CyberSec
Multi-Factor Authentication / 2FA

Tobias Sattler
tobiassattler.com | cybersec.help

Multi-Factor (MFA) and Two-Factor Authentication (2FA)

Multi-Factor Authentication (**MFA**) is an **umbrella** term for Two-Factor Authentication (**2FA**) in which access authorization is verified by multiple independent characteristics (factors). Those factors are:

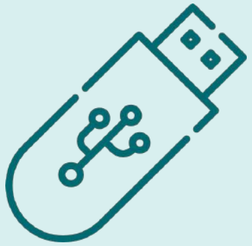
1	Knowledge	**something** only the user **knows**, e.g., password or pin code
2	Possession	something only the user **has**, e.g., mobile phone or credit card
3	Inherence	something only the user **is**, e.g., fingerprint or face id
4	Location	**somewhere** the user **is**, e.g., GPS location or specific Wi-Fi

The combination of 2 or more factors makes security a lot stronger.

How Multi-Factor Authentication works

1 LOGIN

2 AUTHENTICATE



USB Security Key

Text Message / OTP App

Phone Call

Fingerprint recognition

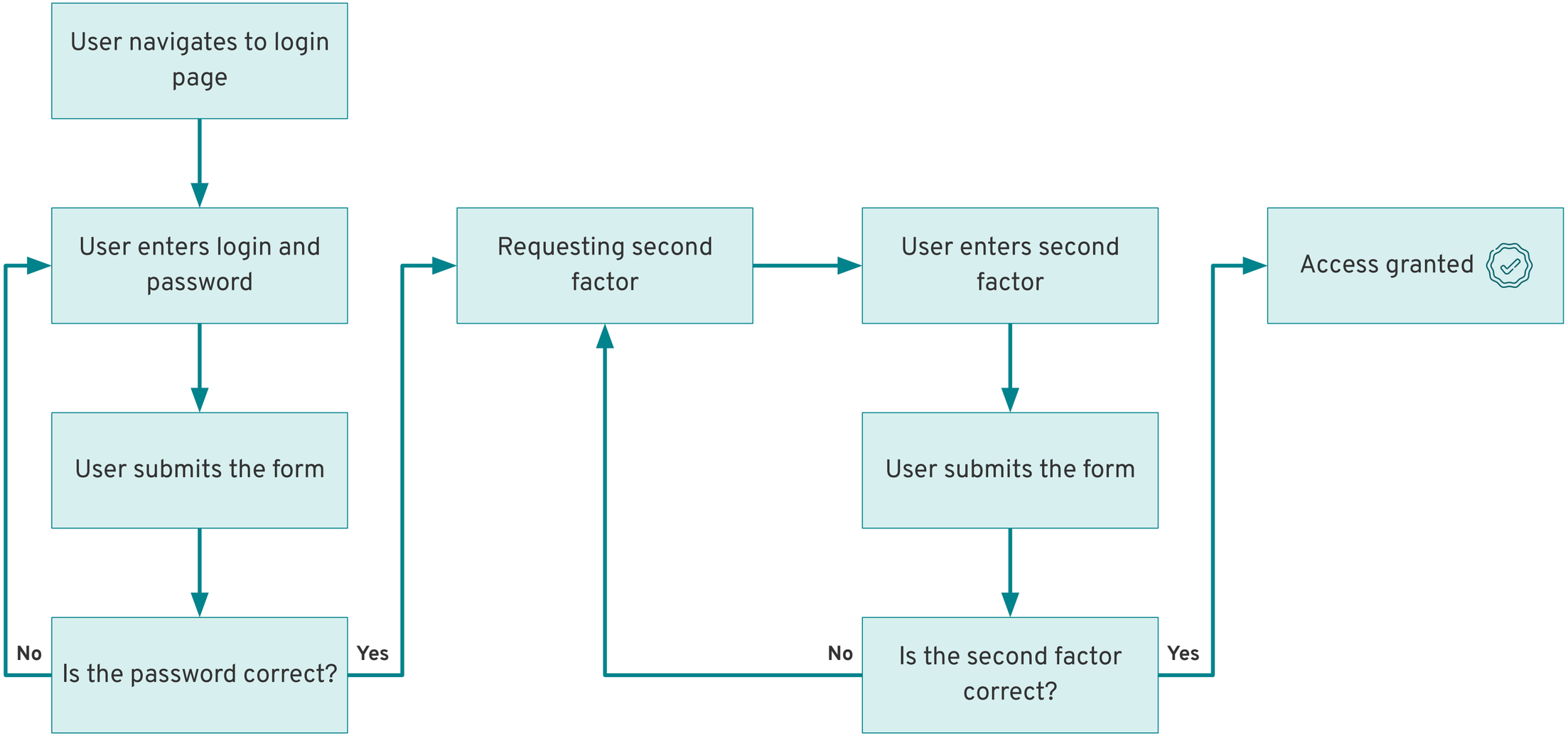
Face recognition

Hardware Token

3 ACCESS

After the login, an additional authentication method is necessary to complete the sign-in process.

Simplified MFA/2FA Flowchart for a website sign-in



One-Time Password (OTP)

1. A one-time password (OTP) is a **password** that is **valid** for a **specific period**, e.g., 60 seconds.
2. It can be used alone or combined with Multi-Factor Authentication (MFA) to add an **extra layer** of **security**.
3. An OTP is valid **only for single-use** and cannot be used a second time. Accordingly, each authentication or authorization requires a new one-time password.
4. There are **multiple implementations**, such as (1) SMS, (2) Hardware tokens, (3) Software tokens, and (4) Hard Copies.

OTP: SMS

1. It is a **standard technology** to deliver an OTP by SMS (Short Message Service).
2. However, this communication mode has **security flaws**, such as spoofing and man-in-the-middle. The National Institute of Standards and Technology (NIST) issued guidance to discourage the use.
3. Nevertheless, do not underestimate the **convenience**. The usage of a cell phone allows one to obtain a code very quickly.
4. Be aware that SMS is not the most secure method of authentication by itself because phone numbers can be recycled and sometimes hijacked.

OTP: Software tokens

1. Instead of SMS, you can retrieve an OTP with a **mobile app**, such as Authy or Google Authenticator.
2. Such a method does not share the same security vulnerabilities as SMS.
3. There is no physical token to carry, they do not contain batteries that will run out, and they are cheaper than hardware tokens. However, **losing** your device bears an **issue**.
4. Software tokens are the **most commonly used** second-factor authentication method because they are both simple to set up and secure.

OTP: Hardware tokens

1. However, hardware or security tokens use their **peripheral device** similar to software tokens.
2. They come in **different flavors** to connect to your devices, such as USB, NFC, RFID, and Bluetooth.
3. Like every technology, a hardware token has its pros and cons. They are considered one of the **most secure** methods, **but** it is also **easy to lose** them.
4. If you have to choose between software and hardware token, then have several considerations to keep in mind: price, ease of use, and confidentiality.

OTP: Hard copies

1. Hard copies are a numbered list of OTPs **printed on paper**.
2. Online banking and some other services have used this method frequently.
3. The user has to enter a specific OTP from that list for every online transaction.
4. By now, it is **not considered safe**, similar to SMS.

Wide-ranging MFA/2FA support

By now, MFA/2FA has become a standard that is supported by a large number of companies and websites. This overview shows an excerpt of those that already support it.

BANKING

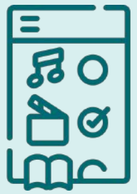
- Bank of America
- Bank of China
- Chase
- Deutsche Bank
- HSBC
- ING
- and many more

COMMUNICATION

- Discord
- Google Chat
- Signal
- Slack
- Telegram
- WhatsApp
- and many more

ENTERTAINMENT

- Discogs
- Google Play
- Plex
- Twitch
- Youtube



GAMING

- Blizzard
- Epic Games
- Rockstar Games
- Steam
- Ubisoft
- Xbox Live
- and many more

HOTELS

- Airbnb
- Booking.com
- Hilton Honors
- Travala
- Vrbo

SOCIAL

- Facebook
- Instagram
- LinkedIn
- Reddit
- TikTok
- Twitter
- and many more

Reference: 2FA Directory, (2021)

Statistics on MFA/2FA

1 **81%** of **security breaches** are due to weak or **stolen passwords**, based on a report by LastPass.

2 In 2019, Microsoft and Google concluded that **MFA/2FA blocks** up to 100% of automated **attacks**.

3 **95%** of the **users** who used **MFA/2FA** used a software-based solution like an **app**.

4 According to market research company Bilendi in 2021, **49%** of those surveyed, just under half of the **German** Internet users, also use **2FA** for at least one other online service.

Biometrics and the future prospect

1. Compared to the other methods, you can consider **biometrics** relatively **new**.

2. Biometrics include **fingerprints**, **vocal**, and **facial recognition**, and they are considered the most difficult to crack.

3. However, companies, such as Apple and Google, did quite a job to make it suitable for the masses. A study from Duo Security says that **77%** of **mobile** devices have **biometric** security **enabled**. Nevertheless, there are almost no website implementations to sign in on websites yet.

4. The assumption is that the **future** will be **passwordless**. There are projects, such as FIDO2, to achieve that.

Conclusion for the use and implementation

1. It would be best to **consider** using a **second factor** to secure your accounts as a user.
2. As a company **offering** services, it is common to provide an **additional security** layer.
3. The **most commonly** used method and technology are **software tokens**, such as Authy and Google Authenticator. You may **also** take a look into **FIDO2** for a passwordless future.
4. Sure, it's less convenient than without, but it increases safety tremendously.

Thank you!

See more on cybersec.help

References: (1) Icons made by Freepik (2) Cover made by TheDigitalArtist