# Authentication (Autentizace)

**Authentication** je proces ověření deklarované identity. Cílem je zajistit, aby osoba nebo systém přistupující ke zdroji byl skutečně oprávněným subjektem.

V IT terminologii je zásadní neplést si tento pojem s **Autorizací**:

- **Autentizace:** „Kdo jsi?“ (Ověření identity).
- **Autorizace:** „Co smíš dělat?“ (Ověření přístupových práv).

---

# Tři faktory autentizace

Tradičně se metody autentizace dělí do tří základních kategorií (faktorů) podle toho, na čem jsou založeny:

## 1. Faktor znalosti (Something you know)

To, co uživatel nosí v hlavě. Nejpoužívanější, ale také nejzranitelnější metoda.

- Příklady: Heslo, PIN, kontrolní otázka, gesto na displeji.

## 2. Faktor vlastnictví (Something you have)

Fyzický předmět, který má uživatel u sebe.

- Příklady: Hardwarový token (YubiKey), chytrá karta, mobilní telefon (příjem SMS kódu), certifikát na USB disku.

## 3. Faktor inherence (Something you are)

Biometrické údaje, které jsou neoddělitelnou součástí těla uživatele.

- Příklady: Otisk prstu, sken oční duhovky, rozpoznání obličeje, analýza hlasu.

---

# Moderní přístupy k autentizaci

## Vícefaktorová autentizace (MFA / 2FA)

Znamená kombinaci alespoň dvou různých faktorů (např. heslo + kód z mobilu). Pokud útočník ukradne heslo, stále nemá přístup k fyzickému zařízení, což dramaticky zvyšuje bezpečnost.

## SSO (Single Sign-On)

Umožňuje uživateli přihlásit se jednou do centrálního systému a získat přístup ke všem propojeným aplikacím bez nutnosti znovu zadávat heslo (např. přihlášení do firemního e-mailu, intranetu a HR systému jedním účtem).

## Passwordless (Bezheslová autentizace)

Moderní směr, který eliminuje hesla úplně. Využívá kryptografii veřejného klíče (např. standard **FIDO2 / Passkeys**). Uživatel se ověří lokálně na svém zařízení (otiskem prstu) a zařízení pak bezpečně potvrdí identitu serveru.

---

# Technické uložení a protokoly

V systémech se autentizační údaje (hesla) nikdy nesmí ukládat v čitelné podobě (plain text). Používají se kryptografické funkce:

- **Hashing:** Heslo se převede na unikátní řetězec (hash). Při přihlášení se porovnávají hashe, nikoliv hesla.
- **Salt (Sůl):** Náhodná data přidaná k heslu před zahashováním, která brání útokům pomocí duplicitních tabulek (Rainbow tables).

## Standardní protokoly:

- **LDAP:** Často používán v rámci Active Directory pro správu uživatelů v sítích.
- **OAuth 2.0 / OpenID Connect (OIDC):** Standardy pro moderní webové a mobilní aplikace (umožňují např. „Přihlásit se přes Google“).
- **Kerberos:** Síťový protokol používaný pro bezpečné ověřování v rámci doménových struktur (Windows).
- **SAML:** Používán zejména pro výměnu autentizačních dat mezi různými doménami (časté u SSO).

---

# Časté útoky na autentizaci

- **Brute Force:** Hádání hesla zkoušením všech kombinací.
- **Phishing:** Podvodné vylákání přihlašovacích údajů od uživatele.
- **Credential Stuffing:** Útočník zkouší uniklá hesla z jedné služby v jiných službách.
- **Man-in-the-Middle (MitM):** Útočník zachytí autentizační data během přenosu.

---

*Související pojmy: Authorization, MFA, Password, Biometrics, OAuth, Hashing, Passkey.*