The Evolution of Authentication

Beyond password-based and SMS-based authentication

Authentication

When you claim to be someone

→

you need to provide further information to prove that you are who you say you are.

Weak and strong authentication

"Strong Authentication is a method of user verification that is considered robust enough to withstand attacks on the system to which the users are authenticating." – https://www.hypr.com/strong-authentication/

- **Strong authentication methods**[1]
- **1FA vs 2FA/MFA**
- **Trends: SSO, passwordless authentication, 'SMS-less', biometrics, behavioral solutions, adaptive authentication, AI**

[1] 1FA can also be quite strong, MFA can also be quite weak

AI Day

November 11, 2021

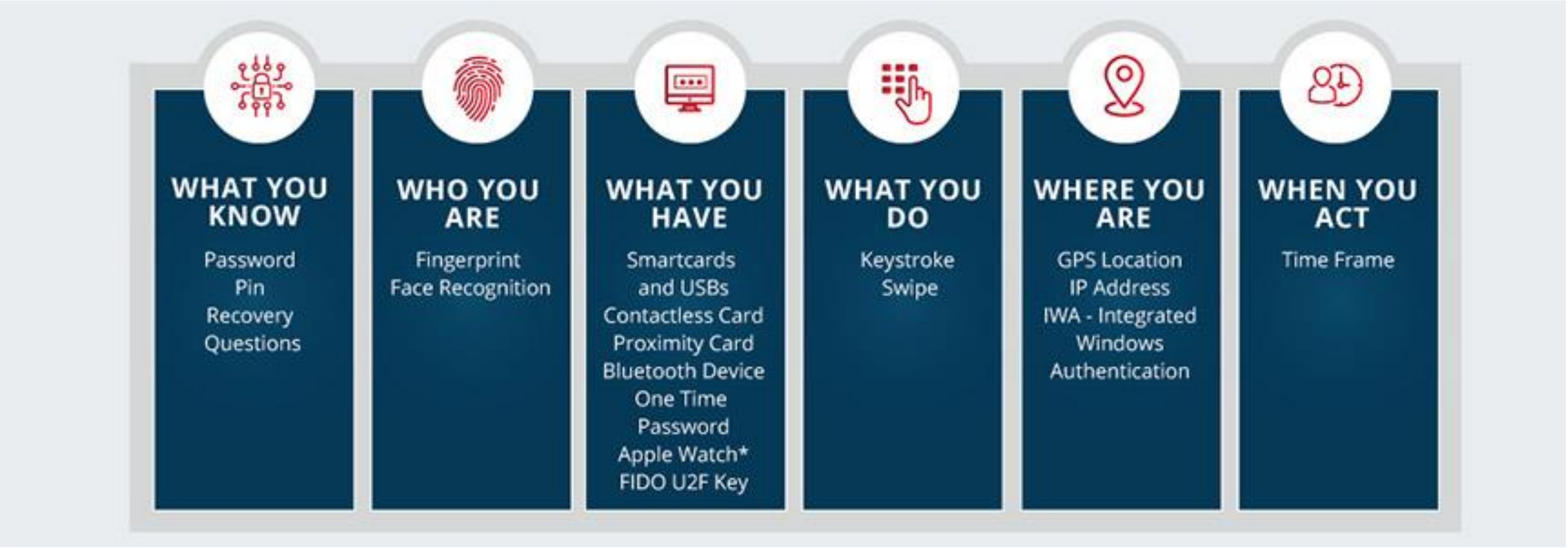
Multifactor Authentication (MFA)

A factor is a type of authentication.

• **Something you know** • **Something you have** • **Something you are** 	e.g. password soft or hard token biometrics

• **Somewhere you are**
  ○ **network location**
  ○ **geolocation**
  ○ **previous known location**
  ▪ **last known location**
• **Something you do (behavior)**
  ○ **previous known behavior**
	e.g. IP-address, MAC-address etc.
	
	e.g. picture password, typing etc.

• **Time frame**	



https://www.ilantus.com/blog/understanding-authentication-what-is-it-all-about/

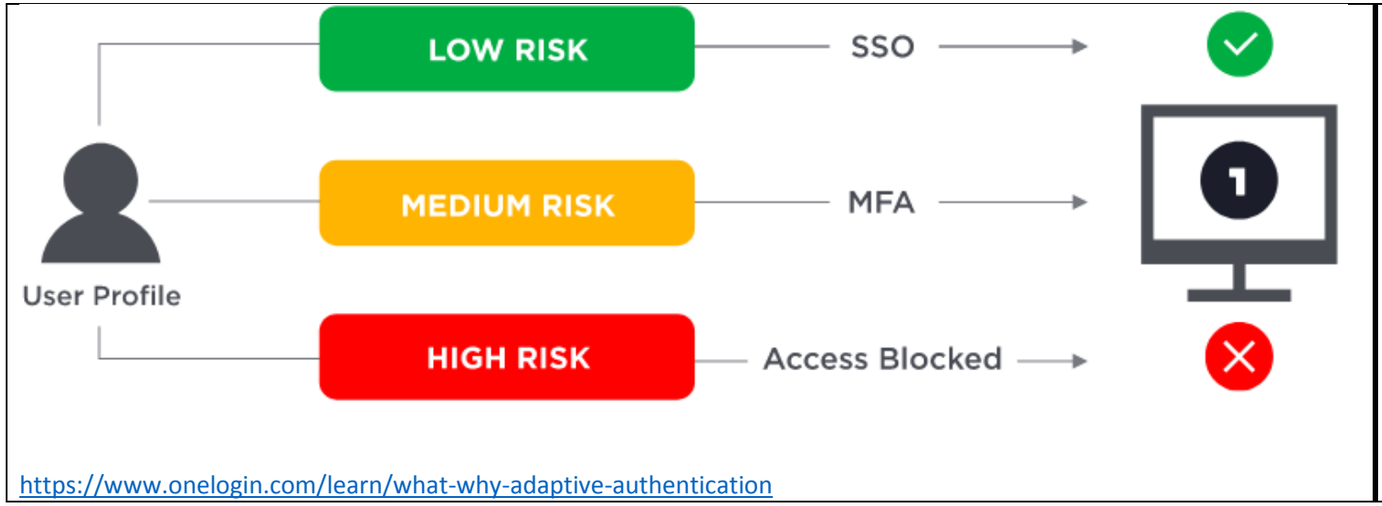
Multi-step authentication vs Multi-factor authentication

Definition-1: Multi-step authentication validates factors separately and Multi-factor authentication validates them all at once.
Definition-2: Multi-step authentication is a subtype of Multi-factor authentication, Multi-step authentication validates factors separately.

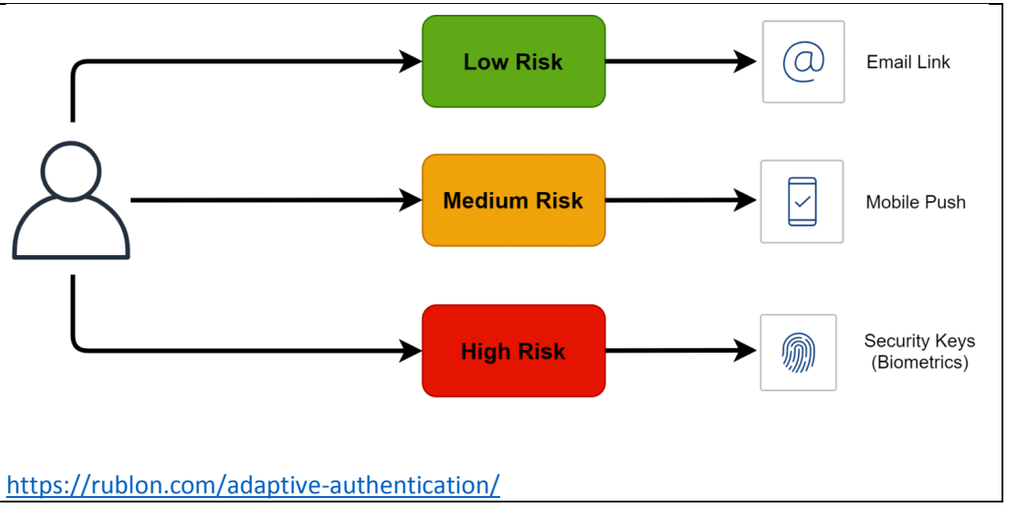
Out-of-Band authentication

Out-of-Band (OOB) means that authentication factors are transmitted via different channels or networks.

Adaptive authentication (risk-based authentication)



https://www.onelogin.com/learn/what-why-adaptive-authentication



https://rublon.com/adaptive-authentication/

Egy hazai bank hírleveléből idézünk:

"Jelenleg az Európai Gazdasági Térség (az Európai Unió tagállamai, valamint Izland, Liechtenstein és Norvégia) határain belüli internetes bankkártyás vásárlások esetén minden kártyakibocsátónak és elfogadónak **kötelező az erős ügyfél-hitelesítés alkalmazása**."

"Ettől bizonyos esetekben el lehet térni, erre kínál lehetőséget a … Banknál most bevezetésre kerülő megoldás. Mostantól egy **intelligens, innovatív rendszer figyeli a gyakran ismétlődő tranzakciókat**, így **a már azonosított, megbízhatónak ítélt kereskedőknél nem lesz szükség az erős ügyfél-hitelesítésre**. Fontos kiemelni, hogy a **tranzakciójóváhagyás** továbbra is biztonságos marad, hiszen azért a **bank vállalja a felelősséget**. Célunk a gördülékenyebb internetes vásárlási élmény nyújtása."

Fel kell-e áldozni az erős hitelesítést?

– Vagy lehetséges erős hitelesítést kényelmesen is alkalmazni?

Is SMS-based authentication secure?

SMS vs other authentication methods (e.g. HOTP, TOTP, app etc.)

Several weaknesses in SMS authentication – 2FA SMS is a bad idea?

Key aspect: convenience:

- **Is password authentication convenient?**
- **Is SMS authentication convenient?**

The cost of authentication:

- **Hidden cost of password authentication**
- **Cost of SMS authentication (implementation, communication, …)**

"NIST is No Longer Recommending Two-Factor Authentication Using SMS", 2016
NIST Special Publication 800-63B

"Paragraph 35 of the EBA opinion on the implementation of the Commission Delegated Regulation (EU) 2018/389 (Regulatory Technical Standards on Strong customer authentication and secure communication) clarifies that “For a device to be considered possession, there needs to be a reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device”.

In this context, a one-time password sent via SMS would constitute a possession element and should therefore comply with the requirements under Article 7 of the Delegated Regulation, provided that its use is ‘subject to measures designed to prevent replication of the elements’, as required under Article 7(2) of this Delegated Regulation. The possession element would not be the SMS itself, but rather, typically, the SIM-card associated with the respective mobile number."

"Subject Matter: Qualification of SMS OTP as an authentication factor

Question: Please clarify whether a One-Time Password (OTP) sent via SMS to a mobile phone qualifies as an ownership factor (“**SOMETHING ONLY THE USER POSSESSES**”), and shall be subject to Article 7 of the RTS on strong customer authentication and secure communication.

Background on the question: **The SMS OTP qualifies as an ownership factor (“something only the user possesses”) because it is received on a device that the CARDHOLDER OWNS and that has been SECURELY ASSOCIATED with the cardholder by the issuer**."
The European Banking Authority (EBA)
https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4039

Attacks

- **Automated attack**
- **Human-operated attack**
- **Human attack**
  - Human-to-Computer
  - **Human-to-Human attack, Social Engineering**
  - **Malicious Insiders**

Literature

https://dojowithrenan.medium.com/the-5-factors-of-authentication-bcb79d354c13

https://www.toolbox.com/it-security/identity-access-management/articles/top-10-multi-factor-authentication-software-solutions/

https://www.ilantus.com/blog/understanding-authentication-what-is-it-all-about/

https://www.cyberark.com/what-is/just-in-time-access/

https://www.kaspersky.com/blog/2fa-practical-guide/24219/

https://www.techrepublic.com/article/top-5-reasons-not-to-use-sms-for-multi-factor-authentication/

https://blog.sucuri.net/2020/01/why-2fa-sms-is-a-bad-idea.html

https://cacm.acm.org/magazines/2020/12/248798-security-analysis-of-sms-as-a-second-factor-of-authentication/fulltext?mobile=false

https://www.wired.com/insights/2014/04/evolution-authentication/

https://atos.net/en/blog/what-will-user-authentication-look-like-in-2030

Contents