WIKIPEDIA

# Zwei-Faktor-Authentisierung

Die **Zwei-Faktor-Authentisierung** (**2FA**), häufig auch *Zwei-Faktor-Authentifizierung* genannt, bezeichnet den Identitätsnachweis eines Nutzers mittels einer Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren). Typische Beispiele sind Bankkarte und PIN beim Geldautomaten, Fingerabdruck und Zugangscode in Gebäuden, oder Passphrase und Transaktionsnummer (TAN) beim Online-Banking. Die Zwei-Faktor-Authentisierung ist ein Spezialfall der Multi-Faktor-Authentisierung.

## Inhaltsverzeichnis



## Anwendung und Zweck

Insbesondere für sicherheitskritische Anwendungsbereiche wird die Zwei-Faktor-Authentisierung empfohlen, so beispielsweise vom deutschen Bundesamt für Sicherheit in der Informationstechnik in seinen IT-Grundschutz-Katalogen.[1] BSI für Bürger und die Stiftung Warentest empfehlen Verbrauchern aber inzwischen, Zwei-Faktor-Authentisierung für möglichst viele webbasierte Dienste bzw. Online-Portale zu nutzen.[2][3] Grund ist, dass Verbraucher häufig ungeeignete oder zu schwache Passwörter wählen und ein und dasselbe Kennwort für mehrere Benutzungskonten bzw. Web-Dienste nutzen.[4] Einmalpasswörter werden nach wenigen Sekunden oder Minuten ungültig – dies wehrt Angreifer ab, die Passwörter erspähen wollen, z. B. durch Mitlesen von Passwörtern bei der Eingabe oder durch einen Keylogger.

In Bankwesen wurde mit der EU-Zahlungsdiensterichtlinie die Zwei-Faktor-Authentisierung für den Europäischen Wirtschaftsraum 2018 verpflichtend eingeführt.[5] Auch Webplattformen wie Amazon[6] oder Google[7] und E-Mail-Provider wie mail.de (seit 2012), posteo (seit 2014) oder mailbox.org bieten den Anwendern an, ihr Benutzerkonto durch Zwei-Faktor-Authentisierung zu schützen.

## Komponenten

Die Zwei-Faktor-Authentisierung ist nur dann erfolgreich, wenn zwei festgelegte Komponenten oder Faktoren zusammen eingesetzt werden und beide korrekt sind. Fehlt eine Komponente oder wird sie falsch verwendet, lässt sich die Zugriffsberechtigung nicht zweifelsfrei feststellen und der Zugriff wird verweigert.

Die Faktoren können sein:[8]

- *geheimnishütender Gegenstand (Besitz)*, wie zum Beispiel ein Sicherheits-Token, eine Bankkarte, eine App, die Einmalkennwörter generiert (siehe unten), oder ein physischer Schlüssel,
- *geheimes Wissen*, wie zum Beispiel ein Passwort, ein Einmalkennwort, eine PIN oder eine Transaktionsnummer (TAN),
- *biometrische Charakteristika (Inhärenz)*, wie zum Beispiel ein Fingerabdruck, das Muster einer Regenbogenhaut (Iris-Erkennung), die menschliche Stimme oder das Gangmuster.

# Mittelbare Zwei-Faktor-Authentisierung

Authentisierung über ein Sicherheits-Token als geheimnishütenden Gegenstand ist mit dem Nachteil behaftet, dass dieser *jederzeit* mitgeführt werden muss, sofern der Nutzer sich jederzeit anmelden können möchte. Wird der Gegenstand gestohlen, verloren oder hat der Nutzer ihn schlicht nicht dabei, sind Zugriffe unmöglich bzw. es entsteht ein hoher Aufwand. Zudem entstehen Kosten für die Erstanschaffung ebenso wie ggf. bei Ersatzbeschaffungen. Um diesen Risiken aus dem Weg zu gehen, ist die sogenannte *mittelbare Zwei-Faktor-Authentisierung* als Alternative entwickelt worden.[9][10] Sie nutzt Mobilgeräte wie Mobiltelefone und Smartphones als geheimnishütenden Gegenstand, also „etwas, was der Nutzer besitzt“ (aber auch verlieren kann). Da das Mobilgerät bei vielen Menschen heutzutage ein ständiger Begleiter ist, muss kein zusätzlicher Token angeschafft und beschützt werden.

Möchte sich der Anwender authentisieren, muss er meist eine Passphrase und ein einmalig gültiges, dynamisch erzeugtes Einmalkennwort eingeben. Diesen Code erhält er per SMS oder E-Mail auf sein Mobilgerät gesendet, oder (besser) die entsprechende App zur Zwei-Faktor-Authentisierung generiert das Einmalkennwort auf dem Mobilgerät.

Hat der Nutzer eine Ziffernfolge verwendet, wird diese automatisch gelöscht, und das System sendet einen neuen Code an das Mobilgerät. Wird der neue Code nicht innerhalb einer festgelegten Frist eingegeben, ersetzt ihn das System automatisch. Auf diese Weise verbleiben keine alten, schon verwendeten Codes auf der mobilen Komponente. Für noch gesteigerte Sicherheit lässt sich festlegen, wie viele Falscheingaben toleriert werden, bevor das System den Zugang sperrt.

Wenn der sich authentisierende Benutzer keine manuelle Dateneingabe mehr zu erledigen braucht, gilt der Prozess als *halbautomatisiert*. Das ist mit der NFC-Methode erreicht. Verwendet wird dazu ein zuvor personalisiertes Mobilgerät.

Erst dann, wenn der sich authentisierende Benutzer keinerlei Handhabung mehr zu erledigen braucht, gilt der Prozess als *vollautomatisiert*. Das ist mit dem Verwenden von Piconetzen (Bluetooth) als internationaler Industrie-Standard erreicht. Verwendet wird dazu ein zuvor personalisiertes Mobilgerät.[11]

# Apps zur Zwei-Faktor-Authentisierung mittels zeitbasierten Einmalkennwörtern (TOTP)

Zunächst installiert der Anwender auf dem mobilen Endgerät, das zur mittelbaren Zwei-Faktor-Authentisierung gegenüber einem oder mehreren webbasierten Diensten verwendet werden soll, eine entsprechende App. Sodann kann ein webbasierter Dienst durch Zwei-Faktor-Authentisierung geschützt werden, indem man die App beim Dienst als zweiten Faktor registriert. Dazu tauschen der Sicherheits-Server des Dienstes und das Endgerät eine Zeichenfolge als *Geheimnis* oder *Token* aus – z. B. indem man mit den Mobilgerät einen QR-Code scannt oder eine entsprechende, vom Sicherheits-Server angezeigte

Zeichenfolge händisch eintippt. Nach diesem ersten Schritt ist das *Geheimnis* im Idealfall nur noch dem Sicherheits-Server und dem persönlichen Gerät des Nutzers bekannt und sollte diesen Speicher auch nie verlassen. Nach einem entsprechenden Funktionstest schaltet der Web-Dienst die Zwei-Faktor-Authentisierung für das Benutzerkonto aktiv.

Will der Benutzer den webbasierten Dienst nun nutzen, wird er – nach Eingabe seines Benutzernamens und Passworts – aufgefordert, ein von der App generiertes Einmalpasswort als zweiten Faktor zur Authentisierung einzugeben. Die App berechnet das Einmalpasswort aus der aktuellen Uhrzeit und dem *Geheimnis*. Aus diesem Grund müssen die Uhren von Client und Server ungefähr synchron sein. In der Regel funktioniert der Vorgang auch im Flugmodus. Der unten stehende Pseudocode liefert pro 30 Sekunden ein neues Passwort. In der Praxis kann der Server so programmiert werden, auch den Vorgänger- und Nachfolger-Code zu akzeptieren, um Zeitabweichungen des Clients von bis zu einer Minute abzudecken. Das zum Erzeugen des Einmalpassworts notwendige Geheimnis wird nicht mehr übertragen und kann deswegen auch nicht abgehört werden.

Es gibt heute eine Reihe von Apps zur Zwei-Faktor-Authentikation via TOTP, einige davon können auf einer großen Zahl von Plattformen eingesetzt werden. Diese Apps implementieren die offenen Standards HOTP (RFC 4226) und TOTP (RFC 6238), wodurch sie gegenüber jedem Webdienst benützt werden können, dessen Sicherheits-Server diese Standards implementiert.

| App | unterstützte Plattformen | Import/Export-Funktion? | Anmerkungen |
|---|---|---|---|
| Google Authenticator | Android, iOS, Blackberry OS | ja[12] | Login in Google-Konten per Push-Notifikation. Für Android entwickelt, war die App ursprünglich bis Version 2.21 Open Source, später wurde sie proprietär. |
| andOTP | Android | ja[13][14] | Open Source |
| FreeOTP Authenticator | Android (zuletzt aktualisiert am 25. Januar 2016) und iOS | keine[15] | Die Open-Source-Software wurde basierend auf der Version des Google Authenticators, die über das GitHub Verzeichnis verfügbar war, entwickelt.[16][17] FreeOTP wird von Red Hat zur Verfügung gestellt. |
| FreeOTP+ | Android | ja | Die Open-Source-Software FreeOTP+ ist ein Fork von FreeOTP, welcher Erweiterungen integriert.[18] |
| Aegis Authenticator | Android | ja | Quelloffene App mit Importmöglichkeit von anderen Apps.[19] |
| Authy (Twilio) | Android, BlackBerry OS, iOS, Windows, Mac OS und Linux | ja | Die Geheimnisse / Token werden (verschlüsselt) in der Cloud gespeichert, dadurch auf mehreren Geräten parallel verwendbar. |
| Microsoft Authenticator | Android und iOS[20] | ja[21] | Login in das Microsoft-Konto per Push-Notifikation |

Auch Passwort-Manager wie LastPass, Bitwarden oder 1Password unterstützen inzwischen Zwei-Faktor-Authentisierung gegenüber Dritten.

# Universelle Zwei-Faktor-Authentisierung

Die FIDO-Allianz hat am 9. Dezember 2014 die erste Version des universellen und lizenzfreien Standards U2F für die Zwei-Faktor-Authentisierung veröffentlicht, die mit verschiedenen Verfahren und Geräten kompatibel ist.[22] Im Februar 2015 kündigte Microsoft an, dass der Standard 2.0 der FIDO-Allianz für die Authentifikation im Internet vom Betriebssystem Windows 10 unterstützt wird.[23]

# Sicherheitsaspekte

Sicherheitsexperten geben zu bedenken, dass SMS-Spoofing und Man-in-the-Middle-Angriffe, bei denen ein Angreifer eine gefälschte Login-Seite präsentiert, verwendet werden können, um in Systeme mit Zwei-Faktor-Authentisierung, die auf Einmalkennwörtern basieren, einzubrechen.[24] FIDO U2F bietet hier zusätzlichen Schutz.

Die beiden Faktoren sollten durch zwei getrennte Übertragungskanäle übermittelt werden.[25] Der Forderung, dass sie nicht am gleichen Ort gespeichert bzw. aufbewahrt werden, wird heute oft nicht mehr nachgekommen, so nutzen zahlreiche Banken heute die E-Banking-App und die App für die Zwei-Faktor-Authentisierung per Einmalkennwort auf demselben Endgerät, sodass bei dessen Verlust nur noch ein etwaiger PIN-Code auf der 2FA-App die Banking-Anwendung schützt. Doch selbst wenn man die App für die Zwei-Faktor-Authentifizierung mittels TOTP auf demselben Gerät installiert hat, auf dem man den 2FA-gesicherten IT-Dienst nutzt, stellt dies einen Zugewinn an Sicherheit gegenüber der Authentisierung durch lediglich Anmeldename und Passwort dar – der sich aus der Einmaligkeit des Einmalpassworts ergibt. Die Nutzung der Authentisierungs-App über ein zweites Gerät verschafft jedoch zusätzlich die Sicherheit eines zweiten Faktors.

Außerdem erlauben die meisten Anbieter, bestimmte Rechner als vertrauenswürdige Clients zu definieren, von denen aus die Anmeldung ohne Einmalpasswort erfolgen darf. Kann ein Angreifer sich Zugang zu einem solchen Rechner verschaffen, ist der zusätzliche Schutz nicht mehr gegeben.

# Weblinks

- *Datenschutz im Netz: Doppelte Sicherung mit Zwei-Faktor-Authentifizierung.* (https://www.test.de/Datenschutz-im-Netz-Doppelte-Sicherung-mit-Zwei-Faktor-Authentifizierung-5177936-0/) In: *Stiftung Warentest.* 19. März 2019 (frei zugänglicher Schnelltest zum Thema).
- Verzeichnis von Websites, die Zwei-Faktor-Authentisierung unterstützen (https://2fa.directory/) (englisch)

# Einzelnachweise


1. SYS.2.1.M1 *Benutzerauthentisierung* (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/SYS/Umsetzungshinweise_zum_Baustein_SYS_2_1_Allgemeiner_Client.html#doc10095990bodyText5), BSI, IT-Grundschutz-Kompendium Edition 2020, abgerufen am 28. August 2020.
2. Zwei-Faktor-Authentisierung für höhere Sicherheit (https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/Zwei_Faktor_Authentisierung/Zwei_Faktor-Authentisierung.html). BSI für Bürger, Bundesamt für Sicherheit in der Informationstechnik
3. Online-Konten schützen mit 2FA. So funktioniert Zwei-Faktor-Authentifizierung (https://www.test.de/Online-Konten-schuetzen-mit-2FA-So-funktioniert-Zwei-Faktor-Authentifizierung-5177936-0/). Test.de, Stiftung Warentest, 11. Dezember 2020
4. one-time password (OTP) (https://searchsecurity.techtarget.com/definition/one-time-password-OTP). TechTarget Network
5. *Zwei-Faktor-Authentifizierung bei Online-Banking kommt. (https://futurezone.at/produkte/zwei-faktor-authentifizierung-bei-online-banking-kommt/245.442.457)* futurezone.at, 2. August 2017 (abgerufen 8. Juli 2019).
6. *Mehr Sicherheit: Amazon führt Zweifaktor-Authentifizierung ein. (https://www.derstandard.at/story/2000048795432/mehr-sicherheit-amazon-fuehrt-zweifaktor-authentifizierung-ein)* In: *Der Standard* online, 5. Dezember 2016.

7. *Zweiter Faktor: Nur wenige User sichern ihren Google-Account zusätzlich ab. (https://www.derstandard.at/story/2000072757014/zweiter-faktor-nur-wenige-user-sichern-ihren-google-account-zusaetzlich)* In: *Der Standard* online, 22. Januar 2018.
8. Zwei-Faktor-Authentifikation: So funktioniert sie (https://www.test.de/Internetsicherheit-Yubikey-kleiner-Schluessel-fuer-grossen-Schutz-4807972-4807984/), test.de, 28. Januar 2015, abgerufen am 20. Februar 2015
9. datenschutzticker.de (https://www.datenschutzticker.de/2020/04/zwei-faktor-authentifizierung/), 29. April 2020 (KINAST Rechtsanwälte)
10. Zwei-Faktor-Authentifizierung (https://www.virtual-solution.com/glossar/zwei-faktor-authentifizierung/) (Virtual Solution AG)
11. Michel Smidt: *Kurz erklärt: Sichere Logins mit Zwei-Faktor-Authentifizierung.* (https://www.univention.de/blog/2017/04/kurz-erklaert-zwei-faktor-authentifizierung/) In: *Univention Blog.* univention, 27. April 2017, abgerufen am 14. August 2018.
12. Stand Januar 2021, in der Version vom 12. Mai 2020
13. *Backup-format.* (https://github.com/andOTP/andOTP/wiki/Backup-format) In: *andOTP wiki.* Abgerufen am 2. Januar 2021 (englisch).
14. *Migration.* (https://github.com/andOTP/andOTP/wiki/Migration) In: *andOTP wiki.* Abgerufen am 2. Januar 2021 (englisch).
15. Stand Januar 2021, in der Version vom 25. Januar 2016
16. Willis, Nathan: FreeOTP multi-factor authentication (https://lwn.net/Articles/581086). LWN.net, 22 January 2014
17. FreeOTP (https://github.com/freeotp/freeotp-android/), github.com
18. FreeOTP+ bei F-Droid (https://f-droid.org/de/packages/org.liberty.android.freeotpplus/)
19. *Aegis Authenticator | F-Droid - Free and Open Source Android App Repository.* (https://f-droid.org/en/packages/com.beemdevelopment.aegis/) Abgerufen am 8. Oktober 2021 (englisch).
20. Microsoft Authenticator: So funktioniert die App (https://praxistipps.chip.de/microsoft-authenticator-so-funktioniert-die-app_112103). Von Nicole Hery-Moßmann, Chip.de, 29. Juni 2019
21. Back up and recover account credentials using the Microsoft Authenticator app (https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-backup-recovery). Microsoft Docs, 3. Juni 2020
22. FIDO 1.0 Specifications are Published and Final Preparing for Broad Industry Adoption of Strong Authentication in 2015 (https://fidoalliance.org/news/item/fido-1.0-specifications-published-and-final), FIDO-Allianz, abgerufen am 12. Dezember 2014
23. Dustin Ingalls: Microsoft Announces FIDO Support Coming to Windows 10 (https://web.archive.org/web/20150215215720/http://blogs.windows.com/business/2015/02/13/microsoft-announces-fido-support-coming-to-windows-10/) (Memento vom 15. Februar 2015 im *Internet Archive*), windows.com, abgerufen am 15. Februar 2015
24. one-time password (OTP) (https://searchsecurity.techtarget.com/definition/one-time-password-OTP). TechTarget Network
25. *Mehrfaktor-Authentifizierung. (https://www.onlinesicherheit.gv.at/praevention/konten_und_passwoerter/mehrfaktor-authentifizierung/249584.html)* A-SIT Zentrum für sichere Informationstechnologie, auf onlinesicherheit.gv.at; abgerufen 8. Juli 2018.

---