JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
PROFESSUR BWL – WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL SCHWICKERT

Lapscheck, Niklas; Schick, Lukas; Schwickert, Axel

FIDO2 – Grundlagen, Prinzipien und praktische Anwendung

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 2 / 2021
ISSN 1613-6667

Arbeitspapiere WI Nr. 2 / 2021

Autoren: Lapscheck, Niklas; Schick, Lukas; Schwickert, Axel

Titel: FIDO2 – Grundlagen, Prinzipien und praktische Anwendung

Zitation: Lapscheck, Niklas; Schick, Lukas; Schwickert, Axel: FIDO2 – Grundlagen, Prinzipien und praktische Anwendung, in: Arbeitspapiere WI, Nr. 2/2021, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2021, 56 Seiten, ISSN 1613-6667.

Kurzfassung: In dem Arbeitspapier WI „FIDO2 – Grundlagen, Prinzipien und praktische Anwendung“ (Nr. 02/2021) wird erläutert, was hinter der Technologie FIDO2 steckt und wie diese grundlegend funktioniert. FIDO2 wurde 2019 durch die FIDO-Allianz veröffentlicht und ermöglicht mittels asymmetrischer Verschlüsselung eine passwortlose Authentifizierung im Web. Besonders aufgrund der weitverbreiteten Nutzung von (schlechten) Passwörtern als einziger Authentifizierungsfaktor wird die Relevanz einer sicheren Alternative immer größer. Dazu werden zunächst die Grundlagen der IT-Sicherheit anhand relevanter Sicherheitsziele erläutert. Darauf aufbauend wird die Authentifizierung mit FIDO2 anhand von sechs Komponenten dargestellt und beispielhaft beschrieben. Basierend auf diesem Prozess wird näher betrachtet, welche Prinzipien hinter FIDO2 stecken und welche Ziele verfolgt werden. Aufgrund der praktischen Relevanz werden im Folgenden einige Online-Dienste vorgestellt, die FIDO2 bereits anbieten. Des Weiteren werden sowohl Potenziale als auch Risiken aufgegriffen und ein beispielhafter Leitfaden zur Registrierung eines Sicherheitsschlüssels dargestellt. Das vorliegende Arbeitspapier soll dem Nutzer einen Überblick verschaffen, wie FIDO2 von anderen Authentifizierungsverfahren abgegrenzt und eine passwortlose Authentifizierung im Web realisiert werden kann.

Schlüsselwörter: Verschlüsselung, Web, Signatur, Schlüssel, Schlüsselpaar, öffentlich, privat, asymmetrisch, Sicherheitsschlüssel, FIDO, Nutzer, WebAuthn, Web Server, Online-Dienst, Web Browser

Inhaltsverzeichnis

Seite

Abbildungsverzeichnis

Seite

Abkürzungsverzeichnis

Azure AD ..... Azure Active Directory

BSI..... Bundesamt für Sicherheit in der Infromationstechnik

CTAP2..... Client to Authenticator Protocol

ERP ..... Enterprise Resource Planning

FIDO ..... Fast Identity Online

HOTP ..... Hash Message Authentication Mode-based One-time Password

HTTPS..... Hypertext Transfer Protocol Secure

MITM..... Man-in-the-Middle

PIN ..... Personal Identification Number

PKI ..... Private Key Infrastructure

SSO ..... Single-Sign-on

TAN..... Transaktionsnummer

TLS..... Transport Layer Security

TOTP..... Time-based One-time Password

TPM..... Trusted Platform Module

U2F..... Universal Second Factor

UAF..... Universal Authentication Framework

USB ..... Universal Serial Bus

W3C ..... World Wide Web Consortium

WebAuthn ..... Web Authentication

1 Problemstellung, Ziel und Aufbau

Der Einsatz von Passwörtern ist im Internet allgegenwärtig. Zum Beispiel erfordern abgesicherte Bereiche einer Web Site im Regelfall die Eingabe einer Nutzername-Passwort-Kombination, um persönliche oder sensible Daten abzurufen. Beispielhaft können an dieser Stelle Kontodaten, Adressen oder Nachrichten genannt werden. Diese Daten sollten ausschließlich dem jeweiligen Nutzer bzw. dem jeweiligen Unternehmen zur Verfügung stehen und Dritten nicht zugänglich sein. Dies nicht nur um die eigene Privatsphäre zu schützen, sondern z. B. auch, um den ungewollten Zugriff auf die eigenen Bankkonten zu verhindern. Zur Absicherung des persönlichen Bereichs wählt der Nutzer daher einen Benutzernamen und definiert sein individuelles Passwort. Als Benutzername werden häufig E-Mail-Adressen oder ein frei wählbares Pseudonym verwendet. Während sich die Nutzer bei der Wahl eines geeigneten Pseudonyms üblicherweise kreativ und einfallsreich zeigen, handelt man häufig leichtfertig und fahrlässig beim Setzen eines sicheren Passworts.

Die Nutzer scheinen schlichtweg zu bequem zu sein, ein den Anforderungen entsprechendes Passwort zu erstellen. Bis heute ist die Zeichenkette “password” eines der am häufigsten verwendeten Passwörter. Sichere Passwörter, die aus einer ausreichend langen Kombination von Buchstaben, Zahlen und (Sonder-)Zeichen bestehen, sind bei vielen Nutzern eher eine Seltenheit. Bei vielen Nutzern besteht daher die ständige Gefahr, dass Unbefugte Kenntnis der Passwörter erlangen.[1]

Hinzu kommt, dass viele Nutzer für unterschiedliche Dienste das gleiche Passwort verwenden. Ca. 73% der Nutzer von Online-Diensten verwenden ein Passwort gleichermaßen für ihr Nutzerkonto bei einem Online Shop als auch für ihren Finanzdienstleister. Wenn überhaupt, erfolgt häufig nur eine geringe Varianz der Passwörter, sodass sich diese nur in einer Zahl oder einem Buchstaben unterscheiden. Es wird geschätzt, dass allein mit 10.000 herkömmlichen Passwörtern Zugang zu etwa 98% aller Konten weltweit verschafft werden könnte. Hier besteht also dringender Handlungsbedarf.[2]

1 Vgl. Kappes, Martin: Netzwerk- und Datensicherheit – Eine praktische Einführung, 2. Auflage, Wiesbaden: Springer Verlag 2013, S. 43-45, vgl. FIDO-Allianz (Hrsg.): Introduction to FIDO’s Identity Verification & Binding Initiative, online im Internet: https://fidoalliance.org/introduction-to-fidos-identity-verification-binding-initiative/, 29. 04.2020 und vgl. IT-Zoom (Hrsg.): Das Ende des Passworts, online im Internet: https://www.it-zoom.de/sn/microsoft/e/das-ende-des-passworts-10312/, abgerufen am 29.04.2020.

2 Vgl. Lindemann, Rolf: Not built on sand – How modern authentification complements federation, in: Lecture Notes in Informatics (LNI), 2013, S. 164.

Die Abhängigkeit und gleichzeitig unsichere Nutzung von Passwörtern zeigt sich besonders in Zeiten der zunehmenden Frequentierung des Internets und einer weltweiten Vernetzung zwischen Transaktions- und Kommunikationspartnern. Die Anzahl an sogenannten „Phishing-Mails“, anhand derer Passwörter über gefälschte Web Sites gestohlen und missbraucht werden, steigt stetig. Zusätzlich muss der Nutzer darauf vertrauen, dass Online-Dienste seine Passwörter vor dem Zugriff Dritter schützen. Unabhängig davon, wie sicher ein Passwort ist, verhindert dies den Diebstahl nicht, wenn der Nutzer selbst das Sicherheitsrisiko darstellt, wenn er z. B. ein aufgeschriebenes Passwort offen an seinem Monitor aufklebt oder unverschlüsselt als Dokument auf dem PC ablegt.[3]

Die FIDO-Allianz stellt sich dieser Thematik und hat es sich zum Ziel gemacht, Sicherheitsmaßnahmen in Form von standardisierten Authentifizierungsverfahren zu entwickeln. Beispielsweise sollen biometrische Verfahren oder eine „Personal Identification Number“ (PIN) zwischen Client und Web-Server genutzt werden, um die Sicherheit im Internet zu erhöhen.[4]

Ziel der vorliegenden Arbeit ist es, die Grundlagen von FIDO2 zu erläutern und einen Überblick über die Funktionsprinzipien und Anwendungsgebiete von FIDO2 zu geben. Darüber hinaus soll erörtert werden, welche Vor- und Nachteile sich aus der Anwendung von FIDO2 ergeben und ob Potenzial zur Massentauglichkeit besteht.

Kapitel 2 befasst sich zunächst mit dem Begriff „FIDO2“ und erläutert dessen Bedeutung und Herkunft. Darauf aufbauend wird FIDO2 in den Kontext der Sicherheitstechnik eingeordnet und seinem Vorgänger FIDO1 gegenübergestellt. Daran anknüpfend werden die Komponenten von FIDO2 beschrieben.

Kapitel 3 erläutert die Prinzipien von FIDO2: Sicherheit, Nutzbarkeit, Privatsphäre und Skalierbarkeit. Diese Prinzipien stellen den Kern von FIDO2 dar. Unter Berücksichtigung der sicherheitstechnischen Grundlagen soll hierbei geklärt werden, wie sich diese Prinzipien in der Anwendung von FIDO2 zeigen.

3 Vgl. Meinel, Christoph; Sack, Harald: Sicherheit und Vertrauen im Internet – Eine technische Perspektive, Wiesbaden: Springer Verlag 2014, S. 3.

4 Vgl. FIDO-Allianz (Hrsg.): What makes FIDO different, online im Internet: https://fidoalliance.org/key-differentiators/, abgerufen am 29.04.2020.

In Kapitel 4 werden die Anwendungsgebiete von FIDO2 und die täglichen Berührungspunkte von Nutzern aufgezeigt. Zunächst werden die Anbieter von Online-Diensten vorgestellt, welche die FIDO2-Schnittstelle nutzen. Anschließend werden die Vorteile von FIDO2 sowohl für den Anbieter als auch den Nutzer herausgestellt. Nachfolgend werden die Nachteile und Risiken von FIDO2 beschrieben. Zuletzt stellt ein Praxisbeispiel den Prozess von der Implementierung bis hin zur Nutzung von FIDO2 beispielhaft dar. Dies soll dem Leser eine anschauliche Demonstration bieten, wie FIDO2 genutzt werden kann.

2 Grundlagen von FIDO2

2.1 Systematisierung der Grundlagen von FIDO2

FIDO2 ist ein Standard der FIDO-Allianz und des World Wide Web Consortiums (W3C), der eine starke Authentifizierungslösung im Web realisiert. Dabei kommen kryptographische Verfahren zum Einsatz, welche die Authentifizierung über das Internet einfacher und sicherer machen. Durch FIDO2 soll sowohl die Abhängigkeit von Passwörtern reduziert, als auch die Sicherheit im Internet verbessert werden. Hierbei spielt vor allem der Schutz vor Phishing-Attacken aber auch der Datenschutz und die Datenintegrität eine besondere Rolle. Phishing-Attacken locken Nutzer durch gefälschte E-Mails und Web Sites an und versuchen, durch eine gefälschte Web Site-Oberfläche, die Nutzer zu verleiten, ihre Kombination aus Nutzernamen und Passwort einzugeben. Kriminelle Dritte wollen so Zugang zu sensiblen Nutzerdaten erhalten. Um dieses Ziel zu erreichen, wird auf ein Zusammenspiel aus vier Komponenten zurückgegriffen. Neben dem Begriff „FIDO2“ und den Grundlagen der Informationssicherheit werden diese Komponenten im vorliegenden Kapitel 2 einleitend beschrieben.

Kapitel 2.2: Zum Begriff „FIDO2“

Das erste Grundlagenkapitel beschäftigt sich mit dem Begriff „FIDO2“ und dessen Bedeutung. FIDO2 setzt sich als Abkürzung aus dem Begriff „Fast Identity Online“ zusammen und wurde von der FIDO-Allianz entwickelt und standardisiert. Dabei wird das Ziel verfolgt, die Nutzung von Passwörtern zu reduzieren. Einerseits werden die Ansprüche an Passwörter immer höher, auf der anderen Seite jedoch geben sich die Nutzer immer weniger Mühe, sichere Passwörter zu generieren. FIDO2 soll mit seinen kryptographischen Verfahren Passwörter obsolet machen und den Nutzern im Internet eine sichere Alternative bieten. Dabei soll den Anwendern aber auch eine gesteigerte Nutzbarkeit durch einfache Prozesse geboten werden.

Kapitel 2.3: FIDO2 und die Grundlagen der Informationssicherheit

Für die Entwicklung IT-gestützter Verfahren lassen sich in Literatur und Praxis wesentliche Sicherheitsziele identifizieren. Die Erfüllung dieser Sicherheitsziele ist auch zentraler Bestandteil von FIDO2. Die Sicherheitsziele, die dem Einsatz von FIDO2 zu Grunde liegen, lassen sich in Vertraulichkeit, Integrität, Authentifizierung und Verbindlichkeit unterscheiden.

Systeme, die das Ziel der „Vertraulichkeit“ erfüllen sollen, müssen dafür sorgen, dass die enthaltenen Informationen vor dem Zugriff Dritter geschützt aufbewahrt und übermittelt werden. Vertraulichkeit kann über den Einsatz kryptographischer Verfahren geschaffen werden. Dazu können sowohl symmetrische als auch asymmetrische Verfahren genutzt werden.

Die „Integrität“ soll gewährleisten, dass Informationen nicht unbemerkt verändert oder von unautorisierten Personen versendet oder empfangen werden. Dazu können ebenfalls asymmetrische Verschlüsselungsverfahren eingesetzt werden.

„Authentizität“ verlangt, dass nur solche Personen Zugang zum IT-System erhalten, die entsprechend ihrer Nutzerrolle dazu berechtigt sind. Um dies sicherstellen zu können, muss eine Überprüfung der Identität vorgenommen werden. Authentifizierung kann sowohl über den Einsatz von Passwörtern, als auch über den Besitz eines Gegenstandes oder mithilfe von biometrischen Verfahren erzielt werden. Welches Verfahren zum Einsatz kommt, hängt von verschiedenen Faktoren ab.

„Verbindlichkeit“ wird dann erzielt, wenn ein Nutzer eine Aktion, an der er beteiligt war, im Nachhinein nicht abstreiten kann. Zum Erreichen des Ziels können unter anderem digitale Signaturen verwendet werden. Diese identifizieren einen Nutzer eindeutig.

Kapitel 2.4: Entwicklung von FIDO1 zu FIDO2

FIDO1, oder auch Universal Second Factor (U2F) genannt, ist der Vorgänger von FIDO2. FIDO1 baut auf dem asymmetrischen Public-Key-Verfahren auf und bietet dem Nutzer eine zweite Sicherheitsschranke zusätzlich zum Passwort. Dadurch soll das Abgreifen von Passwörtern durch Dritte unrentabel werden. Die Weiterentwicklung zu FIDO2 zeichnet sich besonders durch ihren gesteigerten Komfort für den Nutzer aus, zusätzlich zur gesteigerten Sicherheit gegenüber dem klassischen Passwort. Weitere wichtige Faktoren sind die Privatsphäre und Skalierbarkeit.

Kapitel 2.5: Die sechs Komponenten von FIDO2

FIDO2 baut auf sechs Komponenten auf. Diese machen den Kern des Authentifizierungsverfahrens aus. Kernstück dabei spielt die JavaScript-Schnittstelle „Web Authentication“

(WebAuthn), über die die Generierung des asymmetrischen Schlüsselpaares vorgenommen wird. Diese Schnittstelle muss einerseits auf Seiten des Web Browsers (Client) und andererseits auf Seiten des Web Servers implementiert werden. Dadurch ist der Nutzer in der Lage die Technologie FIDO2 verwenden zu können. Gespeichert wird das Schlüsselpaar auf einem FIDO-Gerät, dem Sicherheitsschlüssel, der über eine Nutzergeste durch den Nutzer aktiviert werden kann. Zur Übermittlung der Nutzerdaten wird das Client to Authenticator Protocol 2 (CTAP2) verwendet.

2.2 Zum Begriff „FIDO2“

„FIDO2“ leitet sich aus dem Begriff „Fast Identity Online“ ab und bedeutet sinngemäß „schnelle Identifikationsprüfung über das Internet“. Dahinter verbirgt sich ein Verfahren, das ermöglichen soll Nutzer im Internet eindeutig identifizieren und authentifizieren zu können. Zuvor wurden bereits zwei Standards für die Authentifizierung entwickelt. Eine genauere Erläuterung dieser Standards und der Entwicklung bis hin zu FIDO2 erfolgt in Kapitel 2.4.[5]

Entwickelt wurde FIDO2 durch die FIDO-Allianz. Die FIDO-Allianz ist eine nicht kommerzielle Gemeinschaft von Unternehmen aus den Branchen der Hard- und Software-Hersteller wie bspw. Intel oder Lenovo oder Anbietern von Online-Diensten, z. B. aus dem Bereich des Online-Bankings. Aber auch Technologie-Unternehmen wie bspw. Amazon, Apple oder Microsoft gehören dieser Kooperation an. Gegründet wurde diese Allianz bereits 2012 unter der Führung von PayPal, Lenovo, Nok Nok Labs, Validity Sensors, Infineon und Agnitio mit dem Ziel, Protokolle zur passwortlosen Authentifizierung zu entwickeln und den Nutzern offene und lizenzfreie Standards zur Verfügung zu stellen.[6]

Über die Mitglieder hinaus haben sich weitere Gremien und Arbeitsgruppen der FIDO-Allianz als Kooperationspartner angeschlossen. Darunter befindet sich bspw. das W3C, ein unabhängiges Gremium, als besonders enger Partner, der Standards für das Internet entwickelt und dessen Nutzern zu Verfügung stellt. Das W3C orientiert sich dabei an den Prinzipien der Verfügbarkeit, Internationalisierung, Web-Sicherheit und Privatsphäre. Somit ist das W3C eng verknüpft mit den Grundlagen der Informationssicherheit, die in Kapitel 2.3 näher erläutert werden.[7]

5 Vgl. Eikenberg, Ronald: Schlüssel zum Glück – Was schon heute mit dem Passwortkiller FIDO2 geht, in: c’t, 18/2019, S. 24.

6 Vgl. FIDO-Allianz (Hrsg.): FIDO Members, Online im Internet: https://fidoalliance.org/members/, abgerufen am 03.05.2020.

7 Vgl. W3C (Hrsg.): W3C MISSION, Online im Internet: https://www.w3.org/Consortium/mission.html#principles, abgerufen am 03.05.2020.

Mit der Mitgliedschaft in der FIDO-Allianz verpflichten sich die Unternehmen dem Ziel, das Internet weniger abhängig von Passwörtern zu machen, bzw. diese ganz zu eliminieren. Gleichzeitig soll Nutzern und Anbietern eine gesteigerte Sicherheit bei höherer Nutzerfreundlichkeit und zu annehmbaren Kosten geboten werden. Im Rahmen ihrer unternehmerischen Tätigkeiten gilt es für die Mitglieder, entsprechende Verfahren zu entwickeln, zu zertifizieren und schlussendlich von Standardisierungsgremien als Standard anerkennen zu lassen. Im Rahmen ihrer Mitgliedschaft verpflichten sich die Unternehmen, die Verfahren und Protokolle als Standard allen potentiellen Nutzern zur Verfügung zu stellen.[8]

2.3 FIDO2 und die Grundlagen der Informationssicherheit

Die Sicherheit von Informationssystemen stellt einen dynamischen Prozess dar, der laufend an die internen und externen Risiken und Regularien angepasst werden muss. Besonders in Zeiten der digitalen Vernetzung ist es von großer Bedeutung, ein geeignetes Konzept zur Sicherung der unternehmensinternen Daten und Kommunikation zu entwickeln bzw. bereitzustellen. Darunter fällt auch das Bereitstellen der notwendigen Infrastruktur zur Nutzung von FIDO2. Bei der Wahrnehmung des Sicherheitsmanagements gilt es einige Grundlagen zu berücksichtigen.[9]

Vertraulichkeit: Unter „Vertraulichkeit“ lassen sich alle Maßnahmen zusammenfassen, mit dem Ziel vertrauliche Daten vor dem Zugriff Dritter zu schützen. Nur befugten Personen soll Zugang zu diesen Daten gewährt werden. Um dies zu gewährleisten, können kryptographische Verfahren sichere Kommunikationskanäle schaffen. Diese bringen den Vorteil mit sich, auch in weniger vertrauenswürdigen Umgebungen eine vertrauliche Basis zwischen zwei oder mehreren Kommunikationspartnern herstellen zu können.[10]

Kryptographie ist die Lehre der Verschlüsselung von Informationen und kann genutzt werden, um Vertraulichkeit herzustellen. Verschlüsselung bedeutet in diesem Kontext, dass Informationen unter Verwendung mathematischer Methoden von Klartext in Geheimtext umgewandelt werden. Der Geheimtext soll dabei so „sinnlos“ erscheinen, dass

8 Vgl. FIDO-Allianz (Hrsg.): Alliance Overview, Online im Internet: https://fidoalliance.org/overview/, abgerufen am 03.05.2020.

9 Vgl. Sackmann, Stefan: IT-Sicherheit, Online im Internet: https://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/technologien-methoden/Informatik--Grundlagen/IT-Sicherheit/index.html/?searchterm=sicherheit, abgerufen am 05.05.2020.

10 Vgl. Hansen, Hans Robert; Mendling, Jan; Neumann, Gustaf: Wirtschaftsinformatik, 11. Auflage, Berlin: Walter de Gruyter 2015, S. 374, vgl. Gadatsch, Andreas; Mangiapane, Markus: IT- Sicherheit – Digitalisierung der Geschäftsprozesse und Informationssicherheit, Wiesbaden: Springer Verlag 2017, S. 21 und vgl. Schmoranz, Paul; Schick, Lukas; Schwickert, Axel: Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete, Gießen: Arbeitspapiere Wirtschaftsinformatik, 2/2020, S. 16 f.

ein unbefugter Dritter die Informationen nicht weiterverarbeiten kann. Gängige Verfahren der Kryptographie treten je nach Verwendungszweck in zwei Ausprägungen auf.[11]

- Symmetrische Verschlüsselungsverfahren
- Asymmetrische Verschlüsselungsverfahren

Das symmetrische Verschlüsselungsverfahren wird zunächst exemplarisch an einem Beispiel der Kommunikation per E-Mail veranschaulicht. Abbildung 1 zeigt diese Kommunikation zwischen Alice und Bob auf Basis eines symmetrischen Verfahrens, bei dem der Schlüssel für die Verschlüsselung und Entschlüsselung identisch ist.[12]

(1) Alice erstellt einen geheimen Schlüssel (Secret Key) und tauscht diesen mit Bob aus.

(2) Alice schreibt ihre Nachricht in Klartext und verschlüsselt diesen0 mit dem geheimen Schlüssel, den Alice und Bob miteinander ausgetauscht haben. Es entsteht eine Nachricht mit dem Geheimtext.

(3) Alice schickt die Datei mit dem Geheimtext per E-Mail an Bob. Wenn jemand unterwegs die Datei abgreift und öffnet, findet er nur den unverständlichen Geheimtext.

(4) Bob kann die Geheimtext-Datei mit dem geheimen Schlüssel, den Alice zuvor mit Bob geteilt hat, wieder in Klartext umwandeln.

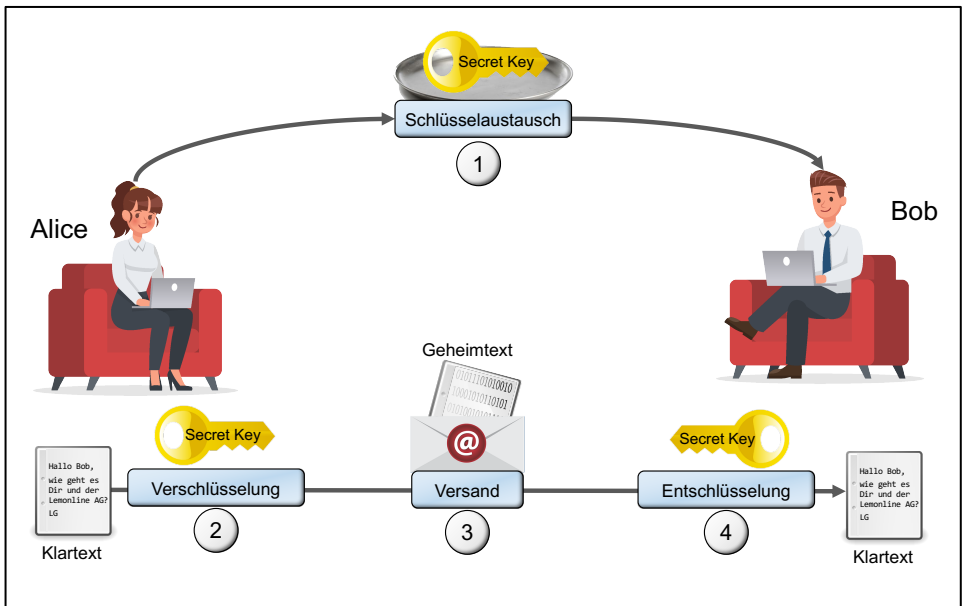

Abb. 1: Das Verfahren der symmetrischen Verschlüsselung

11 Vgl. Kappes, Martin: Netzwerk- und Datensicherheit – Eine praktische Einführung, a.a.O., S. 19.

12 Entnommen aus: Schmoranz, Paul; Schick, Lukas; Schwickert, Axel: Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete, a.a.O., S. 24 f.

Bei der symmetrischen Verschlüsselung muss sich vorab auf einen geheimen Schlüssel geeinigt und dieser ausgetauscht werden. Ein Versand des Schlüssels per Post oder in derselben E-Mail wäre jedoch zu unsicher und führt das Ziel der Verschlüsselung ad absurdum. Der Schlüssel würde der Öffentlichkeit auf dem Silbertablett serviert werden, wenn sich Alice und Bob über denselben Kanal auf einen geheimen Schlüssel einigen, über den sie später verschlüsselt miteinander kommunizieren möchten. Das Risiko wäre zu hoch, dass der geheime Schlüssel von einer unbefugten Person auf dem Weg abgefangen würde. Verschlüsselte Nachrichten könnten dann mitgelesen oder verändert werden. Um sicher zu sein, müsste der geheime Schlüssel folglich bei einem persönlichen Treffen an Bob übergeben werden. Alice möchte aber nicht nur mit Bob, sondern auch mit anderen Personen verschlüsselt im Web kommunizieren. Sie müsste dann für jede Person einen neuen Schlüssel generieren und diesen ebenfalls vorab geheim übergeben. Dieser manuelle Schlüsselaustausch ist bei einem sehr großen und weit entfernten digitalen Empfängerkreis nicht praktikabel. Diese Nachteile des symmetrischen Verfahrens werden zusammenfassend als Schlüsselaustauschproblem bezeichnet. Das Schlüsselaustauschproblem hat zur Folge, dass die Schutzziele der IT-Sicherheit – die Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit erheblich gefährdet sind.[13]

Um der Problematik der unsicheren Schlüsselübergabe entgegenzuwirken kann ein asymmetrisches Verschlüsselungsverfahren angewandt werden. Abbildung 2 zeigt die beispielhafte Kommunikation anhand einer E-Mail. Bob ist nun Eigentümer eines Schlüsselpaars.[14]

13 Entnommen aus: Schmoranz, Paul; Schick, Lukas; Schwickert, Axel: Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete, a.a.O., S. 27.

14 Vgl. Paar, Christof; Pelzl, Jan: Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, Berlin Heidelberg: Springer Vieweg 2016.S. 176.

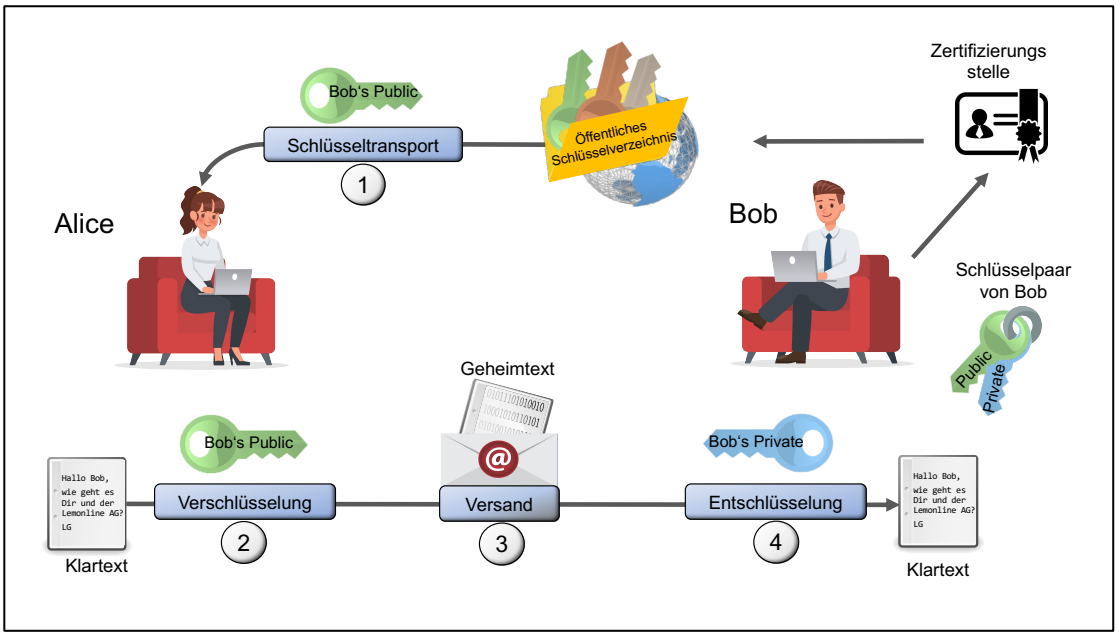

Abb. 2: Das Verfahren der asymmetrischen Verschlüsselung

(1) Bob erstellt ein Schlüsselpaar. Bob hinterlegt seinen öffentlichen Schlüssel in einem öffentlichen Schlüsselverzeichnis. Den privaten Schlüssel behält er für sich.

(2) Alice beschafft sich Bobs öffentlichen Schlüssel aus dem Schlüsselverzeichnis.

(3) Alice schreibt ihre Nachricht in Klartext und verschlüsselt diese mit dem öffentlichen Schlüssel von Bob. Es entsteht eine Nachricht mit dem Geheimtext.

(4) Alice schickt die verschlüsselte Nachricht per E-Mail an Bob. Wenn jemand unterwegs die Datei abgreift und öffnet, findet diese Person nur den unverständlichen Geheimtext.

(5) Nur Bob kann die Geheimtext-Datei mit seinem privaten Schlüssel in Klartext umwandeln, weil die Nachricht zuvor mit dem öffentlichen Schlüssel seines Schlüsselpaars verschlüsselt wurde.

Statt einen einzigen geheimen Schlüssel zur verschlüsselten Kommunikation auszutauschen, können Alice und Bob nun ein Schlüsselpaar verwenden. Das Schlüsselpaar besteht aus einem öffentlichen Schlüssel und einem dazugehörigen privaten Schlüssel. Beide Schlüssel sind durch ein mathematisches Verfahren miteinander verbunden und somit voneinander abhängig. Die Schlüsselpaare sind zudem einzigartig und werden individuell erstellt.[58] Anders als das symmetrische Verfahren, welches Informationen mit einem einzigen geheimen Schlüssel so- wohl verschlüsselt als auch entschlüsselt, wirkt ein asymmetrischer Schlüssel eines Schlüsselpaars nur in eine Richtung. Ist der Klartext mit dem

öffentlichen Schlüssel verschlüsselt worden, kann der Geheimtext nur noch mit dem privaten Schlüssel entschlüsselt werden. Die Algorithmen der asymmetrischen Verschlüsselungsverfahren basieren aus diesem Grund auf sogenannten Einwegfunktionen.[15]

Integrität: Ein weiterer Zweck der asymmetrischen Verschlüsselung dient der „Integrität". Das Schutzziel der Integrität befasst sich mit der Datenherkunft und der Unversehrtheit von Informationen. Dabei soll einerseits sichergestellt werden, dass die gesendeten Daten nicht verfälscht werden und dass der Sender der Daten als vertrauenswürdig erachtet und dementsprechend authentifiziert werden kann. Die Überprüfung dessen kann anhand von Hash-Funktionen vorgenommen werden, wodurch bereits minimale Abweichungen und Manipulationen von Informationen erkannt werden können. Integrität und Authentizität stehen somit in einem besonders engen Verhältnis zueinander.[16]

Authentizität: Im Rahmen der Authentifizierung muss ein Nutzer seine Identität bestätigen und beweisen, dass er auch wirklich die Person ist, für die sie sich ausgibt. Dies erfolgt bspw. wie zuvor beschrieben über kryptographische Verfahren, bei denen sich der Sender über seinen privaten Schlüssel authentifiziert. Der Schlüssel kann dabei die Funktion einer digitalen Unterschrift erfüllen.[17] In Verbindung mit einem asymmetrischen Schlüsselpaar dient eine digitale Signatur als solche Unterschrift. Signaturen weisen ähnliche Eigenschaften auf wie herkömmliche Unterschriften und authentifizieren einen Netzwerkteilnehmer bei seinem Kommunikationspartner, siehe Abbildung 4. Signaturen schaffen somit eine vertrauliche Basis in einem Netzwerk. Die Identitätserkennung schafft darüber hinaus die Möglichkeit, rechtskräftige Geschäfte zwischen dem Sender und dem Empfänger herzustellen und die Vertragsparteien an die Erfüllung ihrer Verpflichtungen zu binden. Identitäten stellen in diesem Kontext Kombinationen von bestimmten Eigenschaften dar, die unterschiedliche Rollen einnehmen können. Die Rolle definiert, welche Aktionen ein Nutzer innerhalb eines Systems ausführen kann.[18]

Der Begriff „Authentifizierung" beschreibt einen Prozess, der die Identität von etwas oder jemandem nachweist. Dazu erfolgt zunächst eine Authentisierung seitens des Nutzers

15 Entnommen aus: Schmoranz, Paul; Schick, Lukas; Schwickert, Axel: Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete, a.a.O., S. 30.

16 Vgl. Rehm, Stefan-Marc: Integrität in der Informationssicherheit, Online im Internet: https://www.haufe.de/compliance/management-praxis/integritaet-informationssicherheit_230130_482556.html, 29.01.2019, vgl. Petrlic, Ronald; Sorge, Christoph: Datenschutz – Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, Wiesbaden: Springer Verlag 2017, S. 10f und vgl. Sorge, Christoph; Gruschka, Nils; Lo Iacona, Luigi; Sicherheit in Kommunikationsnetzen, München: Oldenbourg Verlag 2013, S. 25f.

17 Vgl. Schmoranz, Paul; Schick, Lukas; Schwickert, Axel: Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete, Gießen: Arbeitspapiere Wirtschaftsinformatik, 2/2020, S. 15.

18 Vgl. Tsolkas, Alexander; Schmidt, Klaus: Rollen und Berechtigungskonzepte – Identity- und Access-Management im Unternehmen, 2. Auflage, Wiesbaden: Springer Verlag 2017, S. 23 ff.

durch die Eingabe eines Nutzernamens und eines Geheimnisses. Im Anschluss erfolgt die Prüfung der Identität seitens des Systems, die eigentliche Authentifizierung. Die Überprüfung der Identität erfolgt anhand bestimmter Kriterien, die mit der Identität verknüpft sind. Dazu können verschiedene Verfahren genutzt werden, auf deren Grundlage Zugänge an IT-Systemen, den Nutzerrollen entsprechend, zugeordnet werden können.[19]

Das gängigste Verfahren ist die „wissensbasierte Authentifizierung" mittels zweier zusammengehörender Informationen: Einem Nutzernamen und einem Geheimnis. Dazu muss der Nutzer zunächst seinen Nutzernamen in einer Eingabemaske eintragen. Dabei erfolgt eine Prüfung des Nutzernamens in der Datenbank des Systems. Anschließend wird der Nutzer aufgefordert, das dazugehörige Passwort einzutragen. Das Passwort sollte nur dem Nutzer bekannt sein, also wie ein Geheimnis behandelt werden und speziellen Sicherheitsanforderungen unterliegen. Auch die Authentifizierung an einem Geldautomaten folgt einem solchen Prinzip. Der Inhaber eines Bankkontos authentifiziert sich anhand einer 4-stelligen PIN, die im Normalfall nur dem Inhaber bekannt ist und fest mit seiner Bankkarte verknüpft ist.[20]

Ein mittlerweile häufig im betrieblichen Umfeld angewandtes Verfahren ist die Authentifizierung mittels eines bestimmten Gegenstandes. Um sich gegenüber einem System zu authentifizieren, muss der Nutzer also im Besitz eines Gegenstandes sein, der seine Identität bestätigt. Der Gegenstand bewahrt das Geheimnis für den Nutzer auf. Prominente Beispiele dafür sind unter anderem Chipkarten, die mittels eines Kartenlesegeräts ausgelesen werden können oder auch Sicherheitsschlüssel. Der externe Sicherheitsschlüssel und das IT-System, an dem sich der Nutzer authentifizieren möchte, kommunizieren über ein sogenanntes Challenge-Response-Verfahren gemäß des Client-Server Prinzips[21]. Das IT-System in Form des Servers, an dem sich der Nutzer anmelden möchte, sendet dabei eine „Challenge", eine Aufgabe, an den externen Sicherheitsschlüssel, die dieser lösen muss. Der Sicherheitsschlüssel generiert daraus eine Zeichenkette, deren Inhalt nur er selbst und das System kennen und die der Nutzer zu Beginn jeder Sitzung eingeben muss. Dies entspricht bspw. der Funktionsweise von Transaktionsnummer-Verfahren (TAN), die als zusätzliche Sicherheitsebene beim Online-Banking eingesetzt werden.[22]

19 Vgl. Luber, Stefan; Schmitz, Peter: Was ist Authentifizierung? Online im Internet: https://www.security-insider.de/was-ist-authentifizierung-a-617991/, 26.06.2017.

20 Vgl. Meinel, Christoph; Sack, Harald: Sicherheit und Vertrauen im Internet – Eine technische perspektive, a.a.O., S. 19 f. und vgl. Tsolkas, Alexander; Schmidt, Klaus: Rollen und Berechtigungskonzepte – Identity- und Access-Management im Unternehmen, a.a.O., S. 130.

21 Vgl. Hansen, Hans Robert; Mendling, Jan; Neumann, Gustaf: Wirtschaftsinformatik, a.a.O., S. 140.

22 Vgl. Tsolkas, Alexander; Schmidt, Klaus: Rollen und Berechtigungskonzepte – Identity- und Access-Management im Unternehmen, a.a.O., S. 136 ff. und vgl. Wendzel, Steffen: IT-Sicherheit für TCP/IP- und IoT-Netzwerke – Grundlagen, Konzepte, Protokolle, Härtung, a.a.O., S. 90.

Modernere Authentifizierungsmethoden können körperliche Merkmale zur Identitätsbestimmung heranziehen. Solche werden auch „biometrische Authentifizierungsverfahren“ genannt. Biometrische Verfahren verwenden einerseits solche Merkmale, die bei jedem Menschen vorhanden sind, damit sie von jedem genutzt werden können. Andererseits müssen die Merkmale so einzigartig sein, sodass sich darüber jeder Nutzer von anderen unterscheiden kann. Außerdem dürfen sich diese Merkmale im Laufe der Zeit nicht verändern, sodass die Eigenschaft auch im Alter noch vorhanden ist. Zudem sollten Nutzung und Implementierung nicht kompliziert sein. Solche Verfahren werden häufig zum Entsperren von Smartphones oder auch Tablets genutzt oder werden über diese zur Authentifizierung angeboten. Neuere Modelle können sogar auf eine Gesichtserkennung zurückgreifen. Dieses Prinzip wird unter anderem von Apple z. B. beim Download von Apps genutzt.[23]

Zur Steigerung der Sicherheit können biometrische Verfahren auch mit weiteren Authentifizierungsverfahren kombiniert werden. Bei der „Zwei-Faktor- Authentifizierung“ können unter anderem biometrische Verfahren zusätzlich zur Passworteingabe eingesetzt werden. Dies ist vor allem dann sinnvoll, wenn sensible Daten geschützt werden müssen. Passwörter als alleiniger Sicherheitsfaktor bieten aufgrund vielfältiger technischer und nicht-technischer Angriffsmöglichkeiten nur eine bedingte Sicherheit.[24]

Verbindlichkeit: Das Ziel der „Verbindlichkeit“ soll gewährleisten, dass ein Nutzer, bzw. ein Teilnehmer einer Aktion, seine Teilnahme im Nachhinein nicht abstreiten kann. Besonders relevant ist das Ziel im Bereich des E-Commerce, da dort getätigte Transaktionen rechtskräftig abgeschlossen werden müssen. Dazu müssen beide Parteien der Transaktion einen digitalen Vertrag unterschreiben. Das Unterschreiben solcher Verträge kann über digitale Signaturen vorgenommen werden, die einen Nutzer eindeutig identifizieren. Dies kann unter anderem der private Schlüssel eines Nutzers gewährleisten. Es ist jedoch von besonderer Bedeutung, dass dieser Schlüssel nicht öffentlich zugänglich ist, da Dritte sonst die Möglichkeit besitzen, Geschäfte unter falschem Namen abzuschließen. Abbildung 3 bietet abschließend einen Überblick, welche kryptografischen Verfahren welche Sicherheitsziele erfüllen und gewährleisten.[25]

23 Vgl. Hansen, Hans Robert; Mendling, Jan; Neumann, Gustaf: Wirtschaftsinformatik, a.a.O., S. 382 f. und vgl. Wendzel, Steffen: IT-Sicherheit für TCP/IP- und IoT-Netzwerke – Grundlagen, Konzepte, Protokolle, Härtung, a.a.O., S. 90.

24 Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg): Identitätsmanagement mit sicherer Authentifizierung und Attributweitergabe, Online im Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/14ter/Vortraege-20-05-2015/Moritz_Platt.pdf?__blob=publicationFile&v=1, 17.05.2020.

25 Vgl. Eckert, Claudia: IT-Sicherheit – Konzepte – Verfahren - Protokolle, 8. Auflage, München: Oldenbourg Verlag 2013, S. 12 f.

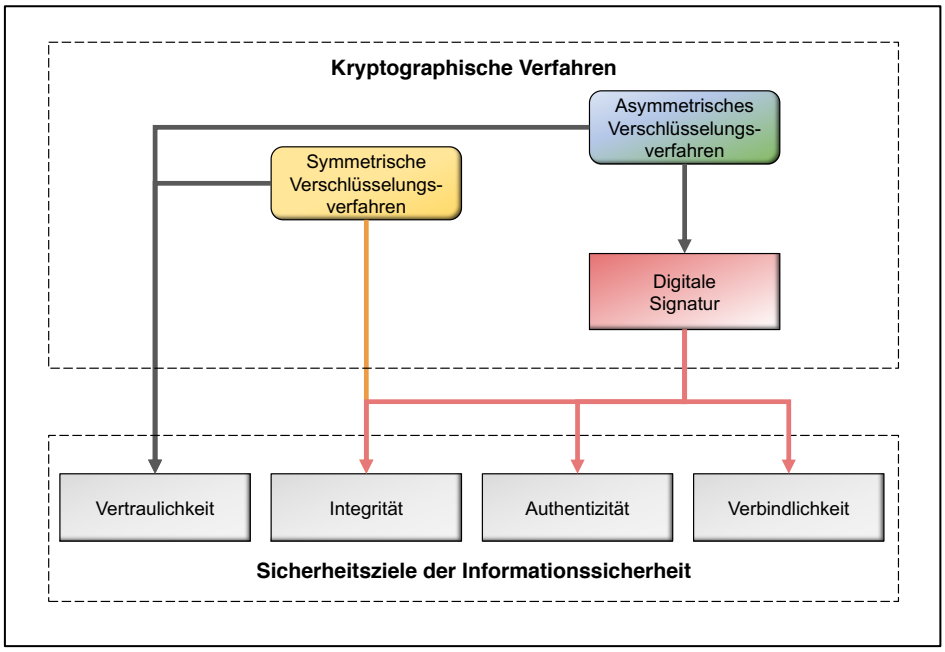

Abb. 3: Kryptographische Verfahren und IT-Sicherheitsziele

Die Gewährleistung der zuvor beschriebenen Sicherheitsziele lässt sich im Rahmen einer „Public Key Infrastruktur (PKI)“ erreichen. Die PKI ermöglicht die Verwaltung und Zuordnung asymmetrischer Schlüssel und stellt eine Art Regelwerk zur Verfügung. Darüber können digitale Signaturen in Form von Hash-Werten aus dem zu signierenden Inhalt ermittelt und Informationen mittels privater Schlüssel signiert werden. Auch Zertifikate können innerhalb einer PKI in Verbindung mit einer Zertifizierungsstelle ausgestellt werden, Personen identifizieren und diese einem System zuordnen. Von einer Zertifizierungsstelle ausgestellte Zertifikate, im X.509-Format[26], dienen der Zuordnung von einem Nutzer und dessen öffentlichen Schlüssel und digitaler Signaturen. Für beide Parteien einer Transaktion soll dadurch eine vertrauenswürdige Umgebung geschaffen werden, in der die Zertifizierungsstelle als vertrauenswürdige Instanz agiert. Dies kann bspw. für geschäftliche Transaktionen besonders wichtig sein.[27]

Vertraulichkeit, Integrität und Authentifizierung ermöglichen gemeinsam eine sichere Verbindung zwischen zwei Endpunkten, dem Server und dem Client. Dies ermöglicht, dass sich keine dritte Person zwischen beide stellen und deren Daten lesen oder manipulieren kann. Sogenannte „Man-in-the-Middle-Angriffe“ (MITM) werden verhindert.

26 Vgl. Russel, Aaron: What is an X.509 Certificate?, Online im Internet: https://www.ssl.com/faqs/what-is-an-x-509-certificate/, 23.09.2019.

27 Vgl. Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit – Grundlagen und Anwendung, 2. Überarbeitete Auflage, Wiesbaden: Vieweg + Teubner Springer Verlag 2011, S. 177 ff., vgl. Schmoranz, Paul; Schick, Lukas; Schwickert, Axel: Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete, a.a.O., S. 1 ff. und vgl. Schick, Lukas; Schwickert, Axel: macOS – Verschlüsseln, Entschlüsseln und Signieren von E-Mails, Gießen: Arbeitspapiere Wirtschaftsinformatik 4/2020, S. 4 f.

Diese sichere Verbindung wird auch als Transport Layer Security (TLS) bezeichnet. Der Client baut zunächst eine Verbindung zu einem Server auf, der sich gegenüber dem Client über ein Zertifikat authentisiert. Anschließend prüft der Client das Zertifikat und den Namen des Servers. Beide Parteien tauschen im Anschluss an die Authentifizierung ein Geheimnis aus, wovon ein Schlüssel zur Kommunikation abgeleitet wird.[28]

2.4 Entwicklung von FIDO1 zu FIDO2

Im Jahr 2014 veröffentlichte die FIDO-Allianz das Universal Authentication Framework (UAF). Wie im oberen Bereich von Abbildung 4 dargestellt, nutzt dieser Standard biometrische Authentifizierungsverfahren, um sich bspw. lokal an Smartphones oder Laptops anmelden zu können. In der Regel findet die Authentifizierung über Fingerabdrucksensoren oder Gesichtserkennung statt. Anschließend wurde dieser Standard als Alternative zur Authentifizierung neben dem Passwort in den Anmeldeprozess von Online-Diensten, bspw. dem E-Mail-Account, implementiert.

Dieser Standard wird als „Universal Second Factor (U2F)“ bezeichnet. Wie in Abbildung 4 mittig dargestellt, muss der Nutzer zusätzlich zum Passwort im Besitz eines weiteren Gegenstandes, wie z.B. eines FIDO-Geräts sein. Dazu kann alternativ auch ein wie oben beschriebenes biometrisches Verfahren zur Authentisierung genutzt werden. Im Rahmen der Nutzung des U2F muss der Nutzer dabei zunächst seinen Nutzernamen und das dazugehörige Passwort eingeben. Wurden diese auf ihre Zusammengehörigkeit überprüft, fordert der Online-Dienst dazu auf, das FIDO-Gerät anzuschließen, um somit die Anwesenheit des Nutzers zu bestätigen. Dieser Vorgang geschieht mit einem asymmetrischem Kryptographieverfahren. U2F nutzt also einen zweiten Faktor, nämlich für die Anwesenheitsprüfung, sodass U2F der Zwei-Faktor- Authentifizierung zugeordnet werden kann. Jedoch lässt sich grundsätzlich nicht jede Zwei-Faktor- Authentifizierung der FIDO-Technologie zuordnen. Die Anwesenheitsprüfung erfolgt häufig über das Auflegen eines Fingers auf den Sicherheitsschlüssel bzw. das Drücken eines Knopfes auf dem Sicherheitsschlüssel. Hierbei muss nicht zwangsläufig Biometrie genutzt werden. Das Drücken

28 Vgl. Kappes, Martin: Netzwerk- und Datensicherheit – Eine praktische Einführung, a.a.O., S. 276 ff., vgl. Heise (Hrsg.): The Transport Layer Security (TLS) Protocol Version 1.2, Online im Internet: https://www.heise.de/netze/rfc/rfcs/rfc5246.shtml, abgerufen am 30.05.2020 und vgl. Schmoranz, Paul; Schick, Lukas; Schwickert, Axel: Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete, a.a.O., S. 43 ff.

eines Knopfes ermöglicht jedoch im Gegensatz zur Biometrie keine an die Person gebundene Nutzung des Sicherheitsschlüssels, sodass dieser durch mehrere Personen zur Authentifizierung an einem System genutzt werden kann.[29]

Im Folgenden werden in Tabelle 1 die Vor- und Nachteile des U2F-Standards aufgezeigt.

FIDO Universal Second Factor	
Vorteile	**Nachteile**
+ U2F nutzt einen zweiten Faktor zur Authentifizierung, zusätzlich zum Passwort + Nächst sichere Alternative zur Authentifizierung mittels Passworts + U2F stellt eine sichere Alternative zu vergleichbaren Zwei-Faktor- Authentifizierungsverfahren (SMS, E-Mail oder App) dar + Nutzung eines passwortlosen bzw. biometrischen Faktors verhindert passwortspezifische Risiken wie Phishing-Attacken + Dritte müssen in Besitz des FIDO-Geräts sein + Einfache Anwendung des zweiten Faktors	– Passwort ist weiterhin Bestandteil des Authentifizierungsprozesses – Nutzer wähnen sich in Sicherheit durch zweiten „sicheren“ Faktor – Viele Nutzer empfinden zwei Faktoren als zu aufwendig, im Verhältnis zum Nutzen durch den Faktor – Zwei-Faktor- Authentifizierung im Allgemeinen konnte sich bisher in der Praxis kaum durchsetzen

Tabelle 1: Vor- und Nachteile von FIDO U2F

In vielen Fällen wurden auch Einmalkennwörter als zweiter Faktor eingesetzt. Diese können in den Ausprägungen „Time-based One-time Password Algorithmus“ (TOTP) und

29 Vgl. Mahn, Jan: Zweifach abgesichert – FIDO2-Hardware einrichten und ausreizen, in: c’t 25/2019, S. 75 f., vgl. FIDO-Allianz (Hrsg.): Universal Second Factor (U2F) Overview: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/FIDO-U2F-COMPLETE-v1.2-ps-20170411.pdf, 11.04.2017, vgl. De Orchi, Tommaso, Schmitz, Peter: FIDO2 bringt den passwortlosen Login, Online im Internet: https://www.security-insider.de/fido2-bringt-den-passwortfreien-login-a-753106/, 16.10.2018 und vgl. Wendzel, Steffen: IT-Sicherheit für TCP/IP- und IoT-Netzwerke, a.a.O., S. 197.

„Keyed-Hash Message Authentication Mode-based One-time Password Algorithmus" (HOTP) genutzt und in den Authentifizierungsvorgang eingebunden werden.[30] Über E-Mails, SMS oder auch per App können Einmalpasswörter an den Nutzer gesendet werden, dabei jedoch auch relativ leicht von Dritten abgefangen werden. Verwendet ein Nutzer bspw. ein Passwort für mehrere Online-Dienste, ist es für Dritte relativ einfach mit dem geklauten Passwort das Einmalpasswort abzufangen. Ähnliches zeigt ein Fall von Hackerangriffen auf den Mobilfunkanbieter AT&T.[31]

Der Standard FIDO2 wurde als Weiterentwicklung von FIDO U2F durch die FIDO-Allianz entwickelt und soll aktiv die vier Aspekte Sicherheit, Nutzbarkeit, Privatsphäre und Skalierbarkeit im Rahmen der Authentifizierung abdecken. Durch die Kooperation mit dem W3C lässt sich FIDO2 als ein offener Webstandard beschreiben, der potentiell von vielen Nutzern weltweit verwendet werden kann. Im engeren Sinne bauen FIDO2 und FIDO U2F auf demselben passwortlosen Fundament des UAF auf, nutzen die Technologie jedoch unterschiedlich.

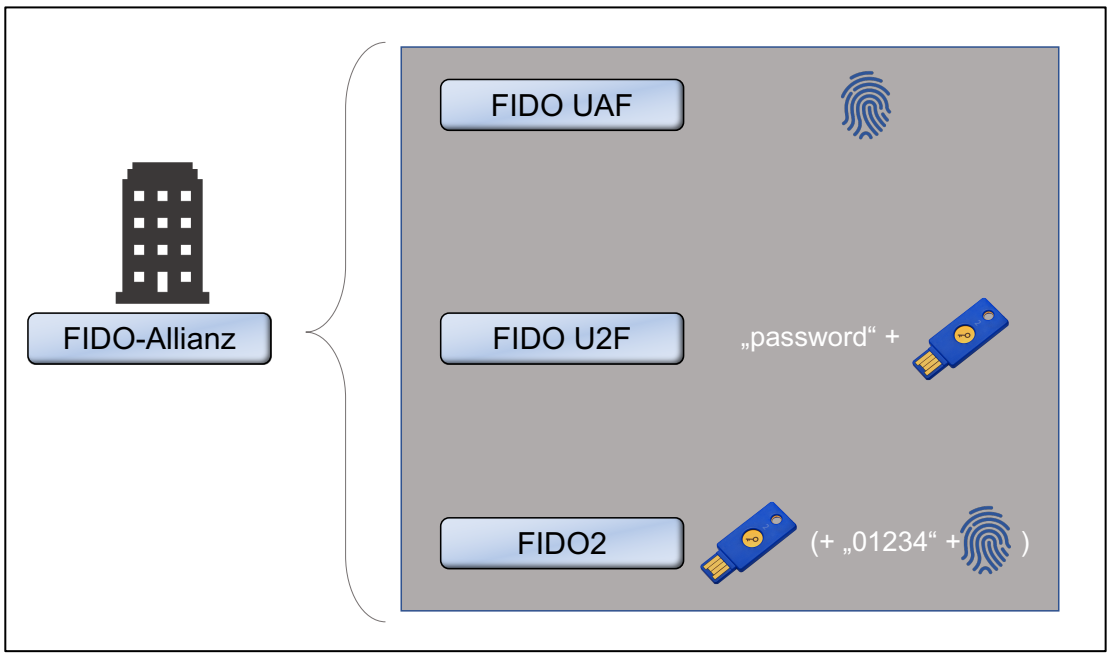

Abb. 4: Drei Standards der FIDO-Allianz

Der Vorteil der FIDO2-Technologie besteht dabei vor allem darin, dass es nicht notwendig ist ein Passwort eingeben zu müssen. Wie in Abbildung 4 unten dargestellt, findet der

30 Vgl. BSI (Hrsg.): Zwei-Faktor-Authentisierung für höhere Sicherheit, Online im Internet: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/Zwei_Faktor_Authentisierung/Zwei-Faktor-Authentisierung_node.html, abgerufen am 08.06.2020 und vgl.Luber, Stefan; Schmitz, Peter: Was ist TOTP?, Online im Internet: https://www.security-insider.de/was-ist-totp-a-875708/, 24.10.2019.

31 Vgl. Krebs on Security (Hrsg.): Hanging Up on Mobile in the Name of Security, Online im Internet: https://krebsonsecurity.com/2018/08/hanging-up-on-mobile-in-the-name-of-security/, 16.08.2018.

Zugang lediglich über den Nutzernamen und einen Sicherheitsschlüssel statt. Somit wurde lediglich eine Verschiebung vom zweiten Faktor, hin zum ersten bzw. einzigen Faktor vorgenommen. Dabei gelten dieselben Kriterien der Anwesenheitsprüfung wie schon beim U2F-Standard. Möchte ein Nutzer dennoch die Vorteile einer nutzergebundenen Authentifizierung erhalten ist es möglich, diese durch den Einsatz von numerischen PINs zu erweitern. Dies können unter anderem im Rahmen der Registrierung eingerichtet werden und als zusätzlicher Faktor in die Authentifizierung integriert werden. Grundsätzlich ist es dabei möglich alle Faktoren miteinander zu kombinieren. Wie in Abbildung 5 zu sehen ist, erhält der Nutzer die Möglichkeit Faktoren basierend auf Wissen, Besitz und Biometrie beliebig zu kombinieren. Dies lässt sich auch als Multi-Faktor-Authentifizierung bezeichnen. Im Gegensatz zur Zwei-Faktor-Authentifizierung ist es dabei unter anderem möglich mehr als zwei Faktoren zu kombinieren. In Abhängigkeit der Sensibilität der zu schützenden Daten können Multi-Faktor-Authentifizierungen genutzt werden und sich in Art und Anzahl der Faktoren unterscheiden. Welche Form der Authentifizierung gewählt wird, kann bspw. durch die System-Administration des Arbeitgebers oder eines Online-Dienstes vorgegeben werden.[32]

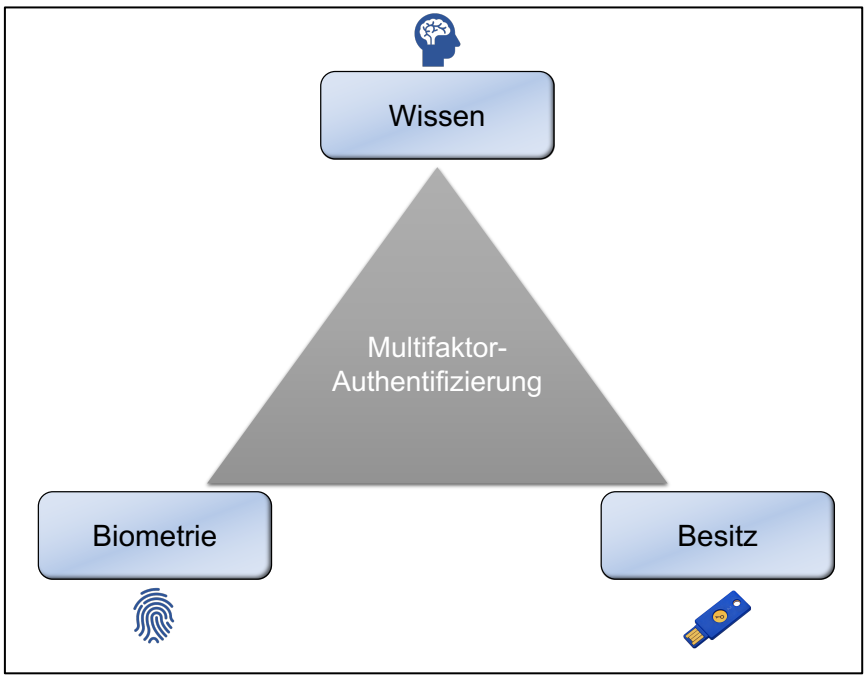

Abb. 5: Die Faktoren der Multifaktor-Authentifizierung

32 Vgl. Ionos (Hrsg.): FIDO2: Der neue Standard für den sicheren Web-Log-in, Online im Internet: https://www.ionos.de/digitalguide/server/sicherheit/was-ist-fido2/, abgerufen am 30.05.2020, vgl. Eikenberg, Ronald: Online-Schlüssel – FIDO2-Sicherheitsschlüssel zum Einloggen ohne Passwort, in: c't 25/2019, S. 67 f und vgl. Handelsblatt (Hrsg.): Wie die Multifaktor-Authentifizierung die Sicherheit erhöht, Online im Internet: https://unternehmen.handelsblatt.com/multifaktor-authentifizierung.html, 23.09.2019.

2.5 Die sechs Komponenten von FIDO2

Die FIDO2-Technologie lässt sich in die sechs Komponenten WebAuthn, Web Server, FIDO-Gerät, CTAP2, Browser/App und Nutzer unterteilen. Diese Komponenten, wie in Abbildung 6 dargestellt, ermöglichen im Zusammenspiel das Authentifizieren über passwortlose Verfahren an den Web Servern von Online-Diensten. Im Folgenden werden die einzelnen Komponenten vorgestellt und erläutert.

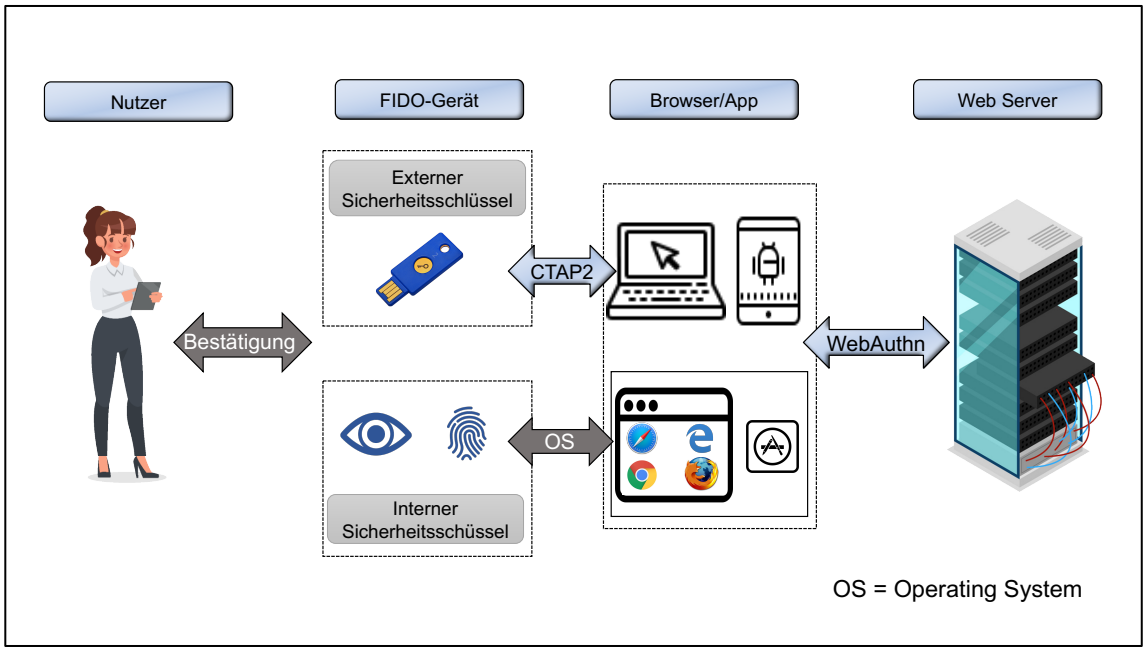

Abb. 6: Die sechs Komponenten von FIDO2

Kernkomponente von FIDO2 ist der W3C Standard WebAuthn, eine Standard-Web-Schnittstelle, in dem das kryptographische Verfahren zur Generierung von Schlüsselpaaren enthalten ist. Über diese JavaScript-Schnittstelle sind Online-Dienste in der Lage den Nutzern die FIDO2-Authentifizierung zu ermöglichen. WebAuthn muss dazu mit einer weiteren Komponente, dem Web Server eines Online-Dienstes, verbunden sein, damit sich Nutzer auf diesem authentifizieren können. Dafür muss WebAuthn zunächst auf dem entsprechenden Web Server installiert und implementiert werden. Registriert sich ein Nutzer an dem Web Server eines Online-Dienstes ist WebAuthn dafür zuständig ein Schlüsselpaar als Kombination aus der Produktionskennung des Sicherheitsschlüssels und der Domain des Online-Dienstes zu generieren. Die Kennung wurde im Rahmen der Produktion durch den Hersteller an den Sicherheitsschlüssel übergeben. Dabei wird für jeden Online-Dienst ein eigenes Schlüsselpaar generiert das ausschließlich zur Authentifizierung an diesem Web Server genutzt werden kann. Gleichzeitig wird eine dienstabhängige Applikationskennung in Form einer ID erzeugt, damit der Sicherheitsschlüssel

erkennen kann, an welchem Online-Dienst die Anmeldung stattfinden soll. Die generierten privaten und öffentlichen Schlüssel werden unterschiedlich verwendet. Während der öffentliche Schlüssel zur Registrierung an den Web Server übergeben wird, verbleibt der private Schlüssel beim Nutzer auf dem Sicherheitsschlüssel. Der private Schlüssel wird fortan lediglich zum Signieren von Serveranfragen im Rahmen von Authentifizierungsvorgängen verwendet, um den Nutzer eindeutig zu identifizieren. Die Signatur erfolgt nur dann, wenn der Nutzer durch eine Aktion sein Einverständnis dazu gibt. Der öffentliche Schlüssel dient dem Web Server zur Zuordnung des Nutzers und dessen Sicherheitsschlüssel. Dieser öffentliche Schlüssel lässt keine Rückschlüsse auf den privaten Schlüssel zu.[33]

Zur Authentifizierung am Web Server eines Online-Dienstes werden Webanwendungen oder auch Web Apps genutzt, welche auf einem Web Server abgelegt sind. In der Regel kann diese Anwendung gemäß der Client-Server-Architektur, durch die Nutzung eines Web Browsers verwendet werden. Web Browser und App als weitere Komponente der FIDO-Technologie, müssen ihrerseits ebenfalls eine Kompatibilität zu WebAuthn aufweisen, um den FIDO2-Standard anbieten zu können. Gängige Web Browser wie „Google Chrome“, „Firefox“, „Safari“ oder auch „Microsoft Edge“ erfüllen diese technischen Voraussetzungen. Über diese Web Browser sind Nutzer somit in der Lage sich über passwortlose Authentifizierungsverfahren an einem Web Server zu authentifizieren, sofern der Online-Dienst dies serverseitig bereitstellt.[34]

Zur Verwendung der Komponente des FIDO-Geräts, stehen Nutzerseitig zwei Optionen zur Verfügung. Dies sind zum einen externe und interne Sicherheitsschlüssel. Dazu wird in Form einer kryptographischen Entität der Nachweis der Nutzeranwesenheit erbracht. Das darin aufbewahrte Schlüsselpaar ist technisch nicht auslesbar und daher vor dem Zugriff Dritter geschützt. Im Rahmen einer vertrauenswürdigen Umgebung können beide Arten von Sicherheitsschlüsseln von einer offiziellen Zertifizierungsstelle zertifiziert werden.

Die Verwendung eines „externen Sicherheitsschlüssels“ ist eine Möglichkeit. Solche Sicherheitsschlüssel stellen die klassische Form der hardwarebasierten Authentifizierung

33 Vgl. W3C (Hrsg.) Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn-1/, 04.03.2019, vgl. WebAuthn Guide (Hrsg.): WebAuthn, Online im Internet: https://webauthn.guide, 12.06.2020, vgl. Steele, Nick: Developments to WebAuthn and the FIDO2 Framework, Online im Internet: https://duo.com/blog/developments-to-webauthn-and-the-fido2-framework, 02.10.2018, vgl. FIDO-Allianz (Hrsg.): FIDO UAF Achitectural Overview, Online im Internet: https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-uaf-overview-v1.1-ps-20170202.html#fido-uaf-client, 02.02. 2017 und vgl. Schmidt, Jürgen: Verschlossen, nicht verrammelt – So funktioniert der passwortlose Login mit FIDO2, in: c’t 18/2019, S. 30 ff.

34 Vgl. FIDO-Allianz (Hrsg.): FIDO2: Web Authentication (WebAuthn), Online im Internet: https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/, abgerufen am 01.05.2020.

über einen Sicherheitsschlüssel dar und können auch als „Token“ bezeichnet werden. Hardwarebasierte Token können bspw. physisch an einem Schlüsselbund mitgeführt werden. In diesen Sicherheitsschlüsseln wird der private Schlüssel zur Signatur von Serveranfragen in Form von Challenges abgelegt und aufbewahrt. So lange der Sicherheitsschlüssel beim Nutzer verbleibt, ist der Nutzer auch in der Lage sich an Web Servern zu authentifizieren. Zur Kommunikation mit dem Endgerät stehen dem Nutzer verschiedene externe Sicherheitsschlüssel zur Verfügung. Abbildung 7 zeigt, dass externe Sicherheitsschlüssel unterschiedliche Transportprotokolle wie Universal Serial Bus (USB), Near Field Communication (NFC) oder auch Bluetooth verwenden können.[35]

Speziell bei der Verwendung eines externen Sicherheitsschlüssels wird ein Protokoll benötigt, dass die Kommunikation zwischen dem Sicherheitsschlüssel und dem Browser oder der Web App ermöglicht. Das CTAP2 ist auf den Sicherheitsschlüsseln implementiert und ist für den Datenaustausch zuständig. Wird bspw. ein Authentifizierungsvorgang durch den Nutzer bestätigt, ist CTAP2 für die Aufnahme und Übermittlung der zu signierenden und signierten Challenge zuständig. Da CTAP2 eine Weiterentwicklung des Vorgängers CTAP1 ist, welcher Bestandteil von FIDO U2F ist, sind Besitzer eines FIDO2-Sicherheitsschlüssels in der Lage auch die FIDO U2F- Authentifizierung zu verwenden.[36]

Die zweite Möglichkeit zur Nutzung von FIDO2 sind „interne Sicherheitsschlüssel“. Interne Sicherheitsschlüssel sind solche Sicherheitsschlüssel, die in Form eines Trusted Platform Modules (TPM) einem sog. Sicherheitselement, fest auf der Hauptplatine eines Rechners oder eines Smartphones eingebaut werden. Diese sind auf der rechten Seite von Abbildung 7 zu erkennen. Dabei fungiert das TPM als eine Art Prozessor, der hardwarebasierte Sicherheitsfunktionen bereitstellt und eine biometrische Authentifizierung mittels Fingerabdrucks oder Gesichtserkennung lokal auf dem Endgerät ermöglicht. Im Gegensatz zu externen Sicherheitsschlüsseln erfolgt die Kommunikation nicht über das CTAP2, sondern über das Betriebssystem des Endgerätes. TPMs kommen aktuell bereits auf Rechnern mit dem Betriebssystem „Windows 10“ und neueren Android-Smartphones zum Einsatz.[37]

---

35 Vgl. Schmidt, Jürgen: Verschlossen, nicht verrammelt – So funktioniert der passwortlose Login mit FIDO2, in: c’t 18/2019, S. 32.

36 Vgl. FIDO-Allianz (Hrsg.): Client to Authenticator Protocol, Online im Internet: https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html#conformance, 30.01.2019.

37 Vgl. BSI (Hrsg.): Das Trusted Platform Module (TPM), Online im Internet: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/TrustedComputing/TrustedPlatformModuleTPM/TrustedPlatformModuleTPM/aufbaustruktur.html, abgerufen am 01.05.2020, vgl. Luber, Stefan; Schmitz, Peter: Was ist ein TPM?, Online im Internet: https://www.security-insider.de/was-ist-ein-tpm-a-811217/, 20.03.2019 und vgl. W3C (Hrsg.): Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn-1/, 04.03.2019.

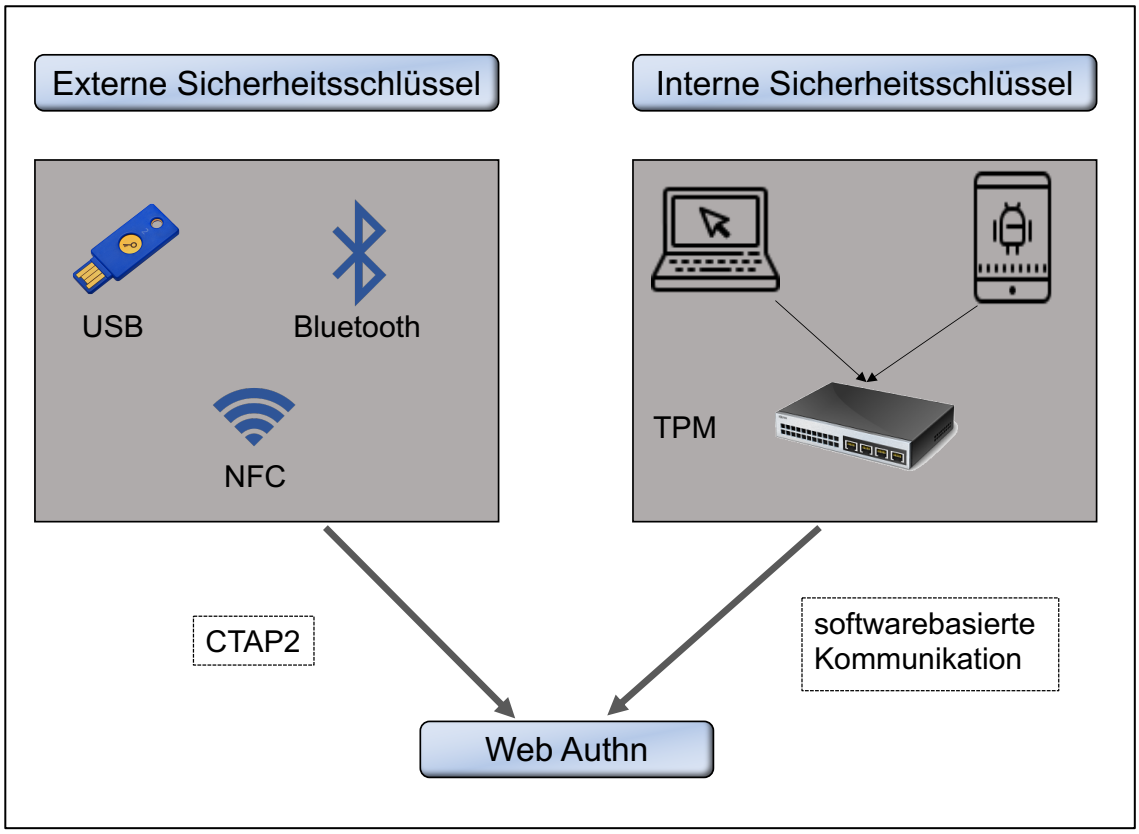

Abb. 7: Kommunikation externer und interner Sicherheitsschlüssel

Der Nutzer selbst stellt die letzte, aber nicht weniger wichtige Komponente im System von FIDO2 dar. Wie bereits erläutert muss der Nutzer selbst sein Einverständnis zur Übermittlung der Nutzerdaten und Anmeldung am Web Server geben. Die Bestätigung des Vorgangs kann der Nutzer über externe wie auch interne Sicherheitsschlüssel durch eine Nutzergeste bzw. eine Aktion tätigen. Dazu muss der Nutzer zunächst seinen Sicherheitsschlüssel mit dem Endgerät verbinden bzw. den internen Sicherheitsschlüssel aktivieren, wenn dies gefordert wird. Anschließend muss der Nutzer eine Geste wie bspw. das Auflegen eines Fingers auf den Sicherheitsschlüssel oder einen Sensor oder das Verwenden einer Kamera zur Gesichtserkennung vornehmen. Dies ist abhängig von der Beschaffenheit des Sicherheitsschlüssels. Stimmen diese Informationen mit den hinterlegten Daten überein, kann das System die Anwesenheit des Nutzers bzw. dessen Identität bestätigen. Die Daten werden über den Web Browser oder die Web App an den Web Server des Online-Dienstes weitergeleitet.[38]

38 Vgl. Windeck, Christoph: Sicherheitschips stärken oder ersetzen Passwörter, Online im Internet: https://www.heise.de/ct/artikel/Sicherheitschips-staerken-oder-ersetzen-Passwoerter-4637602.html, 27.01.2020, vgl. Schmidt, Jürgen: Verschlossen, nicht verrammelt – So funktioniert der passwortlose Login mit FIDO2, a.a.O., S. 32, und vgl. W3C (Hrsg.): Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn-1/, 04.03.2019, Abbildung in Anlehnung an Schmidt, Jürgen: Verschlossen, nicht verrammelt – So funktioniert der passwortlose Login mit FIDO2, in c't 18/2019, S. 32.

Der Registrierungs- und der Authentifizierungsvorgang vollziehen sich weitestgehend gleich. Im Folgenden wird aus Gründen der Einfachheit lediglich der Authentifizierungsprozess anhand von Abbildung 8 für den Nutzer dargestellt und beschrieben. Ausgangssituation ist gemäß dem Challenge Response Verfahren des Client/Server-Prinzips, dass ein Nutzer eine Anfrage zur Authentifizierung an den Web Server stellt.[39]

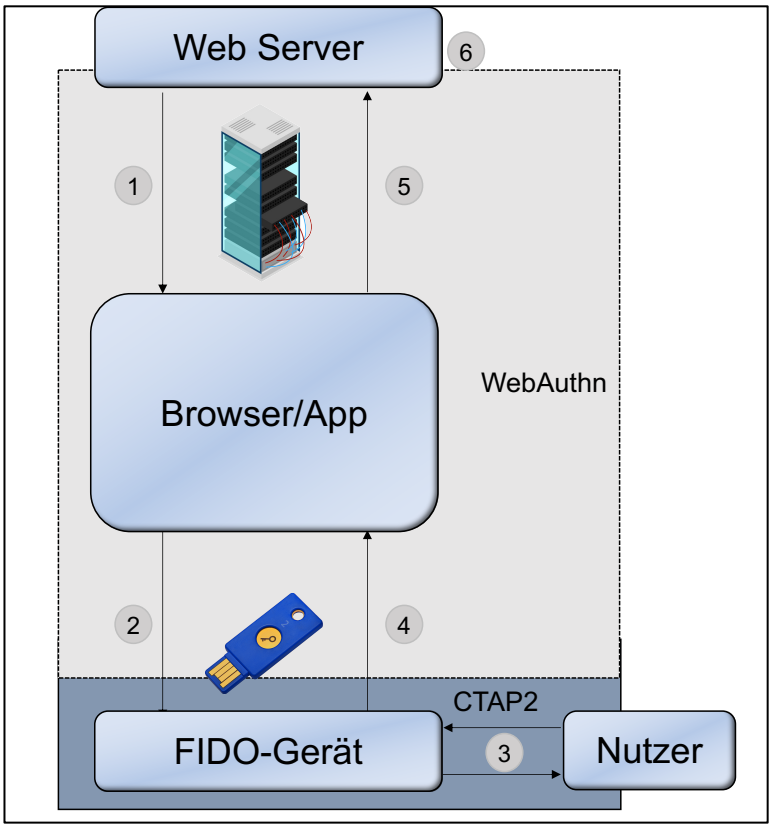

Abb. 8: Authentifizierungsprozess von FIDO2

1) Der Web Server versendet eine Challenge über die Schnittstelle WebAuthn an den Web Browser. Dabei kann es sich bspw. um das Signieren einer zufällig gewählten Zeichenfolge handeln. Ebenfalls wird die Applikationskennung des Online-Dienstes mit übertragen, die durch die Registrierung vergeben wurde und die dem Sicherheitsschlüssel gegenüber verifiziert, welcher Online-Dienst die Challenge sendet.

2) Über den Web Browser wird die Challenge von dem CTAP2 entgegengenommen, sofern der Nutzer einen externen Sicherheitsschlüssel verwendet, und an den Sicherheitsschlüssel weitergeleitet. Eine Verbindung über das „Hypertext Transfer

39 Vgl. Tsolkas, Alexander; Schmidt, Klaus: Rollen und Berechtigungskonzepte – Identity- und Access-Management im Unternehmen, 2. Auflage, Wiesbaden: Springer Verlag 2017, S. 136 f.

Protocol Secure“ (HTTPS) schafft zusätzlich eine sichere Umgebung für die Nutzung von Webanwendungen.

3) Hat der Sicherheitsschlüssel die Anfrage erhalten, ist eine Bestätigung seitens des Nutzers notwendig. Dazu muss der Nutzer aktiv werden. Dies kann bspw. durch das „Antippen“ des Sicherheitsschlüssels, das Drücken eines Knopfes auf dem Sicherheitsschlüssel oder auch mithilfe von biometrischen Verfahren am Endgerät selber erfolgen. Bestätigt der Nutzer den Vorgang, wird die Challenge des Online-Dienstes mit Hilfe des privaten Schlüssels signiert und die Aufgabenstellung gelöst. CTAP2 stößt anschließend den Prozess an, der die beantwortete Challenge an den Web Server sendet. Wird keine Nutzeraktion getätigt oder die Aktion schlägt fehl, sendet der Sicherheitsschlüssel einen Fehler aus.
4) CTAP2 übermittelt die signierte Challenge mitsamt dem öffentlichen Schlüssel an den Web Browser.
5) Der Web Browser übergibt dem Web Server per WebAuthn den öffentlichen Schlüssel zur Identifikation des Nutzers. Gleichzeitig erfolgt die Übermittlung der beantworteten Challenge zur Prüfung durch den Web Server.
6) Der Web Server greift auf die in seiner Datenbank hinterlegten Nutzerdaten zurück und prüft den übermittelten öffentlichen Schlüssel und die Beantwortung der Challenge. Die Signatur des privaten Schlüssels in der Challenge verifiziert dem Web Server schlussendlich die Identität des Nutzers. Kann der Web Server eine Übereinstimmung von Nutzer und öffentlichem Schlüssel erkennen und den privaten Schlüssel anhand der Signatur zuordnen, wird der Nutzer authentifiziert. Der Nutzer kann somit auf sein Konto zugreifen und bspw. eine Transaktion tätigen.[40]

40 Vgl. W3C: Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn/#api, 04.03.2019, Abbildung in Anlehnung an: W3C: Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn/#api.

3 Prinzipien von FIDO2

3.1 Systematisierung der Prinzipien von FIDO2

Die FIDO-Allianz und das W3C haben sich zum Ziel gesetzt, das Internet langfristig unabhängig von klassischen Passwörtern zu machen. Aus dieser Zusammenarbeit resultiert der neue Internet-Standard „FIDO2“. Dieser Standard soll einen Gegenentwurf zur Authentifizierung mittels Passworts darstellen und vier Problembereiche behandeln, denen die Nutzer von Passwörtern klassischerweise gegenüberstehen. Nachfolgend werden diese vier Problembereiche aufgeführt und kurz erläutert.

Kapitel 3.2: Sicherheit

FIDO2 nutzt Schlüsselpaare, als Kombination aus der Schlüsselkennung des Sicherheitsschlüssels und der Domain des Online-Dienstes. Diese Schlüsselpaare sollen das Rückverfolgen von Nutzeraktivitäten im Internet verhindern. Das dahinterstehende asymmetrische Verschlüsselungsverfahren bietet zusätzlich einen sicheren Kommunikationskanal. In diesem Kommunikationskanal können Daten dann sicher an den Web Server übermittelt werden. Somit lassen sich insbesondere Gefahren durch Phishing-, MITM und Brute Force-Attacken reduzieren.

Kapitel 3.3: Nutzbarkeit

Die Nutzbarkeit drückt sich vor allem darin aus, dass FIDO2 sehr einfach und bequem anwendbar ist. Das passwortlose Authentifizierungsverfahren lässt sich über jedes gängige Endgerät in Verbindung mit einem gängigen Web Browser anwenden. Der Nutzer muss lediglich einen externen Sicherheitsschlüssel erwerben. Zudem bedarf es nur weniger Schritte, um sich mittels FIDO2 an einem Nutzerkonto anzumelden.

Kapitel 3.4: Privatsphäre

Der Problembereich der Privatsphäre geht eng mit dem Prinzip der Sicherheit einher. Hierbei liegt der Schwerpunkt besonders darauf, dass Dritte nicht nachvollziehen können, wo Nutzer weitere Nutzerkonten besitzen. Sicherheitsschlüssel lassen sich höchstens ihrem Hersteller zuordnen, erlauben jedoch keinen Rückschluss auf den Nutzer und dessen Aktivitäten im Internet.

Kapitel 3.5: Skalierbarkeit

Die Skalierbarkeit steht in besonderer Verbindung zur Nutzbarkeit. FIDO2 bietet dem Nutzer nicht nur ein besonders sicheres und komfortables Authentifizierungsverfahren. Zusätzlich ermöglicht FIDO2 dem Nutzer die passwortlose Authentifizierung an sämtli-

chen digitalen Endgeräten anzuwenden. Die einzige Bedingung dafür ist, dass Komponenten wie das Betriebssystem, der Web Browser oder der Web Server kompatibel mit FIDO2 sind.

3.2 Sicherheit

"FIDO2 cryptographic login credentials are unique across every website, never leave the user's device and are never stored on a server."[41]

Das Sicherheitsmanagement von IT-Systemen findet im Rahmen der IT-Sicherheitsziele statt, die bereits in Kapitel 2 erläutert wurden. Dabei sollen einerseits Sicherheitsanforderungen definiert und umgesetzt und andererseits Sicherheitslücken geschlossen werden. Sicherheitsmaßnahmen sollen dabei hinreichend hoch sein, um die Wahrscheinlichkeit von Angriffen so niedrig wie möglich zu halten.[42]

Wie im obigen Zitat der FIDO-Allianz aufgeführt, werden für jede Web Site einzigartige und zufällige Schlüsselpaare generiert. Der private Schlüssel, der genutzt wird, um Nachrichten zu signieren, verbleibt dauerhaft auf dem Sicherheitsschlüssel. Sowohl von Seiten des Clients als auch des Web Servers sind diese Daten nicht zugänglich oder auslesbar. So lässt sich verhindern, dass Dritte Zugang zu Informationen der Online-Aktivitäten der Nutzer erhalten.

Der öffentliche Schlüssel wird bei der Registrierung an den Web Server übergeben. Jedoch handelt es sich bei dem öffentlichen Schlüssel ebenfalls um eine zufällige Zeichenkette. Diese lässt wiederum keine Rückschlüsse auf den privaten Schlüssel zu. Dabei dient der öffentliche Schlüssel nicht nur der Anmeldung am Nutzerkonto, sondern auch zur Kommunikation. Gemäß der Schlüsselaustauschproblematik errichtet der öffentliche Schlüssel der asymmetrischen Verschlüsselung einen sicheren Kommunikationskanal. Dieser Kommunikationskanal dient der sicheren Übertragung von Daten innerhalb eines Kommunikationsnetzwerks. Dadurch werden die Sicherheitsziele Datenintegrität, Vertraulichkeit und Authentizität erfüllt.

Asymmetrische Schlüsselpaare können somit besonders effektiv gegenüber MITM-Angriffen eingesetzt werden. Dies bestätigen auch Pereira/Rochet/Wiedling [43] in einer Analyse des FIDO-Protokolls. Sie kommen zu dem Schluss, dass MITM-Angriffe sowohl bei

41 FIDO-Allianz (Hrsg.): FIDO2: WebAuthn & CTAP, Online im Internet: https://fidoalliance.org/fido2/, abgerufen am 13.06.2020.

42 Vgl. Sackmann, Stefan: IT-Sicherheit, 2020, Online im Internet: https://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/technologien-methoden/Informatik--Grundlagen/IT-Sicherheit/index.html/?searchterm=sicherheit, abgerufen am 16.07.2020.

43 Vgl. Pereira, Olivier; Rochet, Florentin; Wiedling, Cyrille: Formal Analysis of the FIDO 1.x Protocol, Online im Internet: https://fps2017.loria.fr/wp-content/uploads/2017/10/04.pdf, abgerufen am 14.06.2020.

einem korrupten Web Server als auch einem korrupten Client nicht möglich sind. Eine Bedingung ist jedoch, dass individuelle Schlüsselpaare für jeden Online-Dienst generiert werden. Abbildung 9 verdeutlicht dazu das Prinzip zum Schutz vor MITM-Angriffen. Zunächst bewirkt das Verwenden asymmetrischer Schlüsselpaare, dass zwei Kommunikationspartner sicher miteinander kommunizieren können. Dritte haben somit keine Möglichkeit, sich zwischen die Kommunikationspartner zu stellen und deren Daten abzufangen. Auf der anderen Seite sorgen dienstspezifische Schlüsselpaare dafür, dass Dritte keine Rückschlüsse auf den Nutzer und dessen Anmeldedaten ziehen können. Selbst wenn Dritte also in der Lage wären, einen sicheren Kommunikationskanal zu unterwandern, könnten sie die Anmeldedaten nicht für ihre Zwecke verwenden.[44]

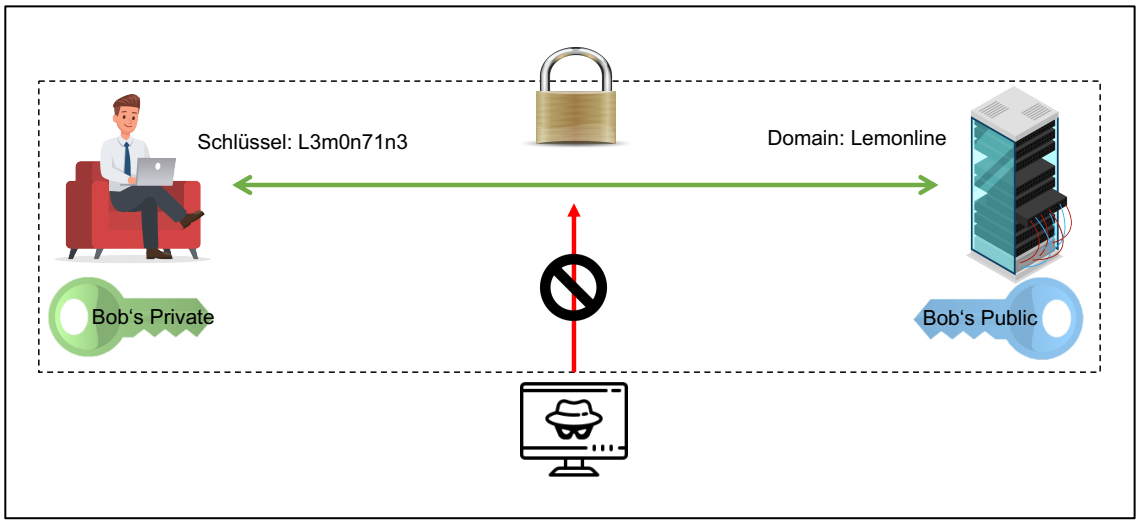

Abb. 9: FIDO2 vs. MITM-Angriffe

Die Signatur mittels privater Schlüssel, wie in Abbildung 10 dargestellt, erfüllt darüber hinaus das Ziel der Verbindlichkeit. Verbindlichkeit kann bspw. im Falle von geschäftlichen Transaktionen eine wichtige Rolle einnehmen. Beispielsweise kann einem Käufer eindeutig die Verpflichtung der Zahlung und dem Verkäufer die Verpflichtung der Nutzungsüberlassung zugeordnet werden.

Damit eine Transaktion abgeschlossen werden kann, benötigt der Web Server eine Bestätigung durch den Nutzer. Wie bereits erläutert, erfolgt die Bestätigung bei FIDO2 in Form einer Nutzergeste. Beispielsweise das Auflegen des Fingers auf den Sicherheitsschlüssel. Der zum Signieren benötigte private Schlüssel wird also nur dann verwendet, wenn der Nutzer die Erlaubnis erteilt. Somit ist nur der Nutzer, der den Sicherheitsschlüssel auch physisch besitzt und die Nutzergeste ausführen kann, in der Lage, eine Transaktion zu tätigen. Es ist also von besonderer Bedeutung, dass der Sicherheitsschlüssel immer

44 Vgl. W3C (Hrsg.): Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn-1/, 04.03.2019.

beim Nutzer verbleibt. Durch den Einsatz biometrischer Verfahren kann zusätzliche Sicherheit hergestellt werden. Biometrische Verfahren verwenden nutzerspezifische Eigenschaften, z. B. ein Fingerabdruck oder ein Gesicht. Diese Faktoren sind fest mit dem Nutzer verbunden. Ziel dabei ist es, unterschiedliche Benutzer, entsprechend ihrer zugewiesenen Rollen, identifizieren zu können und den Schlüssel fest an eine Person zu koppeln.[45]

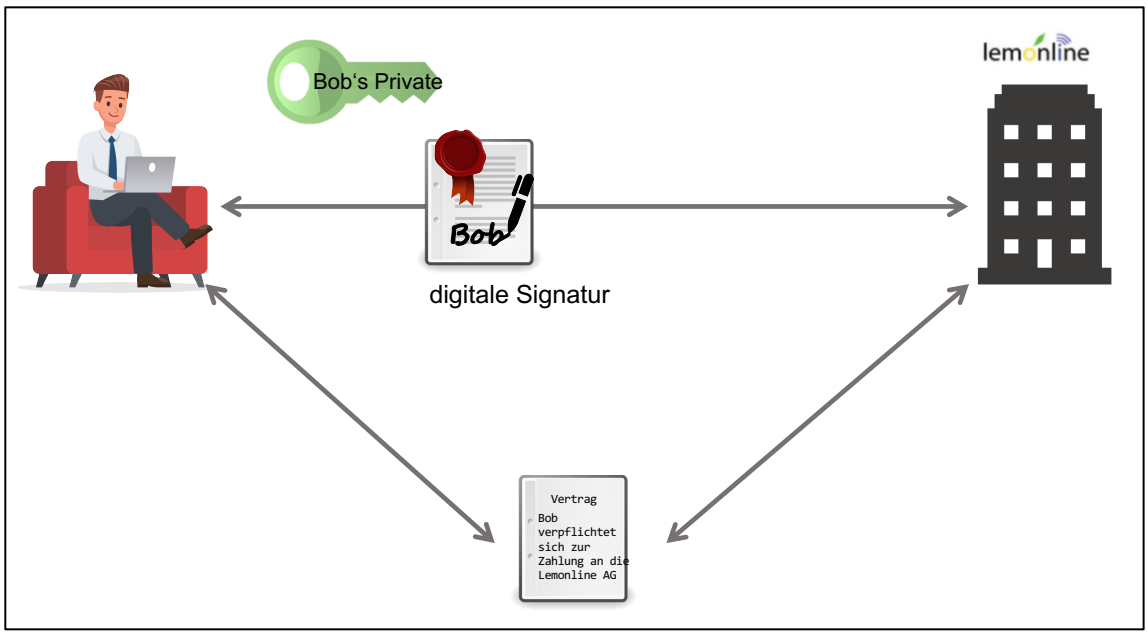

Abb. 10: FIDO2 ermöglicht Verbindlichkeit

"(…) This security model eliminates the risks of phishing, all forms of password theft and replay attacks."[46]

Dieses Zitat sagt aus, dass über FIDO2 das Risiko eliminiert wird, Opfer von passwortbasierten Angriffen zu werden. Für kriminelle Dritte soll es durch FIDO2 grundsätzlich unrentabel werden, die Anmeldedaten von Nutzern stehlen zu wollen. Dies unabhängig davon, ob Dritte die Schwachstelle beim Nutzer selbst oder beim Web Server suchen.[47]

Besonders effektiv kann FIDO2 zum Schutz vor Phishing-Attacken genutzt werden, da keine Passwörter zur Authentifizierung benötigt werden. Wie im linken Bereich von Abbildung 11 dargestellt, stellt das Passwort nicht mehr die notwendige Information dar, um

45 Vgl. W3C (Hrsg.): Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn-1/, 04.03.2019.

46 FIDO-Allianz (Hrsg.): FIDO2: WebAuthn & CTAP, Online im Internet: https://fidoalliance. org/fido2/, abgerufen am 13.06.2020.

47 Vgl. Schimdt, Jürgen: Verschlossen, nicht verrammelt – So funktioniert der passwortlose Login mit FIDO2, a.a.O., S. 31 und vgl. W3C (Hrsg.): Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn-1/, 04.03.2019.

Zugriff auf die Nutzerdaten zu erhalten. Einerseits ist ein Nutzer nur mithilfe des Sicherheitsschlüssels in der Lage, den Authentifizierungsvorgang zu bestätigen. Dafür wird dessen physische Anwesenheit am Sicherheitsschlüssel vorausgesetzt. Dritte müssten somit mindestens im Besitz des jeweiligen Sicherheitsschlüssels sein. Unter Umständen benötigen Dritte sogar die biometrischen Daten des Nutzers. Andererseits gilt ein Schlüssel immer nur für einen Online-Dienst und einen Web Server. Die Anmeldung an einem „gefälschten“ Server ist somit nicht möglich, wenn die registrierten Nutzerdaten eingegeben werden.[48]

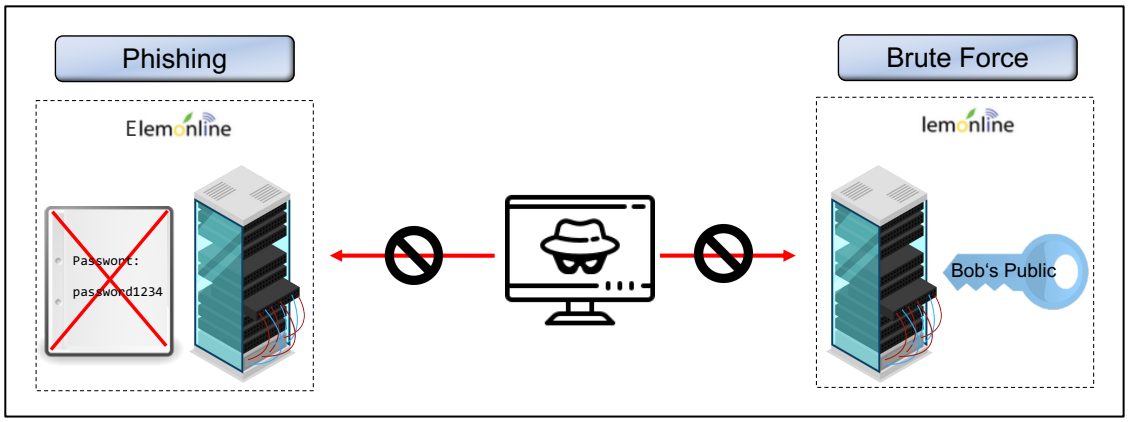

Abb. 11: FIDO2 vs. Phishing- und Brute Force-Attacken

Auch „Brute Force-Attacken“ können durch FIDO2 verhindert werden. Dies sind Angriffe, bei denen sich Dritte durch „einfaches Ausprobieren“ Zugang zu einem Nutzerkonto verschaffen wollen. Wie in Kapitel 1 erläutert, verwenden viele Nutzer vergleichsweise einfache oder leicht abgewandelte Passwörter für mehrere Nutzerkonten. Dabei kann es sehr einfach sein, über Ausprobieren bestimmter gängiger Passwörter, ein Nutzerkonto zu kompromittieren. Dem W3C zufolge soll dies bei FIDO2 über eine „Drosselung“, die in den Sicherheitsschlüsseln implementiert ist, verhindert werden. Wird eine bestimmte Anzahl an fehlgeschlagenen Anmeldevorgängen erreicht, wird der Schlüssel für eine bestimmte Zeit deaktiviert. Mit jedem weiteren Versuch steigt dieser Zeitraum exponentiell an oder kann, wie bei einer Kontokarte, ganz gesperrt werden. Auch der Einsatz eines zusätzlichen Authentifizierungsfaktors kann Nutzer effektiv vor Brute Force-Attacken schützen.[49]

Auch das asymmetrische Schlüsselpaar von FIDO2 bietet einen hinreichenden Schutz vor Brute Force-Attacken. Der rechte Bereich von Abbildung 11 zeigt auf, dass lediglich die

48 Vgl. Schimdt, Jürgen: Verschlossen, nicht verrammelt – So funktioniert der passwortlose Login mit FIDO2, a.a.O., S. 31 und vgl. W3C (Hrsg.): Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn-1/, 04.03.2019.

49 Vgl. W3C (Hrsg.): Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn-1/, 04.03.2019.

öffentlichen Schlüssel auf den Servern der Online-Dienste abgelegt werden. Wie bereits erläutert, lassen sich dadurch keine Rückschlüsse auf die relevanten Anmeldedaten ziehen. Zusätzlich ist der private Schlüssel auf dem Sicherheitsschlüssel abgelegt. Nutzer sind somit effektiv gegen Angriffe von außen geschützt.[50]

3.3 Nutzbarkeit

"Users unlock cryptographic login credentials with simple built-in methods such as fingerprint readers or cameras on their devices, or by leveraging easy-to-use FIDO security keys. Consumers can select the device that best fits their needs."[51]

Der Begriff der Nutzbarkeit beschreibt, wie intuitiv sich ein IT-System durch den Nutzer anwenden lässt. Dabei spielt es eine besonders wichtige Rolle, inwiefern auch Laien in der Lage sein können, das IT-System zu nutzen. Nutzbarkeit kann sich jedoch auch auf die Anforderung beziehen, dass ein System für den Nutzer immer erreichbar und somit „nutzbar" sein soll.

Die FIDO-Allianz betont mit der Aussage auf ihrer Web Site die besondere Nutzbarkeit, die hinter dem Konzept von FIDO2 steckt. Eine besondere Rolle spielt dabei die Wahl des Sicherheitsschlüssels, des Betriebssystems des Computers und des Web Browsers. Es gibt eine Reihe von Unternehmen, die mehrere Sicherheitsschlüssel mit unterschiedlichen Eigenschaften und Funktionen anbieten. Prominente Anbieter von Sicherheitsschlüsseln sind bspw. SoloKey, Yubico oder Feitan. In der Regel können Sicherheitsschlüssel erworben werden, die über USB, NFC oder Bluetooth am Computer angeschlossen werden. Diese sind in den meisten Fällen mit einer Druckfläche oder einem Knopf ausgestattet, die der Nutzer berühren bzw. drücken muss, um den Authentifizierungsvorgang zu bestätigen. Möchte der Nutzer etwas mehr Komfort und Sicherheit erfahren, bieten sich diesem in höherpreisigen Segmenten auch Sicherheitsschlüssel mit Fingerabdrucksensoren.[52]

Besitzt der Nutzer einen Computer mit dem Betriebssystem Windows 10 oder ein neueres Android Smartphone, kann dieser sein Endgerät als internen Sicherheitsschlüssel verwenden. Eine technische Voraussetzung ist jedoch, dass das Betriebssystem in einer entsprechenden Version zur Verfügung steht. Bei Windows 10 ist es die Version 1903. Android ist erst ab Version 7 in der Lage, mit Sicherheitsschlüsseln zu kommunizieren. Hierbei

50 Vgl. W3C (Hrsg.): Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn-1/, 04.03.2019.

51 FIDO-Allianz (Hrsg.): FIDO2: WebAuthn & CTAP, Online im Internet: https://fidoalliance.org/fido2/, abgerufen am 26.05.2020.

52 Vgl. Eikenberg, Ronald: Onlineschlüssel – FIDO2-Sicherheitsschlüssel zum Einloggen mit und ohne Passwort, in c't 25/2019, S. 68 ff.

erfolgt die Bestätigung eines Authentifizierungsvorgangs i. d. R. anhand der Eingabe einer PIN oder über lokale biometrische Verfahren am Endgerät selbst. Im Gegensatz zur klassischen Authentifizierung mittels Passworts wird dabei deutlich, dass Sicherheit und Nutzbarkeit durchaus miteinander einhergehen können. Einerseits sind biometrische Verfahren nutzerseitig leicht einzurichten und zu bedienen. Auch der Erwerb weiterer Hardware ist in diesem Falle nicht mehr nötig. Andererseits ermöglichen biometrische Faktoren, anders als Passwörter, dass ein Endgerät und die dahinterstehende Authentifizierung fest an eine Person gebunden werden. Auch wenn der Laptop oder das Smartphone gestohlen würden, wären kriminelle Dritte dadurch nicht in der Lage, den Sicherheitsschlüssel zu betätigen. Dritten würden die biometrischen Eigenschaften der Nutzer fehlen.[53]

Ein zusätzlicher Aspekt der Nutzbarkeit ist die Wahl des Web Browsers. Dies ist zwar nicht explizit auf der Web Site der FIDO-Allianz erwähnt, leistet jedoch ebenfalls einen wichtigen Beitrag. Der Nutzer hat die Möglichkeit, gängige Web Browser wie Mozilla Firefox, Google Chrome, Microsoft Edge oder Apple Safari zu nutzen, die mit einem Sicherheitsschlüssel kommunizieren können. In diesen Web Browsern wurde die JavaScript-Schnittstelle WebAuthn implementiert, sodass diese den Dienst von FIDO2 nutzen können. Dem Nutzer bietet sich somit in Verbindung mit diversen Sicherheitsschlüsseln eine breite Masse an Konnektivitätsmöglichkeiten. Daraus resultiert, dass ein Nutzer selbstständig und mit geringem technischem Aufwand ein Nutzerkonto FIDO2-tauglich machen kann. Es muss lediglich berücksichtigt werden, dass der Online-Dienst FIDO2 auch anbietet und der Web Browser kompatibel ist.[54]

Jedoch lässt sich das Konzept FIDO2 nicht nur auf seine einzelnen Komponenten reduzieren. So dient das technische Konstrukt als Ganzes der Nutzbarkeit. Das System ist in diesem Falle mehr als nur die Summe seiner Teile. Hat sich der Nutzer für einen Sicherheitsschlüssel entschieden, gilt es, diesen zu registrieren. Alle folgenden Anmeldevorgänge erfordern dann nur noch eine Verbindung zu diesem Sicherheitsschlüssel und das Ausführen einer Nutzeraktion. Im Gegensatz zur klassischen Authentifizierung ist dieser Prozess mit weniger Aufwand für den Nutzer verbunden, da das Passwortmanagement komplett entfällt. Ein beispielhafter Authentifizierungsprozess wird dazu in Kapitel 4.5 beschrieben. Abbildung 12 bietet abschließend eine Übersicht der zuvor erläuterten vier Aspekte der Nutzbarkeit von FIDO2.

53 Vgl. Eikenberg, Ronald: Schlüssel zum Glück – Was schon heute mit dem Passwort-Killer FIDO2 geht, a.a.O., S. 21.

54 Vgl. Schwan, Ben: iOS 13.3: Safari unterstützt diverse Sicherheitskeys, Online im Internet: https://www.heise.de/mac-and-i/meldung/iOS-13-3-Safari-unterstuetzt-diverse-Sicherheitskeys-4584820.html, 13.11.2019.

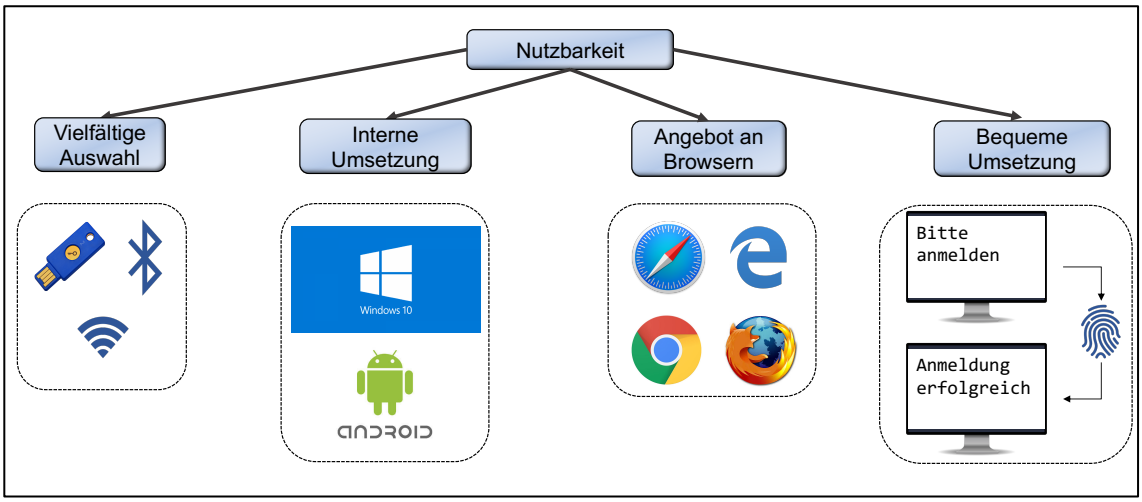

Abb. 12: Vier Aspekte der Nutzbarkeit

3.4 Privatsphäre

„Because FIDO cryptographic keys are unique for each internet site, they cannot be used to track users across sites. Plus, biometric data, when used, never leaves the user's device.“[55]

Der Aspekt der Privatsphäre, wird wie der Aspekt der Sicherheit, maßgeblich durch das Public-Key-Verfahren beeinflusst. Wie in Abbildung 13 dargestellt, ist das Schlüsselpaar sowohl für den Betreiber des Web Servers als auch für Dritte nicht auslesbar. Aufgrund der zufällig kombinierten Zeichenkette lässt das Schlüsselpaar keine Rückschlüsse auf den Nutzer und dessen Aktivitäten zu. Im Falle eines Verlustes ist es nicht möglich, herauszufinden, wem das FIDO-Gerät gehört und welche Aktivitäten damit vorgenommen wurden. Allerdings können Sicherheitsschlüssel anhand ihrer Produktionschargenkennung einem Hersteller zugeordnet werden. Dies ist besonders dann kritisch, wenn nur eine geringe Anzahl an Geräten einer Produktionsserie in Umlauf gebracht wurde. So verlangen die UAF-Spezifikationen bspw., dass Sicherheitsschlüssel einer Charge mit derselben Kennung zu mindestens 100.000 Stück produziert und versendet werden. So kann verhindert werden, Rückschlüsse auf die Käufer zu ermöglichen.

Zusätzlich ist es nicht möglich, unterschiedliche Nutzer gleichzeitig, über denselben Sicherheitsschlüssel, am selben Online-Dienst anzumelden. Dies resultiert besonders aus der Tatsache, dass keine Rückschlüsse auf Anmelde-Aktivitäten im Internet möglich sein sollen. Es wird somit verhindert, dass ein Web Server die verschiedenen Nutzer einem Sicherheitsschlüssel zuordnen kann. Gleichzeitig ist es ebenfalls nicht möglich, dass sich

55 FIDO-Allianz (Hrsg.): FIDO2: Web Authn & CTAP, Online im Internet: https://fidoalliance.org/fido2/, abgerufen am 26.05.2020.

ein Nutzer gleichzeitig an mehreren Online-Diensten anmelden kann. Dies wird insbesondere durch die Nutzung dienstspezifischer Schlüsselpaare realisiert.[56]

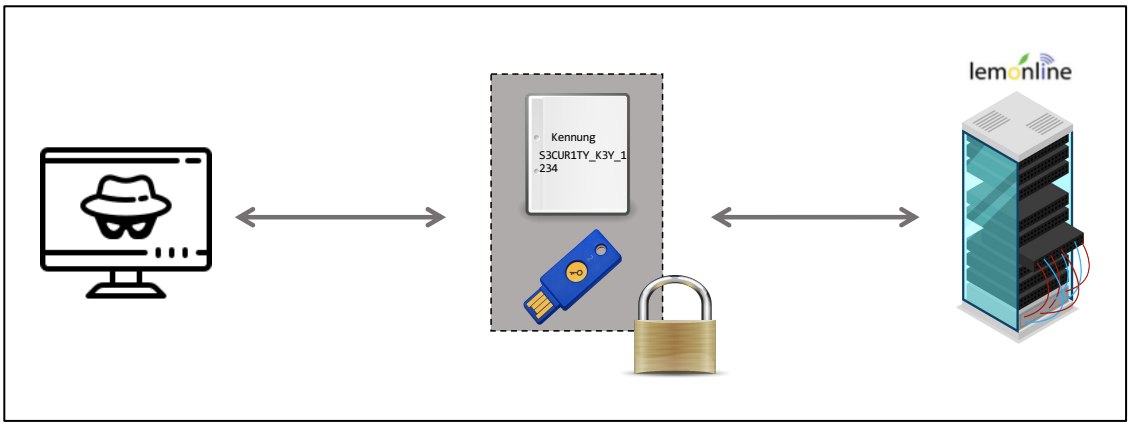

Abb. 13: FIDO2 und der Schutz der Privatsphäre

Für den Nutzer bietet sich weiterhin der Vorteil, dass keine sensiblen, personenbezogenen Daten erhoben werden müssen, um FIDO2 nutzen zu können. Wie in Abbildung 14 dargestellt, werden lediglich ein Nutzername, der ein willkürliches Pseudonym darstellen kann, und der öffentliche Schlüssel im Rahmen der Registrierung an den Web Server übermittelt. Der öffentliche Schlüssel wird nur benötigt, um einem Nutzer das Schlüsselpaar zuordnen zu können, wenn sich ein Nutzer anmelden möchte. Für Unternehmen, sowohl auf Client- als auch auf Server-Seite, kann die Nutzung von FIDO2 eine Hilfestellung sein, die Verordnungen der Datenschutzgrundverordnung (DSGVO) einzuhalten. FIDO2 kann also dabei unterstützen, schwerwiegende Datenlecks zu verhindern. Für Unternehmen wird somit einerseits das Risiko minimiert, dass Reputationsschäden durch Datendiebstahl entstehen. Andererseits werden auch hohe Kosten durch Rechtsstreitigkeiten oder nachträgliches Aufrüsten der IT-Sicherheitsmaßnahmen verhindert.

Verwendet ein Nutzer einen internen Sicherheitsschlüssel oder einen externen Sicherheitsschlüssel mit Fingerabdruck, werden dessen biometrische Daten ebenfalls nicht an den Online-Dienst weitergegeben oder auf dessen Servern abgelegt. Die Aufgabe der biometrischen Authentifizierung liegt allein in der lokalen Bestätigung an dem Sicherheitsschlüssel. Dieser Bestätigungsvorgang bildet in diesem Sinne ein Kernstück der Privatsphäre, da nur mit der physischen Bestätigung des Nutzers der Authentifizierungsvorgang vorgenommen und vollzogen werden kann.[57]

56 Vgl. FIDO-Allianz (Hrsg.): FIDO UAF Architectural Overview, Online im Internet: https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-uaf-overview-v1.1-ps-20170202.html#fido-uaf-client, 02.02.2017.

57 Vgl. W3C (Hrsg.): Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn-1/, 04.03.2019.

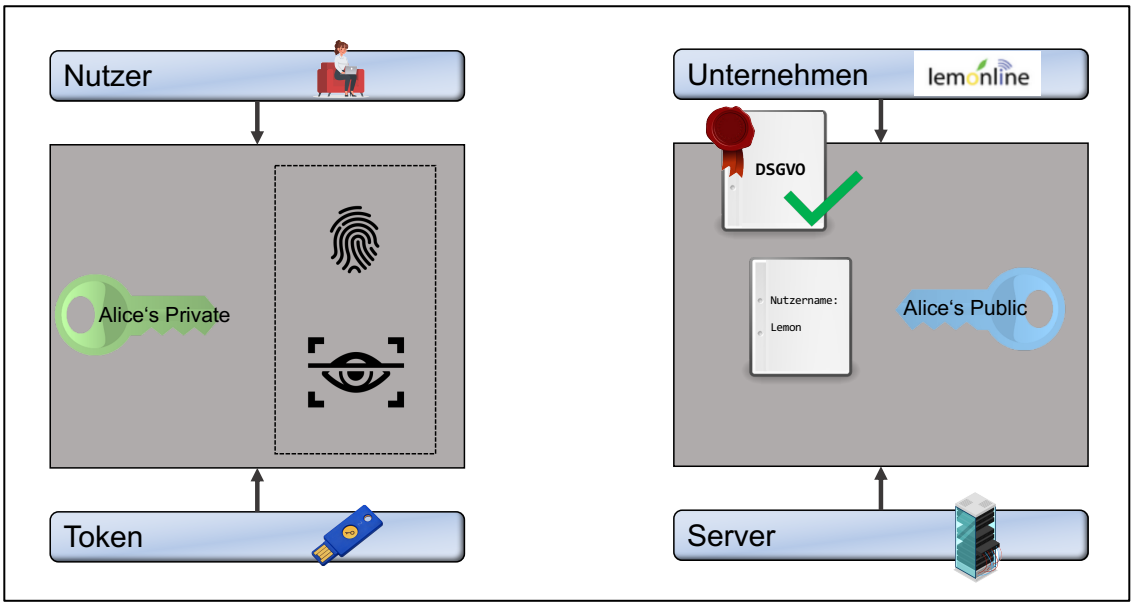

Abb. 14: FIDO2 vs. Datenschutz

3.5 Skalierbarkeit

"Websites can enable FIDO2 through a simple JavaScript API call that is supported across leading browsers and platforms on billions of devices consumers use every day."[58]

Die Skalierbarkeit lässt sich messen als die Eigenschaft eines IT-System auf verschiedenen Betriebssystemen und unter höherer Belastbarkeit funktionieren zu können.[59] Skalierbarkeit stellt somit eine besonders wichtige Voraussetzung dar, um IT-Systeme langfristig im privaten aber besonders auch im betrieblichen Bereich nutzen zu können.

Wie aus dem obigen Zitat der FIDO-Allianz zu entnehmen ist, besteht zwischen der Skalierbarkeit und der Nutzbarkeit eine besondere Beziehung. Im Kontext von FIDO2 bedeutet Skalierbarkeit, dass die Technologie nicht nur für eine ausgewählte und begrenzte Gruppe an Nutzern oder Endgeräte zur Verfügung steht, sondern grundsätzlich von jedem Nutzer, auf jedem gängigen Endgerät und über jeden gängigen Web Browser verwendet werden kann. Ermöglicht wird dies vor allem durch die Schnittstelle WebAuthn, die jeder Online-Dienst über ein entsprechendes Skript auf seinen Web Servern implementieren kann. Hinzu kommt, dass durch die vielen verschiedenen Konnektivitätsmöglichkeiten wie USB A und C, Lightning, NFC, Bluetooth oder als internes TPM die Verwendung des Sicherheitsschlüssels ganz auf die Präferenzen der Nutzer abgestimmt werden kann.

58 FIDO-Allianz (Hrsg.): FIDO2: Web Authn & CTAP, Online im Internet: https://fidoalliance.org/fido2/, abgerufen am 26.05.2020.

59 Vgl. Geißler, Otto: Was ist Skalierbarkeit, Online im Internet: https://www.datacenter-insider.de/was-ist-skalierbarkeit-a-852037/, abgerufen am 14.07.2020.

Dabei spielt es keine Rolle, ob der Nutzer als Betriebssystem Windows, macOS oder Linux verwendet.[60]

Darüber hinaus lässt sich FIDO2 besonders im betrieblichen Umfeld einsetzen. Dies bezieht sich nicht nur auf den Gebrauch an Online-Konten kommerzieller Dienste, sondern auch auf die Nutzung von Online-Anwendungen bspw. von Cloud-Diensten. Die Anmeldung am Microsoft-Konto kann bspw. nicht nur vom Privatnutzer, sondern auch vom Mitarbeiter eines Unternehmens im Rahmen seiner betrieblichen Tätigkeiten verwendet werden. Dazu kann der Nutzer für verschiedene Betriebssysteme und verschiedene Anwendungsfälle denselben Sicherheitsschlüssel nutzen, bzw. dies über das TPM des Laptops oder Smartphones vornehmen. Eine genauere Betrachtung der Einsatzmöglichkeiten von FIDO2, besonders im betrieblichen Umfeld, wird in Kapitel 4.3 vorgenommen. Abbildung 15 zeigt abschließend die vier Aspekte, welche die Skalierbarkeit von FIDO2 bedingen.

Abb. 15: Skalierbarkeit von FIDO2

60 Vgl. GitHub (Hrsg.): https://github.com/strangerlabs/webauthn, abgerufen am 11.06.2020, vgl. W3C (Hrsg.): Web Authentification: An API for accessing Public Key Credentials Level 1, Online im Internet: https://www.w3.org/TR/webauthn/#api, 04.03.2019 und vgl. Eikenberg, Ronald: Online-Schlüssel – FIDO2-Sicherheitsschlüssel zum Einloggen mit und ohne Passwort, a.a.O., S.67 & 70 ff.

4 Praktische Anwendung von FIDO2

4.1 Systematisierung der praktischen Anwendung von FIDO2

Die FIDO2-Technologie wird bereits von Mitgliedern der FIDO-Allianz angeboten. Nutzer können sich passwortlos über interne oder auch externe Sicherheitsschlüssel anmelden. Abseits dieser Unternehmen stehen jedoch nicht viele weitere Online-Dienste zur Verfügung, die ihren Kunden FIDO2 anbieten. Dabei besitzt FIDO2 ein weitaus größeres Potenzial, als die vier Prinzipen zunächst vermuten lassen. Wie bereits erläutert, lässt sich FIDO2 nicht nur im privaten Rahmen anwenden, sondern kann auch als Authentifizierungsmethode in betrieblichen IT-Systemen eingesetzt werden. Dabei gilt es jedoch ebenfalls, einige Risiken zu betrachten, die bei der Verwendung von FIDO2 auftreten können. Nachfolgend werden drei beispielhafte Anbieter der FIDO2-Technologie vorgestellt. Darauf aufbauend wird zunächst ein Beispiel für eine betriebliche Anwendung angeführt, bevor die Risiken der Nutzung von FIDO2 erläutert werden. Abschließend wird eine Reihe von Anwendungsbeispielen gezeigt, die als beispielhafter Leitfaden zur Registrierung von Sicherheitsschlüsseln dienen soll.

Kapitel 4.2: Anbieter

Damit Nutzer an den vier Prinzipien der FIDO-Allianz partizipieren können, wird eine kritische Masse an Online-Diensten benötigt, die FIDO2 zur Verfügung stellen. Besonders das Ziel der Skalierbarkeit kann maßgeblich durch diese Online-Dienste beeinflusst werden. Nutzer sollen über die Verfügbarkeit der Technologie an dessen Verwendung herangeführt werden. Dieses Kapitel stellt drei Mitglieder der FIDO-Allianz vor, die aufgrund ihrer Reputation und Marktposition besonderen Einfluss auf die Verbreitung von FIDO2 haben können.

Kapitel 4.3: Potenzial

Die Vorteile in den Bereichen Sicherheit, Nutzbarkeit, Privatsphäre und Skalierbarkeit machen FIDO2 für den Nutzer attraktiv. FIDO2 stellt somit eine moderne Alternative zur Authentifizierung mittels Passwort dar. Allerdings lässt sich FIDO2 nicht ausschließlich im privaten Bereich anwenden. Die Flexibilität von FIDO2 ermöglicht ebenfalls den Einsatz im betrieblichen Umfeld. Mitarbeiter können FIDO2 zur Anmeldung an Enterprise Resource Planning-Systemen (ERP) einsetzen. Unternehmen bieten sich dabei mehrere Möglichkeiten der Authentifizierung. Diese lassen sich individuell durch die zuständigen Systemadministratoren implementieren und verwalten.

Kapitel 4.4: Risiken

Die Nutzung von FIDO2 birgt dennoch Risiken, die zu beachten sind. Risiken können dabei sowohl auf Seiten des Servers als auch des Clients festgestellt werden. Serverseitig bestehen Risiken besonders im Bereich der Implementierung und Durchführung von FIDO2. Unsichere Authentifizierungsverfahren könnten dafür sorgen, dass Dritte trotz asymmetrischer Verschlüsselung in der Lage sind, sich zwischen Server und Nutzer zu stellen. Ähnliches gilt für den Fall, dass eine Zertifizierungsstelle kompromittiert wird. Auf Seiten des Nutzers besteht vor allem die Gefahr des Verlusts des Sicherheitsschlüssels. Ist ein Nutzer nicht mehr im Besitz seines Sicherheitsschlüssels, ist dieser nicht mehr in der Lage, auf seine damit verbundenen Konten zuzugreifen. Zudem wird die FIDO2-Technologie zwar gut angenommen, jedoch gibt es für den herkömmlichen Nutzer weiterhin ein viel zu geringes Angebot an Online-Diensten, die FIDO2 zur Verfügung stellen.

Kapitel 4.5: Praxisbeispiel

Im Rahmen von Kapitel 4.3 wurde das Potenzial von FIDO2, besonders im betrieblichen Umfeld, erläutert. Darauf aufbauend wird in diesem Kapitel anhand von „Windows Hello“ und einem Microsoft Online-Konto ein beispielhafter Registrierungs- und Authentifizierungsprozess durchlaufen. Windows Hello dient dabei zur Authentifizierung an mobilen Endgeräten in Windows 10. Zusätzlich kann durch Windows Hello aber auch über einen externen Sicherheitsschlüssel Zugriff auf das Online-Konto von Microsoft genommen werden.

4.2 Anbieter

Der wohl prominenteste Anbieter der FIDO2-Techologie ist Microsoft. Ist ein Nutzer im Besitz eines Rechners mit Windows 10 als Betriebssystem, kann dieser über Windows Hello lokale biometrische Authentifizierungsverfahren verwenden. Dies ist sowohl für die Anmeldung am Rechner selbst, aber auch an kompatiblen Apps und Online-Diensten möglich. Für FIDO2-Nutzer resultiert daraus, dass diese nicht zwingend einen externen Sicherheitsschlüssel benötigen, sofern sie einen Rechner mit Windows 10 besitzen. Windows Hello basiert dabei auf den Prinzipien eines internen Sicherheitsschlüssels. Da-

bei zeigt Microsoft, dass lokale Biometrie nicht nur ein erhöhtes Sicherheitslevel bereitstellt, sondern auch eine häufig im Unternehmen benötigte Flexibilität für Nutzer und Infrastruktur ermöglicht. Weitere Details dazu werden in Kapitel 4.3 erläutert.[61]

Ein weiterer prominenter Anbieter der FIDO2-Technologie und Mitglied der FIDO-Allianz ist Google. Google bietet in Form des Titan-Security-Keys sogar einen eigenen Sicherheitsschlüssel an, der auf den Protokollen der FIDO-Technologie basiert. Dennoch dauerte es vergleichsweise lange, bis Google die passwortlose Technologie seinen Nutzern zur Verfügung stellte. Dabei hat Google mit einem Marktanteil von 88 Prozent unter den Suchmaschinen weltweit die Möglichkeit, FIDO2 vielen Nutzern zur Verfügung zu stellen. Lange Zeit versuchte Google, den Nutzern durch die „Single-Sign-on-Technologie“ (SSO)[62] eine sichere und komfortable Alternative zum Passwort zu bieten. Diese Technologie erfreute sich jedoch gerade unter Experten geringer Beliebtheit. Anschließend stellte Google seinen Nutzern die FIDO U2F-Technologie zur Verfügung, um sich am Google-Konto zu authentifizieren.

Dennoch ist es bei Google erst seit kurzem möglich, eine vollkommen passwortlose Authentifizierung zu verwenden. Möchte sich ein Nutzer gänzlich ohne Passwort an seinem Google-Konto anmelden, muss der Nutzer am Smartphone zunächst die entsprechende Google-App installieren und sich dort mit seinen klassischen Nutzerdaten anmelden. Im Rahmen eines Setup-Vorgangs kann das Smartphone dadurch als Sicherheitsschlüssel eingerichtet werden. Gibt der Nutzer zu Beginn eines darauffolgenden Anmeldevorgangs seine E-Mail in die Maske ein, wird eine Bestätigungsanfrage über die Google App an das Smartphone gesendet. Der Nutzer selbst hat dabei die Auswahlmöglichkeit, den Vorgang mit „Ja“ zu bestätigen oder mit „Nein“ abzubrechen. Bestätigt der Nutzer, erfolgt eine abschließende Authentifizierung über die Abfrage der hinterlegten biometrischen Faktoren. Je nach Art des Smartphones werden dabei der Fingerabdruck oder das Gesicht gescannt und überprüft. Der Nutzer selbst muss also keine biometrischen Daten am Google-Konto hinterlegen. Google greift auf die bereits auf dem Smartphone hinterlegten

61 Vgl. von Westernhagen, Olivia: Anmeldung ohne Passwort: „Windows Hello“ wird zum FIDO2-Authenticator, Online im Internet: https://www.heise.de/security/meldung/Anmeldung-ohne-Passwort-Windows-Hello-wird-zum-FIDO2-Authenticator-4418470.html, 10.05.2019 und vgl. Wigleven, Pieter: Windows Hello and FIDO2 Security Keys enable secure and easy authentication for shared devices, Online im Internet: https://www.microsoft.com/en-us/microsoft-365/blog/2018/04/17/windows-hello-fido2-security-keys/, 17.04.2018.

62 Vgl. Luber, Stefan; Schmitz, Peter: Was ist Single Sign-on (SSO)?, Online im Internet: https://www.security-insider.de/was-ist-single-sign-on-sso-a-631479/, 03.08.2017.

Daten zurück. Das Smartphone selbst agiert dabei als Sicherheitsschlüssel in Verbindung mit einer Multi-Faktor-Authentifizierung.[63]

Seit kurzem kann sich auch Apple als weiterer großer Technologiekonzern in die Reihe der Board-Level-Mitglieder[64] einreihen. Seit der Version iOS 13.3 sind auch Apple-Nutzer über den Web Browser Safari in der Lage, sich an Konten von Online-Diensten mittels FIDO2 und externer Sicherheitsschlüssel anzumelden. Bisher war dies nur über andere Browser möglich. Ebenfalls genutzt werden können Apple-Endgeräte wie iPhones, iPads oder MacBooks als interner Sicherheitsschlüssel. Apple-Nutzer können die Technologie dabei über die biometrischen Sensoren an ihren Endgeräten aktivieren. Jedoch ist FIDO2 über interne Sicherheitsschlüssel am Apple-Endgerät nur als zweiter Faktor im Kontext von FIDO U2F nutzbar. Einzige Ausnahme ist die Authentifizierung am Google-Konto, die im vorigen Abschnitt erläutert wurde.[65]

Die drei vorangegangenen Anbieter stellen nur einen Teil der Unternehmen dar, die zum FIDO-Universum gehören. Zur weiteren Analyse der Verbreitung von FIDO lohnt sich ein Blick in die Datenbank der zertifizierten FIDO-Produkte[66]. Wie schon bei dem Vorgänger FIDO U2F ist die Resonanz zum passwortlosen Standard nicht besonders hoch. Es ist jedoch ein gesteigertes Interesse an der passwortlosen Authentifizierungsalternative zu erkennen. Eine genauere Betrachtung von Abbildung 16 und der zertifizierten Server zeigt, dass der Anteil von FIDO2 (63) wesentlich höher ist als bei FIDO U2F (28). Im Vergleich zu FIDO UAF ist dies jedoch wesentlich geringer (93).[67] Dies könnte unter anderem darauf zurückzuführen sein, dass der UAF-Standard zum einen wesentlich älter, aber auch etablierter ist. Schon seit einigen Jahren ist das Bestätigen von Anmeldungen oder Transaktionen über biometrische Verfahren möglich. Ein Beispiel ist das Nutzen eines Fingerabdrucksensors zum Entsperren eines Smartphones. Zudem kann auch das

63 Vgl. Költzsch, Tobias; Grüner, Sebastian: Google führt Logins ohne Passwort ein, Online im Internet: https://www.golem.de/news/fido-google-fuehrt-logins-ohne-passwort-ein-1908-143169.html, 13.08.2019, vgl. Schmidt, Jürgen: Abschied vom Passwort – Passwortloses Anmelden dank FIDO2, in: c't, 18/2019, S. 17 f., vgl. Kaltschmidt, Thomas: Einloggen ohne Passwort – Mehr Schutz: Mac und iOS unterstützen FIDO2, in: Mac&i, 01/2020, S. 128, und vgl. Statista (Hrsg.): Statistiken zu Suchmaschinen, Online im Internet: https://de.statista.com/themen/111/suchmaschinen/, 11.11.2019.

64 Vgl. FIDO-Allianz (Hrsg.): FIDO Members, online im Internet: https://fidoalliance.org/members/, abgerufen am 26.10.2020.

65 Vgl. Schwan, Ben: iOS 13.3: Safari unterstützt diverse Sicherheitskeys, Online im Internet: https://www.heise.de/mac-and-i/meldung/iOS-13-3-Safari-unterstuetzt-diverse-Sicherheitskeys-4584820.html, 13.11.2019 und vgl. Becker, Leo: Smart Lock: iPhone wird Security-Key für Google-Accounts, Online im Internet: https://www.heise.de/mac-and-i/meldung/Smart-Lock-iPhone-wird-Security-Key-fuer-Google-Accounts-4638509.html, 15.01.2020.

66 Vgl. FIDO-Allianz (Hrsg.): FIDO® Certified, Online im Internet: https://fidoalliance.org/certification/fido-certified-products/, abgerufen am 24.07.2020.

67 Vgl. FIDO-Allianz (Hrsg.): FIDO® Certified, Online im Internet: https://fidoalliance.org/certification/fido-certified-products/, abgerufen am 24.07.2020.

hohe wissenschaftliche und wirtschaftliche Interesse passwortloser Verfahren ein Grund für die höhere Akzeptanz sein. Dennoch sollte berücksichtigt werden, dass der FIDO2-Standard erst seit 2019 auf dem Markt angeboten wird, sodass bereits eine relativ hohe Nachfrage nach FIDO2-zertifizierten Produkten auf der Server-Seite zu verzeichnen ist. Gemessen an der geringeren Anzahl zertifizierter U2F-Server bestätigt dies die Annahme eines gesteigerten Interesses an rein passwortlosen Verfahren. Dennoch ist die Authentifizierung mittels zweier Faktoren heutzutage wesentlich häufiger anzutreffen, als passwortlose Varianten. Dabei gilt jedoch zu beachten, dass nicht jede Zwei-Faktor-Authentifizierung auch dem U2F-Standard entspricht. Somit verbleibt zunächst die Frage, wieso bisher so wenige Online-Dienste auf die FIDO2-Technologie im Rahmen ihrer Anmeldeprozesse verzichten.

Doch um die Verbreitung von FIDO2 vollständig zu erfassen, sollte auch die Nachfrage-Seite betrachtet werden. Die Gruppe der Nutzer muss das Konzept ebenfalls akzeptieren und verwenden. Darüber ist es möglich, eine ausreichende Skalierbarkeit zu erreichen und den Standard weiterentwickeln zu können. Bei Betrachtung von Abbildung 16 ist zu erkennen, dass der Anteil an FIDO2-basierten Token im Vergleich aller Standards am geringsten ist. Jedoch kann diese Zahl, gemessen am dem kurzen Verfügbarkeitszeitraum, als verhältnismäßig groß beurteilt werden.[68] Somit lässt sich nutzerseitig ein gewisses Nachfragepotenzial an FIDO2-Geräten erkennen.

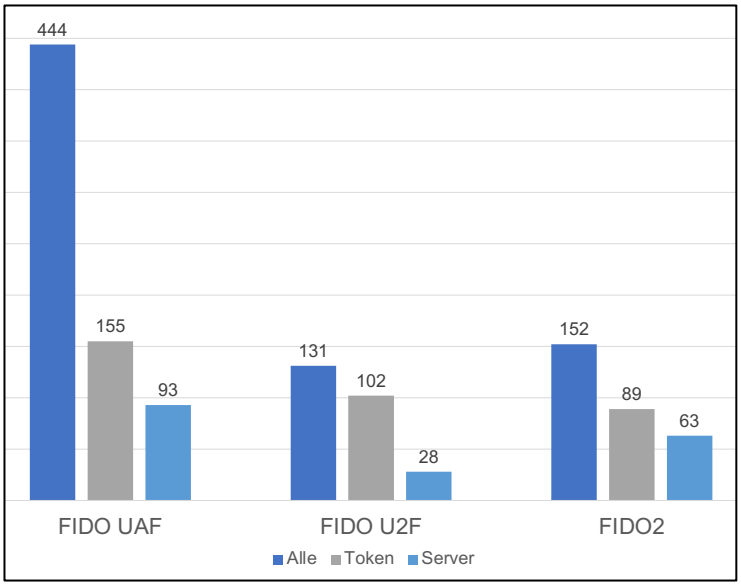

Abb. 16: Zertifizierte FIDO-Produkte nach FIDO-Standard (Stand: 13.08.2020)

68 Vgl. FIDO-Allianz (Hrsg.): FIDO® Certified, Online im Internet: https://fidoalliance.org/certification/fido-certified-products/, abgerufen am 24.07.2020.

4.3 Potenzial

Die gesteigerte Sicherheit, die FIDO2 seinen Nutzern bietet, kommt nicht nur dem privaten Sektor zugute. Auch für unternehmerische Anwendung kann FIDO2 einige Vorteile bereitstellen. Dies resultiert vor allem aus dem einheitlichen Schnittstellendesign, was sich in einer großen Kompatibilität des Verfahrens mit vielen verschiedenen Applikationen ausdrückt.[69] Dabei können sowohl Unternehmen auf der Anbieter- als auch der Nachfrageseite von den besonderen Sicherheitsmaßnahmen profitieren. Flexibilität, Effizienz und Sicherheit können für Unternehmen mit digitalen Geschäftsmodellen oder auch einzelnen Geschäftsprozessen durchaus attraktiv sein. Ein in der Praxis besonders häufig betrachteter Aspekt ist dabei das Auslagern der Server und deren Administration.

Viele Unternehmen nutzen Anwendungssoftware wie die Office-Produkte von Microsoft oder auch ERP-Softwarelösungen von Microsoft oder SAP. Um Kosten einsparen aber dennoch Dienstleistung und Expertise einkaufen zu können, nutzen immer mehr Unternehmen Web- bzw. Cloud-Anwendungen wie bspw. Microsoft 365 oder SAP S/4HANA. Softwarehersteller bieten ihren Kunden dabei an, sogenannte Online-Lizenzen zu erwerben. Die Software wird dabei auf den Servern des Herstellers zur Verfügung gestellt und muss nicht lokal installiert werden. Die Mitarbeiter eines Unternehmens können über eine entsprechende Web-Anwendung darauf zurückgreifen und diese verwalten. Die Mitarbeiter haben die Möglichkeit, von überall auf die entsprechende Software zuzugreifen und bspw. Dokumente nutzen zu können. Voraussetzung ist lediglich, dass die Mitarbeiter eine entsprechende Berechtigung besitzen.[70]

Die Cloud-basierte Identitäts- und Berechtigungsverwaltung „Azure Active Directory“ (Azure AD) von Microsoft stellt die Schnittstelle zwischen Nutzer und System dar. Inhabern einer Microsoft-Lizenz werden verschiedene rollenbasierte Anwendungsmöglichkeiten geboten. Unabhängig von der zugewiesenen Nutzerrolle erhalten alle Nutzer zunächst die Möglichkeit, sich über Azure AD an ihrer Anwendungssoftware zu authentifizieren. Systemadministratoren können ihren Nutzern dabei die Multi-Faktor-Authentifizierung zur Verfügung stellen oder sogar vorschreiben, wenn die Tätigkeit der Mitarbeiter Zugriff auf besonders sensible Unternehmensdaten erfordert. Seit 2019 ist dies nicht mehr nur im Rahmen der Microsoft Authenticator-App und Windows Hello möglich, sondern ist auch mit einem FIDO2-Sicherheitsschlüssel kompatibel. Abbildung 17 zeigt dazu, dass eine Anmeldung am Microsoft-Konto einerseits auf direktem Wege stattfinden kann:

69 Vgl. W3C (Hrsg.): Web Authentication: An API for Accessing Public Key Credentials Level 1, Online im Internet: https://www.w3.org/TR/2019/REC-webauthn-1-20190304/, 04.03.2019.

70 Vgl. Mello, Stefan: Office 365 vs. Office 2019 – Cloud- übertrifft Desktop-Version, Online im Internet: https://www.heise.de/brandworlds/cloud-services/office-365-vs-office-2019-cloud-uebertrifft-desktop-version/, 22.10.2019.

Mithilfe eines externen Sicherheitsschlüssels ist es möglich, sich per Web Browser an seinem Konto anzumelden. Andererseits kann ein Nutzer auch eine Authentifizierung auf indirektem Wege vornehmen: Über den lokalen Authentifizierungsdienst Windows Hello kann sich ein Nutzer ebenfalls auf dem Microsoft-Konto anmelden. Besonders relevant kann dies in Abteilungen sein, in denen sehr sensible Daten genutzt werden, bspw. einer Controlling-Abteilung. Aufgrund der Sensibilität der Daten, kann unter anderem ein biometrisches Verfahren verwendet werden, um sich an dem System zu authentifizieren. Daraus resultiert der besondere Vorteil, dass sich die Nutzer auf jedem Endgerät am System authentifizieren können und dabei nur den Sicherheitsschlüssel benötigen. Ein beispielhafter Registrierungsprozess zur Anmeldung an einem Microsoft-Konto wird in Kapitel 4.5 beschrieben.[71]

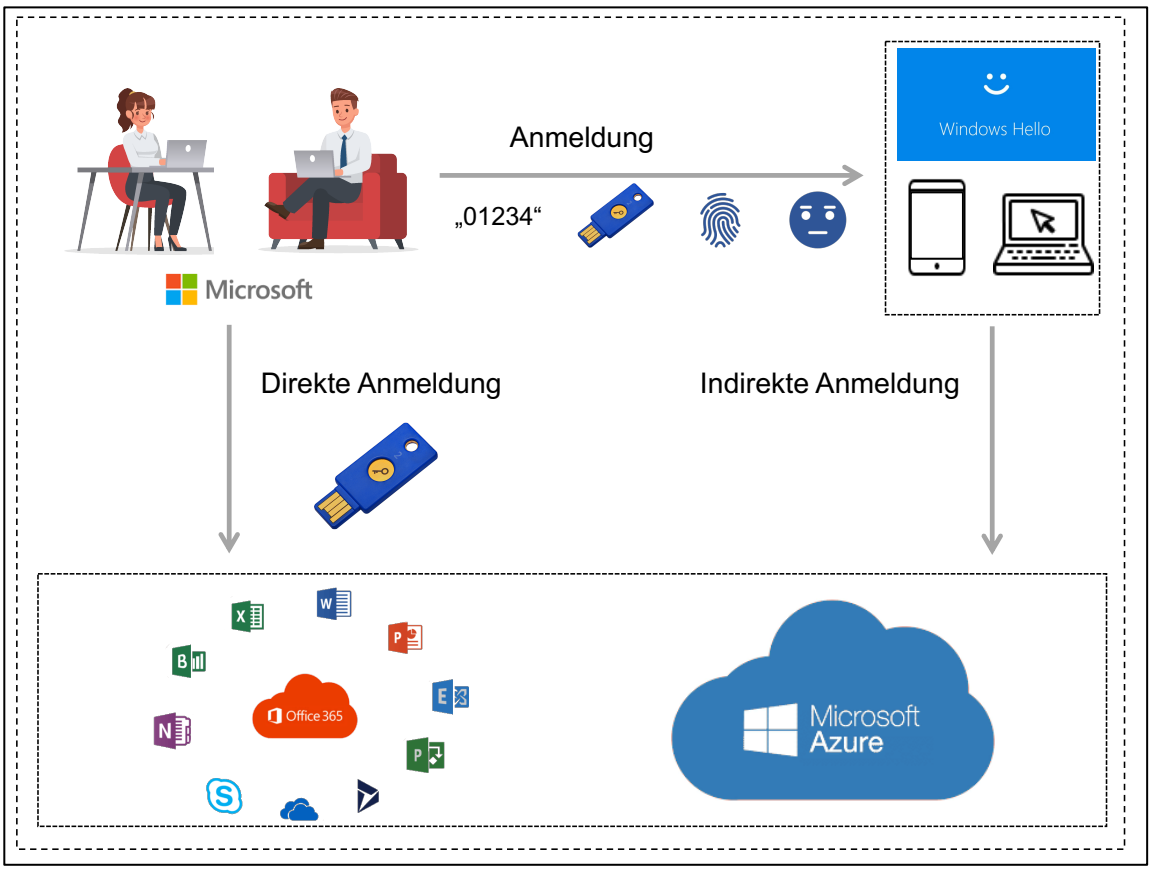

Abb. 17: Authentifizierungsmöglichkeiten am Microsoft-Konto

71 Vgl. Microsoft (Hrsg.): Was ist Azure Active Directory, Online im Internet: https://docs.microsoft.com/de-de/azure/active-directory/fundamentals/active-directory-whatis, 05.06.2020 und vgl. Microsoft (Hrsg): Announcing the public preview of Azure AD support for FIDO2-based passwordless sign-in, Online im Internet: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/announcing-the-public-preview-of-azure-ad-support-for-fido2/ba-p/746362, 07.10.2019.

Der Einsatz von FIDO2 sollte somit nicht nur im privaten sondern besonders im betrieblichen Rahmen in Erwägung gezogen werden. Unternehmensdatenbanken enthalten häufig eine besonders hohe Zahl an sensiblen Daten und sind somit potentielle Opfer für Lösegelderpressungen. Wie der aktuelle Phishing- Report von „Cofense“ zum ersten Quartal 2020 zeigt, sind in Deutschland angesiedelte Unternehmen besonders stark in den Fokus von Cyber-Angriffen gerückt. Gefördert wird dieser Umstand von der Tatsache, dass immer mehr Mitarbeiter während der Corona-Pandemie ihren Arbeitsplatz in das „Home-Office“ verlagert haben. Dies resultiert in einem Abhängigkeitsverhältnis zwischen dem betrieblichen IT-System und den privaten Maßnahmen zur Sicherung der technischen Infrastruktur der Mitarbeiter. Das allgemeine Risiko von Phishing-Angriffen steigt damit enorm, da deutsche Unternehmen aufgrund hoher Kompetenzen, Knowhow und starker Vernetzung besonders viele sensible Daten auf ihren Datenbanken ablegen.[72]

Im Rahmen des Sicherheitsmanagements kann der Einsatz von FIDO2 dazu führen, dass die Sicherheitsziele trotz eines besonders volatilen Unternehmensumfeldes gewahrt werden könnten. Die Implementierung der FIDO2-Technologie in betrieblichen Prozessen ist darüber hinaus relativ leicht auf den entsprechenden Servern vorzunehmen. Grund dafür ist die einheitliche JavaScript-Schnittstelle WebAuthn. Auch die Ausstattung der Mitarbeiter mit Sicherheitsschlüsseln, verglichen mit den potentiellen Schäden durch kompromittierte Systeme, ist vergleichsweise kostengünstig vorzunehmen. Die Administration der Prozesse sollte dabei in der Verantwortung der Systemadministratoren verbleiben. Die Administratoren könnten auch darüber entscheiden, welche und wie viele Faktoren zur Authentifizierung genutzt werden sollen. FIDO2 eröffnet somit das Potenzial, das durch menschliches Fehlverhalten verursachte Risiko für Unternehmen deutlich zu minimieren.

4.4 Risiken

Auf den ersten Blick erscheint FIDO2 als universal einsetzbares und besonders sicheres Authentifizierungsverfahren, das kaum Schwachstellen aufweist. Wie bereits erläutert, ist die Sicherheit von IT-Systemen jedoch nie vollkommen zu gewährleisten. Sicherheit kann nur soweit gewährleistet werden, als dass die Gefahr von Hackerangriffen hinreichend unwahrscheinlich wird. Bei genauerer Betrachtung lassen sich auch bei FIDO2 Schwachstellen für potentielle Angriffe von außen erkennen. Dies kann dazu führen, dass

72 Vgl. TÜV-SÜD (Hrsg): Deutsche Unternehmen sind beliebtes Ziel für Phishing-Angriffe, Online im Internet: https://www.tuvsud.com/de-de/presse-und-medien/2020/juli/deutsche-unternehmen-sind-beliebtes-ziel-fuer-phishing-angriffe, 07.07.2020.

auch bereits genannte Vorteile und positive Eigenschaften von FIDO2 nicht mehr zutreffen können.

Im Bereich der Sicherheit stellt das Challenge-Response-Verfahren ein potentielles Risiko dar. Sichere Systeme nutzen bspw. zufällig gewählte Aufgaben für die Registrierung oder Authentifizierung, die durch den Sicherheitsschlüssel gelöst werden müssen. Verwendet ein System hierbei keine zufällig ausgewählten Aufgaben oder sind diese leicht zu lösen, besteht die Gefahr von Replay-Attacken durch das Abfangen der Challenge. Dieses Szenario wird in Abbildung 18 durch den unteren Pfeil dargestellt. Dem Angreifer würde sich somit die Möglichkeit bieten, eine eigens generierte Antwort an den Server zu senden. Das Schlüsselpaar des eigentlichen Nutzers wäre somit unterwandert. FIDO2 würde dadurch seinen Schutz vor MITM-Angriffen verlieren. In der Praxis hat sich daher die Nutzung von Aufgaben mit einer Länge von mindestens 16 Byte etabliert.[73]

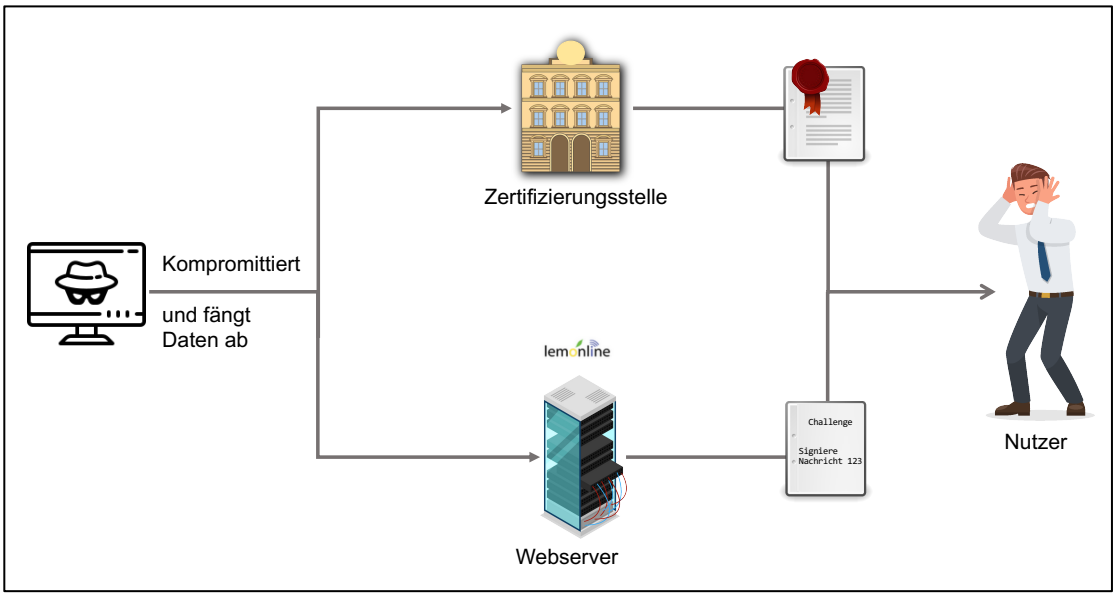

Abb. 18: Gefahr kompromittierter Server oder Zertifizierungsstellen

Auch Zertifizierungsstellen, wie in Abbildung 18 dargestellt, können ein potentielles Opfer durch kompromittierende Angriffe von außen werden. Zertifizierungsstellen agieren als vertrauenswürdige Instanz zwischen Server und Nutzer. Ist ein Zertifikat kompromittiert, kann dieses nicht mehr als vertrauenswürdig erachtet werden, sodass ein neues Schlüsselpaar generiert werden muss. Der Hersteller des Sicherheitsschlüssels muss dem

73 Vgl. W3C (Hrsg.): Web Authentication: An API for accessing Public Key Credentials Level 1, Online im Internet: https://www.w3.org/TR/2019/REC-webauthn-1-20190304/, 04.03.2019.

Nutzer daraufhin ein neues Schlüsselpaar mit der entsprechenden Zertifizierung zur Verfügung stellen. Ansonsten besteht die Möglichkeit, dass Dritte dienstspezifische Schlüsselpaare im Namen eines Nutzers generieren.[74]

Ein weiteres Sicherheitsrisiko stellt der Nutzer selbst dar. Die Komponente Mensch kann dabei als ein wichtiger Erklärungsfaktor genannt werden, um potentielle Sicherheitslücken in IT-Systemen zu erklären. Sollte der Sicherheitsschlüssel eines Nutzers bspw. verloren gehen, gestohlen oder sogar zerstört werden, kann es unter Umständen sehr schwer sein, auf die eigenen Daten zugreifen zu können. Die spezifischen Schlüsselpaare sind i. d. R. fest mit dem Sicherheitsschlüssel gekoppelt und nicht auslesbar. Ein Problem besteht vor allem dann, wenn die betroffenen Konten besonders sensible Daten beinhalten, wie dies bspw. bei betrieblichen Konten, beim Online-Banking oder bei E-Mail-Konten der Fall ist. Hierbei wird der Vorteil des Verzichts auf Datenerhebung und -speicherung seitens der Online-Dienste zur Falle für den Nutzer. Außerdem gilt in diesem Szenario dieselbe Problematik, die schon bei der Verwendung von Passwörtern auftritt. Alle Zugänge sind in einem Verfahren gebündelt, sodass das Risiko bei Verlust erhöht wird. Um diesem Problem vorzubeugen, ermöglicht FIDO2 seinen Nutzern mehrere Sicherheitsschlüssel für einen Dienst zu registrieren. Es gilt allerdings zu relativieren, dass die Nutzung des Sicherheitsschlüssels weiterhin an die physische Anwesenheit und einzigartige Merkmale des Nutzers gekoppelt ist. Die Möglichkeit eines Datenmissbrauchs durch den Diebstahl eines Sicherheitsschlüssels ist somit als hinreichend gering einzuschätzen. Dies ist bspw. besonders bei biometrischen Verfahren gegeben oder wenn eine weitere PIN verwendet werden muss. Die Gefahr durch einen verlorenen oder gestohlenen Sicherheitsschlüssel sollte somit nicht überbewertet werden, da nur bedingt Schaden angerichtet werden kann.[75]

Es gilt jedoch ebenfalls zu berücksichtigen, dass auch biometrische Verfahren nicht gänzlich fälschungssicher sind. So ist es z. B. Dritten möglich, über Rückstände an Gegenständen, bedingt durch den natürlichen Fettfilm der Haut, Fingerabdrücke zu reproduzie-

74 Vgl. BSI (Hrsg): Das Trusted Platform Module (TPM), Online im Internet: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/TrustedComputing/TrustedPlatformModuleTPM/TrustedPlatformModuleTPM/aufbaustruktur.html, abgerufen am 29.07.2020.

75 Vgl. Eikenberg; Ronald; Schmidt, Jürgen: FAQ: Sicher einloggen mit FIDO2, Online im Internet: https://www.heise.de/ct/artikel/FAQ-Sicher-einloggen-mit-FIDO2-4547137.html, 16.10.2019, vgl. Feilner, Markus: Passwortfreie Auth-Verfahren: FIDO 2 und Webauthn, Online im Internet: https://www.linux-magazin.de/ausgaben/2018/08/webauthn/5/, abgerufen am 30.07.2020 und vgl. Kratzenberg, Marco: FIDO2: Login ohne Passwort? Wie es funktioniert und wer es braucht, Online im Internet: https://www.giga.de/artikel/fido2-login-ohne-passwort-wie-es-funktioniert-und-wer-es-braucht/, 27.09.2019.

ren. Da sich der Fingerabdruck im Zeitverlauf eines Lebens nicht mehr verändert, ist somit das komplette System unterwandert. Der Nutzer wird somit gezwungen, auf ein anderes Merkmal oder ein anderes Verfahren zurückzugreifen.[76]

Zusätzlich ergibt sich ein spezielles, nutzerspezifisches Risiko. Bereits 2018 beschäftigten sich Camp/Dingman/Sanchari[77] mit dem Akzeptanzverhalten von Menschen in Bezug auf U2F. Dabei konnte bereits beobachtet werden, dass einige Hemmnisse seitens der Nutzer gegenüber der U2F-Technologie bestanden. Häufige Probleme traten dabei im Rahmen des Registrierungsprozesses auf. Ungeübten Nutzern erschien der Leitfaden zur Registrierung eines Sicherheitsschlüssels als zu komplex und wenig intuitiv. Häufig konnte dies auf mangelndes technisches Verständnis der Nutzer zurückgeführt werden. Ein weiteres Problem bestand in der Akzeptanz der Technologie als solches. Vielen Teilnehmern der Studie war bis zuletzt gar nicht bewusst, wie schlecht Passwörter vor äußeren Angriffen schützen. Dies führte zur Ablehnung der Sicherheitsschlüssel und dem damit verbundenen Aufwand, zusätzliche Authentifizierungen neben dem Passwort einzurichten. Zudem war vielen Teilnehmern ebenfalls nicht bewusst, dass nicht alle Sicherheitsschlüssel biometrische Verfahren zur Erkennung der Nutzer verwenden. Einige Sicherheitsschlüssel verwendeten eine einfache Nutzergeste durch das Berühren oder Drücken eines Knopfes, um den Vorgang zu bestätigen. Für die Teilnehmer selbst ergab sich daraus kein erkennbarer Vorteil in Sachen Sicherheit und Nutzbarkeit.

Die Erkenntnisse dieser Studie könnten einen Erklärungsansatz für die bisher eher geringe Akzeptanz von FIDO U2F bieten. Die Erfahrungen mit U2F und die darauf aufbauenden Erwartungen bzgl. FIDO2 könnten wiederum einen Erklärungsansatz für die bisher geringe Resonanz zu FIDO2 darstellen. Zwar lässt sich ein hohes Interesse an FIDO2 grundsätzlich erkennen, doch wird seitens der Online-Dienste gezögert, FIDO2 anzubieten. Schlussendlich können die Vorteile von FIDO2 den Nutzer jedoch nicht erreichen, wenn bereits die Möglichkeit zur Nutzung der Technologie nicht gegeben ist.

Zudem besitzen typische Nutzer häufig eine Vielzahl von Online-Konten. Viele Geschäftsmodelle werden heutzutage digital umgesetzt und die Märkte finden immer mehr auf digitalen Plattformen statt. Will ein Nutzer also all seine Online-Konten gegen passwortbasierte Angriffe resistent machen, muss die Registrierung für jedes Konto einzeln stattfinden. Dies könnte einen großen organisatorischen Aufwand mit sich bringen. Zumal viele Registrierungsvorgänge von Online-Diensten nicht standardisiert sind. Darüber

76 Vgl. Hansen, Hans Robert; Mendling, Jan; Neumann, Gustaf: Wirtschaftsinformatik, a.a.O., S. 382 f.

77 Vgl. Camp, L. Jean; Dingman, Andrew; Sanchari, Das: Why Jonny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key, Online im Internet: https://fc18.ifca.ai/preproceedings/111.pdf, abgerufen am 05.07.2020.

hinaus wird FIDO2 bisher nicht von vielen Online-Diensten angeboten. Dem Nutzer bietet sich also in vielen Fällen gar nicht die Möglichkeit der Registrierung.

Ein Nutzer wird somit dem Risiko ausgesetzt, entweder keine Verwendung für den Sicherheitsschlüssel zu haben oder ihn, wie unter anderem bei Apple der Fall, für U2F einsetzen zu müssen. Zusätzlich wird für die Nutzung von FIDO2 ein Mindestmaß an notwendiger Hard- und Software benötigt, die nicht jeder Nutzer zwangsläufig vorweisen kann. Dies kann für den Nutzer zusätzliche Kosten verursachen.[78]

4.5 Praxisbeispiel

Einrichtung von „Windows Hello“: Windows 10 Nutzer haben die Möglichkeit, in kurzer Zeit eine sichere, aber auch bequeme Methode zu etablieren, sich am eigenen Laptop oder Microsoft-Konto anzumelden. Im Folgenden wird in Form eines Praxisbeispiels ein beispielhafter Vorgang zur Einrichtung des Authentifizierungsverfahrens von Windows „Hello“ beschrieben.

Zur Einrichtung der Authentifizierungsverfahren muss der Nutzer in die Systemeinstellungen und die „Anmeldeoptionen“ navigieren. Dies ist in Abbildung 19 zu sehen. Dort befindet sich eine Übersicht der verschiedenen Optionen zur Authentifizierung. Dabei kann zwischen der Authentifizierung mittels Gesichtserkennung, Fingerabdruck, PIN, Sicherheitsschlüssel und Kennwort gewählt, bzw. mehrere Faktoren können miteinander kombiniert werden. Die Optionen Gesichtserkennung, Fingerabdruck und PIN basieren auf der Verwendung eines TPMs. Der Sicherheitsschlüssel selbst stellt die externe Option dar. Microsoft empfiehlt die Verwendung des Fingerabdrucks und einer zusätzlichen PIN.

78 Vgl. Kratzenberg, Marco: FIDO2: Login ohne Passwort? Wie es funktioniert und wer es braucht, Online im Internet: https://www.giga.de/artikel/fido2-login-ohne-passwort-wie-es-funktioniert-und-wer-es-braucht/, 27.09.2019.

Abb. 19: Übersicht der Authentifizierungsverfahren in „Windows Hello"

Zur Einrichtung der Authentifizierung mittels Fingerabdrucksensor verlangt Windows das Auflegen des Fingers, i. d. R. den Zeigefinger, auf den Sensor. Anschließend muss der zu registrierende Finger abwechselnd aufgelegt und erkannt werden. Der Nutzer muss hier unterschiedliche Winkel zum Auflegen verwenden, da der Finger auch in der Anwendung nicht immer im selben Winkel aufgelegt wird.

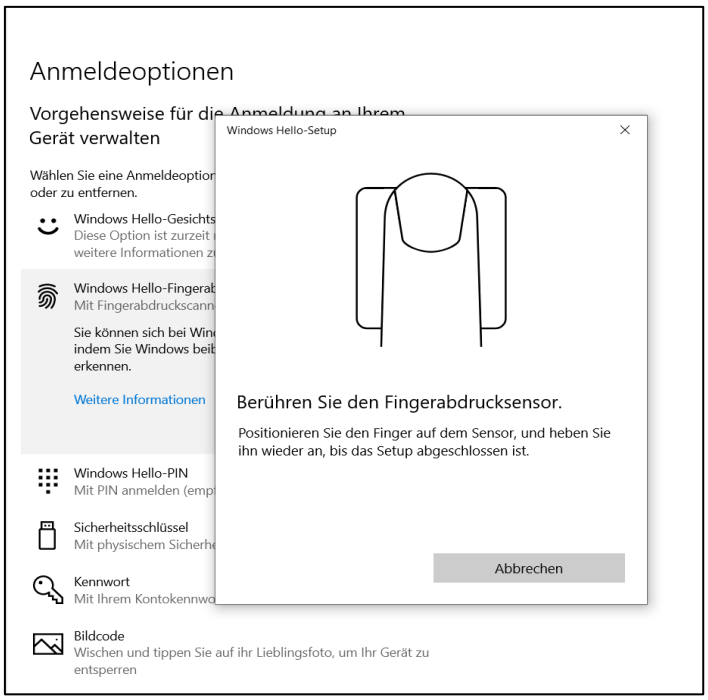

Abb. 20: Registrierung eines Fingerabdrucks I

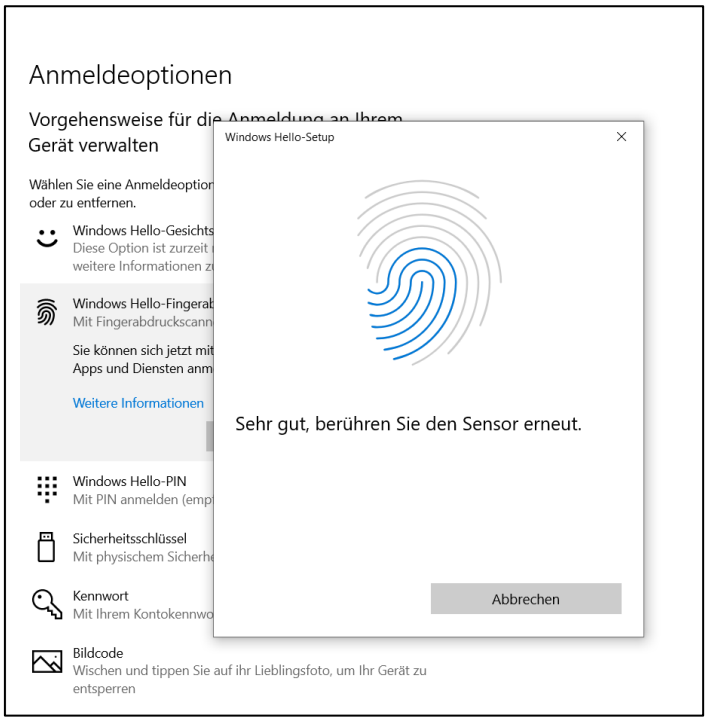

Abb. 21: Registrierung eines Fingerabdrucks II

Wurde der Fingerabdruck erfolgreich registriert, muss der Nutzer künftig kein Passwort mehr eintippen, um sich an seinem Windows-Rechner anzumelden. Für den Fall, dass der Fingerabdruck jedoch nicht zur Verfügung steht oder nicht funktioniert, bspw. durch Verletzungen oder Substanzen auf den Fingern, richtet Windows eine Art Rückfallebene ein. Dazu wird der Nutzer aufgefordert, eine PIN einzurichten, die ihn anstelle oder auch zusätzlich zum Fingerabdruck eindeutig identifiziert. Aus Sicherheitsgründen kann das Setup ohne die Einrichtung einer zusätzlichen PIN nicht abgeschlossen werden. Es soll der Fall vermieden werden, dass ein Nutzer ohne PIN nicht mehr auf sein Konto zugreifen könnte und ihm der Zugang zu seinem Endgerät verwehrt wäre.

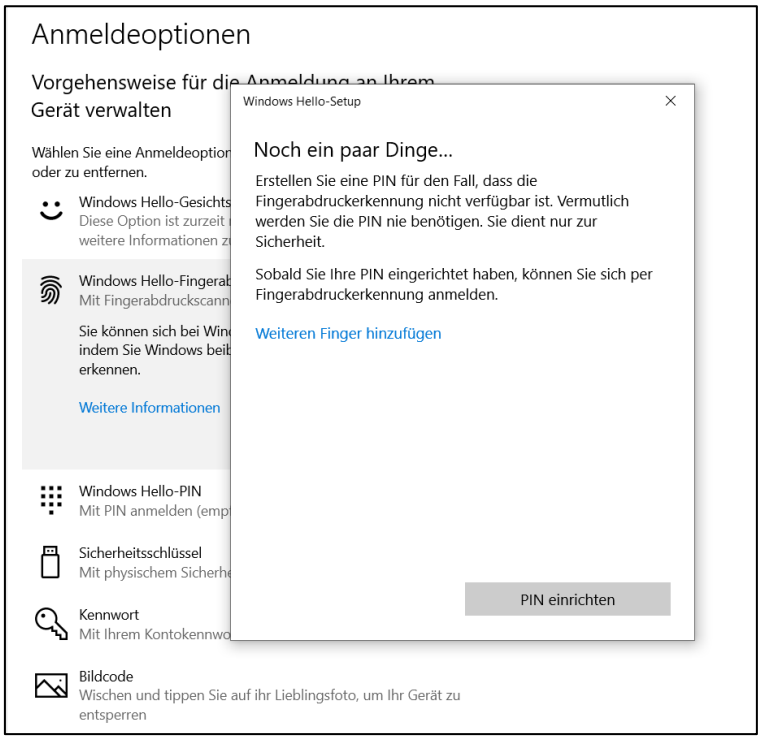

Abb. 22: Einrichtung einer PIN

Einrichtung des Sicherheitsschlüssels für das Microsoft-Online-Konto: Zur Authentifizierung am Microsoft-Online-Konto kann ein Nutzer einen externen Sicherheitsschlüssel verwenden. Dazu muss der Nutzer zunächst über den Browser zur Anmeldeseite von Microsoft navigieren und sich mittels E-Mail und Passwort anmelden.

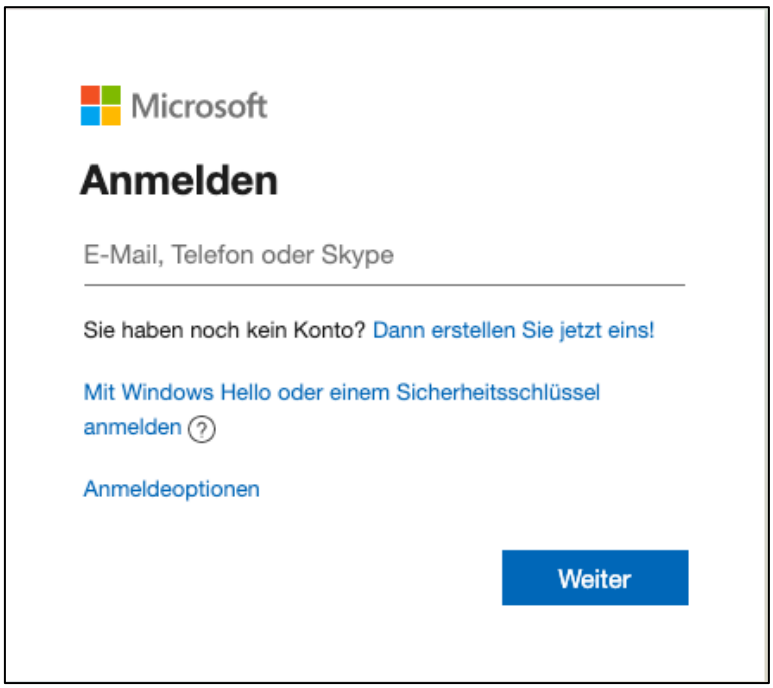

Abb. 23: Startseite Anmeldung Microsoft-Konto

Bei erfolgreicher Anmeldung kann der Nutzer am oberen Rand des Bildschirms in den Bereich „Sicherheit“ navigieren.

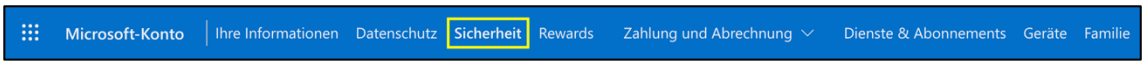

Abb. 24: Navigationsleiste Microsoft-Konto

Nach dem Anklicken des Sicherheits-Icons werden dem Nutzer eine Reihe von Sicherheitsfunktionen geboten, die auf das Microsoft-Konto angewandt werden können. Die Funktion „Windows Hello und Sicherheitsschlüssel“ befindet sich mittig in der Ansicht. Über die Option „Sicherheitsschlüssel einrichten“ erreicht der Nutzer das Setup zum Registrieren eines externen Sicherheitsschlüssels. Die Option „Windows Hello einrichten“ ermöglicht das Nutzen des internen Sicherheitsschlüssels auf dem Laptop oder Smartphone. Dazu können die bereits bestehenden biometrischen Authentifizierungsverfahren genutzt werden, sofern ein Nutzer diese vorab eingerichtet hat. Alternativ wird ein Setup zum Registrieren, bspw. des Fingerabdrucks, eingeleitet. Das Registrieren beider Optionen verläuft sehr ähnlich, sodass eine Option beispielhaft für das jeweils andere Registrierungsverfahren genutzt werden kann.

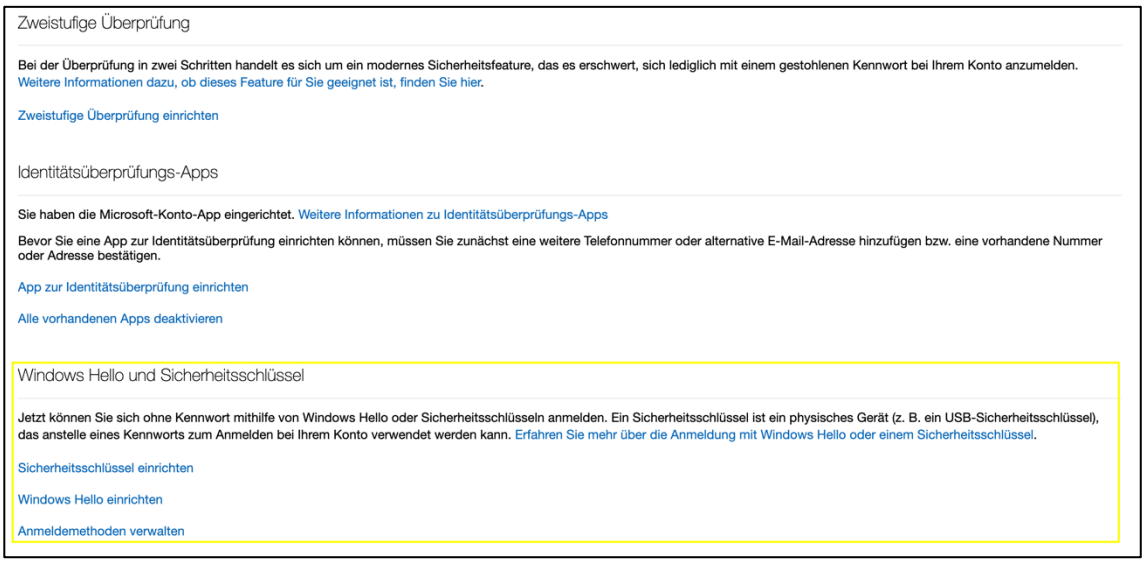

Abb. 25: Auswahl Sicherheitsalternativen

Nach Auswahl der Option „Sicherheitsschlüssel einrichten“ beginnt das Setup zum Einrichten des Sicherheitsschlüssels. In einem ersten Schritt muss der Nutzer das Transportprotokoll auswählen, welches der Sicherheitsschlüssel unterstützt. Microsoft unterstützt dazu die Protokolle USB und NFC und erläutert kurz dessen Anwendung.

Abb. 26: Auswahl der unterstützten Transportprotokolle

Hat sich der Nutzer über das Anklicken einer Auswahlmöglichkeit und des „Weiter-Button“ für eine der beiden Optionen entschieden, muss der Sicherheitsschlüssel entsprechend seines Transportprotokolls mit dem Endgerät verbunden werden. In diesem Beispiel wird ein USB-Sicherheitsschlüssel verwendet.

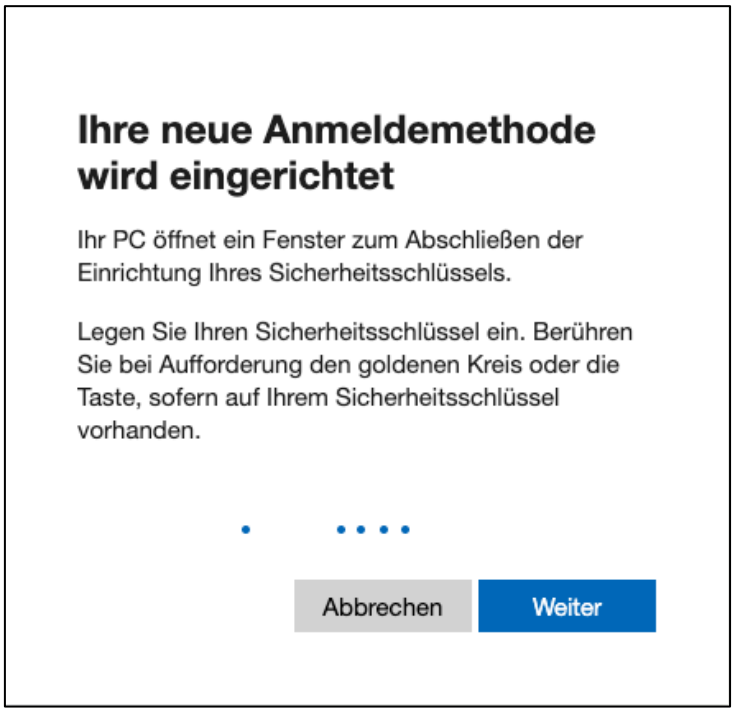

Abb. 27: Ihre neue Anmeldemethode wird eingerichtet

Der Nutzer wird zunächst aufgefordert, eine PIN einzutragen. Diese PIN stellt eine weitere Authentifizierungsmethode zusätzlich zum Sicherheitsschlüssel dar und soll den Nutzer eindeutig identifizieren. Wie bereits erläutert, kann einem Sicherheitsschlüssel, bspw.

über die Einstellungen in Windows Hello oder dem jeweiligen Browser, eine universelle PIN eingerichtet und zugeordnet werden. Diese PIN wird fest mit dem Sicherheitsschlüssel verbunden, gilt für jeden Online-Dienst und muss bei jedem Authentifizierungsvorgang eingegeben werden. Hat der Nutzer keine PIN vergeben, entfällt die Multifaktor-Authentifizierung.

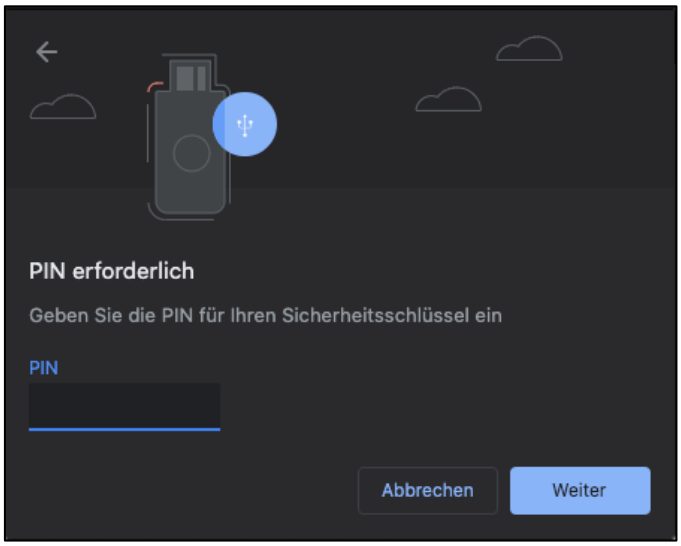

Abb. 28: PIN-Eingabe Sicherheitsschlüssel

Nach erfolgreicher PIN-Eingabe muss der Nutzer anschließend eine Anwesenheitsgeste ausführen. In den gängigsten Fällen besitzt der Sicherheitsschlüssel einen Knopf bzw. eine Druckfläche, die der Nutzer antippen muss. Zur Orientierung kann die zu berührende Fläche auf dem Sicherheitsschlüssel aufblinken.

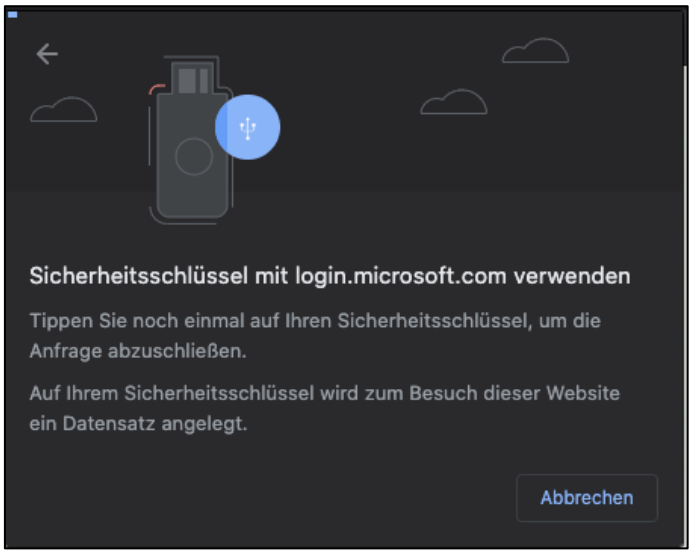

Abb. 29: Ausführung der Bestätigungsgeste

Wurde die Geste ausgeführt, muss der Nutzer dem Online-Dienst lediglich den Zugriff auf die im Sicherheitsschlüssel aufbewahrten Daten freigeben.

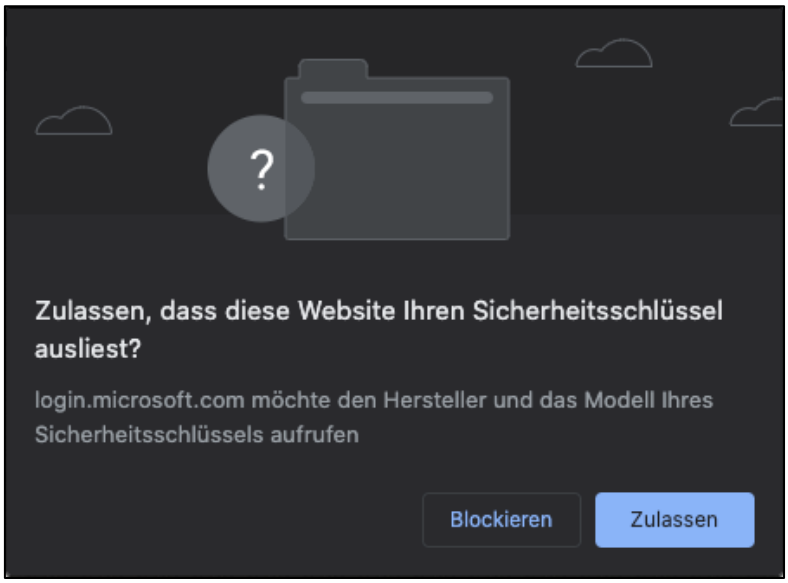

Abb. 30: Zugriff auf Sicherheitsschlüssel gewähren

Anschließend darf der Nutzer einen Namen für seinen Sicherheitsschlüssel vergeben. Der Name dient der Orientierung für den Fall, dass ein Nutzer mehrere Sicherheitsschlüssel besitzt und evtl. Konten mehrfach über Sicherheitsschlüssel absichert.

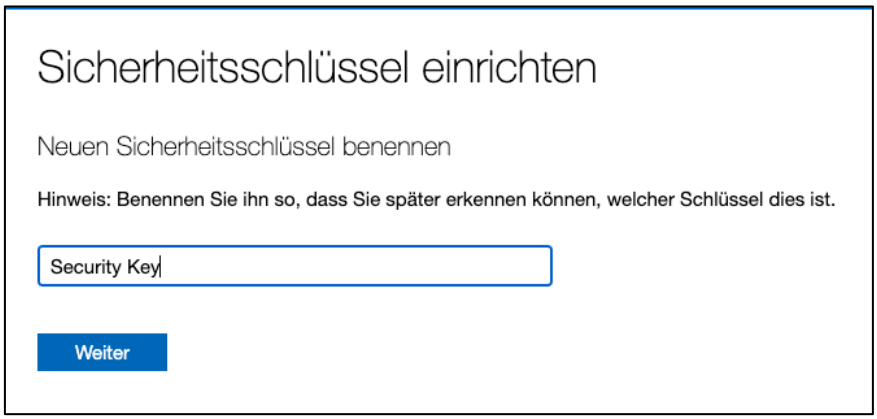

Abb. 31: Neuen Sicherheitsschlüssel benennen

Hat der Nutzer seinen Sicherheitsschlüssel benannt, ist die Registrierung des Sicherheitsschlüssels abgeschlossen und das Setup wird beendet. Ab dem nächsten Anmeldeversuch kann sich der Nutzer über seinen Sicherheitsschlüssel authentifizieren, ohne ein Passwort verwenden zu müssen.

Abb. 32: Registrierung abgeschlossen

5 Ausblick

„Warum sollte ich mir ein neues Passwort zulegen? Mit meinem alten Passwort komme ich sehr gut zurecht und bisher ist noch nie etwas passiert!“

So ähnlich klingt es, wenn Internet-Nutzer auf schlechte bzw. Passwörter im Allgemeinen angesprochen werden. Die Resistenz der Nutzer ist groß und solange Passwörter standardmäßig als Authentifizierungsverfahren genutzt werden, wollen die Nutzer ihr Verhalten dahingehend nicht verändern. Auch Möglichkeiten wie Passwortmanager oder eine simple Zwei-Faktor-Authentifizierung werden nur in wenigen Fällen genutzt. Eine Zwei-Faktor-Authentifizierung wie FIDO U2F ist zwar die nächst beste Alternative zu klassischen Authentifizierungsverfahren, beinhaltet jedoch immer noch passwortbasierte Risiken. Zusätzlich wähnen sich viele Nutzer aufgrund des zweiten Faktors in Sicherheit, sodass häufig auf ein sicheres Passwort verzichtet wird.

Diese Problematik ist in der Praxis bekannt und rückt zunehmend in den Fokus von Unternehmen und Sicherheitsexperten - einerseits zur Vermeidung von Datendiebstahl aufgrund schlechter Passwörter der Kunden und andererseits aber auch durch unvorsichtiges Handeln der eigenen Mitarbeiter. [79] Dies ist vor allem der Tatsache geschuldet, dass immer mehr Geschäftsprozesse oder ganze Geschäftsmodelle vollkommen digital und mittels Internet ablaufen. Somit steigt auch das Risiko digitaler Angriffe durch Dritte exponentiell an, sodass das Sicherheitsmanagement eine immer größere und wichtigere Rolle einnimmt bzw. einnehmen muss. Viele Versuche sichere Alternativen zur Authentifizierung im Web zu standardisieren und großflächig anzubieten, schlugen fehl oder wurden schlichtweg einfach nicht angenommen. So sind andere bisherige Alternativen der Multi-Faktor-Authentifizierung weiterhin anfällig für Phishing-Attacken oder sind aus Sicht der Nutzer zu umständlich oder aufwendig.[80]

Auf Basis der Studie zum Akzeptanzverhalten von Camp/Dingman/Sanchari[81] kann es durchaus sinnvoll erscheinen, einheitliche FIDO2-Anwendungen zu implementieren. Das bedeutet, dass sowohl Hersteller von FIDO2-Geräten als auch Online-Dienste versuchen sollten, einheitliche Prozesse zur Einrichtung und Verwaltung zu entwickeln. Hierzu könnten die FIDO-Allianz oder das W3C zur Unterstützung herangezogen werden. Ziel

79 Vgl. Truta, Filip: Passwords Remain the Main Method of Authentication and Top Cause of Data Breaches, Online im Internet: https://businessinsights.bitdefender.com/passwords-remain-the-main-method-of-authentication-and-top-cause-of-data-breaches, 10.03.2020.

80 Vgl. Süddeutsche Zeitung (Hrsg.): Wie wir und in Zukunft im Social Web authentifzieren; Online im Internet: https://advertorial.sueddeutsche.de/internet-sicherheit/Wie-wir-uns-in-Zukunft-im-Social-Web-authentifizieren/, abgerufen am 25.08.2020.

81 Camp, L. Jean; Dingman, Andrew; Sanchari, Das: Why Jonny Doesn’t Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key, Online im Internet: https://fc18.ifca.ai/preproceedings/111.pdf, abgerufen am 05.07.2020.

sollte es sein, die Hürden der durch die Nutzer unzureichend wahrgenommenen Anwenderfreundlichkeit von FIDO2 abzubauen.

Experten sind sich einig, dass der neue Web-Standard FIDO2 das Thema „Web-Authentifizierung“ weiter vorantreibt und die Sicherheit erhöht. Langfristig besitzt FIDO2 durchaus das Potenzial, eine wichtige Rolle im Bereich der Sicherheit von IT-Systemen einzunehmen. Dennoch wird es Zeit benötigen, dass der Standard vollkommen an die Gegebenheiten angepasst wird und die Nutzer daran vollends teilhaben können. Ein erster Schritt in diese Richtung muss von den Unternehmen und Online-Diensten getätigt werden. Nur diese sind in der Lage, Nutzern die Relevanz der Thematik zu vermitteln, indem sie die Technologie anbieten. Je mehr Online-Dienste kompatibel zu FIDO2 werden, desto mehr Nutzer werden mit der Technologie in Kontakt kommen. Dies bedingt eine höhere Bekanntheit unter den Nutzern und führt zu einer größeren Wahrscheinlichkeit, hinreichend akzeptiert zu werden. Je höher die Akzeptanz ist, desto mehr Nutzer wollen auch an den Vorteilen der Technologie partizipieren und werden FIDO2 verstärkt verwenden. Nutzer können dabei bspw. privat oder auch im Unternehmen untereinander ihre Erfahrungen mit FIDO2 teilen und sich somit gegenseitig der Technologie näherbringen. Daraus resultiert weiter ein verstärktes Angebot der FIDO2-Technologie seitens der Online-Dienste, um die Bedürfnisse der Kunden zu erfüllen. Abgeschwächt werden könnte dieser Effekt jedoch durch die Tatsache, dass nur solche Nutzer FIDO2 verwenden können, die Besitzer neuerer Hard- und Software sind, die FIDO2 auch unterstützen.

Dass die großen Unternehmen der FIDO-Allianz erste Versuche und konkrete Umsetzungen gestartet haben, kann dabei als erster Schritt der Verbreitung von FIDO2 betrachtet werden. Dennoch müssen auch andere Unternehmen diesem Trend folgen. Doch bisher mangelt es noch an großflächiger Nutzung der Zwei-Faktor-Authentifizierung, was einen schnellen Ausbau auf FIDO2 beeinträchtigen kann, bzw. das Vertrauen in passwortlose Authentifizierungsmethoden bisher nicht steigern konnte. Eine schnelle Adaption von FIDO2 kann somit bedeutend erschwert werden.

Mittelfristig lassen sich Passwörter aus dem Unternehmenskontext nicht eliminieren. Einerseits sind Passwörter in Unternehmen in unterschiedlichsten Systemen auf vielen Hierarchieebenen im Einsatz, andererseits müssen zunächst die zur Umsetzung benötigten Ressourcen wie bspw. Knowhow, Hard- und Software und Kapital beschafft und freigesetzt werden. Eine Umsetzung von FIDO2 lässt sich somit nur sukzessiv erzielen und sollte unbedingt unter Einbezug der Mitarbeiter vorgenommen werden. Nur Mitarbeiter,

die verstehen, was hinter der FIDO2-Technologie steckt, können FIDO2 effizient und komfortabel zur Risikominimierung anwenden.[82]

82 Vgl. Micijevic, Anis: Digitale Revolution - Diese Technologie könnte Passwörter überflüssig machen, Online im Internet: https://www.handelsblatt.com/technik/digitale-revolution/digitale-revolution-diese-technologie-koennte-passwoerter-ueberfluessig-machen/25455626.html, 22.01.2020 und vgl. Klaus, Lena: FIDO2 – Zukunft ohne Passwort, Online im Internet: https://it-service.network/blog/2019/09/26/fido2/, 26.09.2019.

Literaturverzeichnis

1. **Becker, Leo:** Smart Lock: iPhone wird Security-Key für Google-Accounts, Online im Internet: https://www.heise.de/mac-and-i/meldung/Smart-Lock-iPhone-wird-Security-Key-fuer-Google-Accounts-4638509.html, 15.01.2020.
2. **Bundesamt für Sicherheit in der Informationstechnik (Hrsg):** Das Trusted Platform Module (TPM), Online im Internet: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/TrustedComputing/TrustedPlatformModuleTPM/TrustedPlatformModuleTPM/aufbaustruktur.html, abgerufen am 01.05.2020.
3. **Bundesamt für Sicherheit in der Informationstechnik (Hrsg):** Identitätsmanagement mit sicherer Authentifizierung und Attributweitergabe, Online im Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/14ter/Vortraege-20-05-2015/Moritz_Platt.pdf?__blob=publicationFile&v=1, 17.05.2020.
4. **Bundesamt für Sicherheit in der Informationstechnik (Hrsg):** Zwei-Faktor-Authentisierung für höhere Sicherheit, Online im Internet: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/Zwei_Faktor_Authentisierung/Zwei-Faktor-Authentisierung_node.html, abgerufen am 08.06.2020.
5. **Camp, L. Jean; Dingman, Andrew; Sanchari, Das:** Why Jonny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key, Online im Internet: https://fc18.ifca.ai/preproceedings/111.pdf, abgerufen am 05.07.2020.
6. **De Orchi, Tommaso; Schmitz, Peter:** FIDO2 bringt den passwortlosen Login, Online im Internet: https://www.security-insider.de/fido2-bringt-den-passwortfreien-login-a-753106/, 16.10.2018.
7. **Eckert, Claudia:** IT-Sicherheit – Konzepte – Verfahren - Protokolle, 8. Auflage, München: Oldenbourg Verlag 2013, S. 12 f.
8. **Eikenberg, Ronald:** Schlüssel zum Glück – Was schon heute mit dem Passwortkiller FIDO2 geht, in: c't, 18/2019, S. 20-24.
9. **Eikenberg, Ronald:** Online-Schlüssel – FIDO2-Sicherheitsschlüssel zum Einloggen ohne Passwort, in: c't 25/2019, S. 66-73.
10. **Eikenberg; Ronald; Schmidt, Jürgen:** FAQ: Sicher einloggen mit FIDO2, Online im Internet:https://www.heise.de/ct/artikel/FAQ-Sicher-einloggen-mit-FIDO2-4547137.html, 16.10.2019.

11. **Feilner, Markus:** Passwortfreie Auth-Verfahren: FIDO 2 und Webauthn, Online im Internet: https://www.linux-magazin.de/ausgaben/2018/08/webauthn/5/, abgerufen am 30.07.2020.

12. **FIDO-Allianz (Hrsg):** Alliance Overview, Online im Internet: https://fidoalliance.org/overview/, abgerufen am 03.05.2020.

13. **FIDO-Allianz (Hrsg):** Client to Author Protocol, Online im Internet: https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html#conformance, 30.01.2019.

14. **FIDO-Allianz (Hrsg):** FIDO Members, Online im Internet: https://fidoalliance.org/members/, abgerufen am 03.05.2020.

15. **FIDO-Allianz (Hrsg):** FIDO® Certified, Online im Internet: https://fidoalliance.org/certification/fido-certified-products/, abgerufen am 24.07.2020.

16. **FIDO-Allianz (Hrsg):** FIDO UAF Achitectural Overview, Online im Internet: https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-uaf-overview-v1.1-ps-20170202.html#fido-uaf-client, 02.02. 2017.

17. **FIDO-Allianz (Hrsg):** FIDO2: WebAuthn & CTAP, Online im Internet: https://fidoalliance.org/fido2/, abgerufen am 13.06.2020.

18. **FIDO-Allianz (Hrsg):** FIDO2: Web Authentication (WebAuthn), Online im Internet: https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/, abgerufen am 01.05.2020.

19. **FIDO-Allianz Hrsg):** Universal Second Factor (U2F) Overview: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/FIDO-U2F-COMPLETE-v1.2-ps-20170411.pdf, 11.04.2017.

20. **FIDO-Allianz (Hrsg):** What makes FIDO different, online im Internet: https://fidoalliance.org/key-differentiators/, abgerufen am 29.04.2020.

21. **Gadatsch, Andreas; Mangiapane, Markus:** IT- Sicherheit – Digitalisierung der Geschäftsprozesse und Informationssicherheit, Wiesbaden: Springer Verlag 2017.

22. **Geißler, Otto:** Was ist Skalierbarkeit, Online im Internet: https://www.datacenter-insider.de/was-ist-skalierbarkeit-a-852037/, abgerufen am 14.07.2020.

23. **GitHub (Hrsg):** https://github.com/strangerlabs/webauthn, abgerufen am 11.06.2020.

24. **Handelsblatt (Hrsg):** Wie die Multifaktor-Authentifizierung die Sicherheit erhöht, Online im Internet: https://unternehmen.handelsblatt.com/multifaktor-authentifizierung.html, 23.09.2019.

25. **Hansen, Hans Robert; Mendling, Jan; Neumann, Gustaf:** Wirtschaftsinformatik, 11. Auflage, Berlin: Walter de Gruyter 2015.

26. **Heise (Hrsg):** The Transport Layer Security (TLS) Protocol Version 1.2, Online im Internet: https://www.heise.de/netze/rfc/rfcs/rfc5246.shtml, abgerufen am 30.05.2020.

27. **Ionos (Hrsg):** FIDO2: Der neue Standard für den sicheren Web-Log-in, Online im Internet: https://www.ionos.de/digitalguide/server/sicherheit/was-ist-fido2/, abgerufen am 30.05.2020.

28. **IT-Zoom (Hrsg.):** Das Ende des Passworts, online im Internet: https://www.it-zoom.de/sn/microsoft/e/das-ende-des-passworts-10312/, abgerufen am 29.04.2020.

29. **Kaltschmidt, Thomas:** Einloggen ohne Passwort – Mehr Schutz: Mac und iOS unterstützen FIDO2, in: Mac&i, 01/2020, S. 128-129.

30. **Kappes, Martin:** Netzwerk- und Datensicherheit – Eine praktische Einführung, 2. Auflage, Wiesbaden: Springer Verlag 2013.

31. **Klaus, Lena:** FIDO2 – Zukunft ohne Passwort, Online im Internet: https://it-service.network/blog/2019/09/26/fido2/, 26.09.2019.

32. **Költzsch, Tobias; Grüner, Sebastian:** Google führt Logins ohne Passwort ein, Online im Internet: https://www.golem.de/news/fido-google-fuehrt-logins-ohne-passwort-ein-1908-143169.html, 13.08.2019.

33. **Kratzenberg, Marco:** FIDO2: Login ohne Passwort? Wie es funktioniert und wer es braucht, Online im Internet: https://www.giga.de/artikel/fido2-login-ohne-passwort-wie-es-funktioniert-und-wer-es-braucht/, 27.09.2019.

34. **Krebs on Security (Hrsg.):** Hanging Up on Mobile in the Name of Security, Online im Internet: https://krebsonsecurity.com/2018/08/hanging-up-on-mobile-in-the-name-of-security/, 16.08.2018.

35. **Lindemann, Rolf:** Not built on Sand – How modern authentification complements federation, in: Lecture Notes in Informatics (LNI), 2013, S. 164-168.

36. **Luber, Stefan; Schmitz, Peter:** Was ist Authentifizierung? Online im Internet: https://www.security-insider.de/was-ist-authentifizierung-a-617991/, 26.06.2017.

37. **Luber, Stefan; Schmitz, Peter:** Was ist ein TPM?, Online im Internet: https://www.security-insider.de/was-ist-ein-tpm-a-811217/, 20.03.2019.

38. **Luber, Stefan; Schmitz, Peter:** Was ist Single Sign-on (SSO)?, Online im Internet: https://www.security-insider.de/was-ist-single-sign-on-sso-a-631479/, 03.08.2017.

39. **Luber, Stefan; Schmitz, Peter:** Was ist TOTP?, Online im Internet: https://www.security-insider.de/was-ist-totp-a-875708/, 24.10.2019.

40. **Mahn, Jan:** Zweifach abgesichert – FIDO2-Hardware einrichten und ausreizen, in: c't 25/2019, S. 74-77.

41. **Meinel, Christoph; Sack, Harald:** Sicherheit und Vertrauen im Internet – Eine technische Perspektive, Wiesbaden: Springer Verlag 2014.

42. **Mello, Stefan:** Office 365 vs. Office 2019 – Cloud- übertrifft Desktop-Version, Online im Internet: https://www.heise.de/brandworlds/cloud-services/office-365-vs-office-2019-cloud-uebertrifft-desktop-version/, 22.10.2019.

43. **Micijevic, Anis:** Digitale Revolution - Diese Technologie könnte Passwörter überflüssig machen, Online im Internet: https://www.handelsblatt.com/technik/digitale-revolution/digitale-revolution-diese-technologie-koennte-passwoerter-ueberfluessig-machen/25455626.html, 22.01.2020.

44. **Microsoft (Hrsg):** Announcing the public preview of Azure AD support for FIDO2-based passwordless sign-in, Online im Internet: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/announcing-the-public-preview-of-azure-ad-support-for-fido2/ba-p/746362, 07.10.2019.

45. **Microsoft (Hrsg):** Was ist Azure Active Directory, Online im Internet: https://docs.microsoft.com/de-de/azure/active-directory/fundamentals/active-directory-whatis, 05.06.2020.

46. **Paar, Christof; Pelzl, Jan:** Kryptografie verständlich – Ein Lehrbuch für Studierende und Anwender, Berlin Heidelberg: Springer Vieweg 2016.

47. **Pereira, Olivier; Rochet, Florentin; Wiedling, Cyrille:** Formal Analysis of the FIDO 1.x Protocol, Online im Internet: https://fps2017.loria.fr/wp-content/uploads/2017/10/04.pdf, abgerufen am 14.06.2020.

48. **Petrlic, Ronald; Sorge, Christoph:** Datenschutz – Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, Wiesbaden: Springer Verlag 2017.

49. **Rehm, Stefan-Marc:** Integrität in der Informationssicherheit, Online im Internet: https://www.haufe.de/compliance/management-praxis/integritaet-informationssicherheit_230130_482556.html, 29.01.2019.

50. **Russel, Aaron:** What is an X.509 Certificate?, Online im Internet: https://www.ssl.com/faqs/what-is-an-x-509-certificate/, 23.09.2019.

51. **Sackmann, Stefan:** IT-Sicherheit, Online im Internet: https://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/technologien-methoden/Informatik--Grundlagen/IT-Sicherheit/index.html/?searchterm=sicherheit, abgerufen am 05.05.2020.

52. **Schick, Lukas; Schwickert, Axel:** macOS – Verschlüsseln, Entschlüsseln und Signieren von E-Mails, Gießen: Arbeitspapiere Wirtschaftsinformatik 4/2020.

53. **Schmidt, Jürgen:** Abschied vom Passwort – Passwortloses Anmelden dank FIDO2, in: c't, 18/2019, S. 16-18.

54. **Schmidt, Jürgen:** Verschlossen, nicht verrammelt – So funktioniert der passwortlose Login mit FIDO2, in: c't 18/2019, S. 30-32.

55. **Schmoranz, Paul; Schick, Lukas; Schwickert, Axel:** Hybride Verschlüsselung im Web – Grundlagen, Verfahren und Anwendungsgebiete, Gießen: Arbeitspapiere Wirtschaftsinformatik, 2/2020.

56. **Schwan, Ben:** iOS 13.3: Safari unterstützt diverse Sicherheitskeys, Online im Internet: https://www.heise.de/mac-and-i/meldung/iOS-13-3-Safari-unterstuetzt-diverse-Sicherheitskeys-4584820.html, 13.11.2019.

57. **Sorge, Christoph; Gruschka, Nils; Lo Iacona, Luigi:** Sicherheit in Kommunikationsnetzen, München: Oldenbourg Verlag 2013.

58. **Spitz, Stephan; Pramateftakis, Michael; Sowboda, Joachim:** Kryptographie und IT-Sicherheit – Grundlagen und Anwendung, 2, überarbeitete Auflage, Wiesbaden: Vieweg + Teubner, Springer Verlag, 2011.

59. **Statista (Hrsg.):** https://de.statista.com/themen/111/suchmaschinen/Statistiken zu Suchmaschinen, Online im Internet: 11.11.2019.

60. **Steele, Nick:** Developments to WebAuthn and the FIDO2 Framework, Online im Internet: https://duo.com/blog/developments-to-webauthn-and-the-fido2-framework, 02.10.2018.

61. **Süddeutsche Zeitung (Hrsg.):** Wie wir und in Zukunft im Social Web authentifizieren; Online im Internet: https://advertorial.sueddeutsche.de/internet-sicherheit/Wie-wir-uns-in-Zukunft-im-Social-Web-authentifizieren/, abgerufen am 25.08.2020.

62. **Truta, Filip:** Passwords Remain the Main Method of Authentication and Top Cause of Data Breaches, Online im Internet: https://businessinsights.bitdefender.com/passwords-remain-the-main-method-of-authentication-and-top-cause-of-data-breaches, 10.03.2020.

63. **Tsolkas, Alexander; Schmidt, Klaus:** Rollen und Berechtigungskonzepte – Identity- und Access-Management im Unternehmen, 2. Auflage, Wiesbaden: Springer Verlag 2017.

64. **TÜV-SÜD (Hrsg):** Deutsche Unternehmen sind beliebtes Ziel für Phishing-Angriffe, Online im Internet: https://www.tuvsud.com/de-de/presse-und-medien/2020/juli/deutsche-unternehmen-sind-beliebtes-ziel-fuer-phishing-angriffe, 07.07.2020.

65. **von Westernhagen, Olivia:** Anmeldung ohne Passwort: „Windows Hello“ wird zum FIDO2-Authenticator, Online im Internet: https://www.heise.de/security/meldung/Anmeldung-ohne-Passwort-Windows-Hello-wird-zum-FIDO2-Authenticator-4418470.html, 10.05.2019.

66. **WebAuthn Guide (Hrsg):** WebAuthn, Online im Internet: https://webauthn.guide, 12.06.2020.

67. **Wendzel, Steffen:** IT-Sicherheit für TCP/IP- und IoT-Netzwerke – Grundlagen, Konzepte, Protokolle, Härtung, Wiesbaden: Springer Verlag 2018.

68. **Wigleven, Pieter:** Windows Hello and FIDO2 Security Keys enable secure and easy authentication for shared devices, Online im Internet: https://www.microsoft.com/en-us/microsoft-365/blog/2018/04/17/windows-hello-fido2-security-keys/, 17.04.2018.

69. **Windeck, Christoph:** Sicherheitschips stärken oder ersetzen Passwörter, Online im Internet: https://www.heise.de/ct/artikel/Sicherheitschips-staerken-oder-ersetzen-Passwoerter-4637602.html, 27.01.2020.

70. **W3C (Hrsg)**: Web Authentication: An API for accessing Public Key Credentials Level1, Online im Internet: https://www.w3.org/TR/webauthn-1/, 04.03.2019.

71. **W3C (Hrsg):** W3C MISSION, Online im Internet: https://www.w3.org/Consortium/mission.html#principles, abgerufen am 03.05.2020.

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: http://wi.uni-giessen.de

Herausgeber: Prof. Dr. Axel Schwickert
Prof. Dr. Bernhard Ostheimer

c/o Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungs-, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr-, Vortrags- und Kolloquiumsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Prof. Dr. Axel Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Prof. Dr. Bernhard Ostheimer, Fachbereich Wirtschaft, Hochschule Mainz.

Hinweise: Wir nehmen Ihre Anregungen zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit einem der Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Web-Adresse
http://wi.uni-giessen.de/