig ist anzumerken, dass ein Wegfall von Third-Party-Cookies die Schaltung von zielgerichteter Werbung nicht völlig unterbindet, aber eine genaue Bildung von Nutzerprofilen durchaus erschweren kann. Nicht von solchen Maßnahmen betroffen sind Werbeformen, die sich nicht am individuellen, durch seitenübergreifendes Tracking erstellten, Nutzerprofil orientieren, sondern etwa am Seiteninhalt[79] oder allgemeinen, der einbindenden Website bekannten,

---

72 „Tracking Prevention in WebKit“, *WebKit*, 24.06.2020, https://webkit.org/tracking-prevention/ (zugegriffen am 30.03.2021).

73 Deckelmann, Selena: „Latest Firefox release includes Multiple Picture-in-Picture and Total Cookie Protection“, *The Mozilla Blog*, 23.02.2021, https://blog.mozilla.org/blog/2021/02/23/latest-firefox-release-includes-multiple-picture-in-picture-and-total-cookie-protection (zugegriffen am 30.03.2021).

74 MSEdgeTeam: „Tracking Prevention in Microsoft Edge (Chromium) - Microsoft Edge Development“, ohne Datum, https://docs.microsoft.com/en-us/microsoft-edge/web-platform/tracking-prevention (zugegriffen am 30.03.2021).

75 The Chromium Projects: „The Privacy Sandbox“, ohne Datum, https://www.chromium.org/Home/chromium-privacy/privacy-sandbox (zugegriffen am 23.11.2020).

76 „User Privacy and Data Use - App Store“, *Apple Developer*, ohne Datum, https://developer.apple.com/app-store/user-privacy-and-data-use/ (zugegriffen am 23.06.2021).

77 Competition and Markets Authority (CMA): „CMA to investigate Google’s ‘Privacy Sandbox’ browser changes“, 08.01.2021, https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes (zugegriffen am 12.01.2021); Geradin, Damien, Dimitrios Katsifis und Theano Karanikioti: „Google as a de facto privacy regulator: Analyzing Chrome’s removal of third-party cookies from an antitrust perspective“, SSRN Scholarly Paper ID 3738107, Rochester, NY: Social Science Research Network, 26.11.2020, https://papers.ssrn.com/abstract=3738107 (zugegriffen am 27.11.2020).

78 Rescorla, Eric: „Privacy analysis of FLoC“, *The Mozilla Blog*, 10.06.2021, https://blog.mozilla.org/en/privacy-security/privacy-analysis-of-floc/ (zugegriffen am 28.06.2021).

79 Etwa: Eine Nachrichtenseite könnte auf Artikeln mit Sportberichterstattung Werbung schalten, die sich auf Sportdienstleistungen fokussiert, ohne dafür auf Nutzerverfolgung und Profilbildung zurückgreifen zu müssen.

demographischen und geographischen Merkmalen.[80] Gleichzeitig ist, wie Google selbst beziffert, bei nicht-zielgerichtetem Display-Advertising im Vergleich zu zielgerichtetem Display-Advertising ein Umsatzrückgang von über 50 %, bei Nachrichtenseiten von über 60 % zu erwarten.[81] Andere Quellen wiederum sehen die Auswirkungen offener und prognostizieren keine Umsatzrückgänge bis hin zu Umsatzwachstum[82].

Neben der Auswirkung auf die Bildung von Nutzerprofilen hat eine Beschränkung von Tracking-Maßnahmen und insbesondere Third-Party-Cookies auch eine indirekte Auswirkung auf SSO-Lösungen.[83] Von den oben genannten SSO-Technologien sind davon insbesondere SDKs betroffen. Da bei SDKs ein Code der Authentifizierungsdienstanbieter auf fremden Websites ausgeführt wird, befindet sich die Information zum Log-in-Status des Nutzers in einem Third-Party-Cookie. Kann auf das ursprünglich gesetzte Cookie allerdings nichtmehr zurückgegriffen werden, ist eine Authentifizierung des Nutzers nicht unmittelbar möglich.[84] Um dennoch ein Single-Sign-On zu ermöglichen, bestehen weitere Möglichkeiten (vgl. unten mit OAuth 2 und OpenID Connect), diese erfordern aber u.U. zusätzliche Klicks durch den Nutzer und technische Anpassungen des Authentifizierungsdiensteanbieters.

Als Mittelweg, um einerseits viele Werbeformen und die damit verbundenen Datensammlungen und Nutzerprofilbildungen zu unterbinden, andererseits aber Single-Sign-On über SDKs weiterhin zu erlauben, bieten Browser die Möglichkeit, nur Cookies von Websites zu blockieren, die noch nicht besucht wurden. Damit können Werbetreibende weiterhin keine Cookies mehr platzieren, aber Authentifizierungsanbieter wie soziale Netzwerke können weiter auf ihre Cookies zugreifen, da die Cookies bereits im Zuge früherer Besuche gesetzt wurden.[85] Dies steigert gleichzeitig auch die Attraktivität für Plattformen, SSO-Dienste anzubieten, da somit weiterhin eine Profilbildung und Datensammlung möglich ist, die einem reinen Werbenetzwerk durch die Abschaffung von Third-Party-Cookies verwehrt bliebe.

Andere Web-basierte Authentifizierungsmethoden wie OAuth 2 oder OpenID Connect sind nicht unmittelbar von Third-Party-Cookies betroffen, da die Informationen über einen Log-in hier nach Aufruf einer Website des Authentifizierungsdienstanbieters in Form einer URL übertragen werden. Cookies sind hierfür nicht notwendig bzw. werden

---

80 Geographische Informationen sind bspw aus der IP-Adresse oder der Web Location API („Location - Web APIs | MDN“, 08.04.2021, https://developer.mozilla.org/en-US/docs/Web/API/Location (zugegriffen am 26.04.2021).) auslesbar.

81 „Next steps to ensure transparency, choice and control in digital advertising“, *Google*, 22.08.2019, https://blog.google/products/ads/next-steps-transparency-choice-control/ (zugegriffen am 26.04.2021).

82 Norwegian Consumer Council / Forbrukerrådet: „Time to ban surveillance-based advertising“, 22.06.2021, S. 10, https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/ (zugegriffen am 24.06.2021).

83 Keith Folz: „Cookies, Single Sign-On, and You - The Akamai Blog“, 17.01.2020, https://blogs.akamai.com/2020/01/cookies-single-sign-on-and-you.html (zugegriffen am 30.03.2021).

84 „Troubleshooting | Google Sign-In for Websites“, *Google Developers*, ohne Datum, https://developers.google.com/identity/sign-in/web/troubleshooting (zugegriffen am 30.03.2021).

85 „Verbesserter Tracking-Schutz im Firefox Browser“, *Firefox Forward*, 28.02.2019, https://blog.mozilla.org/firefox/de/verbesserter-tracking-schutz-von-firefox/ (zugegriffen am 30.03.2021).

ebenjene bei allen Akteuren ausschließlich in der Form von First-Party-Cookies verwendet. Da aber auch Werbetreibende vermehrt auf Informationssammlung über Adressparameter ausweichen, sind auch diese von Einschränkungen in Browsern betroffen.[86] Insbesondere ein automatisches Log-in bzw. erneutes Log-in ist dadurch erschwert möglich, wenngleich ein Single-Sign-On an sich auch mit neuerer „Tracking Prevention" weiterhin funktioniert, aber ggf. geringfügige Anpassungen erforderlich sind.[87] Single-Sign-On wird durch ein Phase-Out von Third-Party-Cookies demnach nicht unterbunden, abhängig von der konkreten Einbindung sind aber ggf Anpassungen erforderlich.

Nicht betroffen von allen Änderungen ist der WebAuthn-Standard, da durch die Auslagerung der Authentifizierung auf einen Hardware-Security-Token oder an das Betriebssystem keine Cookies oder andere seitenübergreifende Informationstransfers benötigt werden.

Zusammenfassend lässt sich somit festhalten, dass eine Einbindung von Single-Sign-On-Diensten in Websites derzeit in unterschiedlichen Varianten möglich ist. Gleichzeitig wird aber die Variante, die eine potenziell große Datensammlung durch den SSO-Anbieter – die Bereitstellung von dynamisch eingebundenen SDKs – durch einen stärker werdenden Fokus der Browser-Hersteller auf den Datenschutz der Nutzer künftig nicht mehr im vollen Umfang möglich sein. Apps sind von diesen Einschränkungen vorerst nicht betroffen.

---

86 Deckelmann, Selena: „Latest Firefox rolls out Enhanced Tracking Protection 2.0; blocking redirect trackers by default", 04.08.2020, https://blog.mozilla.org/blog/2020/08/04/latest-firefox-rolls-out-enhanced-tracking-protection-2-0-blocking-redirect-trackers-by-default (zugegriffen am 11.01.2021).

87 hpsin: „How to handle Intelligent Tracking Protection (ITP) in Safari - Microsoft identity platform", 19.05.2020, https://docs.microsoft.com/en-us/azure/active-directory/develop/reference-third-party-cookies-spas (zugegriffen am 30.03.2021).

4 Wettbewerbliche Aspekte

4.1 Netzwerkeffekte

Authentifizierungsdiensteanbieter verbinden zwei unterschiedliche Nutzergruppen miteinander, nämlich die (vorwiegend privaten) Nutzerinnen und Nutzer ihres Authentifizierungsdienstes, also ihre eigenen Nutzer, mit den Diensteanbietern, die ihren SSO-Dienst für die Authentifizierung bei der Nutzung des jeweiligen Diensts benutzen. Sie agieren damit als Plattform.[88]

Plattformen realisieren indirekte Netzwerkeffekte und Skaleneffekte. Bei Authentifizierungsdiensten solcher Plattformen besteht ein grundsätzlich positiver indirekter Netzwerkeffekt. Für Endnutzer von solchen Authentifizierungsdienstanbietern steigt der Nutzen mit jedem weiteren Dienst, dessen Nutzung für sie durch ein SSO möglich ist. Gleichzeitig steigt der Nutzen für Diensteanbieter mit der Anzahl der Endnutzer, über die ein Authentifizierungsanbieter verfügt. Während der Aufwand für die Integration einer SSO-Lösung mit einmaligen Fixkosten verbunden ist, ist ein weiterer Nutzer in der Regel mit keinen weiteren (Grenz-)Kosten verbunden. D.h. der durchschnittliche Aufwand sinkt auf potenzielle Nutzer heruntergebrochen mit der Größe der Nutzerbasis des Authentifizierungsanbieters. Es bestehen also entsprechende Skaleneffekte.

Zu beachten ist weiter, dass es für Diensteanbieter durch Nutzung spezieller Intermediäre und Programmlösungen möglich ist, mehrere Authentifizierungsdienste gleichzeitig zu implementieren. Eine Auswahl unterstützter Authentifizierungsdienste durch den Anbieter *auth0*[89] ist etwa in Abbildung 5 zu sehen.[90] D.h. Diensteanbieter können mehrere Anbieter nebeneinander verwenden. Auf dieser Seite der Plattform besteht dadurch eine eine Möglichkeit für Multi-Homing. Dies ist etwa vergleichbar mit der Möglichkeit von Kreditkartenzahlungen in Geschäften: Händler können einzelne Kreditkartenanbieter akzeptieren, aber auch genauso Lösungen einsetzen, die die Akzeptanz einer Vielzahl von Kreditkartenanbietern ermöglichen.[91] Nutzerinnen und Nutzer profitieren bei solchen Lösungen von einer größeren Wahlfreiheit unter den verwendbaren Accounts. Dennoch sind sie dann grundsätzlich auf den erstmalig verwendeten Account gebunden, ein späterer Wechsel des verwendeten SSO-Dienstes muss auch von der einbindenden Plattform unterstützt werden (s.u.).

---

88 RTR.Telekom.Post: „Monitoring von Kommunikations-Plattformen und Gatekeepern des offenen Internetzugangs“, 19.05.2020, S. 10, https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/plattformen-monitoring-methoden.de.html (zugegriffen am 11.06.2021).

89 Der Anbieter auth0 wurde im März 2021 seinerseits vom Konkurrenten *Okta* für 6,5 Mrd. USD übernommen. online, heise: „Identitätsübernahme: Okta kauft Startup Auth0 für 6,5 Milliarden US-Dollar“, *iX Magazin*, 05.03.2021, https://www.heise.de/news/Identitaetsuebernahme-Okta-kauft-Startup-Auth0-fuer-6-5-Milliarden-US-Dollar-5072967.html (zugegriffen am 31.03.2021).

90 Auth0: „Social Identity Providers“, *Auth0 Docs*, ohne Datum, https://auth0.com/docs/ (zugegriffen am 31.03.2021).

91 RTR.Telekom.Post: „Monitoring von Kommunikations-Plattformen und Gatekeepern des offenen Internetzugangs“, S. 22.

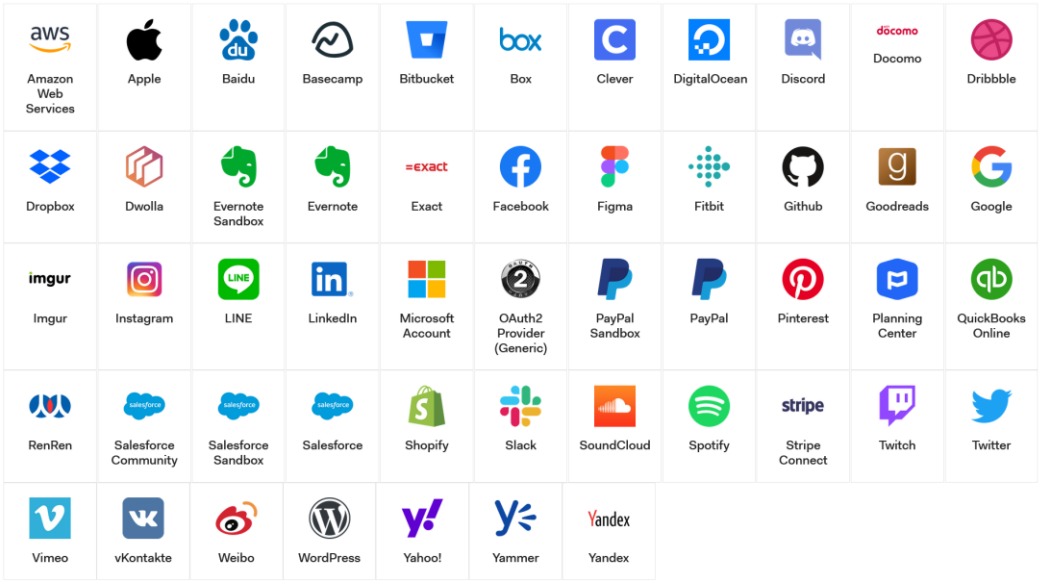

Abbildung 5: Auswahl an SSO-Anbietern beim Dienst "auth0 "

Sowohl für einbindende Dienste als auch für Endnutzer von Authentifizierungsdiensten besteht aufgrund der indirekten Netzwerkeffekte ein starker Lock-in-Effekt. Will etwa eine Endnutzerin eines sozialen Mediums ihren Account kündigen, so verliert sie damit auch die Möglichkeit, auf die Dienste von Dritten zuzugreifen, wenn sie dort bisher den SSO-Dienst des sozialen Mediums genutzt hat. Gleiches gilt auch für den Diensteanbieter: Wurde Nutzern dort die Möglichkeit angeboten, sich mit Accounts von Authentifizierungsdiensten einzuloggen, ist es nicht mehr ohne weiteres möglich, diese Option in der weiteren Produktgestaltung zu entfernen. Abhängig von den Informationen, die ein Authentifizierungsanbieter über seine Endnutzer dem einbindenden Diensten mitteilt, können unter Umständen alternative Log-in-Möglichkeiten verwendet werden und Nutzeraccounts über die E-Mail-Adresse zusammengeführt werden.[92] Wird vom Authentifizierungsanbieter keine E-Mail-Adresse der Nutzer zur Verfügung gestellt,[93] besteht grundsätzlich keine Möglichkeit der Zusammenführung unterschiedlicher Accounts. Eine solche müsste vom Diensteanbieter dann im Einzelfall implementiert werden.

Dadurch, dass bei Verwendung von SSO-Diensten einbindende Diensteanbietern bestimmte Attribute der Nutzer nicht mehr erfassen können – etwa unter Verwen-

92 Siehe etwa die Anleitung von Strava, um Accounts, die mit „Login with Facebook“ angelegt wurden, von Facebook zu entkoppeln, indem ein Account mit der bei Facebook hinterlegten E-Mail-Adresse angelegt wird „How to switch to an email & password login – Strava Support“, 09.03.2021, https://support.strava.com/hc/en-us/articles/216918817-How-to-switch-to-an-email-password-login?mobile_site=true (zugegriffen am 31.03.2021). Ähnliche Erfahrungsberichte finden sich auch von anderen Diensten, die ein SSO eines Social Networks einbinden, wobei ein Entkoppeln nicht immer möglich ist, etwa bei Spotify „I want to disconnect Facebook from my Spotify“, 15.03.2016, https://community.spotify.com/t5/Spotify-Answers/I-want-to-disconnect-Facebook-from-my-Spotify/tap/1308147 (zugegriffen am 31.03.2021).

93 Etwa bei der Nutzung von „Login with Apple“, wenn der Nutzer bei der Anmeldung die Option „E-Mail-Adresse verbergen“ gewählt hat.

dung von „Sign-In with Apple“, wo anonymisierte E-Mail-Adressen verwendet werden[94] – kann es zu Nachteilen bei der Kundenbindung kommen. Haben einbindende Dienste keinen direkten Zugriff auf diese Attribute mehr, sind sie, um etwa gezielte Marketing-Aktionen durchzuführen, auf eine Zusammenarbeit mit dem SSO-Anbieter angewiesen.[95] Der SSO-Anbieter wiederum kann durch die weite Einbindung des eigenen Dienstes noch bessere Besucherprofile bilden und diese sowohl für die eigene Plattform als auch zur Verbesserung eigener konkurrierender Dienste verwerten. Insoweit neben der reinen Log-in-Funktionalität auch andere Dienste durch den SSO-Anbieter – etwa Zahlungsdienste oder Zugang zu einem Werbenetzwerk – bereitgestellt werden, kann der SSO-Anbieter die Rolle eines Gatekeepers einnehmen.

Zusammenfassend lässt sich festhalten, dass für Plattformen mit einer hohen Anzahl an Endnutzern ein wettbewerblicher Anreiz besteht, Single-Sign-On-Dienste anzubieten. Dadurch wird es ihnen möglich, ihre Marktposition auch außerhalb des eigenen Dienstes auf Drittservices auszudehnen. Als technische Konsequenz der Einbindung wird es ihnen so auch ermöglicht, Nutzungsverhalten ihrer Nutzer außerhalb der eigenen Webpräsenz nachzuvollziehen und Daten darüber zu sammeln, zu verknüpfen und entsprechend zu verwerten.

4.2 Beurteilung nach dem Entwurf zum Digital Markets Act (DMA)

Im Vorschlag der Kommission für eine Verordnung über bestreitbare und faire Märkte im digitalen Sektor („Gesetz über digitale Märkte“, „Digital Markets Act“ [DMA])[96] geht die Kommission direkt auf die Rolle von Authentifizierungsdiensteanbietern im Wettbewerb ein. So sollen nach Artikel 5 lit. e des Vorschlags Gatekeeper in deren zentralen Plattformdiensten dazu verpflichtet werden, *„davon abzusehen, von gewerblichen Nutzern zu verlangen, im Zusammenhang mit Dienstleistungen, die sie über die zentralen Plattformdienste dieses Gatekeepers anbieten, einen Identifizierungsdienst des Gatekeepers zu nutzen, anzubieten oder mit ihm zu operieren“*. In den entsprechenden Erwägungsgründen 14 und 40 begründet die Kommission diese Verpflichtung damit, dass *„Gatekeeper durch ihre Macht als Gatekeeper von ihren zentralen Plattformdiensten auf Nebendienstleistungen* (wie Identifizierung, Anm.) *zu übertragen, was die Auswahl an Diensten und deren Bestreitbarkeit beeinträchtigen würde“*. Identifizierungsdienste wiederum sind *„für gewerbliche Nutzer […] von entscheidender Bedeutung, da sie es […] ermöglichen können, Dienste […] zu optimieren und das Vertrauen in Online-Transaktionen zu stärken.“*

Als „zentrale Plattformdienste“ bestimmt der Digital Markets Act in Artikel 2 Z 2 etwa „Online-Vermittlungsdienste“ wie App Stores (lit. a), Online-Suchmaschinen (lit. b), Online-Dienste sozialer Netzwerke (lit. d), Cloud-Computing-Dienste (lit. g) und

---

94 Siehe Kapitel 2.3.

95 Etwa bei Facebooks „Lookalike Audiences”, wo Werbung für Kunden geschalten werden kann, die nach Einschätzung Facebooks den Bestandskunden ähneln. Worauf genau diese Ähnlichkeit basiert, wird von Facebook dabei nicht offengelegt, siehe „Lookalike Audiences von Facebook“, *Facebook for Business*, ohne Datum, https://de-de.facebook.com/business/a/custom-to-lookalike-audiences (zugegriffen am 28.06.2021).

96 „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor“, 15.12.2020, https://eur-lex.europa.eu/legal-content/de/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN (zugegriffen am 31.03.2021).

Betriebssysteme (lit. f). Ein Betreiber solcher Dienste wiederum ist nach Artikel 3 Abs. 1 des Entwurfes des DMA dann „Gatekeeper“, wenn er *erhebliche Auswirkungen auf den Binnenmarkt hat* (lit. a), *einen zentralen Plattformdienst betreibt, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dient* (lit. b) und *hinsichtlich seiner Tätigkeiten eine gefestigte und dauerhafte Position innehat oder absehbar ist, dass er eine solche Position in naher Zukunft erlangen wird* (lit. c). In Artikel 2 Abs. 2 werden auch noch Schwellenwerte für Umsatz und Nutzer gelegt, um die oben genannten Kriterien als erfüllt anzunehmen.

Als konkretes Beispiel einer Auswirkung des Digital Markets Acts kann die in 2.2 angeführte Geschäftspraktik von Apple dienen: Als „App Store“ nach Art. 2 Z 2 lit. a des Digital Markets Act könnte der Apple App Store ggf. als „zentraler Plattformdienst“ anzusehen sein. In den Geschäftsbedingungen dieses App Stores schreibt Apple vor, dass alle Apps, die im Apple App Store veröffentlicht werden und die Authentifizierungsdienste Dritter anbieten, im Wesentlichen auch den Authentifizierungsdienst von Apple anbieten müssen. Damit verlangt Apple in seiner Position als Gatekeeper in den Nutzungsbedingungen eines zentralen Plattformdienstes von Nutzern, Apples Identifizierungsdienst anzubieten.

Diese Nutzungsbedingungen wären also gegebenenfalls nach dem vorgeschlagenen Digital Markets Act als Verstoß gegen Art. 5 lit. e anzusehen und damit unzulässig. Um diesen Verstoß auszuräumen, müsste Apple es den App-Entwicklern erlauben, Apps zu veröffentlichen, die zwar SSO-Dienste Dritter verwenden, aber kein „Login with Apple“ anbieten.

Auf die besondere Rolle von Apple als Produzent von Hardware und Software seiner Geräte und der Tatsache, dass derzeit alle Apps unter Apples Betriebssystem iOS über den Apple App Store bezogen werden müssen, sind in den USA bereits Verfahren anhängig,[97] in Europa nimmt die Europäische Kommission auch im *Impact Assessment* zum Digital Markets Act Stellung.[98] Hinsichtlich der App Store-Regeln für Musikstreaming-Anbieter wurde von der Europäischen Kommission bereits ein Verfahren eingeleitet und Beschwerdepunkte an Apple übermittelt.[99]

Der Entwurf zum Digital Markets Act scheint sohin geeignet, mögliche Wettbewerbsprobleme im Zusammenhang mit Single-Sign-On-Diensten zu verringern.

---

97 „Epic Games, Inc. v. Apple Inc.“, ohne Datum.

98 „Impact assessment of the Digital Markets Act | Shaping Europe’s digital future“, ohne Datum, https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act (zugegriffen am 31.03.2021).

99 Europäische Kommission: „Kartellrecht: Kommission übermittelt Apple Mitteilung der Beschwerdepunkte zu App-Store-Regeln für Musikstreaming-Anbieter“, Pressemitteilung, 30.04.2021, https://ec.europa.eu/commission/presscorner/detail/de/ip_21_2061 (zugegriffen am 28.06.2021).

5 Fazit

Im vorliegenden Text wurde die Wettbewerbsdynamik bei Single-Sign-On-Anbietern näher beleuchtet. Es wurde aufgezeigt, wie Netzwerkeffekte dazu führen, dass bei der Einführung solcher Angebote vor allem große Plattformen profitieren, und wie, aus der Technik bedingt, Single-Sign-On-Dienste zur Datensammlung verwendet werden können – wenngleich erwartbar scheint, dass der mögliche Umfang dieser Datensammlung durch die technische Weiterentwicklung von Browsern in Richtung zu mehr Privatsphäre abnimmt.

In Österreich werden SSO-Lösungen von etlichen großen Websites eingebunden, wobei diese oftmals einen niedrigschwelligen Zugang zu Diskussionsforen ermöglichen sollen, etwa insbesondere bei Nachrichtenplattformen. Dabei zeigten sich auch die Auswirkungen der App-Store-Politik von Apple, die dazu führt, dass auch Apples SSO-Dienst, trotz der relativen Neuheit, bereits weit vertreten ist. Auch im Telekom-Sektor ist das Thema relevant, da seitens österreichischer Betreiber die Einführung eines SSO-Dienstes geplant ist.

Sowohl auf österreichischer als auch auf europäischer Ebene werden eigene SSO-Lösungen konzipiert, wobei ein solcher SSO-Dienst auf europäischer Ebene im derzeitigen Vorschlag mit einer Pflicht zur Einbindung eben jenes Dienstes für sehr große Online-Plattformen einhergehen soll. Im Gegensatz dazu soll bei privaten Akteuren der Vorschlag zum europäischen Digital Markets Act dazu führen, dass Gatekeeper in ihren zentralen Plattformdiensten wie etwa App-Stores die Verwendung von eigenen SSO-Diensten nicht mehr vorschreiben dürfen.

Zusammenfassend befinden sich die technischen, rechtlichen und politischen Rahmenbedingungen für Single-Sign-On-Dienste sowie Log-in- und Identifizierungsdienste im Allgemeinen derzeit im Umbruch. Dieser Umbruch bedingt gleichzeitig auch massive Veränderungen in manchen Geschäftsmodellen, sodass weitere intensive Diskussionen zu erwarten sind.

Quellenverzeichnis

Amazon.de: „Login mit Amazon nutzen“, ohne Datum, https://www.amazon.de/gp/help/customer/display.html?nodeId=G4CY3HAXTSFLGC22 (zugegriffen am 23.06.2021).

Ankit Babbar: „Designing OAuth Auth Flow“, *DEV Community*, 19.09.2020, https://dev.to/babbarankit/designing-oauth-auth-flow-96i (zugegriffen am 16.06.2021).

Auth0: „Social Identity Providers“, *Auth0 Docs*, ohne Datum, https://auth0.com/docs/ (zugegriffen am 31.03.2021).

Bradley, John, Nat Sakimura und Michael B. Jones: „JSON Web Token (JWT)“, ohne Datum, https://tools.ietf.org/html/rfc7519 (zugegriffen am 30.03.2021).

Competition and Markets Authority (CMA): „CMA to investigate Google’s ‘Privacy Sandbox’ browser changes“, 08.01.2021, https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes (zugegriffen am 12.01.2021).

CPI: „DOJ Looks Into Complaints Regarding The ‚Sign In With Apple‘ Button“, *Competition Policy International*, 24.02.2021, https://www.competitionpolicyinternational.com/doj-looks-into-complaints-regarding-the-sign-in-with-apple-button/ (zugegriffen am 23.04.2021).

Deckelmann, Selena: „Latest Firefox release includes Multiple Picture-in-Picture and Total Cookie Protection“, *The Mozilla Blog*, 23.02.2021, https://blog.mozilla.org/blog/2021/02/23/latest-firefox-release-includes-multiple-picture-in-picture-and-total-cookie-protection (zugegriffen am 30.03.2021).

---: „Latest Firefox rolls out Enhanced Tracking Protection 2.0; blocking redirect trackers by default“, 04.08.2020, https://blog.mozilla.org/blog/2020/08/04/latest-firefox-rolls-out-enhanced-tracking-protection-2-0-blocking-redirect-trackers-by-default (zugegriffen am 11.01.2021).

E-Government Innovationszentrum: „ID Austria - Anbindung“, ohne Datum, https://eid.egiz.gv.at/anbindung/allgemeines/ (zugegriffen am 11.06.2021).

Europäische Kommission: „Kartellrecht: Kommission übermittelt Apple Mitteilung der Beschwerdepunkte zu App-Store-Regeln für Musikstreaming-Anbieter“, Pressemitteilung, 30.04.2021, https://ec.europa.eu/commission/presscorner/detail/de/ip_21_2061 (zugegriffen am 28.06.2021).

Geradin, Damien, Dimitrios Katsifis und Theano Karanikioti: „Google as a de facto privacy regulator: Analyzing Chrome’s removal of third-party cookies from an antitrust perspective“, SSRN Scholarly Paper ID 3738107, Rochester, NY: Social Science Research Network, 26.11.2020, https://papers.ssrn.com/abstract=3738107 (zugegriffen am 27.11.2020).

hickeys: „Microsoft Store-Richtlinien - UWP applications“, ohne Datum, https://docs.microsoft.com/de-de/windows/uwp/publish/store-policies (zugegriffen am 19.03.2021).

hpsin: „How to handle Intelligent Tracking Protection (ITP) in Safari - Microsoft identity platform“, 19.05.2020, https://docs.microsoft.com/en-us/azure/active-

directory/develop/reference-third-party-cookies-spas (zugegriffen am 30.03.2021).

---: „Microsoft identity platform and OpenID Connect protocol - Microsoft identity platform“, 22.05.2020, https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-protocols-oidc (zugegriffen am 14.05.2021).

Keith Folz: „Cookies, Single Sign-On, and You - The Akamai Blog“, 17.01.2020, https://blogs.akamai.com/2020/01/cookies-single-sign-on-and-you.html (zugegriffen am 30.03.2021).

MSEdgeTeam: „Tracking Prevention in Microsoft Edge (Chromium) - Microsoft Edge Development“, ohne Datum, https://docs.microsoft.com/en-us/microsoft-edge/web-platform/tracking-prevention (zugegriffen am 30.03.2021).

Norwegian Consumer Council / Forbrukerrådet: „Time to ban surveillance-based advertising“, 22.06.2021, https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/ (zugegriffen am 24.06.2021).

online, heise: „Identitätsübernahme: Okta kauft Startup Auth0 für 6,5 Milliarden US-Dollar“, *iX Magazin*, 05.03.2021, https://www.heise.de/news/Identitaetsuebernahme-Okta-kauft-Startup-Auth0-fuer-6-5-Milliarden-US-Dollar-5072967.html (zugegriffen am 31.03.2021).

Reschke, Julian F. und Roy T. Fielding: „Hypertext Transfer Protocol (HTTP/1.1)“, RFC 7230, 06.2014, https://tools.ietf.org/html/rfc7230 (zugegriffen am 30.11.2020).

Rescorla, Eric: „Privacy analysis of FLoC“, *The Mozilla Blog*, 10.06.2021, https://blog.mozilla.org/en/privacy-security/privacy-analysis-of-floc/ (zugegriffen am 28.06.2021).

RTR: „1. Workshop „Mobile Connect Global ID““, *RTR*, 08.10.2018, https://www.rtr.at/TKP/aktuelles/veranstaltungen/veranstaltungen/MobileconnectglobalID/1._Workshop_-Mobile_Connect_Global_ID-.de.html (zugegriffen am 22.03.2021).

RTR.Telekom.Post: „Monitoring von Kommunikations-Plattformen und Gatekeepern des offenen Internetzugangs“, 19.05.2020, https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/plattformen-monitoring-methoden.de.html (zugegriffen am 11.06.2021).

Schmidt, Jürgen: „Passwortloses Anmelden dank FIDO2“, *c't Magazin*, 19.08.2019, https://www.heise.de/ct/artikel/Passwortloses-Anmelden-dank-FIDO2-4494951.html (zugegriffen am 11.06.2021).

The Chromium Projects: „The Privacy Sandbox“, ohne Datum, https://www.chromium.org/Home/chromium-privacy/privacy-sandbox (zugegriffen am 23.11.2020).

Wiewiorra, Lukas, Andrea Liebe und Serpil Taş: „Die wettbewerbliche Bedeutung von Single-Sign-On- bzw. Login-Diensten und ihre Relevanz für datenbasierte Geschäftsmodelle sowie den Datenschutz“ WIK/462 (06.2020), https://www.wik.org/presse/meldungen/detailansicht?tx_ttnews%5BbackPid%5D=85&tx_ttnews%5Btt_news%5D=2352&cHash=617b726b6deeaa6238797e15c1db8eb5 (zugegriffen am 15.03.2021).

„Add sign in with Microsoft - Microsoft identity platform“, ohne Datum, https://developer.microsoft.com/en-us/identity/add-sign-in-with-microsoft (zugegriffen am 19.03.2021).

„‚Allianzen sehr mühsam zustande zu bringen‘: Markus Breitenecker sucht Mitspieler in Medienbranche“, *Der Standard*, 24.06.2021, https://www.derstandard.at/story/2000127651163/allianzen-sehr-muehsam-zustande-zu-bringen-markus-breitenecker-sucht-mitspieler (zugegriffen am 24.06.2021).

„APA setzt im Jubiläumsjahr auf Stärkung der Digital-Strategie“, *DER STANDARD*, 25.03.2021, https://www.derstandard.at/story/2000125345804/apa-setzt-im-jubilaeumsjahr-auf-staerkung-der-digital-strategie (zugegriffen am 23.04.2021).

„Authentication“, *MobileConnect*, ohne Datum, https://mobileconnect.io/authentication/ (zugegriffen am 19.03.2021).

„Can I use... WebAuthn“, 12.06.2021, https://caniuse.com/webauthn (zugegriffen am 30.03.2021).

„Consider allowing RPs to indicate that they want platform authenticators to be synced across devices · Issue #969 · w3c/webauthn“, *GitHub*, 25.06.2018, https://github.com/w3c/webauthn/issues/969 (zugegriffen am 30.03.2021).

„Devices, the weak link in achieving an open internet“, ARCEP, 02.2018, https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf (zugegriffen am 05.07.2021).

„Draft BEREC Report on the ex ante regulation of digital gatekeepers“, BoR (21) 34, BEREC, 11.03.2021, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/9880-draft-berec-report-on-the-ex-ante-regulation-of-digital-gatekeepers (zugegriffen am 05.07.2021).

„Epic Games, Inc. v. Apple Inc.“, ohne Datum.

„European Net ID Foundation – European Net ID Foundation“, ohne Datum, https://enid.foundation/ (zugegriffen am 19.03.2021).

„Fashion ID GmbH & Co. KG. gegen Verbraucherzentrale NRW e. V.“, 29.07.2019, http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=16385238 (zugegriffen am 30.11.2020).

„Firefox Lockwise – Passwortmanager — Hab deine Passwörter überall parat.“, *Mozilla*, ohne Datum, https://www.mozilla.org/de/firefox/lockwise/ (zugegriffen am 31.03.2021).

„Getting Started - Sign in with Apple - Apple Developer“, ohne Datum, https://developer.apple.com/sign-in-with-apple/get-started/ (zugegriffen am 19.03.2021).

„Hide My Email for Sign in with Apple“, *Apple Support*, ohne Datum, https://support.apple.com/en-gb/HT210425 (zugegriffen am 19.03.2021).

„How to switch to an email & password login – Strava Support“, 09.03.2021, https://support.strava.com/hc/en-us/articles/216918817-How-to-switch-to-an-email-password-login?mobile_site=true (zugegriffen am 31.03.2021).

„I want to disconnect Facebook from my Spotify“, 15.03.2016, https://community.spotify.com/t5/Spotify-Answers/I-want-to-disconnect-Facebook-from-my-Spotify/ta-p/1308147 (zugegriffen am 31.03.2021).

„Ihre Passwörter auf allen Geräten verwenden - Android-Gerät - Google Chrome-Hilfe“, ohne Datum, https://support.google.com/chrome/answer/6197437?co=GENIE.Platform%3DAndroid&hl=de (zugegriffen am 23.06.2021).
„Impact assessment of the Digital Markets Act | Shaping Europe’s digital future“, ohne Datum, https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act (zugegriffen am 31.03.2021).
„Location - Web APIs | MDN“, 08.04.2021, https://developer.mozilla.org/en-US/docs/Web/API/Location (zugegriffen am 26.04.2021).
„Lookalike Audiences von Facebook“, *Facebook for Business*, ohne Datum, https://de-de.facebook.com/business/a/custom-to-lookalike-audiences (zugegriffen am 28.06.2021).
„Market study into mobile app stores“, ACM/18/032693, ACM, 11.04.2019, https://www.acm.nl/sites/default/files/documents/market-study-into-mobile-app-stores.pdf (zugegriffen am 05.07.2021).
„Mobile Connect“, *KPN API Store*, 05.04.2019, https://developer.kpn.com/apis/kpn-mobile-connect-api (zugegriffen am 23.06.2021).
„myDPD - Login“, ohne Datum, https://www.mydpd.at/login (zugegriffen am 25.06.2021).
„New Guidelines for Sign in with Apple - News - Apple Developer“, ohne Datum, https://developer.apple.com/news/?id=09122019b (zugegriffen am 19.03.2021).
„Next steps to ensure transparency, choice and control in digital advertising“, *Google*, 22.08.2019, https://blog.google/products/ads/next-steps-transparency-choice-control/ (zugegriffen am 26.04.2021).
„OAuth 2.0 — OAuth“, ohne Datum, https://oauth.net/2/ (zugegriffen am 30.03.2021).
„OpenID Connect | OpenID“, 01.08.2011, https://openid.net/connect/ (zugegriffen am 30.03.2021).
„Operators | Mobile Connect Developer Portal“, ohne Datum, https://developer.mobileconnect.io/operators?title=&name_list=AT&field_mobile_connect_status_value=All (zugegriffen am 22.03.2021).
„Overview | Sign In With Google“, *Google Developers*, ohne Datum, https://developers.google.com/identity/gsi/web/guides/overview (zugegriffen am 30.03.2021).
„Passwortmanager“, *KONSUMENT* 2018/4 (22.03.2018), https://www.konsument.at/passwortmanager042018.
„Richtlinienübersicht für Entwickler“, ohne Datum, https://play.google.com/about/developer-content-policy/ (zugegriffen am 19.03.2021).
„Same-origin policy - Web security | MDN“, 19.02.2021, https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy (zugegriffen am 24.03.2021).
„Sign In With Google | Google Developers“, ohne Datum, https://developers.google.com/identity/gsi/web (zugegriffen am 30.03.2021).
„Social Login - Time to implement it in your apps“, *Auth0*, ohne Datum, https://auth0.com/learn/social-login/ (zugegriffen am 19.03.2021).

„The HTML autocomplete attribute - HTML: HyperText Markup Language | MDN“, 27.03.2021, https://developer.mozilla.org/en-US/docs/Web/HTML/Attributes/autocomplete (zugegriffen am 31.03.2021).
„Tracking Prevention in WebKit“, *WebKit*, 24.06.2020, https://webkit.org/tracking-prevention/ (zugegriffen am 30.03.2021).
„Troubleshooting | Google Sign-In for Websites“, *Google Developers*, ohne Datum, https://developers.google.com/identity/sign-in/web/troubleshooting (zugegriffen am 30.03.2021).
„Use your Google Account to sign in to other apps or services - Computer - Google Account Help“, ohne Datum, https://support.google.com/accounts/answer/112802?co=GENIE.Platform%3DDesktop&hl=en (zugegriffen am 19.03.2021).
„User Privacy and Data Use - App Store“, *Apple Developer*, ohne Datum, https://developer.apple.com/app-store/user-privacy-and-data-use/ (zugegriffen am 23.06.2021).
„Verbesserter Tracking-Schutz im Firefox Browser“, *Firefox Forward*, 28.02.2019, https://blog.mozilla.org/firefox/de/verbesserter-tracking-schutz-von-firefox/ (zugegriffen am 30.03.2021).
„Verwenden von OAuth 2.0 für den Zugriff auf Google APIs“, *Google Developers*, 15.04.2021, https://developers.google.com/identity/protocols/oauth2?hl=de (zugegriffen am 14.05.2021).
„Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor“, 15.12.2020, https://eur-lex.europa.eu/legal-content/de/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN (zugegriffen am 31.03.2021).
„Web - Facebook Login - Dokumentation“, *Facebook for Developers*, ohne Datum, https://developers.facebook.com/docs/facebook-login/web/ (zugegriffen am 24.03.2021).
„Web Authentication: An API for accessing Public Key Credentials - Level 2“, ohne Datum, https://www.w3.org/TR/webauthn/ (zugegriffen am 30.03.2021).
„Web Authentication API - Web APIs | MDN“, 16.03.2021, https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API (zugegriffen am 30.03.2021).
„Web Authentication: Resident Credential“, ohne Datum, https://www.w3.org/TR/webauthn/#resident-credential (zugegriffen am 30.03.2021).
„WebAuthn Is Great and It Sucks“, *Okta Security*, 16.04.2020, https://sec.okta.com/articles/2020/04/webauthn-great-and-it-sucks (zugegriffen am 11.06.2021).
„Zur Offenheit des Internets: Betriebssysteme, Apps und App Stores“, RTR Fachbereich Telekom und Post, 06.2019, https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/OffenesInternetApps2019.de.html (zugegriffen am 05.07.2021).