Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Správa identít a prístupov (IAM)

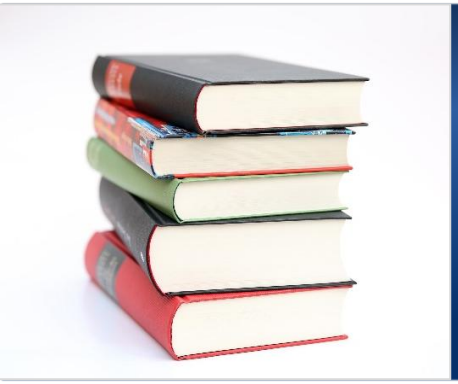
Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti

prof. Ing. Pavel Segeč, PhD.

KC KYB UNIZA, https://kc.uniza.sk

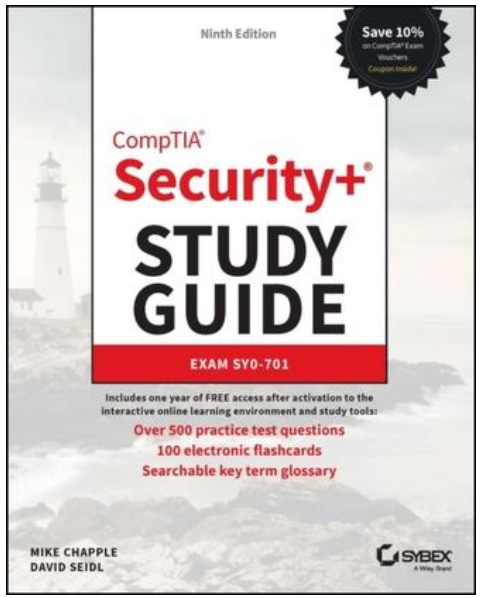
pavel.segec@fri.uniza.sk

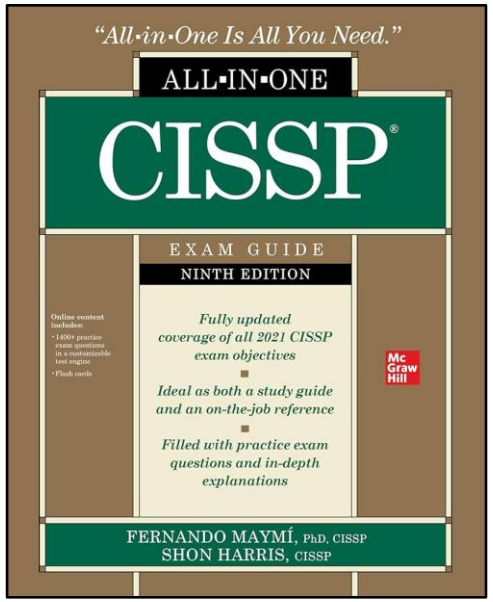


Obsah

- Blok I: Fundamenty IAM, identita, autentifikácia, autorizácia, audit/monitor
- Blok II: Modely riadenia prístupu a ich implementácia
- Blok III – Moderné IAM technológie – protokoly a tokeny

- **Literatúra**
  - CompTIA Security+
  - CISSP All-in-One Exam Guide





Blok I: Fundamenty IAM, identita, autentifikácia, autorizácia

Identity and Access Management

- ***IAM*** je súbor **procesov, technológií a pravidiel**, ktorý zabezpečuje:
  - správu digitálnych identít (**kto**)
  - riadenie prístupu k systémom, dátam a službám (**kam**)
  - overovanie a vynucovanie oprávnení používateľov a zariadení (**ako** a **čo**)
- **Význam v kybernetickej bezpečnosti**
  - Strategický integrujúci bezpečnostný rámec
    - Znižuje riziko neoprávneného prístupu a úniku dát
    - Podporuje efektívne riadenie bezpečnosti na princípe minimálnych oprávnení (*Least Privilege Principle*)
    - Umožňuje efektívne kontrolovať, monitorovať a audítovať používanie informačných systémov a služieb
    - Podporuje súlad s normami a reguláciami (napr. ISO 27001, NIS2)
  - Príklad: Prihlasovanie cez SSO, riadenie prístupov do interných systémov podľa rolí...
- IAM z pohľadu MKYB je o **zodpovednosti, viditeľnosti a kontrole**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

IAM piliere - Základné technické funkcie IAM (IAM ich prepája)

- **Identifikácia / identita**
  - Určuje, kto je používateľ systému
  - A ako ho jedinečne identifikovať
- **Autentifikácia**
  - Overuje identitu používateľa (je tým, za koho sa vydáva?)
- **Autorizácia**
  - Rozhoduje čo môže používateľ robiť a k akým zdrojom má prístup
    - *Access Control modely / mechanizmy*
- **Audit a monitorovanie**
  - Sleduje prístupy a zaznamenáva činnosti (kto, kedy, čo robil) za účelom kontrol a auditu

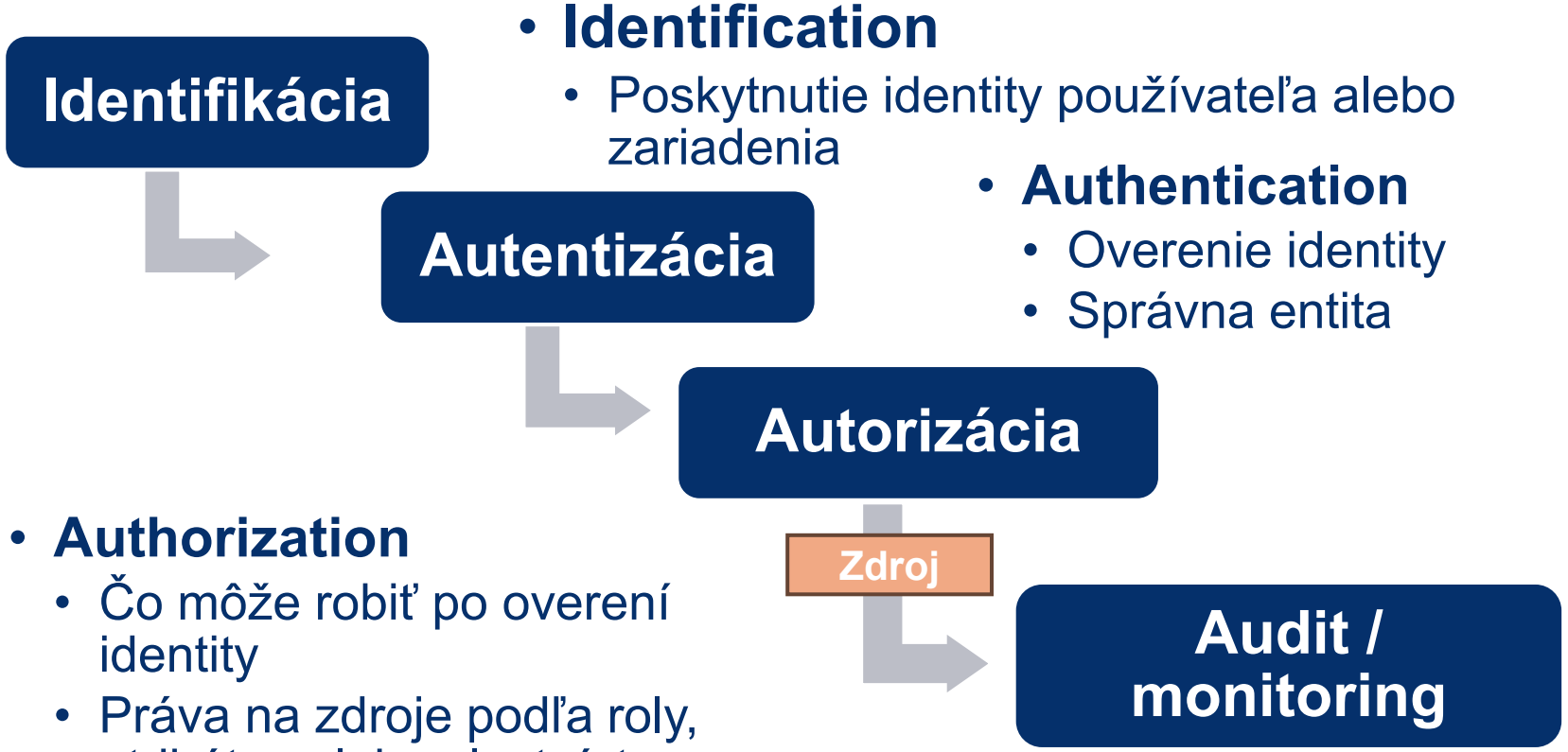
- **Správa používateľských účtov a údajov** (identity and credential lifecycle)
  - Riadi životný cyklus účtov (vytváranie, zmena, rušenie účtov, obnova hesiel)
- *IAM = Identity management + User and credential management + Session management + Accouting*

- IAM podporuje moderné princípy
  - **Least Privilege** (najnižšie možné oprávnenia)
  - **Separation of Duties** (Oddelenie povinností / úloh)
  - **Zero Trust** („N*ever trust, always verify*“)
    - Perimeter sa stiera, identita je perimeter
  - **Accountability** (vystopovateľnosť)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kroky IAM procesu – AAA rámec

- **AAA -** formálne pomenúva a technicky realizuje to, čo IAM robí = Koncept riadenia prístupu
- Treba **zabezpečiť poradie** vykonania (nesprávne poradie môže viesť k **nekorektnému alebo nebezpečnému stavu** systému)
  - Aplikačná zraniteľnosť, ktorá vzniká z chýb v návrhu sekvencie krokov



- **Identification**
  - Poskytnutie identity používateľa alebo zariadenia
- **Authentication**
  - Overenie identity
  - Správna entita
- **Authorization**
  - Čo môže robiť po overení identity
  - Práva na zdroje podľa roly, atribútov alebo vlastníctva
- **Accounting (Auditing)**
  - Evidencia a zodpovednosť
  - Záznamy kto čo spravil, kedy, kde a prečo

Autentifikácia (identita, identifikácia a verifikácia)

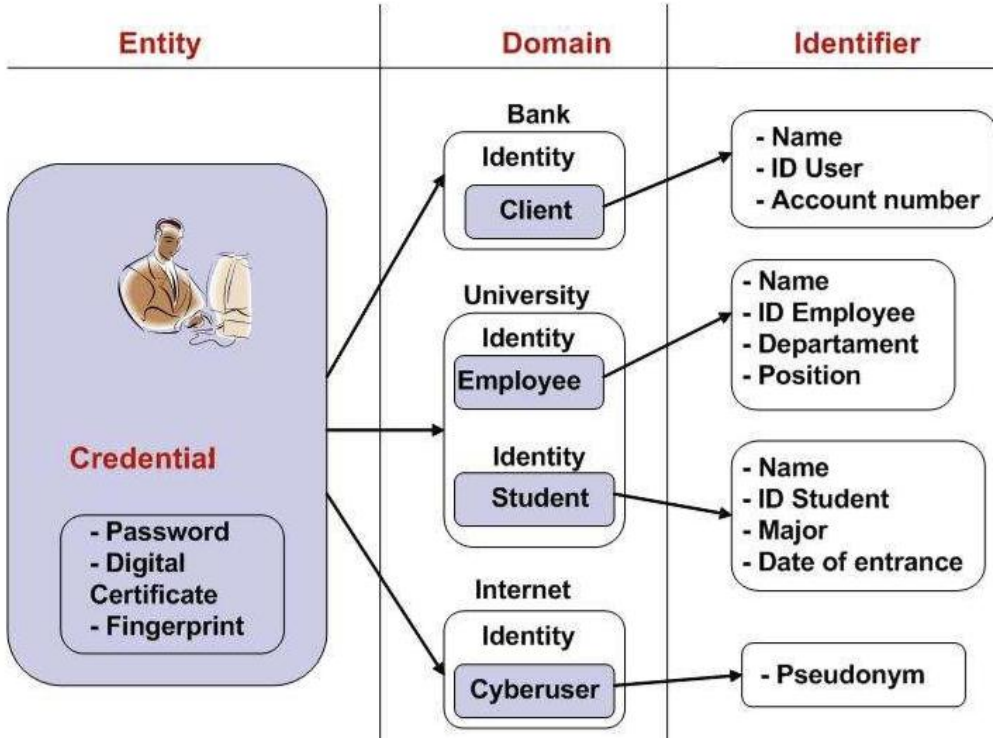
- Typy autentifikácie a ich riadenie
- Faktory autentifikácie (1FA, 2FA, MFA)

Identita – fyzická a digitálna

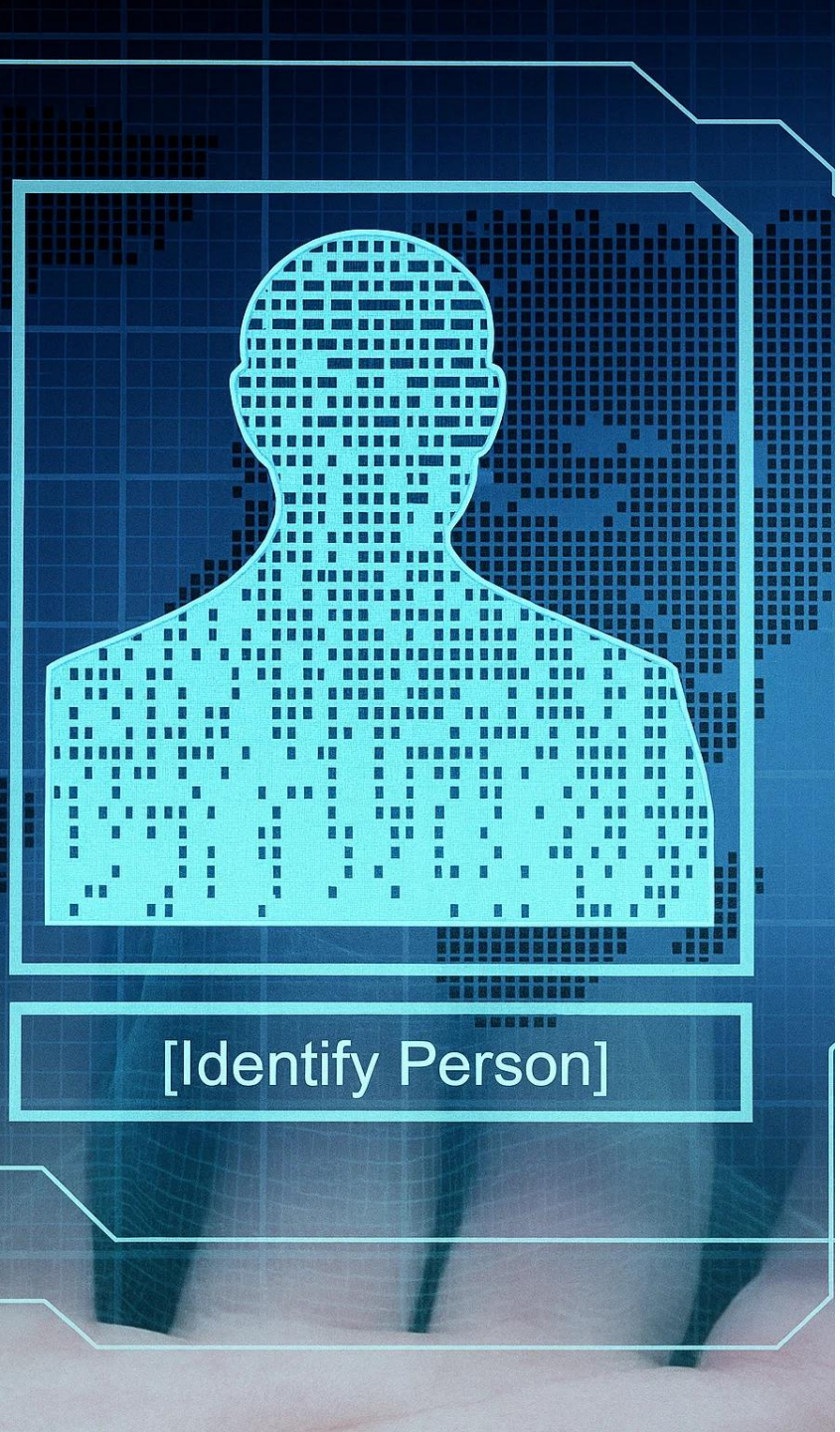
- **Identita** = **Kto sme**
  - Fundamentálny koncept pri riadení prístupu
  - Charakteristické znaky a vlastností osoby
  - Spôsob pre ostatných spoznať a overiť, že sme to my
- Fyzický svet = **Fyzická identita** (bežná identita)
  - Totožnosť konkrétnej fyzickej osoby
  - **Príklady:** Občiansky preukaz, pas, vodičský preukaz, preukaz zamestnanca ...
  - **Overenie**: Pomocou dokumentov alebo údajov
- Online svet = **Digitálna identita**
  - **Súbor elektronicky zachytených a uložených atribútov a poverení**, ktoré jedinečne identifikujú entitu v digitálnom prostredí v danej doméne
    - Predstavuje **digitálny ekvivalent fyzickej identity**
  - **Príklady:** Používateľské meno, e-mail, telefónne číslo, unikátny eID identifikátor, rodné číslo, otlačok, hlas, IP adresa a iné
  - **Overenie:** napr. zadaním mena pri prihlasovaní do online účtu

Digitálna identita – základné pojmy

- **Digitálna Identita**
  - Súbor atribútov, ktoré jedinečne charakterizujú **entitu** v dig. systéme
    - Osoba (PaloS., AD1234) / Systém (server, API client) / Služba (cron job, integrácia)
- **Identifikátory (atribúty)**
  - Tvoria digitálnu identitu
  - Príklady: dátum narodenia, e-adresa, zamestnanecké číslo, skupiny, roly, nick, JWT token ...
- **Poverenia (credentials)**
  - Slúžia na autentifikáciu identity
  - Typicky *prihlasovacie údaje (napr. meno a heslo)*
- **Entita**
  - Osoba, skupina, organizácia, proces alebo zariadenie schopné vykonať transakciu / akciu
  - **Problém**: Jedna entita = viac digit. identít v rámci rovnakej domény
    - Zhoršuje audit, správu prístupov, compliance



Zdroj: Federated Identity Architectures-Uciel Fragoso-Rodriguez



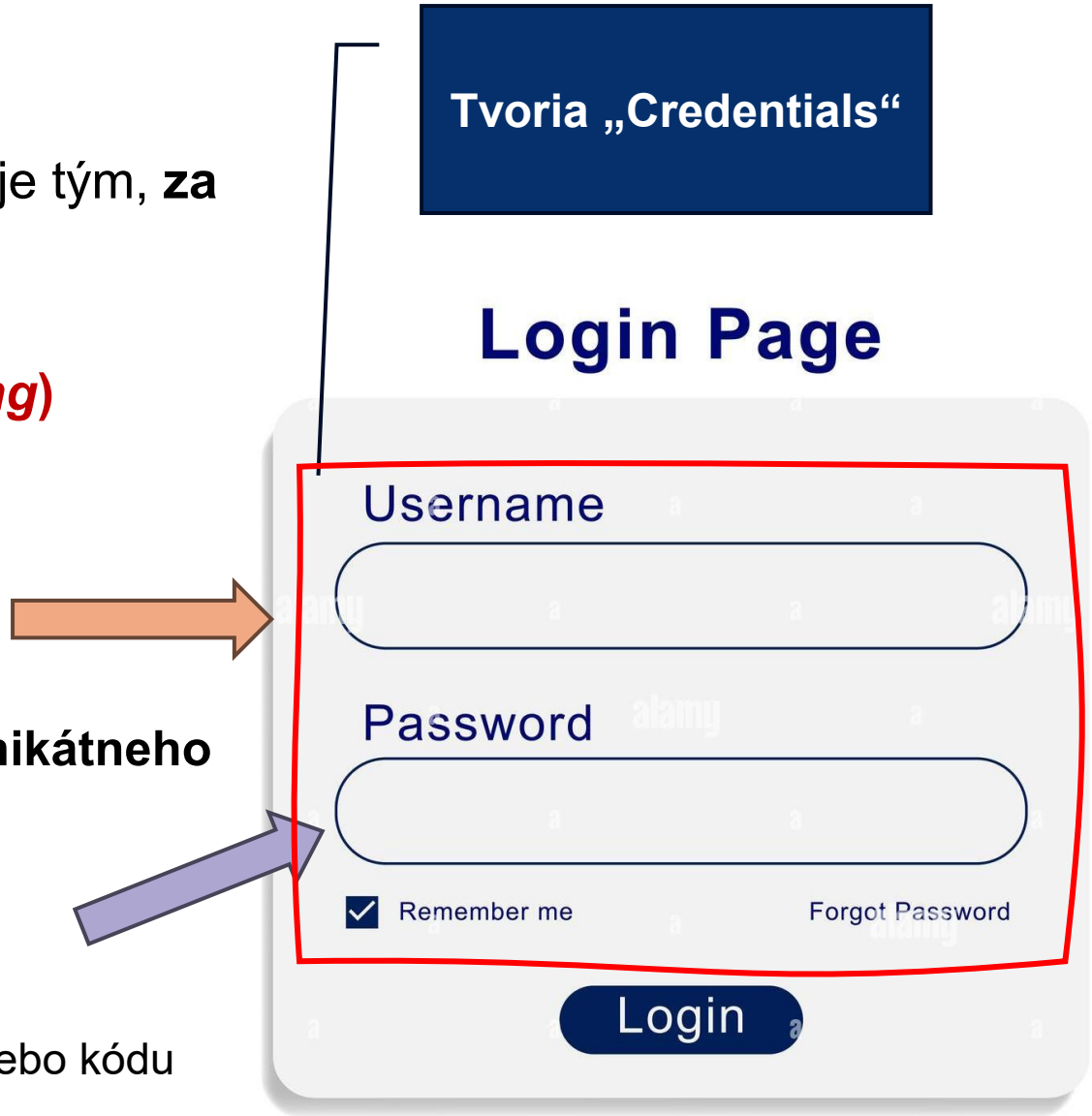
Ako na identity

- Typické **chyby** pri riešení identít
  - Duplikované ID
  - Neštandardné názvy (user1, managerXY)
  - Zdieľané ID medzi viacerými používateľmi
  - Popisné ID → únik rolí („admin_Jozef“)

- Odporúčania pre tvorbu identít – Best Practices
  - **Jedinečnosť** – každý ID musí byť unikátne
  - **Názvoslovie** – používať jednotnú schému (ad_jpublic, svc_appX, psegec_001)
  - **Nediskrétnosť** – ID nemá odhaľovať rolu, oddelenie, oprávnenie
  - **Nedeliteľnosť** – identity sa nesmú zdieľať medzi používateľmi
  - **Vystopovateľnosť** – musí byť možné spätne určiť, komu identita patrí

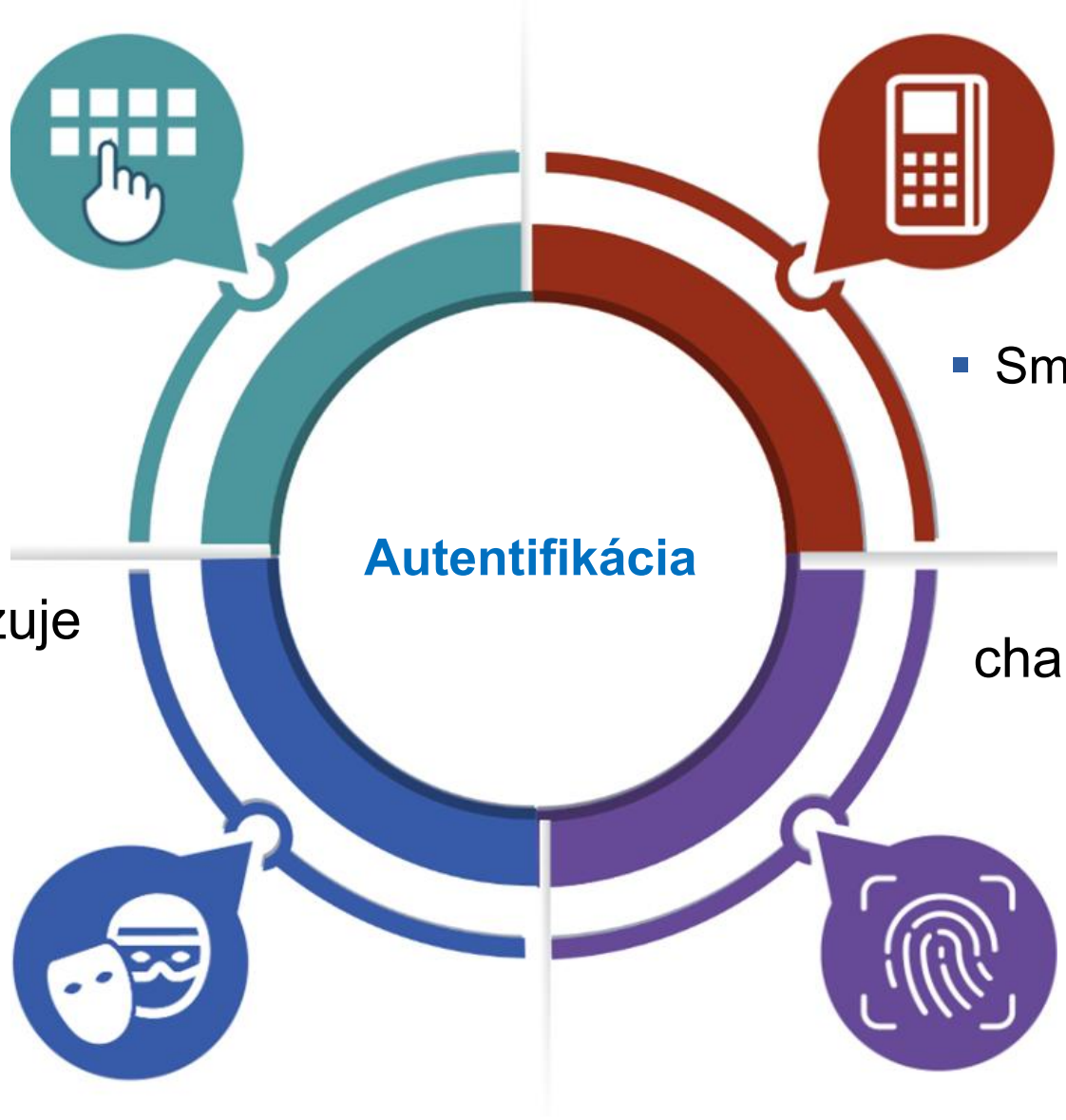
Autentifikácia (autentizácia)

- **Autentifikácia**
  - Proces, pri ktorom **systém overuje**, že entita je tým, **za koho sa vydáva**
- **Pozostáva**
  - **Identifikácia (*identification, identity proofing*)**
    - Procedúra kde používateľ/systém alebo entita prezentuje svoju totožnosť
      - „Predstavujem“ sa systému kto som
        - Identifikujem sa ako jeho platný používateľ
        - Zadaním napr. e-mailovej adresy alebo mena
    - Predpokladá vykonanie procesu priradenia **unikátneho identifikátora** entite v systéme => rieši ILM
  - **Verifikácia (*verification*) alebo autentizácia**
    - Overenie systému, že pozná danú identitu
      - *Proces overenia totožnosti používateľa/služby ...*
      - Zadaním autentifikačného faktora, napr. hesla alebo kódu zo SMS
      - Potvrdenie dôveryhodnosti ***Identity***

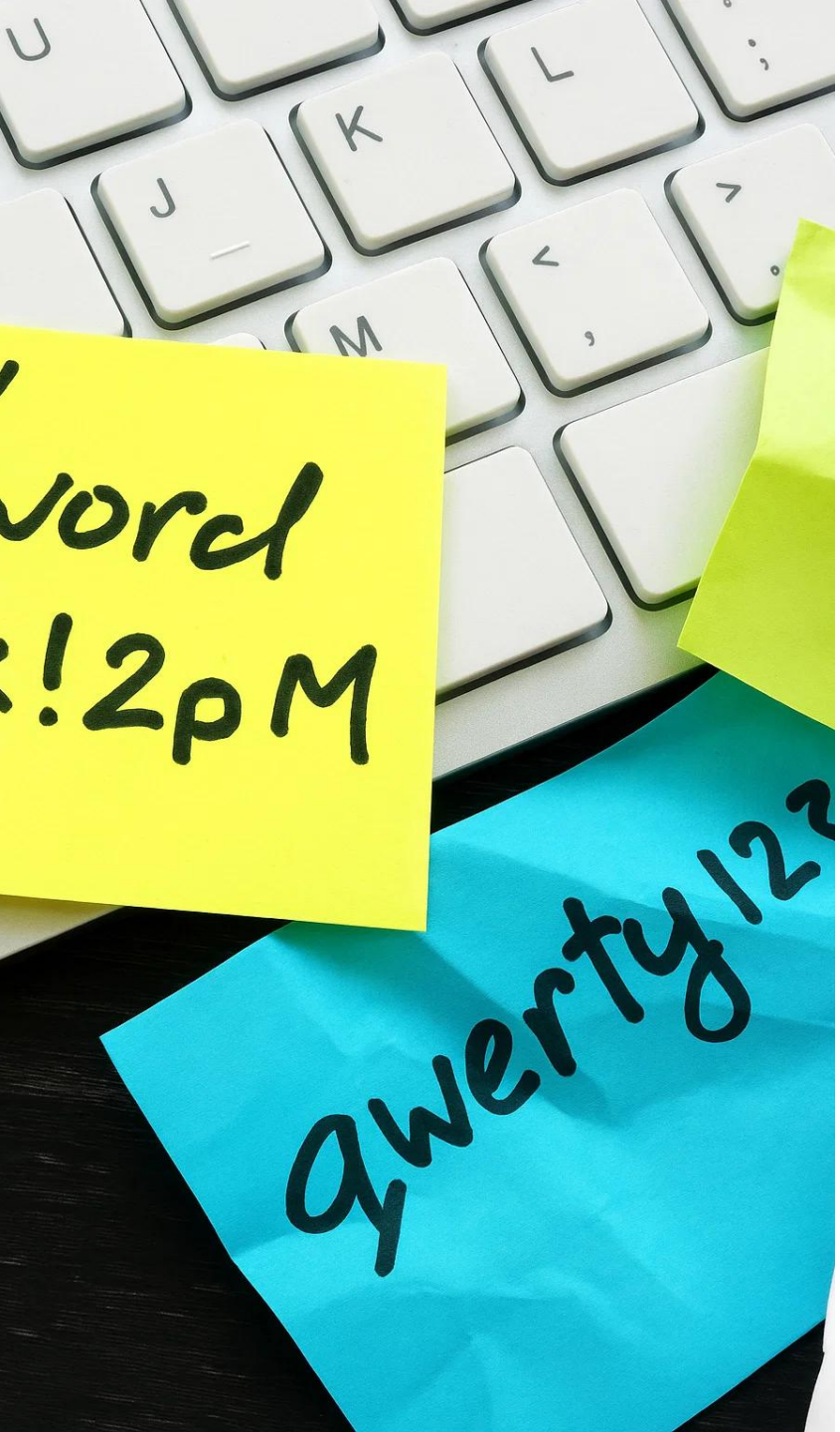


Metódy (faktory) autentifikácie

- **Niečo, čo viem len ja** (tajomstvo) **- KBA**
  - PIN
  - Heslo
  - Fráza
  - Kód
  - Jednorazové heslo
  - ...
- **Niečo, čo robím** (čo ma charakterizuje - behavior**)**
  - Ako rozprávam
  - Ako píšem na klávesnici
  - Pohyb myšou
  - Rukopis ...



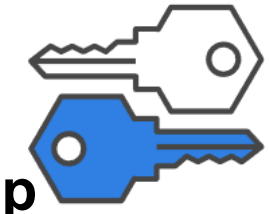
- **Niečo, čo mám / vlastním**
  - Mobil, SMS
  - Pamäťová karta (s chipom) + reader (i.e. banková karta)
  - Smart karta (napr. NFC karty)
  - OTP token
  - ...
- **Niečo, čo som** (moja jedinečná charakteristika - biometrika)
  - Odtlačok prsta
  - Sken sietnice
  - Sken tváre
  - Veľkosť prsta/dlane
  - ....



Autentifikácia

Jedno a viacfaktorová autentifikácia

- **Jednofaktorová autentifikácia**
  - Používa jeden spôsob overenia totožnosti
  - V princípe, ak je **správne implementované a použitá**, môže poskytovať bezpečnú autentizáciu používateľa
  - Riziká:
    - Slabé heslá, opakované heslá, komplikovaný systém, pôsobenie útočníka ...
- Riešenie ==> **Dvoj (2FA) a viacfaktorová autentifikácia (Strong auth)**

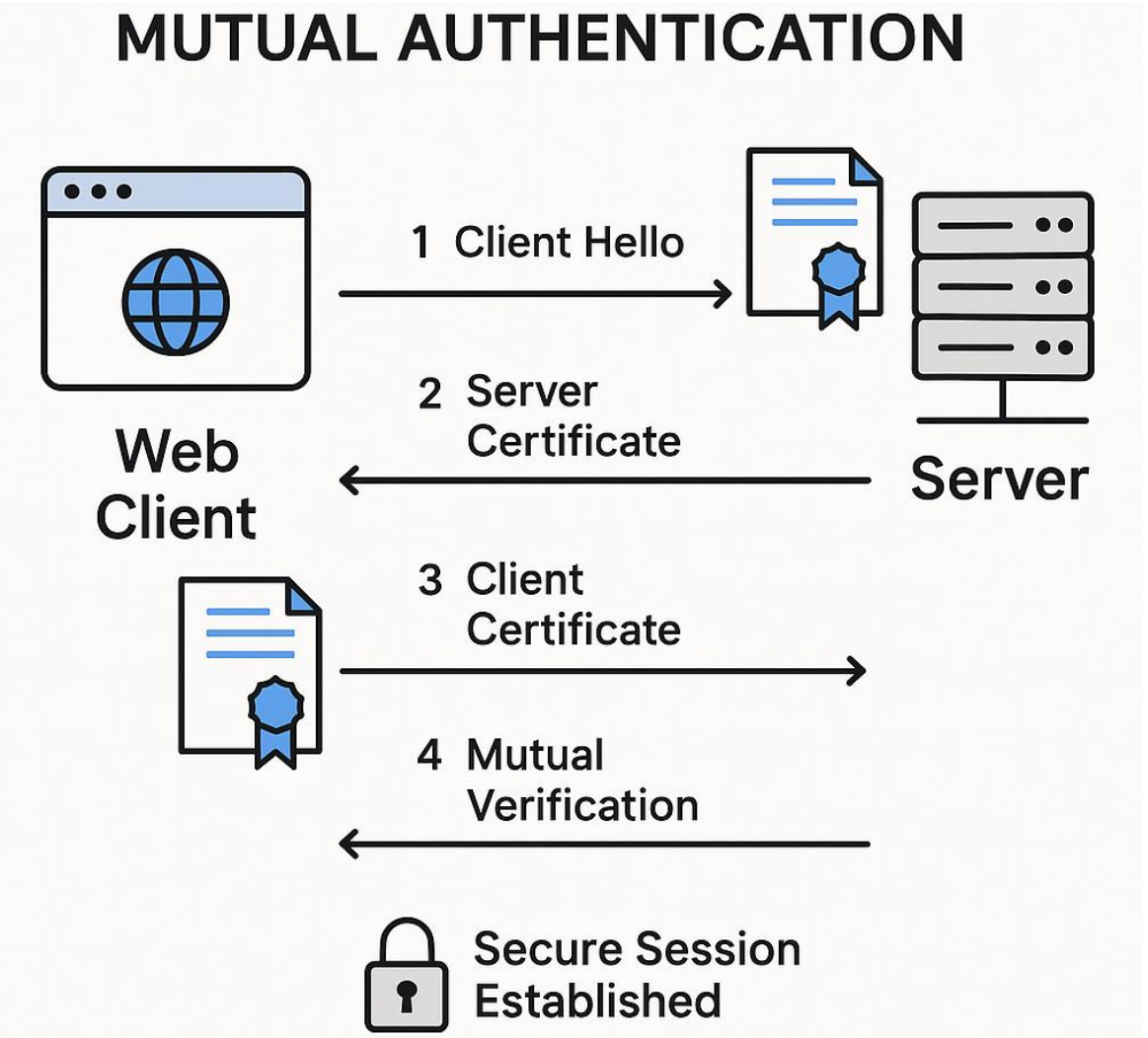


  - Navýšenie počtu faktorov => **moderný prístup**
    - Zadáš heslo (niečo, čo vieš)
    - Potvrdíš kód zo SMS alebo mobilnej aplikácie (niečo, čo máš)
  - Zníženie rizika krádeže identity
  - Bežné napr. v bankovníctve, štátnych portáloch, e-mailových službách

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy autentifikácie

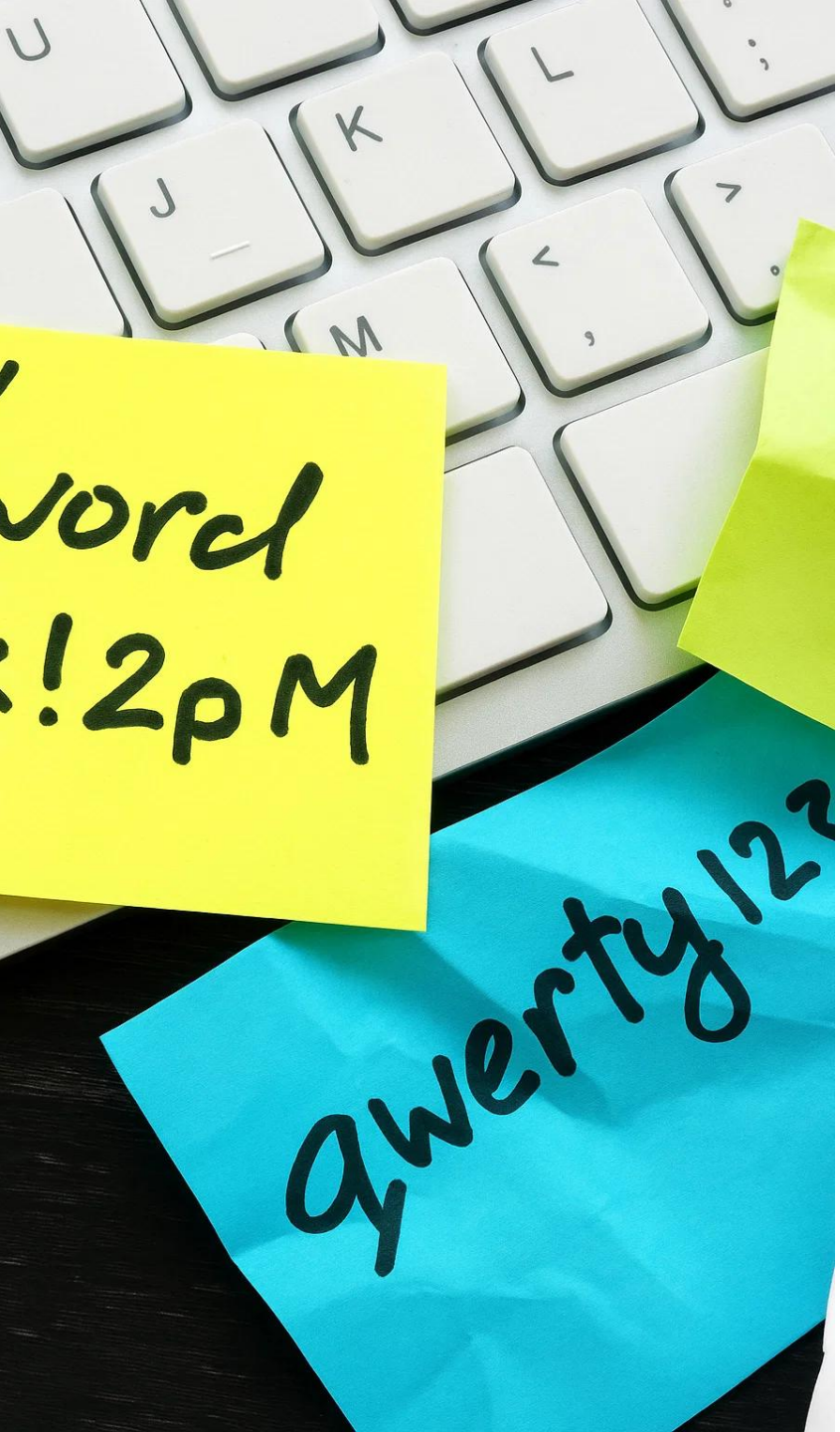
- **Jednosmerná autentifikácia (One-Way Authentication)**
  - Najbežnejšia forma
  - Používateľ overuje svoju identitu voči systému
  - Príklad: login do e-mailu cez heslo, https
- **Obojstranná autentifikácia (Mutual Authentication)**
  - Systém overuje **aj identitu používateľa**, aj **naopak**
  - Zabraňuje spoofingu servera (napr. MITM útok)
  - Použitie pre kritické systémy
    - Napr. v:
      - Bankovníctve (HSM, certifikáty),
      - VPN (client certs),
      - TLS (server + client cert)
      - …



Autentifikácia založená na znalosti (Something You Know)

- **Definícia:**
  - Autentifikačné metódy založené na **tajnej informácii, ktorú pozná iba používateľ**
- **Metódy**
  - **Heslá (passwords)**
    - Reťazec znakov, ktorý pozná len používateľ
    - Najčastejšia metóda, ale zároveň najzraniteľnejšia
  - **Prístupové frázy (passphrases)**
    - Dlhší a zmysluplný text (napr. „RánoPijemZelenýČaj“)
    - Ľahšie zapamätateľný / ťažšie uhádnuteľný
  - **PIN kódy**
    - Krátky číselný kód
    - Používaný v mobiloch, bankomatoch alebo smart kartách
  - **Kognitívne otázky (cognitive passwords)**
    - Otázky na osobnú históriu používateľa (napr. „meno prvého psa“)
    - Používajú sa najmä pri obnove hesla alebo pri nepravidelnom prístupe
  - **CAPTCHA** (na odlíšenie človeka od robota)
    - Obrázkový alebo textový test na odlíšenie človeka od robota
      - Nie je primárna metóda, ale doplnková forma overenia identity

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Autentifikácia

Koncept hesiel - problémy

- Ľahko uhádnuteľné alebo slabé heslá
  - Používatelia si často volia jednoduché heslá
  - Príklad: 123456, password
- Recyklácia hesiel naprieč službami
  - Jedno niknuté heslo = prístup k viacerým účtom (credential stuffing)
- Úniky z databáz
  - Heslá (aj hashované) unikajú z narušených služieb
  - Príklad: LinkedIn, Adobe
- Náchylnosť na phishing
  - Heslá je možné získať oklamaním používateľa
  - Príklad: falošné prihlasovacie stránky
- Možnosť zachytenia (keylogger, shoulder surfing)
  - Heslo možno odsledovať fyzicky alebo softvérovo
- Zastarané pravidlá (napr. časté zmeny)
  - Znižujú použiteľnosť, ale nezvyšujú bezpečnosť
- Chýba viazanosť na zariadenie alebo kontext
  - Heslo neoveruje, kto alebo odkiaľ sa prihlasuje

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Autentifikácia

Koncept hesiel - útoky

- **Sledovanie siete** (electronic monitoring / sniffing)
  - Odpočúvanie siete, zachytávanie nešifrovaných údajov (HTTP, Telnet)
  - Umožňuje replay attack, teda znovupoužitie platného prenosu
- **Získanie súboru s hashmi hesiel**
  - Kompromitácia databázy + Offline lámanie hesiel
- **Brute-force útok**
  - Skúšanie všetkých kombinácií
  - Úspešný pri slabých heslách
- **Slovníkový útok (dictionary attack)**
  - Skúšanie bežných slov zo slovníka
    - dw0rsec/rockyou.txt: rockyou.txt wordlist
  - Rýchlejší pri jednoduchých heslách
- **Rainbow table útok**
  - Použitie predvypočítaných tabuliek hash-ov
  - Efektívne bez salting-u
- **Sociálne inžinierstvo** (social engineering)
  - Manipulácia používateľov (phishing, podvodné emaily)
  - Nezávislé od technickej ochrany
- **Keylogging** / malware
  - Zachytávanie stlačených klávesov.

Koncept hesiel – Best practise – Firemné prostredie

- **Politika zloženia hesiel**
  - Min. 10-12 znakov (odporúčané), kombinácia znakov
  - Rotácia len pri podozrení z kompromitácie (NIST SP 800-63B)
  - Max/min vek hesla, zákaz opätovného použitia
- **Zakázanie slabých alebo kompromitovaných hesiel**
  - Kontrola proti známym databázam (HaveIBeenPwned, wordlisty)
  - NIST: rotácia len pri podozrení z kompromitácie
- **Ochranné mechanizmy**
  - Account Lockout: po 3–5 chybách dočasná blokácia
  - Session Timeout / Inactivity logout
  - AAA Accouting - Logovanie pokusov o prihlásenie – dátum, čas, user ID, zariadenie
- **Manažéri hesiel**
  - Bezpečná centrálna správa hesiel
- **Vzdelávanie používateľov a adminov**
  - Bezpečné používanie hesiel, phishing awareness

- FINAL => **Vyhýbaj sa zbytočne zložitým politikám a pravidlám**
  - Začnú sa hľadať cesty na obchádzanie
  - Rovnováha medzi **bezpečnosťou** a **použiteľnosťou**

Niečo, čo mám / vlastním (Something You Own)

- **Definícia**
  - Založené na **vlastníctve objektu** – fyzický alebo logický dôkaz identity
- **Metódy – príklad**
  - **OTP (One-Time Password) / TOTP**
    - Jednorazový kód generovaný zariadením alebo aplikáciou
      - Google / MS authenticator, SMS kód, atď.
    - Výhoda: odolné voči replay útokom, phishing sťaženejší
  - **Smart karty a bezpečnostné kľúče**
    - Karty s čipom alebo USB
      - Obsahujú **privátny kľúč** a kryptomodul (napr. YubiKey / FIDO2)
    - TPM (Trusted Platform Module) zariadenie
    - Uchovávajú privátny kľúč, autentifikácia cez PIN alebo challenge–response
    - PassKey riešenia (**MFA:** kľúč vyžaduje dotyk + prípadne **PIN/biometriu** (odtlačok/FaceID)
  - **Hardvérové tokeny (NFC/RFID, fobs)**
    - Klientske zariadenia, ktoré generujú alebo prenášajú kód

„Hard“ HW autentifikácia

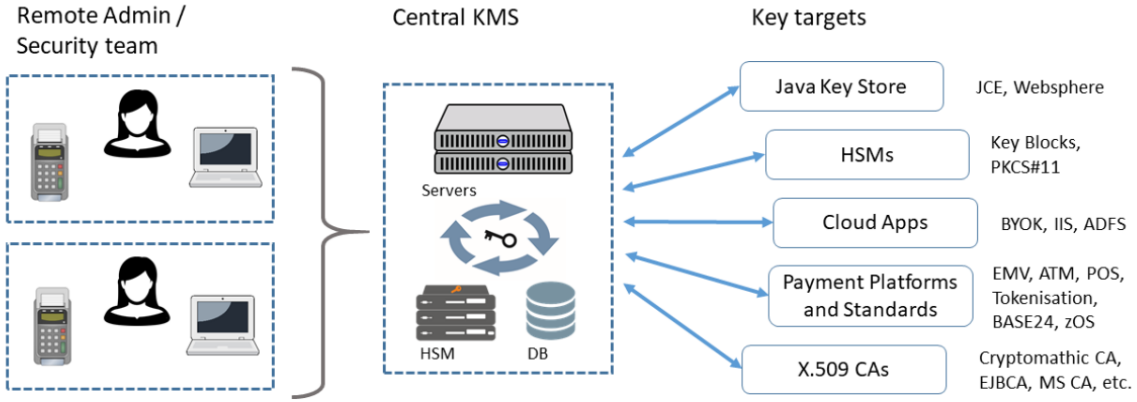
- Klasický **druhý faktor** – používajú sa tam, kde je potrebná vyššia úroveň bezpečnosti než heslá
  - V praxi => najčastejšie sa viažu na **VPN a admin prístupy**
- **Výhody:**
  - Silnejšie než len použitie hesla (2FA)
  - Odolnosť voči phishingu (najmä OTP) a replay útokmi
  - Možnosť offline generovania OTP
  - Hardvérové tokeny – vyššia fyzická bezpečnosť
- **Nevýhody:**
  - Riziko straty, krádeže alebo poškodenia tokenu
    - Potreba viac kľúčov
  - Softvérové OTP môžu byť zneužité pri kompromitovanom zariadení
  - Potreba synchronizácie (synchronné tokeny)
  - Náklady na infraštruktúru (napr. čítačky kariet, správa PKI)
  - Falošné čítačky – *skimming* (napr. pri kartách – Flipper Zero)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

„Hard“ autentifikácia – voliteľný backend

- **KMS (Key Management Server / System)**
  - Softvérový systém alebo služba, ktorá centralizovane spravuje **šifrovacie kľúče** počas ich životného cyklu
  - **Funkcie**
    - generovanie kľúčov, distribúcia, rotácia, archivácia, expirácia, zrušenie
    - prístupové politiky (kto môže použiť ktorý kľúč)
    - auditovanie a logovanie
  - **Použitie**
    - cloudové služby (**AWS KMS**, **Azure Key Vault**, **Google Cloud KMS**)
    - integrácia s PKI pre vydávanie a správu certifikátov

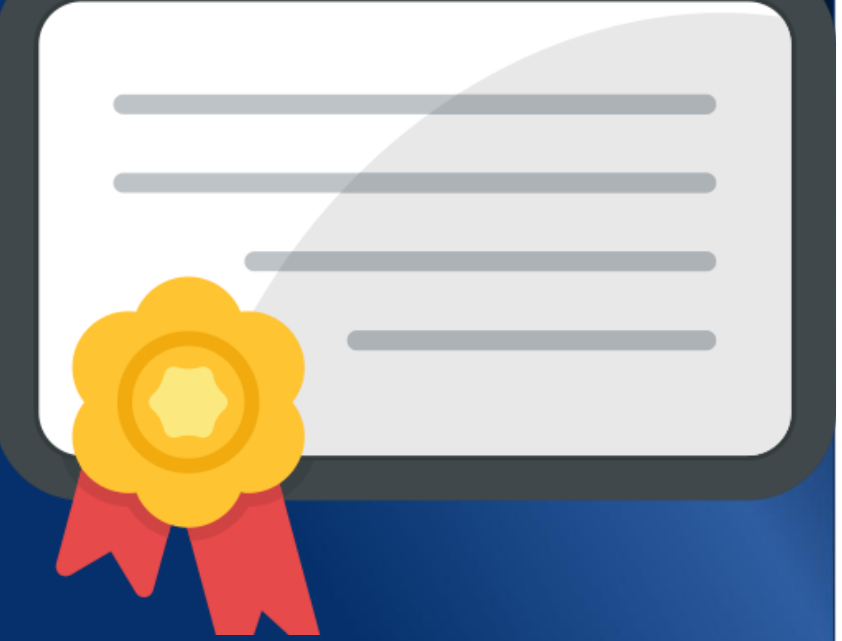
- **HSM (Hardware Security Module)**
  - Špecializované hardvérové zariadenie (karta, appliance alebo modul)
    - bezpečne generuje kryptografické kľúče,
    - ukladá ich tak, aby nikdy neopustili HSM v čitateľnej podobe,
    - vykonáva kryptografické operácie (podpis, šifrovanie, dešifrovanie) **priamo vo vnútri zariadenia**
  - **Výhoda**
    - Útočník sa k súkromným kľúčom nedostane ani pri kompromitácii servera
  - **Použitie**
    - PKI certifikačné autority (CA),
    - bankovníctvo (ochrana PIN, karty, podpisy transakcií),
    - hardvérová autentifikácia (uloženie privátnych kľúčov na tokenoch / smart kartách)
  - HSM je teda **„trezor“ pre kľúče**, ktorý poskytuje najvyššiu úroveň bezpečnosti



Best Practice pre HW tokeny a bezpečnostné kľúče

- **Použitie HW tokenov (OTP/TOTP/HOTP)**
  - Vhodné pre **VPN prístupy** a **privilegovaný admin prístup** na sieťové zariadenia
  - Integrácia cez AAA server (RADIUS/TACACS+) → politika „heslo + OTP“
- **Cisco best practice**
  - Nasadzovať HW tokeny pre **vysoko privilegovaných používateľov** (admini, root access)
  - Politiky viazať na role (admin login vyžaduje token, bežný user nie)
- **Prevádzkové zásady**
  - Token musí byť **vždy v držbe používateľa** – never share!
  - Nastaviť životnosť OTP kódov (30–60 sekúnd TOTP)
  - Vynucovať ochranu PIN-om (smart karty, USB kľúče)
    - Alebo biometriou
  - Centrálne monitorovať stratu/odcudzenie tokenu → okamžitá deaktivácia

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



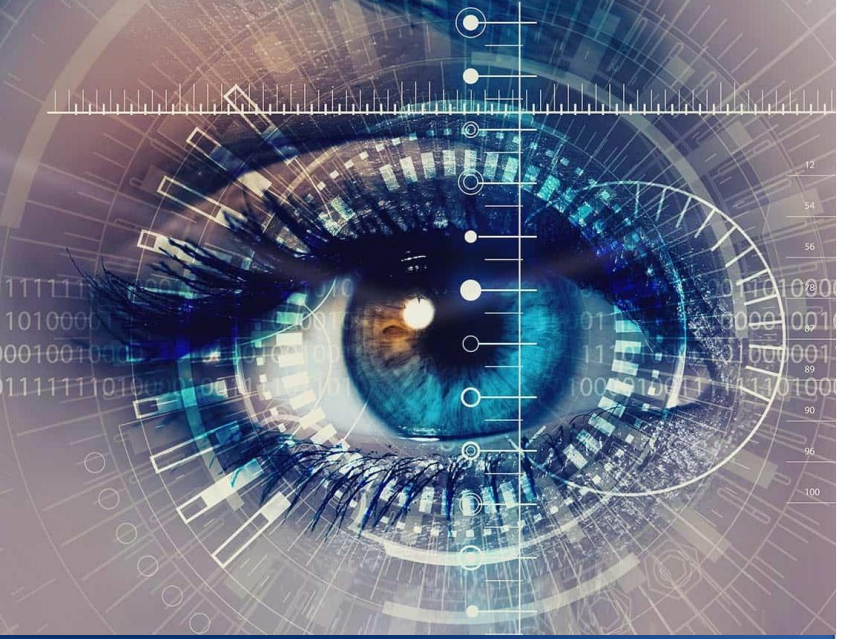
Certifikáty v sieťovej autentifikácii

- **Certifikáty**
  - Digitálny certifikát = kryptografický dôkaz identity (X.509 štandard)
  - Vydaný certifikačnou autoritou (CA), viaže identitu na verejný kľúč
  - Zlatý štandard pre sieťovú autentifikáciu
- **Princíp fungovania**
  - Overenie identity prebieha kryptografickým podpisom a validáciou CA reťazca
    - Privátne a verejné kľúče
  - Podpora revokácie cez CRL
- **Výhody**
  - Silná ochrana pred phishingom a MITM útokmi
  - Integrácia s AAA
  - Vysoká úroveň dôveryhodnosti pri autentifikácii
  - Najvyššia úroveň bezpečnosti
- **Nevýhody**
  - Potreba správy PKI (životný cyklus certifikátov)
  - Zložitejšia administrácia a distribúcia
  - Vyššia komplexita pre používateľov a admino

Best Practice pre certifikáty v sieťovej autentifikácii

- **(Cisco) best practice**
  - Vždy používať **silné algoritmy** – RSA ≥ 2048 bit, alebo ECDSA P-256/P-384
  - Nastaviť **maximálnu dobu platnosti** certifikátu (≤ 1–2 roky)
  - Automatizovať vydávanie/obnovu cez **SCEP/EST alebo certifikačný agent (ISE, MS ADCS)**
  - Validovať certifikáty voči CRL/OCSP → zabrániť používaniu zrušených certifikátov
  - Používať **separačné CA pre infra** a oddeliť internú CA od verejnej
- **Prevádzkové zásady**
  - Uchovávať privátne kľúče v **HSM alebo TPM** (nie v plaintext súboroch)
  - Používať unikátne certifikáty pre každé zariadenie a používateľa
  - Segmentovať PKI hierarchiu (Root CA offline, SubordinateCA online)
  - Implementovať proces revokácie (CRL publikácia)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Niečo, čo som (Something You Are)

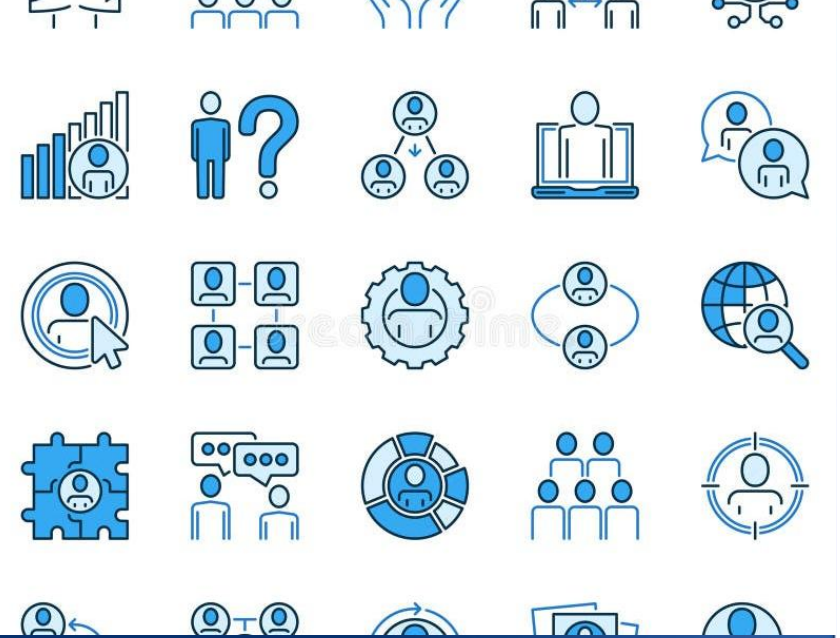
- **Definícia**
  - Overenie identity na základe jedinečných fyziologických charakteristík
- **Metódy – fyzická biometrika**
  - Otlačok prsta (najrozšírenejšie, rýchle, lacné)
  - Iris scan (dúhovka) (najpresnejšie, drahé, infračervené skenovanie)
  - Retina scan (očné pozadie) (vysoko presné, veľmi invazívne – citlivé na zdravie)
  - Facial recognition (FaceID, 3D mapovanie tváre)
  - Geometria/palm scan (tvar ruky, línie)
- **Výhody**:
  - Veľmi ťažko napodobniteľné
  - Nie je potrebné si nič pamätať
  - Vysoká presnosť (najmä iris scan, fingerprint)
  - Stabilita znakov počas života
- **Nevýhody**:
  - Miera úspešnosti / rozpoznania
    - False Reject Rate / False Acceptance Rate (dôležité pre citlivé prostredia)
  - Náklady a implementácia
    - Hardvér, čas na enrollment
  - Súkromie
    - Etické a právne otázky (napr. GDPR)
    - Odmietanie zamestnancami
  - Zmena biometrie
    - Choroba, vek, úrazy môžu ovplyvniť spoľahlivosť

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Porovnanie biometrických metód

Kritérium	Fingerprint	Face	Hand Geometry	Iris	Voice
Prekážky univerzality	Opotrebované prsty, poranenie	Žiadne	Poranenie ruky	Zrakové postihnutie	Problémy s rečou
Unikátnosť	✅ Vysoká	❌ Nízka	⚠️ Stredná	✅ Vysoká	❌ Nízka
Trvácnosť (permanencia)	✅ Vysoká	⚠️ Stredná	⚠️ Stredná	✅ Vysoká	❌ Nízka
Zberateľnosť (collect.)	⚠️ Stredná	✅ Vysoká	✅ Vysoká	⚠️ Stredná	⚠️ Stredná
Výkon (presnosť)	✅ Vysoký	❌ Nízky	⚠️ Stredný	✅ Vysoký	❌ Nízky
Akceptovateľnosť	⚠️ Stredná	✅ Vysoká	⚠️ Stredná	❌ Nízka	✅ Vysoká
Odolnosť voči obchádzaniu	✅ Vysoká	❌ Nízka	⚠️ Stredná	✅ Vysoká	❌ Nízka

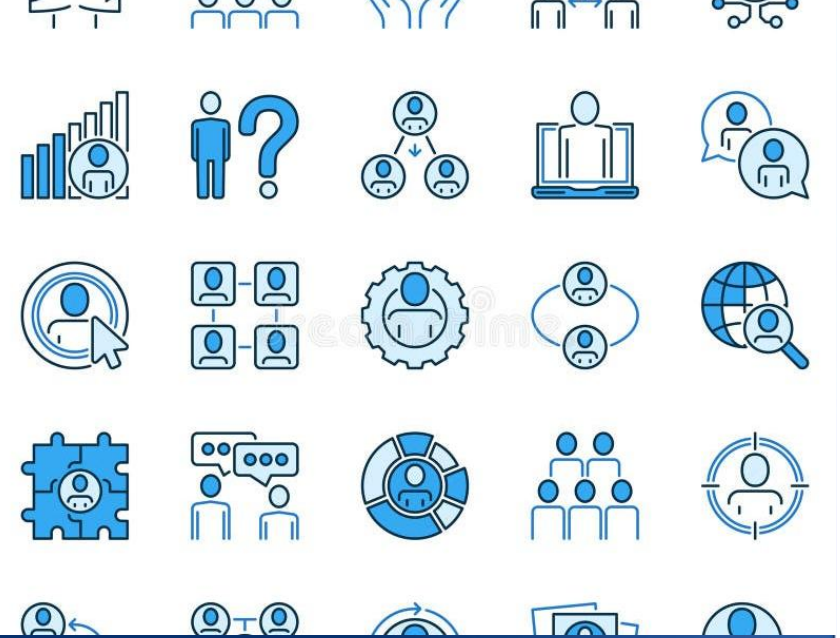
- Zdroj: internet



Niečo, čo robím (Something You Do)

- **Definícia**
  - Overenie identity na základe jedinečných behaviorálnych charakteristík
  - Unikátneho správania, ktoré je ťažko napodobniteľné, ale zároveň variabilné v čase
- **Metódy - Behaviorálna biometrika**
  - **Dynamika podpisu**
    - Sleduje: silu, rýchlosť, tlak, uhol a rytmus pohybu pri podpise
    - Príklady použitia: elektronické podpisové tablety, banky, digitálne zmluvy
  - **Dynamika písania na klávesnici (keystroke dynamics)**
    - Sleduje: dobu stlačenia klávesov, intervaly medzi údermi, špecifické sekvencie
    - Príklady použitia: autentifikácia v kritických systémoch, vojenské a výskumné prostredia
  - **Hlasový odtlačok (voice print)**
    - Sleduje: frekvenciu, tón, tempo, výslovnosť a intonáciu
    - Príklad: hlasová autentifikácia v call centrách, online bankovníctvo
  - **Pohyb myši**
    - Sleduje: trajektóriu kurzora, rýchlosť pohybu, mikrozastavenia, zmeny smeru
    - Príklad použitia: behaviorálna analýza používateľa v podnikových systémoch
  - **Chôdza (gait analysis)**
    - Sleduje: dĺžku kroku, polohu tela, rytmus a kadenciu pohybu.
    - Príklad : kamerové systémy na letiskách, bezpečnostné zóny, verejné priestranstvá

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



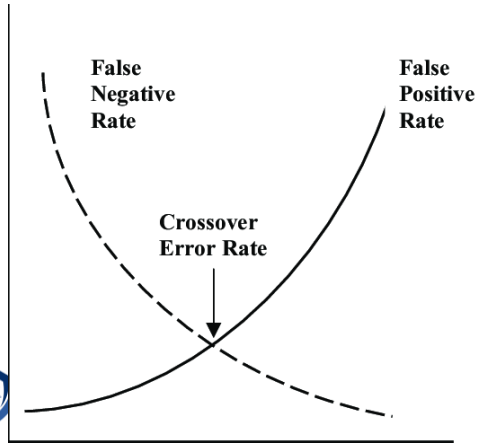
Niečo, čo robím (Something You Do)

- **Behaviorálna biometrika**
  - **Charakteristiky**
    - Závislé od kontextu a prostredia
    - Vyžadujú viac vzoriek pre spoľahlivú analýzu
    - Vhodné na kontinuálne overovanie identity (nie len pri prihlásení)
  - **Výhody**
    - Nízka invazívnosť – používateľ nemusí vedome konať
    - Môže prebiehať neustále (continuous authentication)
      - Podporuje tento koncept
    - Vhodné ako doplňujúca metóda (MFA)
  - **Nevýhody**
    - Menej presné ako fyziologické metódy
    - Citlivé na zmeny správania (únava, stres, choroba)
    - Vyššie požiadavky na AI/ML analýzu a kalibráciu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

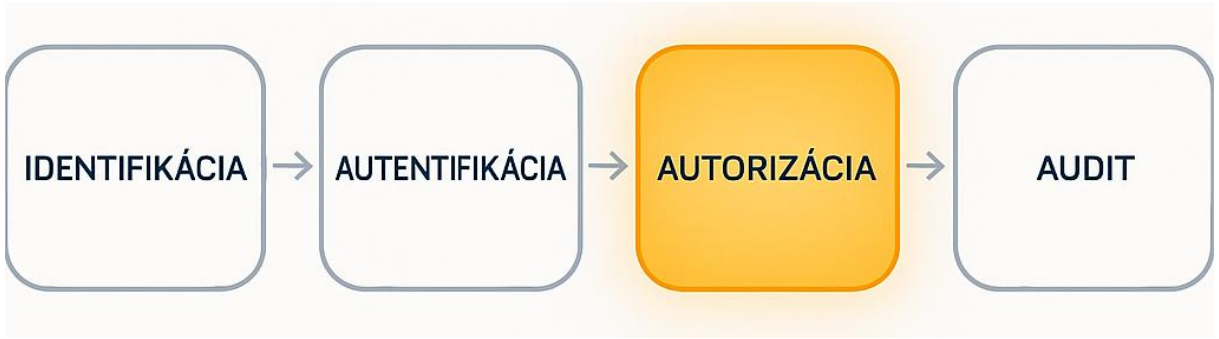
Chyba biometrických systémov

- Zaznamenávajú chyby
- Pred nákupom over chybovosť v biometrických systémoch: FAR, FRR a CER
  - 🚫 **False Rejection Rate (FRR)**
    - **Chyba typu I**
      - Oprávnený používateľ je nesprávne odmietnutý.
      - Vyjadruje pohodlie používateľa – systém je príliš „prísny“
  - ❌ **False Acceptance Rate (FAR)**
    - Známy ako **Chyba typu II**
      - Neoprávnený používateľ je nesprávne akceptovaný systémom
      - Vyjadruje bezpečnostné riziko – systém je príliš „mäkký“
  - ⚖️ **Crossover Error Rate (CER)**
    - Bod, kde sa FAR = FRR
    - Nižšia CER = lepší biometrický systém (nižšia chybovosť)
    - Kľúčová metrika pri porovnávaní a výbere biometrických riešení



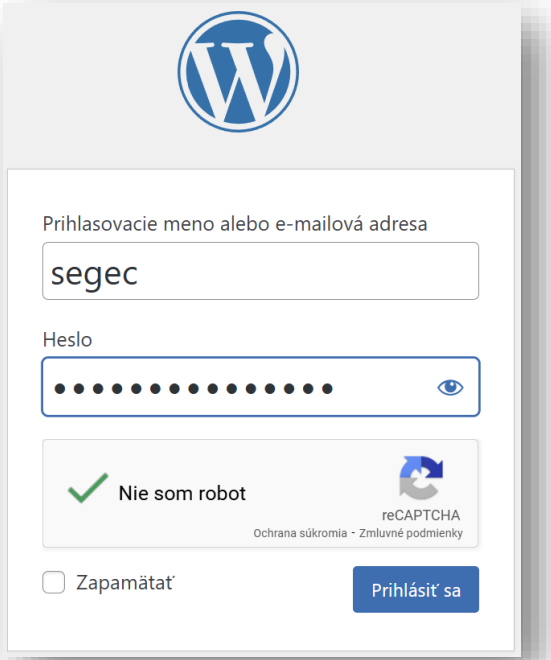
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

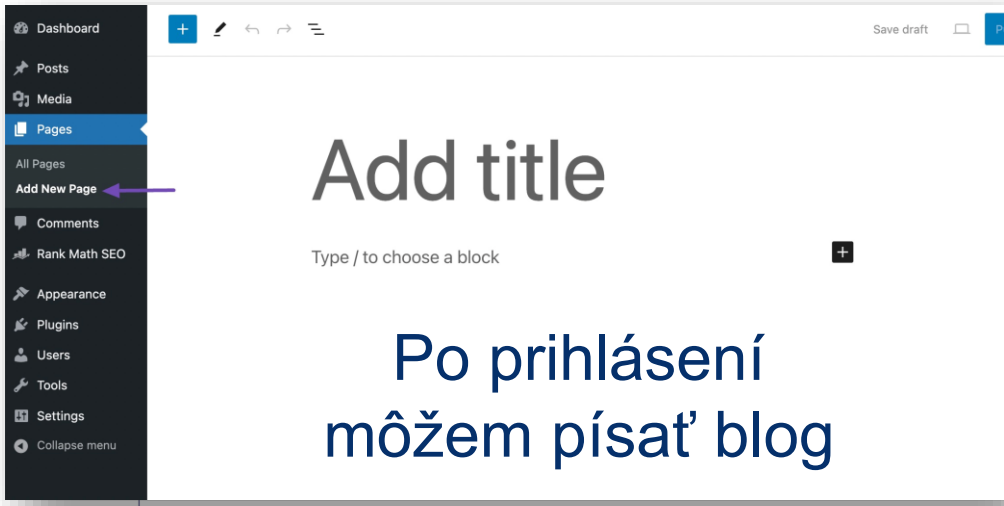
Autorizácia



Autentizácia a autorizácia

- **Autorizácia**
  - **Autentifikácia (Kto?) ≠ Autorizácia (Čo?)**
    - Autorizácia => **vykonáva sa po úspešnej autentifikácii**
  - Rozhoduje, či ***overená entita*** (používateľ, systém, služba) má ***právo (oprávnenie, povolenie)*** vykonať určitú ***akciu*** nad daným zdrojom
    - Kto => môže robiť Čo, Kde a Kedy?
    - Určuje tzv. prístupové práva po overení identity
- **Cieľ autorizácie v IAM**
  - **Obmedziť prístup** len na to, čo je **nevyhnutné** pre daného používateľa alebo službu
  - Znížiť riziká vyplývajúce z **nadmerných práv** alebo nesprávne pridelených oprávnení





Základné prvky autorizácie

Komponent	Otázka	Príklad
Subjekt (Who?)	Kto žiada prístup?	Používateľ, služba api_hr, proces
Objekt (What?)	K čomu sa chce dostať?	Dokument, súbor, databáza, služba
Akcia (How?)	Čo chce vykonať?	read, write, delete, execute
Podmienka (When/Where/Why?)	Za akých okolností?	IP adresa, čas, zariadenie

- **Vzťah** subjekt – objekt – akcia – podmienka **= Politika**
  - Autorizácia sa vykonáva na základe toho, či *subjekt* má právo vykonať *akciu* na *objekte* za daných *podmienok*
  - Politiky môžu byť jednoduché (napr. iba používateľ) alebo komplexné (zahŕňajúce viaceré atribúty)

Príklad politiky (JSON)

```
{
 "effect": "allow",
 "action": „write",
 "resource": "data_storage",
 "condition": {
   "ip": "10.0.0.0/8",
   "role": „head"
 }
}
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Statická vs. dynamická autorizácia

- **Statická autorizácia**
  - Pravidlá a oprávnenia sú pevne definované vopred
  - Rozhodnutie sa nemení podľa kontextu
  - Založené na:
    - priradených roliach
    - skupinách
    - pevne priradených ACL
  - Príklad:
    - Používateľ v danej skupine má stále rovnaké práva
      - Nezáleží na čase, mieste ani type zariadenia
  - **Typické modely:** DAC, MAC, základný RBAC

- **Dynamická autorizácia**
  - Rozhodovanie je podmienené aktuálnym kontextom
  - Politiky sa vyhodnocujú v reálnom čase
  - Zohľadňujú:
    - Poloha: Prihlásenie z neznámej krajiny môže vyžadovať dodatočné overenie.
    - Zariadenie: Používa sa známe alebo nové zariadenie?
    - Čas: Prihlásenie mimo pracovných hodín môže byť podozrivé.
    - Správanie: Nezvyčajné akcie (napr. veľké sťahovanie dát).
  - Na základe kontextu môže systém povoliť prístup
  - **Typické modely:** ABAC, RuBAC, RiskBAC

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Autorizácia

Odporúčania a osvedčené postupy (Best practise)

- **Pravidlo najnižších oprávnení (Least privilege)**
  - Udeľovať iba minimálne nevyhnutné oprávnenia potrebné na vykonanie úloh
  - Zabraňuje prideleniu rozsiahlych oprávnení a hrozbám
    - Neautorizovaný prístup, data leaking, bezpečnostné zneužitia
- **Pravidelná revízia prístupových práv**
  - Detekcia nadbytočných a neaktuálnych práv (napr. po zmene roly)
  - Súčasť compliance (ISO 27001, NIST AC-2)
  - Pozn. podľa AWS => až 50 % nižšie riziko pri pravidelných kontrolách (Achieve Least Privilege - CloudSec.Cybr)
- **Pravidelná kontrola a aktualizácia prístupových politík**
  - Reaguje na zmeny v rolách, štruktúre organizácie, systémoch
- **Segregácia právomocí (Separation of Duties)**
  - Prevencia eskalácie práv
  - Napr. schvaľovanie vs. vykonávanie transakcií
- **Časovo obmedzené práva (Just-in-Time access)**
  - Práva udeľované na obmedzený čas (napr. incident response, support)
  - Znižuje dlhodobý „attack surface“
- **Kritické prístupy chrániť pomocou MFA**
  - Kombinácia faktorov (napr. heslo + token) na silnejšie overenie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Audit a logging (Accounting)

Posledné „A“ v AAA

Audit a logging (Accounting)

- **Audit (Accounting / Accountability)**
  - Systematické zaznamenávanie relevantných aktivít súvisiacich s identitami a prístupmi
    - Kto, kedy, čo robil a s akým výsledkom
- Účel logovania a auditovania
  - **Forenzná analýza**
    - Rekonštrukcia incidentov (kto čo spravil pred únikom dát)
  - **Detekcia anomálií, incidentov a poručení politík**
    - Identifikácia podozrivého správania (napr. neobvyklé prihlásenia, prístupy)
  - **Dodržiavanie compliance**
    - Súlad s reguláciami (GDPR, NIS2, ISO 27001) a internými politikami
  - **Zodpovednosť**
    - Transparentnosť operácií a možnosť priradiť akcie konkrétnym identitám.
  - **Trasovanie**
    - Čo sa dialo v systéme
  - ...
- **Chyby pri absencii auditu:**
  - Žiadna stopa po incidente
  - Nemožnosť preukázať súlad
  - Nedôvera interného auditu / CSIRT

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

%LINK -3 UPDOWN: Interface FastI

Čo sa vo všeobecnosti loguje?

- **Systémové udalosti**
  - Výkon a stav systému (CPU, RAM, služby)
  - Prístupy k systémovým nastaveniam
  - Použitie administračných nástrojov
  - *Príklad: Sysmon, Event ID 4688 (Windows)*
- **Aplikačné udalosti**
  - Prístupy k databázam, súborom, systémom
  - Zmeny konfigurácií aplikácií
  - Bezpečnostné chyby, výnimky, neštandardné volania API
  - *Príklad: CloudTrail, syslog, SIEM udalosti*
- **Používateľské akcie**
  - Úspešné / neúspešné prihlásenia
  - Použitie privilegovaných účtov (root, admin, servisné účty)
  - Zmeny oprávnení a rolí (pridanie, zmena, odobratie)
  - Prístup k citlivým zdrojom (ZP, osobné údaje, finančné dáta)
  - Zmeny v IAM politikách, konfiguračných súboroch
  - *Príklad: Windows 11 logs, Active Directory logs, Azure AD logs, Okta events*

Audit a logging (Accounting)

Čo sa loguje v IAM?

- **Identita & jej životný cyklus**
  - Vytvorenie/aktivácia/deaktivácia účtu, zmeny atribútov (meno, oddelenie, manager)
  - Priradenie/odobratie rolí/skupín; nadobudnutie a ukončenie privilégií (PIM/JIT)
  - Prepojenie/odpojenie externých identít (Google/Azure B2B)
- **Poverenia & autentifikátory**
  - Zmena/reset hesla, MFA enrollment/unenrollment (FIDO2, TOTP, SMS), recovery operácie
  - Registrácia/revokácia passkeys/FIDO2, zmena PIN/biometrie
  - Vydanie/obnova certifikátov/SSH kľúčov, revokácie (CRL)
- **Autentifikácia (AuthN)**
  - Úspešné/neúspešné prihlásenia (IdP aj aplikácia), dôvod zlyhania (heslo, MFA, lockout)
  - Rizikové signály: IP/geo, zariadenie, user agent, neobvyklý čas, reputácia
  - Session: vznik/obnova/ukončenie, session ID (hash), dôvod odhlásenia/expirácie
- **SSO & Federácia (SAML/OIDC)**
  - Vydanie SAML Assertion / OIDC ID tokenu (issuer, audience, exp)
  - Refresh/rotácia tokenov, použitie refresh tokenu, neúspešné pokusy
  - Revokácia/introspekcia tokenov (opaque), zablokovanie relácie
  - Zmeny trust vzťahov: metadata, certifikáty (rotácia podpis/šifrovanie), client registration
- **Autorizácia (AuthZ) & enforcement**
  - PDP rozhodnutie: allow/deny, policy ID a verzia, vstupné atribúty/kontext (minimálne: subject, resource, action)
  - PEP výsledok: uplatnenie rozhodnutia, deny dôvod (chýbajúci scope/role/atribút, časové/geo obmedzenie)
- **Administrácia IdP/IAM**
  - Konfiguračné zmeny IdP (MFA policy, password policy, session TTL), zmeny redirect URI, client secrets
  - Role a akcie administrátorov (create/delete tenant, vypnutie politiky, export logov)
  - Kľúče a certifikáty IdP (rotácia, expirácia, HSM/KMS operácie)

Best practise

Osvedčené postupy

- **Minimálne polia v každej udalosti**
  - **event_type** (authn_success, authn_failure, token_issue, pdp_deny…)
  - **timestamp (UTC)** a **realm**
  - **actor** (kto konal) a **subject** (koho sa týka)
  - **source** (IdP/PEP/app)
  - **client**: IP, user-agent, zariadenie/geo (ak je)
  - **result**: success/failed + **reason** (napr. bad_password, mfa_rejected)
- **AAA logy vždy centralizovať**
  - Neponechávať iba na zariadení (buffer limited)
  - **Centralizovať do špecializovaného nástroja**
    - **Logstash/Elasticsearch + Kibana (ELK stack)**
    - **Graylog** (open-source, s web UI)
    - **Splunk, IBM QRadar, ArcSight** (komerčné SIEM)
- **Bezpečné ukladanie logov**
  - Immutable, hashované, zabezpečená komunikácia
- **Retencia a archív logov**
  - Minimálne 90 dní pre prevádzkové účely, 1 rok pre bezpečnostné/compliance účely
  - ISO 27001 a GDPR môžu mať špecifické požiadavky
- **Pravidelný review logov + alertovanie**

- **Nevýhoda**
  - Big data
    - Ak logujem všetko => zahltenie dátami
- Challenge
  - **Vypracovať riešenie ktoré dáva zmysel a nájsť vhodný nástroj**
    - Napr. zadanie zlého hesla
      - Potrebujem vedieť o všetkých zle zadaných heslách všetkými používateľmi?
      - Alebo až keď jeden zadá veľa krát za sebou?
      - ==> Allerting
  - **Monitoring a korelácia**
    - Vysoký počet login pokusov → alert (možný brute-force útok)
    - Policy/IdP konfigurácia zmenená mimo údržby
    - Refresh re-use / masová token_revoke

Správa identít, poverení a relácii (Identity, Credential & Session management) v IAM

AAA / Access & Authentication management

Životný cyklus riadenia identít používateľov - fázy

- **Identity Lifecycle Management**
  - Zameriava sa na kto používateľ je
  - Správa digitálnych identít je proces

FÁZY

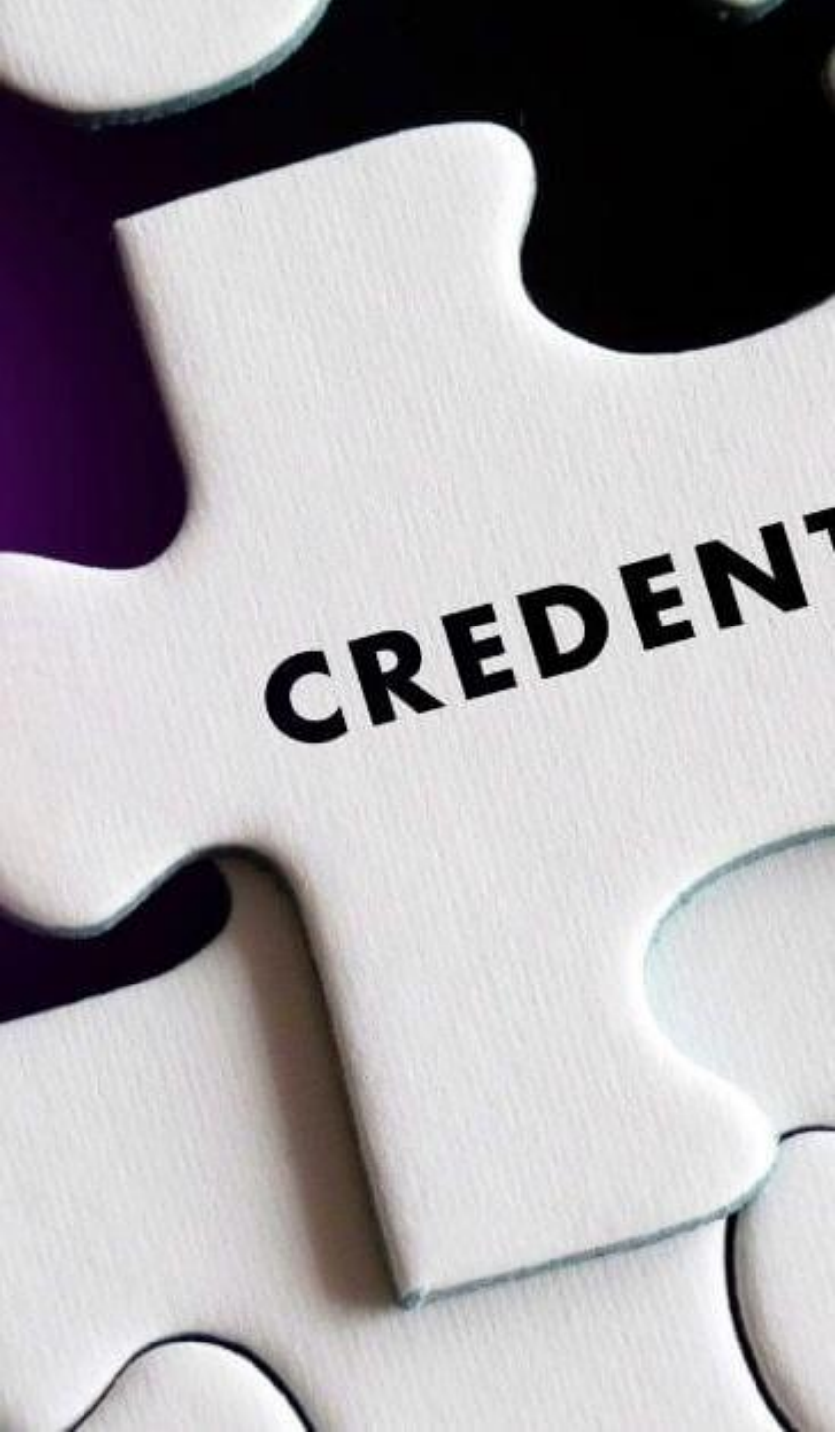
- **Problémy pri neriešení ILM:**
  - Neodstránené účty po odchode osoby (→ insider threat)
  - Prístupy bez vlastníka („orphaned access“)
  - Neaktuálne roly → privilege creep
  - Zdieľané kontá → chýba accountability
  - Chýbajúci audit → nie je záznam o deaktivácii účtu

- **Životný cyklus riadenia identít**
  - **Identita – vznik a overenie**
    - Príjem zamestnanca - založenie účtu v HR systéme
    - Overenie totožnosti → ID proofing → napr. podľa NIST SP 800-63A
    - Priradenie unikátneho identifikátora → napr. psegec
  - **Onboarding (provisioning)**
    - Vytvorenie účtu v systémoch → napr. v AD, email, ERP, cloud služby
    - Priradenie rolí, skupín, prístupov, autentifikačných údajov (heslo, MFA)
      - Automatizovane cez IAM systém (SCIM 2) alebo ručne (low maturity)
  - **Prevádzka účtu a zmeny**
    - Zmeny (napr. tím, rola, projekt)
      - Potreba zníženia alebo zvýšenia oprávnení, presun, zmena pracovnej náplne
    - Monitoring aktivít, periodická revízia oprávnení
  - **Offboarding (deprovisioning)**
    - Zrušenie prístupov, deaktivácia účtu
    - Odobratie tokenov, kariet, certifikátov
  - **Audit a archivácia**
    - Zachovanie záznamu o prístupe na účely forenznej analýzy
    - Označenie ako neaktívny, uloženie do archívu
    - Odpojenie od identity providera (SSO, AD)

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Automatizácia ILM - SCIM 2.0

- SCIM 2.0 (**System for Cross-domain Identity Management**)
  - Otvorený štandard určený na **automatizovanú správu identít a ich atribútov** medzi rôznymi systémami a aplikáciami
  - Používa sa najmä v prostredí **cloudových služieb** a **identity providerov** (napr. Azure AD, Okta, Ping Identity)
- **Hlavné vlastnosti SCIM 2.0**
  - **Protokol:** REST API (HTTP) + JSON formát dát
  - **Účel:** Provisioning a deprovisioning používateľov a skupín (napr. vytváranie, aktualizácia, mazanie)
  - **Štandardizované schémy:** Definuje jednotné atribúty (napr. userName, emails, groups), aby rôzne systémy vedeli spolupracovať
  - **Výhoda:** Znižuje potrebu vlastných konektorov a skriptov, čím zjednodušuje integráciu medzi SaaS aplikáciami a identity systémami
- **Príklad použitia**
  - Firma má **Azure AD** a používa SaaS aplikácie (Slack, Salesforce)
  - Pomocou SCIM 2.0 sa automaticky:
    - Vytvorí nový používateľ v Slacku, keď je pridaný do Azure AD
    - Deaktivuje účet, keď zamestnanec odíde



Správa poverení (Credential management)

Poverenia a prečo na nich záleží

- **„Credentials“ - prihlasovacie údaje (poverenia)**
  - Údaje alebo objekty na **preukázanie identity**
    - Používateľské poverenia (heslá, passkeys, MFA), **aplikačné** (API kľúče, klientské tajomstvá), **strojové** (certifikáty, SSH)
- **Problém**
  - Zneužitie poverení je najčastejším zdrojom incidentov
    - 80 % útokov začína zneužitím poverení
      - *Zdroj Verizon Data Breach Investigations Report*
- **Kontext správy poverení (credential man. (CM))**
  - Credential ≠ identita – jedna identita môže mať viac poverení
  - CM sazameriava na to ako sa používateľ autentifikuje
    - Správa prihlasovacích údajov: heslá, certifikáty, tokeny, kľúče.
  - **Cieľ CM**
    - Chrániť prihlasovacie a prístupové údaje (heslá, kľúče, tokeny) počas celého životného cyklu
    - Minimalizovať riziká (nadmerné oprávnenia, zabudnuté účty, schvaľovanie ...)
    - Zabezpečiť konzistentnosť a auditovateľnosť

Účel a funkcie správy poverení (CM)

- **Registrácia & vytváranie prihlasovacích údajov**
  - Generovanie silných hesiel, kľúčov, tokenov alebo certifikátov
  - Na všetkých relevantných systémoch a platformách (AD, aplikácie, cloud...)
- **Uloženie** údajov
  - Šifrované úložiska (napr. password vault, HSM); zálohy
- **Distribúcia** údajov
  - Bezpečný prenos údajov k systémom alebo používateľom
- **Obnova a rotácia**
  - Resetovanie hesiel, rotácia kľúčov, obnova certifikátov
- **Politiky platnosti**
  - Expirácia, rotácia a obmedzenie opakovaného použitia údajov
  - Prevencia tzv. „orphaned accounts“ – zabudnuté aktívne kontá
- **Revokácia**
  - Okamžité zneplatnenie pri **odchode osoby**, zmene roly alebo podozrení
  - Stiahnutie z trezora/IdP, odvolanie certifikátu (CRL)
- **Audit a monitoring**
  - Záznamy o vydaní, použití, zmene, zrušení; výnimky a schválenia
  - Napojenie na SIEM a pravidelné recertifikácie poverení

Riešenia pre správy poverení v IAM / Technické metódy

- **Správca hesiel (Password Managers)**
  - Programy/služby, ktoré bezpečne ukladajú používateľské heslá
    - OS app, browser plugin
  - **Prínos:** Dlhé, unikátne heslá bez nutnosti si ich pamätať
  - **Riziko:** Kompromitácia správcu hesiel ==> prístup ku všetkému
  - Príklad: Keepass, Bitwarden, 1Password ...
- **Synchronizácia hesiel (Password Synchronization)**
  - Rovnaké heslo pre viaceré systémy (FIM a SSO)
  - Typicky sa kombinuje s MFA
  - **Prínos:** menej hesiel, jednoduchšie spravovanie
  - **Riziko:** jeden únik hesla kompromituje všetky systémy
- **Multi-Factor Authentication (MFA) a jeho manažment / passwordless prístup**
  - Správa viacerých autentifikačných faktorov (heslo + token/biometria).
  - **Prínos**: Zvyšuje bezpečnosť autentifikácie.
  - **Riziko**: Komplexita implementácie a používateľské chyby.
- **Self-Service – SSPR (Password Reset + Profile Update)**
  - Samo-obnova zabudnutého hesla - odľahčuje admin/help desk
  - Vyžaduje dodatočné silné overenie (MFA, otázky...)
  - **Prínos**: Odľahčuje helpdesk
  - **Riziko**: Vyžaduje silné overenie

Úloha: **kedy, kde a pre koho** sa má daná metóda použiť

Riešenia pre správy poverení v IAM / Procesné metódy

- **Assisted Password Reset (pomocou helpdesku)**
  - Obnova hesla cez administrátora/helpdesk
  - Vyžaduje formálny postup overenia identity
    - e-mail, zamestnanecké ID, telefonát ...
  - **Riziko:** Vysoké riziko sociálneho inžinierstva (napr. cez phishing, spoofing)
    - Príklad: Twitter => Zneužitie resetu cez Helpdesk Twitter (2020) + poslanie tweetov na Bitcoin (120000 BTC)
- **Just-in-Time Access (JIT)**
  - Dynamické a dočasné poverenie len na čas potreby
  - Používa sa pre adminov alebo privilegované akcie
  - **Prínosy:** Znižuje riziko stálych vysokých oprávnení
  - Príklad: Microsoft PIM (Privileged Identity Management), AWS IAM Roles s časovým obmedzením
- **Credential Vaulting**
  - Centralizované bezpečné ukladanie všetkých poverení v trezore
  - Prístup kontrolovaný IAM politikami
  - **Prínos**: Minimalizuje riziko neoprávneného prístupu
  - **Riziko**: Centrálny bod zlyhania pri kompromitácii
  - Príklad: HashiCorp Vault, CyberArk…

Úloha: **kedy, kde a pre koho** sa má daná metóda použiť

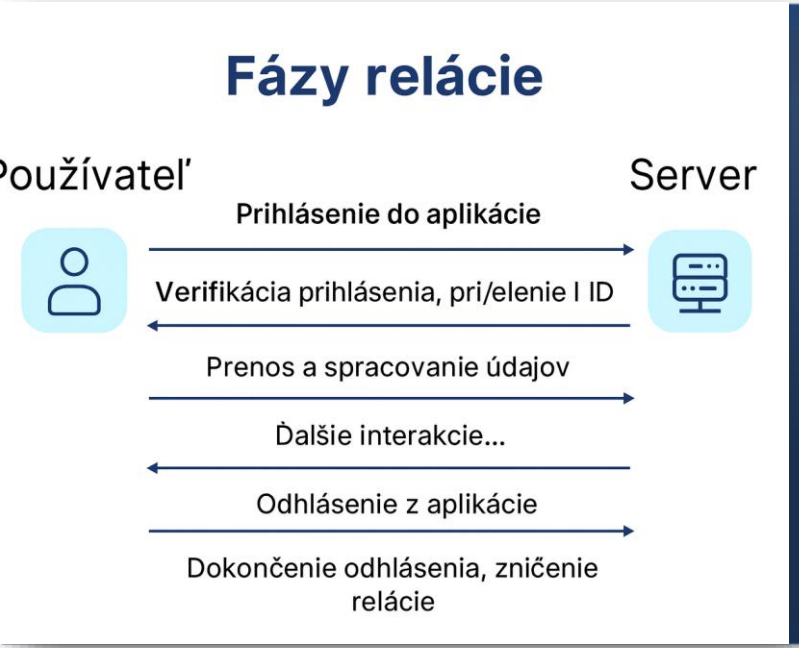
Moderné prístupy

- **Manažér/správca hesiel**
  - Aplikácie, ktoré bezpečne uchovávajú tvoje heslá v tzv. trezore hesiel
  - Výhody:
    - Obsahujú password generátory
    - Uchovávajú všetky tvoje heslá na jednom mieste
    - Prístupné z viacerých zariadení (mobil, PC, tablet)
    - Zabezpečené šifrovaním a hlavným heslom
    - Automatické vypĺňanie prihlasovacích údajov
  - Príklady aplikácií:
    - Bitwarden – open-source, bezpečný a bezplatný
    - KeePass2
    - 1Password – vhodný pre rodiny a firmy
- **„Passwordless“ prístup - Autentifikácia bez hesla**
  - Nevyužíva tradičné heslá
  - Spolieha na **biometriu**, smart karty, bezpečnostné kľúče alebo SSH kľúče
  - Príklady:
    - Touch ID / Face ID – biometria na Apple zariadeniach
    - Smart karty – používajú PIN a certifikáty
    - SSH kľúče – bezpečné prihlásenie bez hesla
    - Bezpečnostné tokeny – napr. YubiKey
  - Výhody:
    - Vyššia bezpečnosť – žiadne heslá na zapamätanie alebo ukradnutie
    - Ochrana pred phishingom
    - Rýchle a pohodlné prihlásenie
    - Zníženie administratívnej záťaže

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Privileged Access Management (PAM)

- **Privileged Access Management (PAM)**
  - Obmedzuje a riadi administrátorské a citlivé účty (privilegované: root/admin, DB admin ...)
  - Umožňuje dočasné pridelenie privilégií podľa potreby (kedy a ako)
  - Zabezpečuje audit a monitoring citlivých prístupov (audit stopa)
- Kľúčové vlastnosti riešenia PAM
  - **Efemérne oprávnenia:** Jednorazové, časovo obmedzené prístupy
  - **Prístup podľa role:** Napr. admin na zálohovanie, ale nie na zmenu účtov
  - **Automatické zrušenie práv** po skončení úlohy alebo relácie
  - **Logovanie a monitoring** – kto, kedy, kde a prečo použil zvýšený prístup
- Hlavné techniky: JIT / krátkodobé poverenia, password vaulting,
- **Príklady nástrojov:**
  - Microsoft PAM (v rámci AD Privileged Access Workstation)
  - CyberArk, BeyondTrust, HashiCorp Boundary
  - AWS Session Manager, Azure Privileged Identity Management

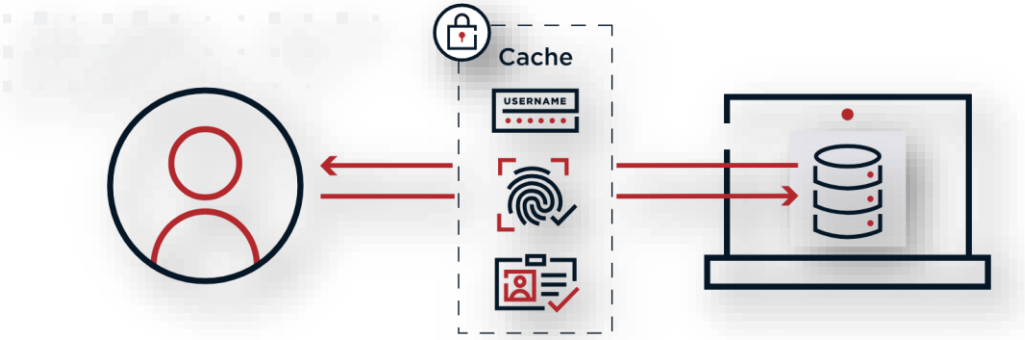


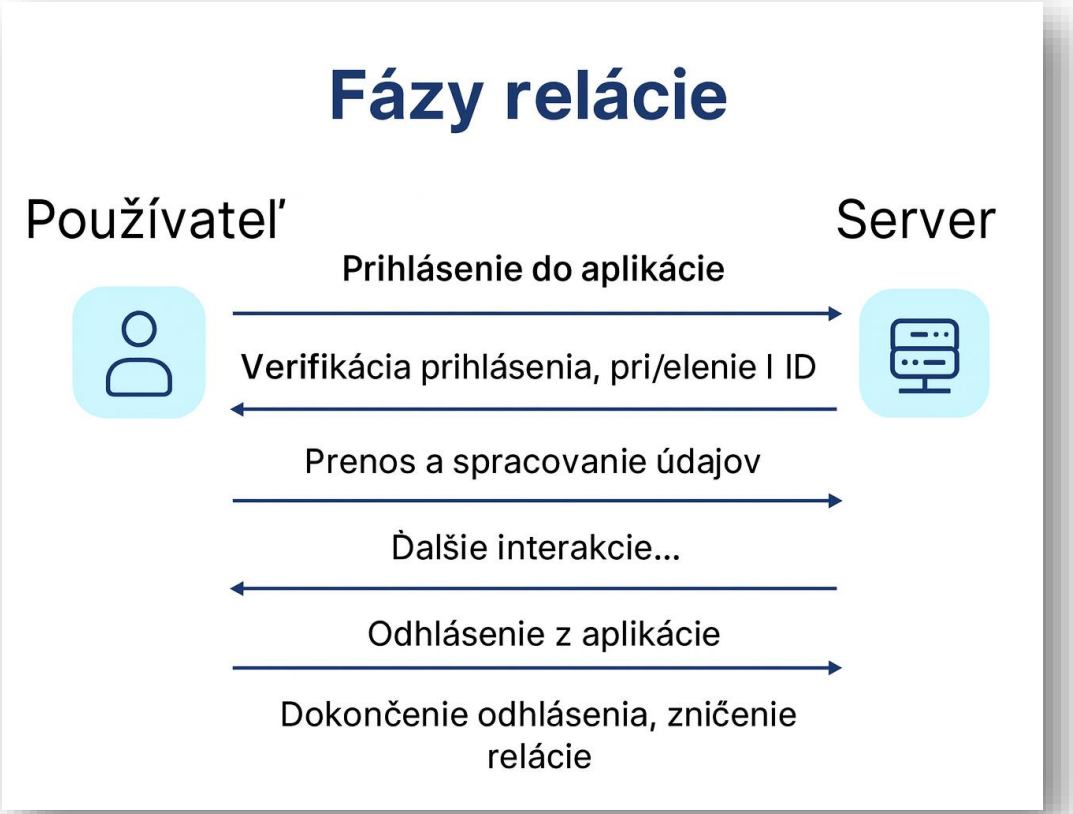
Správa relácii (Session management)

Riadenie spojenia po overení

Relácia - princípy

- **Relácia (session)**
  - Časovo **obmedzené stavové** spojenie medzi používateľom a systémom
    - Vzniká po úspešnej autentifikácii používateľa
- **ID relácie**
  - *Session ID* alebo *token* generovaný serverom
    - Klient posiela ID pri každej požiadavke
    - Nie je treba sa znovu autentizovať / neposiela sa meno a heslo
- Životný cyklus relácie
  - Vytvorenie → používanie → sledovanie → ukončenie (timeout/logout/admin)
- **Cieľ**
  - Umožniť **opakovaný prístup** podľa práv počas trvania reláci





Identifikácia relácie (príklad HTTP)

- **Session ID (identifikátor relácie)**
  - Unikátny náhodný identifikátor
  - **Generuje server** per klienta pri vytvorení relácie
  - Doručenie klientovi:
    - Najčastejšie cez HTTP cookie (hlavička)

```
Set-Cookie: session_id=abc123; HttpOnly; Secure;
SameSite=Strict
```

    - Menej často cez URL parameter
      - Neodporúča sa kvôli bezpečnosti !!!

```
https://example.com/dashboard?session_id=abc123)
```

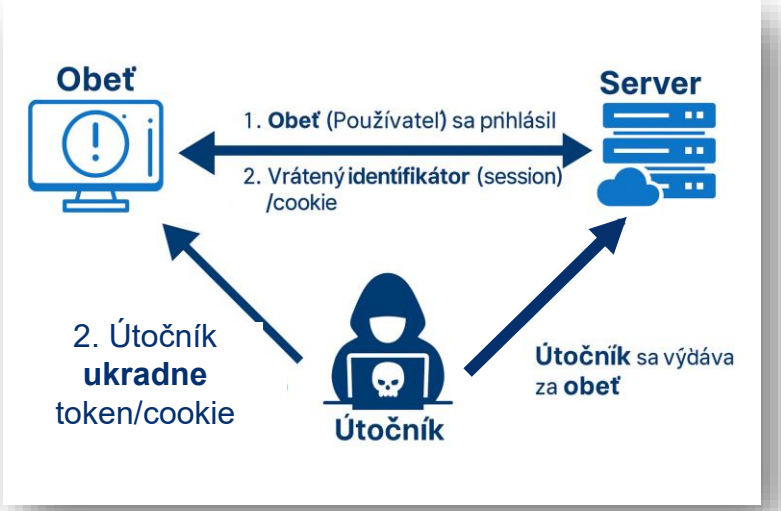
- **Token (napr. JWT – JSON Web Token)**
  - Šifrovaný alebo podpísaný token, ktorý obsahuje informácie o používateľovi a platnosti
  - Doručenie klientovi:
    - V odpovedi servera

```
{
  "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9..."
}
```

    - **Klient ho potom posiela** späť v hlavičke požiadavky:

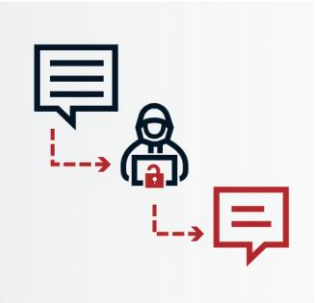
```
Authorization: Bearer eyJhbGciOiJ...
```

Relácie – problémy a riziká



- Ak relácia nie je **správne riadená =>** môže byť **zneužitá**
- Typické útoky
  - **Man in the middle**
    - Útočník sa **vkladá do cesty medzi klienta a server**
    - Môže meniť alebo zachytávať dáta relácie.
      Najčastejšie ak nie je použitý **HTTPS**, alebo je TLS zle nakonfigurovaný
  - **Session Hijacking**
    - Útočník získa session ID (napr. z cookies alebo cez sieť)
    - Získa oprávnenia používateľa bez prihlásenia
    - Bežné pri slabom zabezpečení relácie (napr. neobmedzené trvanie, nešifrovaný prenos)
  - **Replay attacks**
    - Opätovné použitie predchádzajúcej platnej relácie
      - Napr. útočník zachytí request a „prehrá ho znova“
    - Ak systém neoveruje kontext alebo aktuálnosť relácie
  - **Nechránené komunikácie**
    - Nešifrované dáta (protokoly ako telnet, http ...)
    - Prečítanie údajov, odchytenie bezpečnostných údajov
  - **Nesprávna správa relácií na strane servera / Nedostatočné časovače**
    - Dlhé nečinné relácie
    - Systém **neukončí reláciu** po nečinnosti a útočník môže prevziať otvorený prístup
  - **...**

Session Hijacking



Man-in-the-Middle Attacks

Zabezpečenie relácie

- **Data in Use**
  - Údaje spracovávané v systéme
    - Session ID/token uložený v pamäti
    - Prehliadač, aplikácia alebo server
  - Riziká:
    - Únik session ID pri zlom ukladaní
    - Lokálny malware (napr. keylogger, infostealer)
    - Zdieľané počítače alebo prehliadače
  - Opatrenia
    - Ochrana pred únikom údajov z pamäte
    - Vyhýbať sa zdieľaným zariadeniam bez ochrany

- **Data in Transport**
  - Údaje prenášané medzi klientom a serverom
  - Dôležité opatrenia:
    - Vždy HTTPS s TLS 1.2+  https://w
    - Nastavenie cookies s Secure (iba cez HTTPS) / HttpOnly (neprístupné cez JavaScript) / SameSite (ochrana proti CSRF)
    - Žiadne session ID v URL

- **Bezpečnosť session ID/tokenov**
  - Dĺžka, náhodnosť a jedinečnosť identifikátorov
  - Obmedzená platnosť

- **Obnova a rotácia identifikátora**
  - Obnova sessionID po re/autentifikácii
    - Po zmene hesla alebo úrovne oprávnení
  - Krátka životnosť + pravidelná obnova tokenov

Správa relácií – kde?

- **Server-side session management (stavový)**
  - Klient: drží len cookie s ID
  - Server: drží stav relácie (DB)
    - Proces identifikácie prebieha vyhľadávaním v serverovej pamäti alebo databáze
  - **Výhody**
    - Centrálna kontrola + zneplatnenie relácie kedykoľvek
    - Nižší objem dát na klienta
  - **Nevýhody**
    - Vyžaduje škálovanie s rozdelením stavu medzi servermi => zvýšenie spotreby pamäte a serverových zdrojov
- **Client-side session management (bezstavový)**
  - Klient: má podpísaný token (napr. JWT)
    - údaje o relácii, identite, roli a expirácií
  - Server: len overí dig. Podpis, stav nedrží
  - **Výhody**
    - Zvyšuje škálovateľnosť (bezstavové API)
    - Nie je treba session tabuľky na serveri
    - Modernejší prístup
  - **Nevýhody**
    - Zneplatnenie tokenu / revokácia
    - Vyššie riziko kvôli ukladaniu dát na klientovi
    - Nutnosť správy certifikátov/kľúčov

Správa relácií – manažérske minimum

- **Čo riadime**
  - Vytvorenie silnej relácie po AuthN (session ID/token) + väzba na identitu a rolu
  - Priebežná ochrana relácie (šifrovanie, obnova ID, cookie zásady)
  - Ukončenie relácie (idle/absolute timeout, povinný logout/invalidácia)
- **Bezpečnostné zásady**
  - Vždy TLS, žiadny session ID/token v URL
  - Cookies Secure/HttpOnly/SameSite; chránené úložisko na klientovi
  - Session renewal po prihlásení, zmene privilégií alebo po danom čase
- **Detekcia & reakcia**
  - Monitorovať anomálie (geo/IP/zariadenie/čas)
  - Pri podozrení blokovať / vynútiť obnovu relácie
  - Centralizované logovanie → SIEM/SOAR pre audit a forenziku
- **Zodpovednosti (KYB)**
  - Vynucovanie (PEP): aplikácia/API, web server/WAF, IdP/SSO, PAM
  - Politiky & dohľad: bezpečnostný manažér, SOC

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Blok II: Modely riadenia prístupu

Autorizačné modely / riadenie oprávnení

Riadenie prístupu – čo je to?

- ***Riadenie prístupu*** *(Access Control)*
  - Proces zabezpečenia, že iba **oprávnené entity** (subjekty) môžu pristupovať ku konkrétnym **zdrojom** (objektom) (*všeobecne*) => asset-om / aktívam
- Riadenie prístupu
  - nadväzuje na **Identifikáciu** → poznáme, kto je používateľ (napr. login, ID)
  - nadväzuje na **Autentifikáciu** → overíme, že je to naozaj on (napr. heslo, token, biometria)
  - Implementuje **Autorizáciu (riadenie prístupu)** → rozhodnutie *či, k čomu a ako* má používateľ/entita prístup
- **Cieľ riadenia prístupu**
  - Ochrana citlivých údajov, systémov a služieb
  - Minimalizácia rizika neoprávneného prístupu (interného aj externého)
  - Zavedenie **kontroly a zodpovednosti** – kto čo robí, kedy, ako a prečo

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy kontrol prístupu

Širšie typy kontroly prístupu (kategórie)**:**

- 🧱 **Fyzická kontrola** prístupu
  - Vstup do fyzického objektu
  - Zabezpečenie pomocou preukazu, zámky, turnikety, kamery, ochranka, psy ....
- 💻 **Logická (technická) kontrola** prístupu
  - Súbor technických opatrení (mechanizmov)
    - **kto** má prístup k **akým systémom, dátam a službám**
    - **ako, kedy a za akých podmienok** je tento prístup povolený
    - zabezpečujú, že prístup je **autentifikovaný, autorizovaný a auditovaný**
    - Technológia: Heslá, smart karty, biometria, firewall, protokoly, SW systémy
- 📋 **Administratívna kontrola** prístupu
  - Nastavuje rámec riešenia prístupu (čo a ako)
  - Politiky, školenia, prideľovanie rolí a právomocí

V kontexte KYB **logické AC = technické AC**
=> Implementácia **AAA (Autentifikácia, Autorizácia, Audit)**

Prístupové metódy

- Riadenie prístupu *(access control)*?
  - **==>** popis pomocou modelu / rámca (DAC, RBAC, ...)
  - **==>** implementácia pomocou *prístupových metód* v *procese pridelenia oprávnení*

- **Prístupová metóda** = **Konkrétny nástroj alebo technika (postup)**
  - Spôsob, akým systém rozhoduje o tom, aké práva máme
    - Čo smieme robiť po autentifikácii
      - Prihlasovanie meno a heslo pomocou Win Login, Linux PAM ...
      - Pravidlá firewallu, ACL, IP filtre
      - Autorizácia cez OAuth2, SAML, Kerberos ...
    - ...
  - Sú všade tam, kde je potrebné kontrolovať prístup
    - Či už v operačnom systéme, aplikácii, cloudových službách ...
  - ***Implementuje* autorizačné pravidlá** (Čo je povolené / zakázané)

Základné prvky autorizačných pravidiel

- **Kľúčové prvky:**

Prvok	Význam	Príklad
Identita (subject)	Entita so zaregistrovanou identitou(človek, služba, systém)	j.kovac, svc_backupsrv01
Skupina (group)	Logické zoskupenie identít Zjednodušenie hromadného riadenia prístupu	HR_users, DB_readonly
Rola (role)	Súbor oprávnení viazaný na funkciu	Fin_Analyst, Sys_Admin
Politika (policy)	Štruktúrované pravidlo určujúce prístupové práva	JSON, XML, YAML...
Objekt (resource)	Chránený digitálny zdroj	API endpoint, databáza, VM, aplikácia
Akcia (action)	Operácia, ktorú chce subjekt vykonať	read, write, delete
Podmienka (condition)	Konkrétna situácia alebo kontext	čas, IP, MFA, typ zariadenia

```
IF role == „Head_department" AND resource == "Employee_DB"
THEN permit action == "read/write"
```

Model = rámec alebo princíp

Modely technického riadenia prístupu

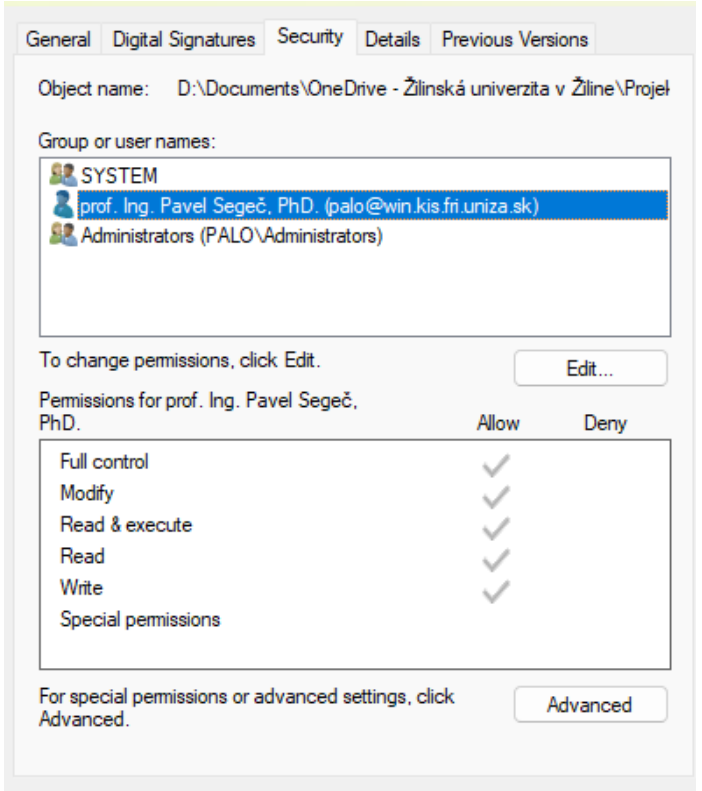
Model	Vysvetlenie	Príklad použitia
DAC (Discretionary Access Control)	Vlastník objektu rozhoduje, kto má aké práva	Zdieľané dokumenty na univerzite (učiteľ zdieľa súbor študentom)
MAC (Mandatory Access Control)	Centrálne definované pravidlá, používateľ nemôže meniť prístup	Klasifikované dáta (napr. vojenský systém s úrovňami "Tajné", "Dôverné")
RBAC (Role-Based Access Control)	Prístup na základe roly, nie identity	AIS (ak máš rolu "Študent", máš prístup len k svojim výsledkom)
ABAC (Attribute-Based Access Control)	Rozhodovanie podľa atribútov (čas, miesto, zariadenie, pozícia...)	Prístup k e-learningu povolený len z univerzitnej siete počas semestra
Iné....		

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Voliteľné riadenie prístupu - DAC (Discretionary Access Control)

Autorizácia na základe vlastníka - DAC

- **DAC** => starší, základny model
- **Ako DAC funguje?**
  - Každý **objekt** (súbor, priečinok) má svojho **vlastníka**
  - **Vlastník** zdroja (napr. súboru, miestnosti) **má plnú kontrolu** nad objektom
    - Rozhoduje Kto k nemu má prístup
    - Aké **operácie** môže vykonávať
- **DAC implementácia -** Access Control List
  - Zoznam, kto môže kam pristupovať a čo robiť
  - ***Asociovaný s objektom*** pre ktorý vlastník definuje prístup
  - Príklady
    - V IP sieťach Firewall
      - Riadi ktorá IP adresa kam na ktorú inú IP adresu a cez aký protokol
    - Operačné systémy – napr. MS Windows OS
      - Práva prístupu k súborom
    - Office 365 / Sharepoint / MS Teams / Cloud systémy (AWS, Azure)
      - Pridelenie prístupu používateľovi, skupine tímu

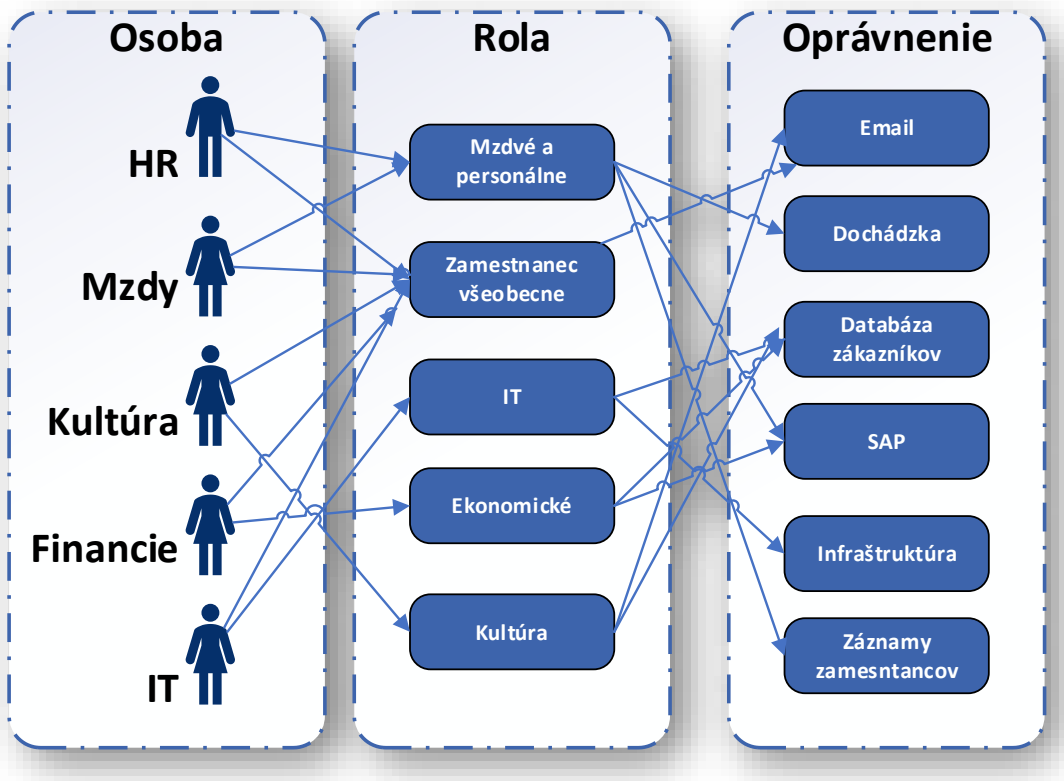


Autorizácia na základe vlastníka - DAC

- **Výhody**
  - Jednoduchosť: Menšie prostredia a individuálne potreby
  - Flexibilita: Priama kontrola používateľov nad ich vlastnými dátami
  - Autonómia: Používatelia môžu sami spravovať svoje zdroje bez nutnosti administrátorského zásahu
- **Nevýhody**
  - Škálovateľnosť: Obťažná správa vo veľkých a komplexných prostrediach
    - Kde je mnoho súborov a používateľov
  - Žiadna centrálne kontrola - menší prehľad o stave a auditovateľnosť
  - Riziko chýb: Pri chybných nastaveniach používateľmi
- **Kde sa používa?**
  - Osobné súbory a projekty
  - V menej prísnych systémoch (osobné počítače)
  - Menšie prostredia s menej používateľmi a zdrojmi (malé firmy)
  - Situácie, kde je kľúčová flexibilita a autonómia vlastníka dát

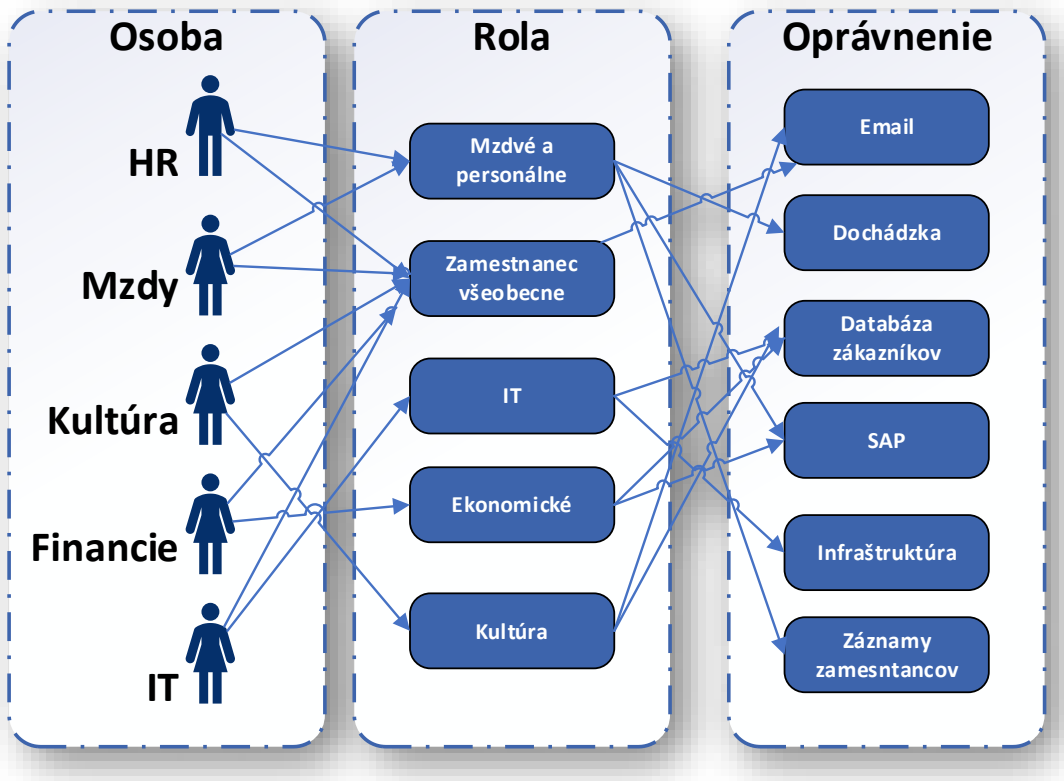
Autorizácia na základe rolí - RBAC

- **Autorizácia na základe rolí - RBAC (Role-Based Access Control)**
  - Prístupové **práva** prideľované **rolám, nie jednotlivcom**
    - Príklad AIS – minimálny príklad rolí a práv
      - **Študent**: vlastné známky, rozvrh, registrácia kurzov, interné oznamy
      - **Učiteľ**: zadávať známky svojich predmetov, nahrávať materiály, komunikovať so študentmi
      - **Študijné oddelenie:** upravovať študijné záznamy, registrácie študentov, správa kurzov
  - Role, práva a priradenie - Centralizovane a štandardizovane priradené
  - **Princípy RBAC**
    - Centralizovaná správa oprávnení
    - Prístup závisí od role
      - RBAC nie je o konkrétnom používateľovi, ale o **funkčnej pozícii**



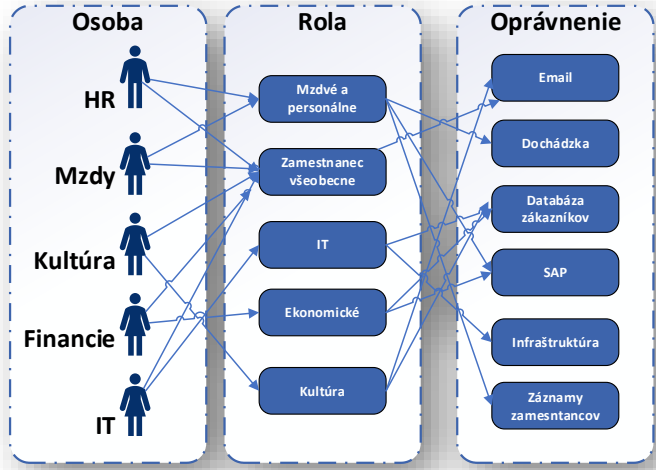
Autorizácia na základe rolí - RBAC

- **Základné komponenty RBAC modelu**
  - **Subjekt** (používateľ): Entita žiadajúca o prístup k zdroju
  - **Rola**: pracovná pozícia alebo funkcia s preddefinovanou sadou oprávnení
    - Napr. „Študent“, „Učiteľ“, “Vedúci“
  - **Oprávnenie (permission):** Povolenie na vykonanie akcie na konkrétnom objekte
    - Napr. read, write, delete ...
  - **Objekt:** Zdroj, ku ktorému sa pristupuje (napr. databáza, aplikácia, súbor)
- **Priradenia**
  - Používateľ/subjekt ⟶ má pridelené roly
  - Rola ⟶ má pridelené oprávnenia
  - Oprávnenia ⟶ definujú akcie na objektoch
- **Výsledok**
  - Práva alebo prístup závisí od roly používateľa v organizácii



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Autorizácia na základe rolí - RBAC



- **Ako to funguje?**
  1. **Definícia Oprávnení a rolí**
     - Ku každému objektu (súbor, aplikácia, API) sú definované oprávnenia (napr. read, write, delete)
     - Vytvorenie rolí (napr. "Študent", "Učiteľ", "Správca AIS", "Personalista")
       - Definované podľa rôznych kritérií, ako napríklad oprávnenia, zodpovednosti, nákladového strediska, organizačnej jednotky a ďalších
     - Každej roli sa priradí špecifický súbor oprávnení
  2. **Hierarchia Rolí (voliteľné)**
     - Role môžu byť usporiadané hierarchicky
     - Dedenie oprávnení
       - Napr. rola "Vedúci Katedry" môže dediť všetky práva roly "Učiteľ" a mať k tomu ďalšie administratívne práva
  3. **Priradenie Používateľov k rolám**
     - Používatelia sú priradení k príslušným rolám
       - Napr. "Jana Nováková je Študent", "Peter Mrkvička je Učiteľ"
     - Používateľ automaticky získa všetky oprávnenia danej roly
- Príklad implementácie: MS Active Directory

Autorizácia na základe rolí - RBAC

- **Výhody**
  - **Zjednodušená a efektívna správa prístupov**
    - Oprávnenia sa priraďujú rolám, nie jednotlivcom
    - Pri zmene pozície používateľa stačí zmeniť rolu
  - **Lepšia auditovateľnosť a kontrola**
    - Jednoduché sledovanie, kto má aké práva a prečo
  - **Hierarchia rolí**
  - **Konzistencia**
    - Zaručuje jednotné pravidlá prístupu naprieč organizáciou
  - **Podpora princípu najmenej potrebných práv (least privilege)**
    - Každý má len tie práva, ktoré potrebuje podľa roly
  - **Škálovateľnosť**
    - Novým zamestnancom stačí priradiť existujúcu rolu
  - **Podpora compliance (napr. ISO 27001, GDPR)**
    - Jasne definované prístupové politiky

- **Nevýhody**
  - **Komplexita rolí**
    - Vyžaduje dôkladnú analýzu organizačnej štruktúry
    - Vytvorenie a údržba veľkého počtu rolí môže byť náročná
    - Problém rozrastania rolí
  - **Riziko prekrytia**
    - Nesprávne priradenie rolí vedie k nadmerným právam (privilege creep)
    - Zabudnutie priradenia
  - **Obmedzená flexibilita a granularita**
    - Dynamické zmeny práv cez úpravu rolí môže byť pomalé
    - Bez atribútov je obtiažne pokrývať výnimočné prípady (prístup podľa času či miesta)

- **Kde sa používa? => 2025 -** Veľmi rozšírený
  - Väčšie a stredne veľké organizácie
  - Korporáty, verejná správa, nemocnice, školstvo
  - Cloudové služby a aplikácie
  - IT infraštruktúra a správa siete

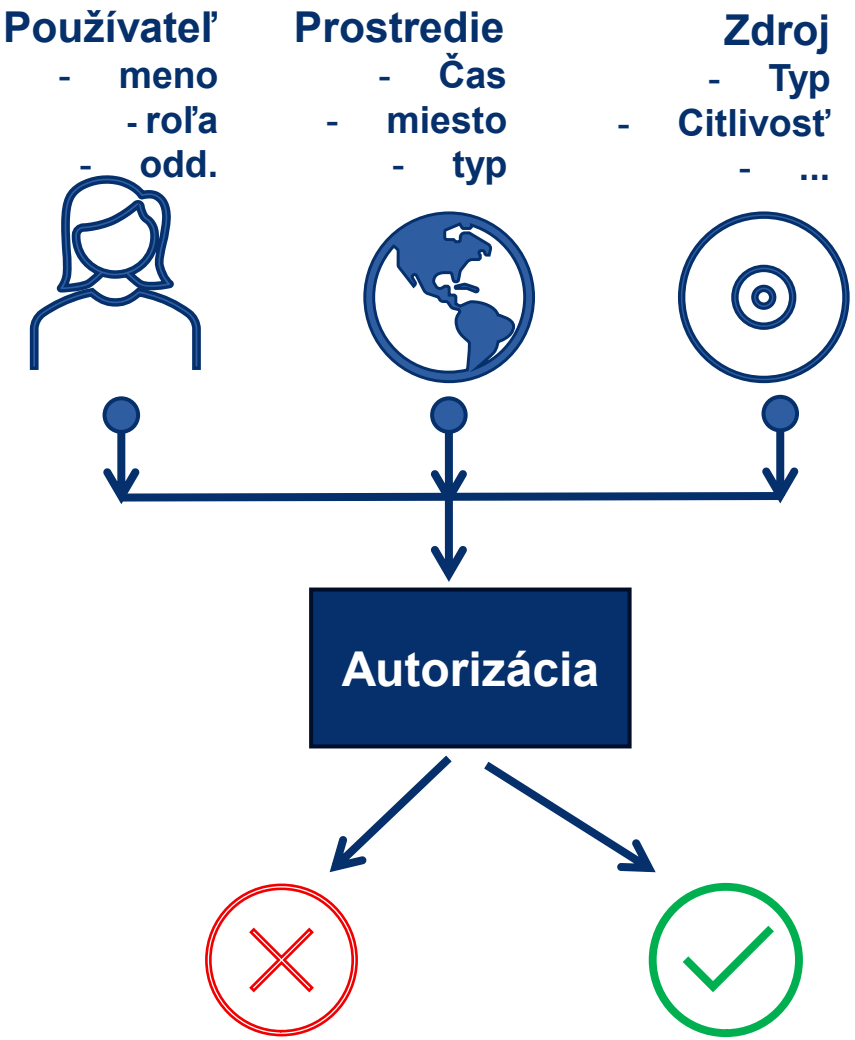
Verzie RBAC

- **Varianty RBAC:**
  - **Flat RBAC**
    - Každá rola má presne definované oprávnenia – jednoduché, ale môže byť neflexibilné
  - **Hierarchické RBAC**
    - Roly môžu dediť oprávnenia z iných rolí (napr. „Vedúci katedry“ dedí oprávnenia „Učiteľ“)
  - **Constraint-Based RBAC (obmedzenia)**
    - Obmedzenia na používanie rolí
      - napr. časové obmedzenie prístupu, schválenie ...
  - **Temporal RBAC (TRBAC)**
    - Špecifický podtyp Constraint-Based RBAC
    - Prístup len počas určeného časového okna (napr. externista má prístup Po–Pi 9:00–17:00)
  - **Rule RBAC (RuBAC)**
    - Pravidlá, ktoré určujú čo sa môže a čo nie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

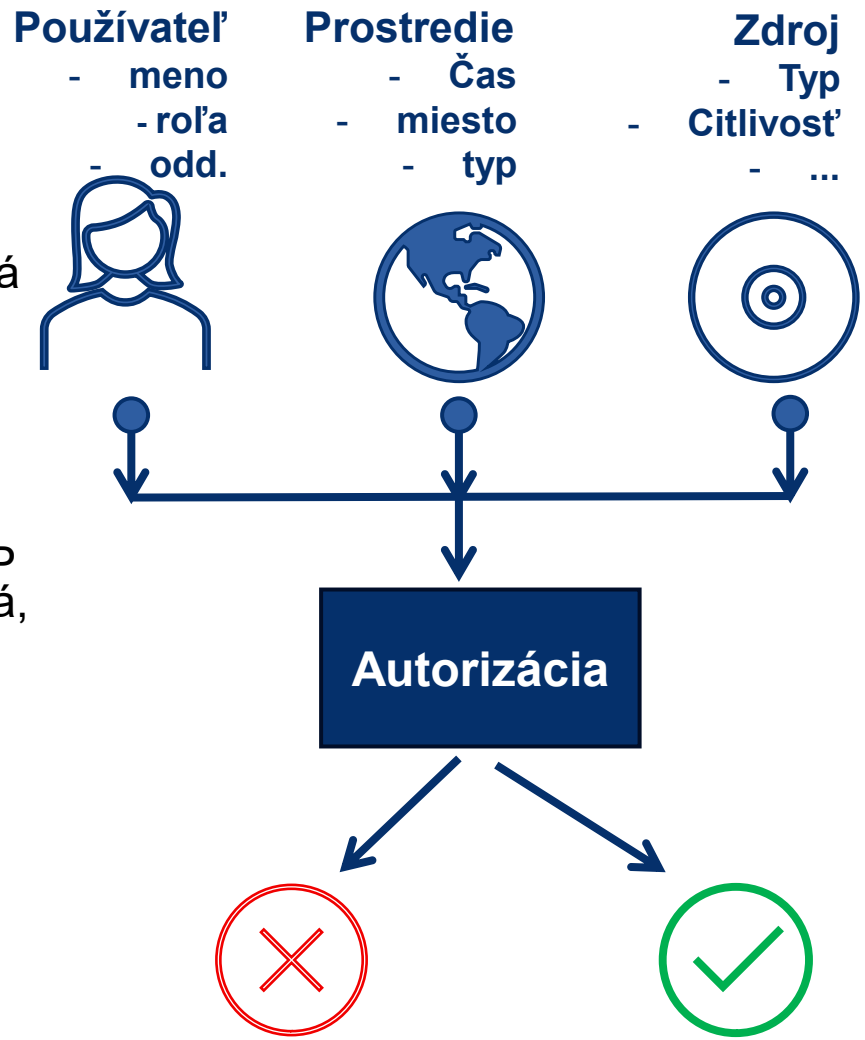
Autorizácia na základe atribútov - ABAC

- **Autorizácia na základe atribútov - ABAC (Attribute-Based Access Control)**
  - Moderný a flexibilný model
  - Model AC kde **r**ozhodnutia o prístupe sa zakladajú na hodnotách **atribútov** – entít, ktoré vstupujú do požiadavky
  - Spôsob pridelenia práv
    - Nerozhodujú len role a oprávnenia
  - **Princíp**
    - Prístup sa riadi dynamickými politikami relevantnými v čase a kontexte
    - Politiky referencujú na **kombináciu viacerých atribútov objektu**



Autorizácia na základe atribútov - ABAC

- **Základné komponenty ABAC**
  - **Atribúty subjektu (používateľ) -** Kto žiada prístup?
    - Napr. rola, oddelenie, pozícia, špecifické certifikácie, status – študent/zamestnanec ...
  - **Atribúty objektu (zdroj) -** K čomu sa pristupuje?
    - Napr. typ súboru, úroveň citlivosti dát, vlastník zdroja, geografická poloha servera, značky/tagy
  - **Akcia -** Čo sa má urobiť?
    - Typ prístupu – čítanie, zápis, mazanie, schvaľovanie, exportovanie...
  - **Atribúty prostredia (kontext) -** Za akých podmienok?
    - Napr. Dátum, čas (pracovná doba), lokalita (kancelária, doma), IP adresa, spôsob požiadavky (mobil vs. desktop), typ siete (firemná, verejná) ...
- **Ako to funguje?**
  - **S**ystém vyhodnocuje politiky založené na atribútoch používateľa (napr. meno, oddelenie) a kontexte (čas, IP adresa)
  - Prístup je povolený, iba ak všetky podmienky sú splnené
  - Kroky
    - 1) Zhromaždenie atribútov
    - 2) Aplikácia politiky
    - 3) Overenie a povolenie/zamietnutie prístupu



Autorizácia na základe atribútov - ABAC

- **Výhody:**
  - **Moderný prístup**
  - **Mimoriadna flexibilita a granularita**
    - Umožňuje definovať veľmi presné a detailné prístupové politiky
  - **Redukcia "role sprawl„**
    - Znižuje potrebu vytvárania obrovského množstva špecifických rolí (ako pri RBAC)
  - **Dynamické rozhodovanie**
    - Prístup sa vyhodnocuje v reálnom čase na základe aktuálnych atribútov a meniacého sa kontextu
    - Nie vopred pridelených rolí
  - **Škálovateľnosť**
    - Ľahšie sa prispôsobuje meniacim sa požiadavkám a rastu organizácie
    - Hodí sa pre veľké systémy s rôznorodými používateľmi a zdrojmi

- **Nevýhody**
  - **Zložitosť definície a implementácie politík**
    - Náročné na návrh a implementáciu komplexných pravidiel
  - **Závislosť na atribútoch**
    - Vyžaduje presnú a aktuálnu správu všetkých relevantných atribútov
  - **Výkon**
    - Dynamické vyhodnocovanie môže mať v vplyv na výkon
  - **Riziko chýb**
    - Nesprávne definované politiky môžu viesť k neoprávnenému prístupu.

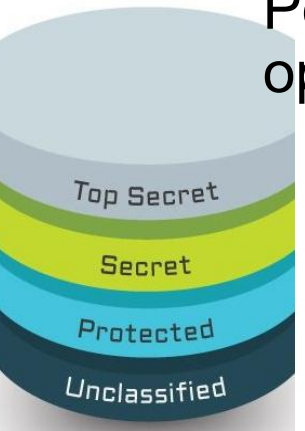
- **Kde sa používa?**
  - Pre prostredia s veľmi komplexnými, dynamickými a granulárnymi požiadavkami na prístup
  - Keď existujúce modely (DAC, RBAC) nie sú dostatočné
  - V prostrediach s vysokým počtom rolí alebo častými zmenami v organizačnej štruktúre/oprávneniach
  - Vhodné pre cloudové a hybridné prostredia (prístup potrebný z rôznych miest a zariadení)

Povinné riadenie prístupu - MAC

- **Povinné riadenie prístupu - MAC (Mandatory Access Control)**
  - Objekt a subjekt majú **priradené bezpečnostné označenie (label)**
    - napr. klasifikácia dôvernosti objektu = *tajné*,
    - oprávnenia subjektu (clearance) = *tajné*
  - **Politiku** prístupu určuje **systém / centrálna autorita**
    - Podľa úrovne klasifikácie zdrojov a bezpečnostnej previerky používateľa
  - **Vlastník nemá právo meniť** prístupové práva k objektom
    - Používateľ ani vlastník nemôže priradiť prístup alebo zdieľať dáta s niekým iným
  - **Kľúčový princíp**
    - Používa sa **centralizovaná a povinná** politika
    - **Hierarchia a pravidlá** rozhodujú o prístupe (napr. klasifikácia dát)
    - Rozhodnutie o prístupe: **na základe porovnania bezpečnostných atribútov**
      - Úroveň oprávnenia (user_clearance) ≥ úroveň klasifikácie (object_classification)

Povinné riadenie prístupu - MAC

- **Výhody**
  - **Vysoká bezpečnosť**: Centrálne nastavené a vynucované pravidlá
  - **Konzistentnosť**: Jednotné označenia a politiky naprieč celým systémom
  - **Auditovateľnosť**: Prísne pravidlá uľahčujú sledovanie a preverovanie prístupu
  - **Obrana proti chybám používateľov:** Používatelia nemôžu zmeniť oprávnenia
- **Nevýhody**
  - **Obmedzená flexibilita**: Používatelia nemôžu meniť prístup, sťaženie práce v dynamických prostrediach
  - **Komplexita**: Zložité nastavenie a správa politík. Časovo náročné
  - **Náročnosť na škálovanie**: V rozsiahlych systémoch zdrojovo náročné



- **Kde sa používa?**
  - V systémoch s vysokou bezpečnosťou
    - Vládne organizácie, armáda, ...
  - Systémy spracovávajúce **extrémne citlivé alebo klasifikované informácie**

Porovnanie prístupových modelov

Model	Základ rozhodovania	Kto rozhoduje o prístupe	Flexibilita	Auditovateľnosť	Bezpečnostné riziko	Zložitosť implementácie	Príklady použitia
DAC	Vlastníctvo objektu	Vlastník objektu	Vysoká	Nízka	Stredné až vysoké	Nízka	OS, súborové systémy (Windows ACL, Unix chmod)
MAC	Bezpečnostné štítky a úrovne	Centrálna autorita	Nízka	Vysoká	Nízke	Vysoká	Vojenské a vládne systémy (SELinux, Cisco TrustSec)
RBAC	Roly používateľov	Správca rolí	Stredná	Stredná až vysoká	Stredné	Stredná	Firemné systémy, AD, Oracle DB, univerzitné systémy
ABAC	Atribúty subjektu, objektu, kontextu	Politika založená na atribútoch	Veľmi vysoká	Vysoká	Nízke až stredné	Vysoká	Cloud, IoT, moderné aplikácie (AWS IAM, XACML, Azure)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Vykonanie (enforcement) a kontrola (governance) prístupových rozhodnutí

- **Model autorizácie** (DAC, MAC, RBAC, ABAC...)
  - Definuje princíp **ako sa rozhoduje o oprávneniach**
  - Nedefinuje vykonanie
- **Potreba zabezpečiť**
  - Reálne uplatnenie v systéme
  - Určíť
    - Kto rozhoduje, kto vynucuje, kto sleduje vykonanie
- ==> Rieši **Architektúra rozhodovania o prístupe** (Access Decision Architecture)
  - **Kľúčové komponenty – PAP, PIP, PDP, PEP**

```
Požiadavka → PEP → PDP (použije PIP + PAP) → Rozhodnutie → PEP vykoná akciu
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

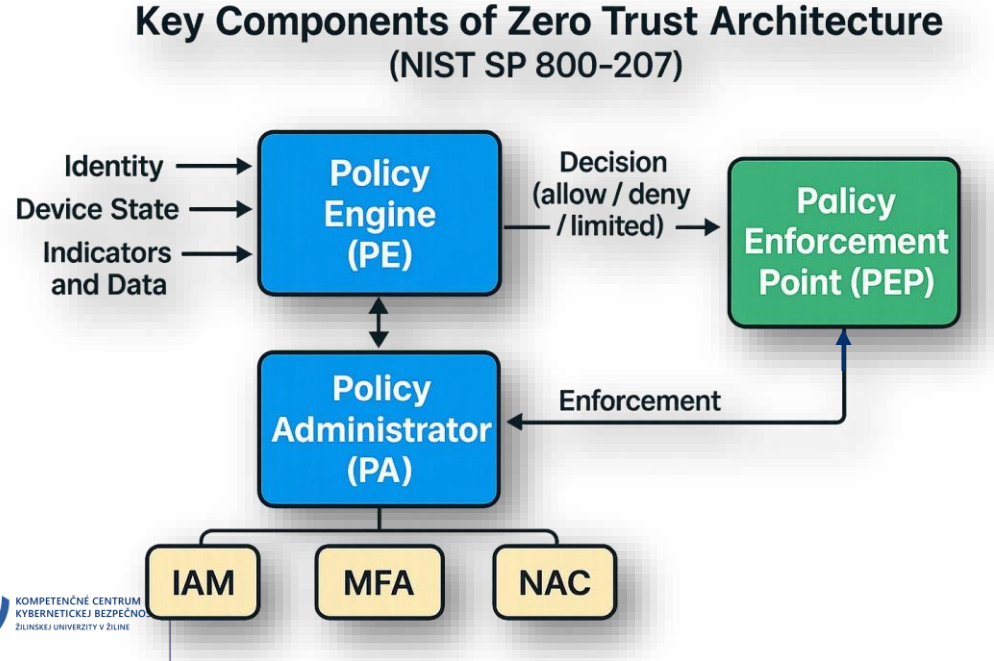
Architektúra rozhodovania o prístupe

- **PAP** (Policy Administration Point)
  - Miesto, kde sa politiky vytvárajú, upravujú a spravujú
  - Rozhranie pre administrátorov
  - *Príklad: Správcovská konzola IAM riešenia, nástroj na správu politík*
- **PIP** (Policy Information Point)
  - Zdroje údajov o subjektoch, objektoch, prostredí
  - Poskytuje kontextové dáta (atribúty, čas, stav) pre PDP
  - *Príklad: LDAP/Active Directory (pre atribúty používateľa), databáza zdrojov (pre atribúty objektu), senzor času/geolokácie (pre atribúty prostredia)*
- **PDP** (Policy Decision Point)
  - Mozog systému
  - Vyhodnocuje politiku a prijíma rozhodnutie „Allow/Deny“
  - *Príklad: Autorizačný server*
- **PEP** (Policy Enforcement Point)
  - Zachytí požiadavku z PDP
  - Vykoná rozhodnutie – povolí alebo zamietne prístup
  - Bod v systéme (aplikácia, firewall, operačný systém), ktorý odchytáva žiadosť o prístup
  - *Príklad: Webový server, databáza, firewall*

Používateľ žiada prístup k zdroju → **[PEP odchyí] → pošle žiadosť na → [PDP]**
[PDP] → získa údaje z → [PIP] + [PAP] →
→ [PDP] → rozhodne → Allow / Deny →
→ [PEP] → aplikuje rozhodnutie

Zero Trust Architektúra – logické komponenty

- **Policy Decision Point (PDP) - Policy Engine (PE) - mozog**
  - Rozhoduje o udelení/odmietnutí prístupu
  - Vstupy z PIP: identita (IAM), stav zariadenia (NAC, EDR), rizikové skóre (UEBA), threat intel (SIEM dáta), kontext (čas, miesto, typ požiadavky)
  - Výstup: rozhodnutie „allow / deny / limited“ do PEP
- **Policy Administration Point (PAP) - Policy Administrator (PA) - správca**
  - Vytvára, udržiava a spravuje pravidlá pre PE
  - Prekladá rozhodnutie PE do konkrétnych akcií
  - Vydáva tokeny, certifikáty alebo session keys
  - Distribuuje politiky do enforcement bodov
  - Jednoducho: konfiguruje PE a PIP
- **Policy Enforcement Point (PEP)**
  - Reálne uplatňuje rozhodnutie z PE
  - Príklad: ZTNA agent na koncovom zariadení, sieťová brána, FW, proxy, VPN GW
  - Overuje každý request a povoľuje len schválenú komunikáciu
- **Policy Information Point (PIP)**
  - Podporné dátové zdroje a telemetria pre PE
    - Identity provider (IdP) – AD, LDAP, Azure AD
    - Device posture – MDM (MobDevManag), EDR (stav zariadenia, patching, AV)
    - Threat intelligence – IOC, reputačné feedy
    - Logging & SIEM – spätná väzba pre kontinuálne učenie



Blok III: Moderné IAM technológie, architektúra a rozhodovanie

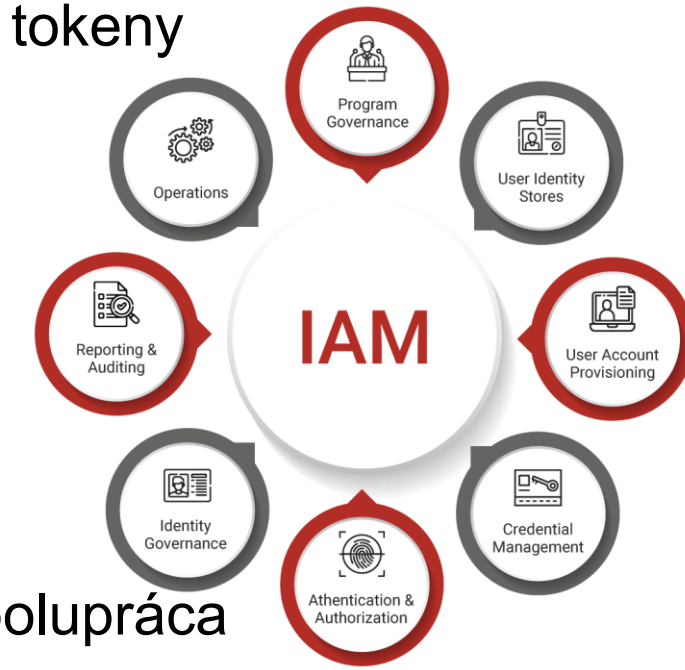
SSO a federácia

IAM technológie: autentifikačné protokoly a federácia

Tokeny

IAM technológie a nástroje

- Historický vývoj IAM
  - Od lokálnych účtov (on-prem AD) k cloudovým a hybridným modelom
- Súčasnosť => **Potreba** integrácie v komplexných ekosystémoch
  - Moderné prostredia: **cloud, hybrid, multi-cloud, SaaS** – potreba jednotného prístupu
  - Nové požiadavky: federácia, SSO, štandardizované protokoly, tokeny
  - **Trend**: Identita sa stáva **centrálnym prvkom bezpečnosti**
    - Zero trust, Paswordless autentifikácia ...
- IAM = Integračná vrstva bezpečnosti
  - Spája identitu, autentifikáciu, autorizáciu a audit
  - Funguje naprieč aplikáciami, sieťami a cloudovými službami
- Výzvy
  - Interoperabilita medzi aplikáciami
  - Škálovanie v cloude: Cloud, hybrid, multi-cloud, SaaS, B2B spolupráca
  - Zabezpečenie tokenov a federácie



IAM architektúra – 1) Správa identít

- Správa používateľských účtov a profilov
- **Identity Lifecycle management**
  - Vytvorenie účtu → zmena atribútov → zrušenie účtu
  - Provisioning a deprovisioning používateľov (automatizácia, HR integrácia)
  - **Kategórie identít**
    - Bežní používatelia, zamestnanci, študenti
    - Privilegované účty (administrátori, root)
- **Credential Management**
  - Životný cyklus hesiel/kľúčov/certifikátov (trezor, HSM/KMS, rotácia, revokácia)
- **Adresár / User Store**
  - Centrálne úložisko pre identity používateľov a ich atribúty (*Active Directory, LDAP, SQL databáza ...)*
- **Štandardy správy identít**
  - SCIM (System for Cross-domain Identity Management) pre výmenu údajov medzi systémami => Interoperabilita a **Automatizácia**

IAM architektúra - 2) Autentifikácia (AuthN)

- Overenie identity používateľa
- **Identity Provider (IdP)**
  - Centrálna autorita autentifikácie
  - Uchováva identity a atribúty používateľov
  - Vydáva potvrdenie o úspešnej autentifikácii (token, ticket)
    - **Security Token Service (STS)** – služba, generuje a validuje tokeny (SAML assertions, OIDC ID tokeny, OAuth access tokeny)
  - *Public Internet: AzureAD, GoogleIdentity, AppleID, …*
  - *Vlastné: KeyCloak, FreeIPA, Authentik, MS AD, Okta ...*
- **Autentifikačné protokoly**
  - Štandardy bezpečnej výmeny autentifikačných údajov
  - Umožňujú dôveru medzi IdP a aplikáciami
  - *Príklady: SAML, OpenID Connect (OIDC), OAuth 2.0, Kerberos*
- **Single Sign-On (SSO)**
  - Jedno prihlásenie → prístup k viacerým službám
- **Federácia identít (FIM)**

IAM architektúra – 3) Autorizácia

- Riadenie prístupových práv podľa politiky
  - Určuje, čo môže používateľ robiť po autentifikácii
  - Rozhoduje na základe rolí, atribútov a kontextu
- Kľúčové komponenty –
  - Modely: RBAC, ABAC? DAC, MAC ...
  - Rozhodovacia architektúra
    - **PAP (Policy Administration Point)** - správa politík
      - Vytvárajú/verzionujú a publikujú politiky
    - **PIP (Policy Information Point)** - zdroj atribútov (role, skupiny, kontext)
      - LDAP, HR/IS, CMDB, riziko, compliance, geolokácia
    - **PDP (Policy Decision Point)** - rozhoduje, či je prístup povolený
      - Vyhodnocuje politiku nad kontextom požiadavky
    - **PEP (Policy Enforcement Point)** - vynucuje rozhodnutie pri prístupe
      - Reverzný proxy, firewall, API gateway (Kong/NGINX/Envoy), logika v aplikácii
- **Autorizačné protokoly**
  - Štandardy bezpečnej autorizácie prístupu
  - Zaisťujú kontrolu oprávnení medzi aplikáciami a službami
  - *Príklady: SAML, OAuth 2.0, Kerberos*
- **Výsledok / cieľ**
  - Centralizované a konzistentné uplatňovanie politík prístupu naprieč systémami

IAM architektúra – 4) Podporné komponenty a iné

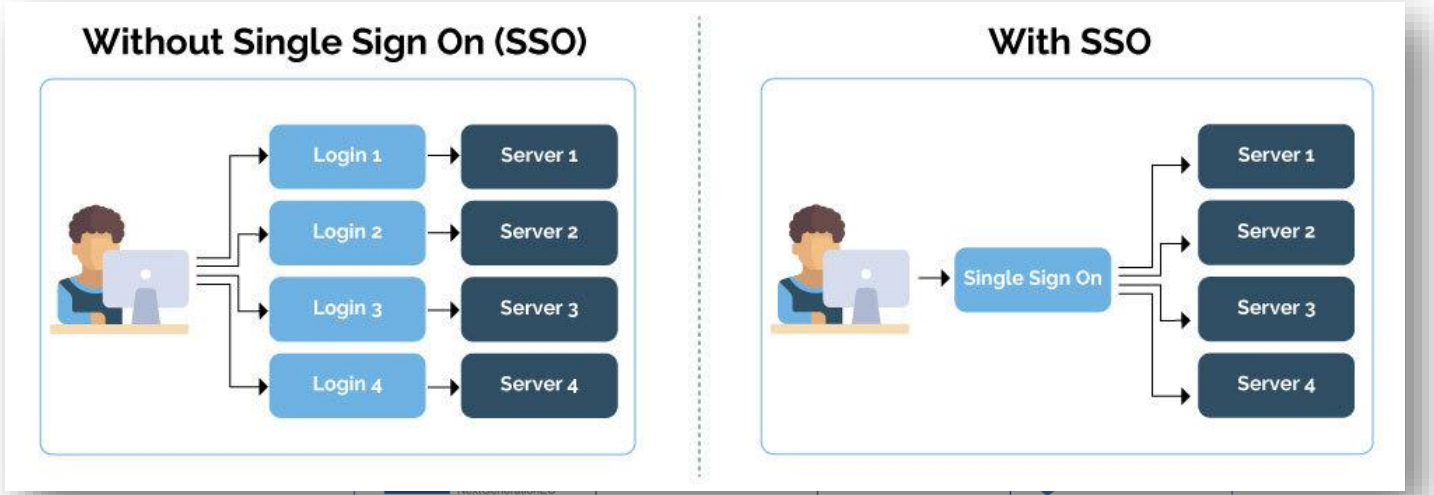
- **Audit & Reporting**
  - Záznamy o prístupoch: kto, kedy, k čomu pristupoval
  - Podpora compliance a forenznej analýzy
- **SSO Engine**
  - Mechanizmus pre jednotné prihlásenie (Single Sign-On)
  - Spracovanie tokenov a session
- **PAM (Privileged Access Management)**
  - Ochrana účtov s vysokými oprávneniami
  - Schvaľovanie a monitorovanie administrátorských prístupov
  - JIT pre adminov, trezor servisných účtov, session recording
- **Integrácia & API**
  - Prepojenie s aplikáciami, cloudom a sieťovými prvkami
  - Rozšíriteľnosť cez štandardizované protokoly a API

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Single Sign-On (SSO)

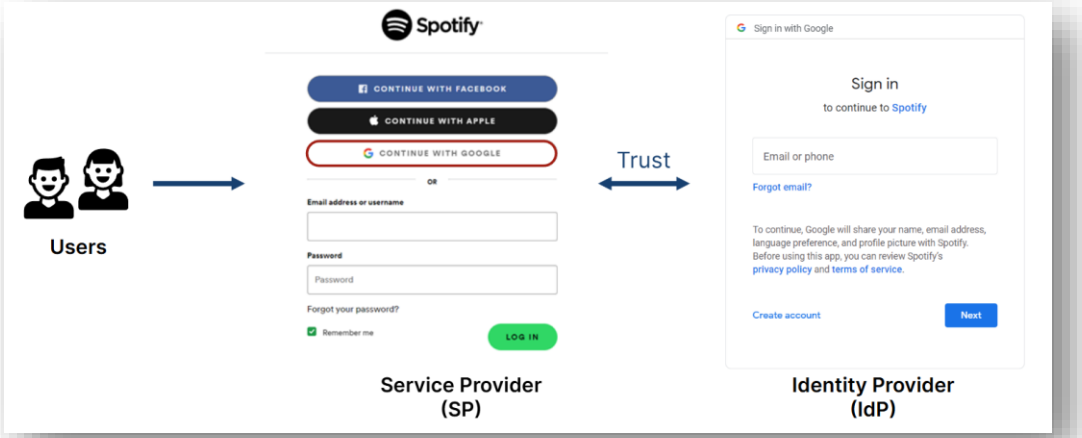
- Autentifikačný proces (**jedná** organizácia alebo federácia)
- Umožňuje používateľovi
  - Prihlás **sa raz**
  - Prístup k **viacerým nezávislým aplikáciám**
    - bez nutnosti opakovane zadávať prihlasovacie údaje.

      („*authenticate once, access many*“)
- **Základný princíp**
  - Centrálna autentifikácia u Identity Providera (IdP)
  - Aplikácie dôverujú výsledku



Single Sign On (SSO) - Základné komponenty

- **Používateľ (User)**
  - Osoba, ktorá sa chce prihlásiť do aplikácie
  - Komunikuje s aplikáciou cez prehliadač alebo klienta
- **Identity Provider (IdP)**
  - Centrálna autorita autentifikácie
  - Ukladá identity (adresár, databáza)
  - Vykonáva autentifikáciu
  - Vydáva auth token (SAML assertion)
    - ktorý potvrdzuje identitu
  - ***Príklady***:
    - *Cloud IdP: Azure AD (Entra ID), Google Identity, Apple ID*
    - *On-prem/Open-source/komerčné IdP: Keycloak, FreeIPA, Authentik, Okta*



- **Service Provider (SP) / Relaying party**
  - Aplikácia alebo služba, ktorú používateľ používa
  - Deleguje autentifikáciu na IdP (nemá vlastnú DB hesiel)
  - Dôveruje tokenu generovanému IdP
  - ***Príklady:*** *Slack, Dropbox, GitHub, ... (a overenie/prihlásenie cez Google alebo Microsoft)*
- **Ďalšie komponenty**
  - **STS (Security Token Service)** – vydáva a overuje tokeny
  - **Session Management** – udržiava stav prihlásenia (cookie, ticket, token)
  - Protokolová vrstva, bezp. tokeny

Ako funguje SSO?

IdP vygeneruje a odošle token späť do SP
Token (SAML, OIDC, OAuth2) obsahuje identitu a atribúty
SP tokenu dôveruje a poskytne prístup

Používateľ sa autentifikuje na IdP
Zadá prihlasovacie údaje (heslo, MFA, biometria)
IdP overí totožnosť

Používateľ otvorí aplikáciu (SP)
* Napr. webová aplikácia (Moodle, Slack, Git, Spotify....)
* SP vyžaduje autentifikáciu

Service Provider presmeruje používateľa na IdP
Aplikácia deleguje autentifikáciu na dôveryhodného poskytovateľa identít

SSO - Kľúčové výhody/nevýhody

Výhody

- **Používateľský komfort v rámci jednej org.**
  - Jedno prihlásenie pre viac aplikácií => zníženie „prihlasovacej únavy“
  - Znižuje redundanciu hesiel
- **Zníženie nákladov**
  - Centralizovaná správa identít v IdP
- **Zvýšenie produktivity a vyššia bezpečnosť**
  - Menej hesiel, podpora MFA
  - Heslá nie sú zdieľané s tretími stranami, tokeny majú obmedzenú platnosť
- **Flexibilita**
  - Umožňuje presné definovanie oprávnení (napr. iba čítanie údajov, nie úprava)
- **Interoperabilita**
  - Široko podporovaný štandard v moderných službách (Google, Twitter, GitHub)

Nevýhody

- **Single Point of Failure**
  - Ak zlyhá centrálny systém, zlyhá prístup všade
- **Kompromitácia SSO**
  - Ak sa kompromituje používateľ

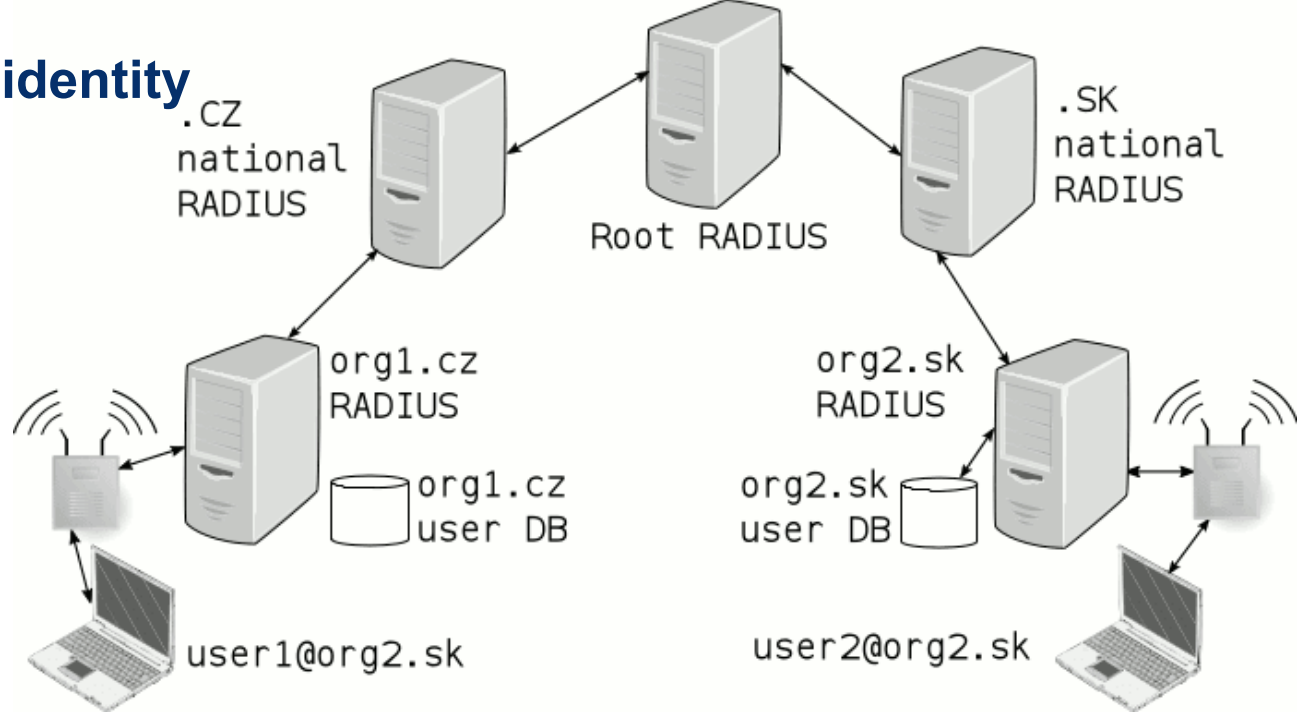
  = kompromitácia asociovaných aplikácii
  - Dodržuj bezpečnostné princípy
- Setup a vyladenie môže byť náročné
- Limitovaná vizibilita logovania aktivít
  - Cloud riešenia môžu abstrahovať IP a sešn dáta
- Rôzne aplikácie používajú rôzne procesy SSO
- Nemožné nájsť **JEDNO SSO riešenie** pre všetkých / všetko (je viac typov)

SSO → Často základ pre IAM projekty

Federácia identít (FIM)

- **FIM = Nadstavba nad SSO**
  - Koncept zdieľania a overovania identít **naprieč organizáciami a doménami**
- **Rozdiel oproti SSO**
  - SSO = prihlásenie v rámci **jednej organizácie**
  - Federácia = prihlásenie platí **medzi viacerými organizáciami/doménami**
- **Princíp**
  - Dohoda o dôvere medzi **Identity Provider-om (IdP)** a **Service Provider-om (SP)** v inej organizácii
    - IdP a SP si **vymenia metadáta** (certifikáty, endpointy, podporované protokoly)
    - Bezpečnostný token vydaný IdP sa akceptuje v externom SP
  - Vytvára sa tzv. **„Circle of Trust“** – skupina organizácií, ktoré si dôverujú
- **Umožňuje**
  - Používateľ môže používať **jednu identitu** na prístup k viacerým systémom rôznych organizácií
  - Bez potreby zakladať si nový účet v každej službe

Federácia identít v praxi - Eduroam



- **Čo je Eduroam**
  - Medzinárodná federácia pre akademické a výskumné siete
  - Poskytuje jednotný prístup k Wi-Fi pre študentov a zamestnancov univerzít
- **Princíp fungovania (dot1x)**
  - Používateľ sa autentifikuje pomocou **domácej identity** (univerzitný účet)
  - Eduroam presmeruje požiadavku na **domáce IdP** cez federáciu (RADIUS hierarchia)
  - Hostiteľská univerzita dôveruje odpovedi domáceho IdP → prístup k Wi-Fi je povolený
- **Výhody**
  - Jedno konto = prístup k Wi-Fi **na tisícoch univerzít a inštitúcií po celom svete**
  - Pohodlie pre študentov, výskumníkov a zamestnancov
  - Jednotné zabezpečenie a politika (WPA2-Enterprise, EAP autentifikácia)
- **Príklad**
  - Študent UK sa prihlási na Wi-Fi siete **Eduroam** na UNIZA v Žiline alebo na STU v BA
  - Autentifikácia prebehne proti jeho domácej univerzite (UK Bratislava), ale prístup je udelený na hostiteľskej univerzite

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Federácia identít – FIM navyše k SSO

Výhody navyše oproti SSO

- Funguje **naprieč organizáciami a doménami**
- **Pohodlie pre používateľov**
  - Jedna identita na viaceré systémy a organizácie
- **Jednoduchšia spolupráca**
  - B2B integrácie, organizačné federácie, zdieľanie zdrojov
- **Znižovanie nákladov**

Nevýhody k SSO

- **Právne/regulačné otázky**
  - **Z**odpovednosť za údaje, GDPR, prenos identity do inej jurisdikcie
- **Závislosť na dôvere**
  - Organizácie musia správne nastaviť dôveru (certifikáty, metadáta)
- **Komplexnejšia správa**
  - Čím viac partnerov vo federácii, tým náročnejšia údržba

IAM technológie: AAA tokeny a protokoly

OAuth 2.0 a OIDC (tokeny, autorizácia aplikácií)

SAML, Kerberos – SSO, dôvera medzi doménami

RADIUS, TACACS+ – centrálne AAA protokoly

Interoperabilita v IAM - nevyhnutnosť

- Rôznorodé prostredia
  - Cloud, on-premise, mobilné aplikácie, SaaS – musia spolupracovať
  - Bez interoperability by vznikli izolované ostrovy
- **Čo je interoperabilita?**
  - Schopnosť systémov a organizácií komunikovať, zdieľať dáta a spolupracovať
  - Základ pre federáciu identít a jednotné politiky
- **Praktický prínos**
  - Jednoduchšie B2B spolupráce
  - Možnosť kombinovať rôznych vendorov a cloud služby
- **Ako ju zabezpečiť?**
  - Štandardizované protokoly a frameworky
    - SAML – SSO vo vnútri a medzi organizáciami
    - OAuth 2.0, OpenID Connect – webové a cloud aplikácie
    - LDAP – adresárové služby, zdroj atribútov o identitách
    - Kerberos, RADIUS, Tacacs+ – intranet, sieťové prístupy
- Pozor na limity
  - Nie všetko je kompatibilné (napr. webové aplikácie s OAuth nepodporujú Kerberos)

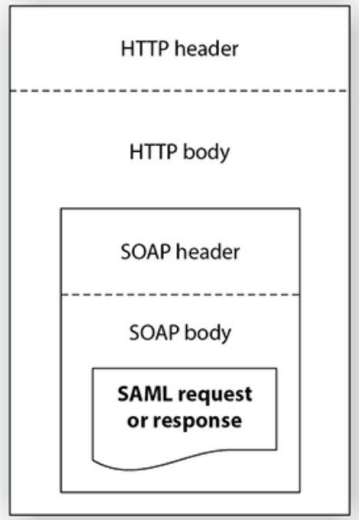
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

SAML - Security Assertion Markup Language

- **Čo je SAML**
  - Otvorený štandard (2002) pre **autentifikáciu a autorizáciu** v SSO a FIM
  - Používa **XML-based SAML Assertions** (SAML tvrdenie) na bezpečné zdieľanie identít a oprávnení
  - Komunikácia cez **HTTP Redirect** alebo **POST**
- **Princíp fungovania**
  - Používateľ sa autentifikuje voči **Identity Provider (IdP)**
  - IdP vydá **SAML Assertion** – podpisaný XML token
  - Aplikácia (**Service Provider, SP**) dôveruje assertion a poskytne prístup
- **Výhody**
  - Robustný pre komplexné podnikové scenáre (napr. SAP, Oracle)
  - Hlavne pre web-based SSO a federácie medzi organizáciami
  - Vysoká bezpečnosť – šifrovanie, digitálne podpisy
  - Podpora vo **federáciách** (eduGAIN, Shibboleth)
  - Osvedčený
- **Nevýhody**
  - Založený na XML – relatívne zložitý a ťažkopádny
  - Slabšia podpora mobilných a moderných webových aplikácií
  - Postupne je vytláčaný novšími protokolmi (OIDC, OAuth2)

SAML Assertion - príklad

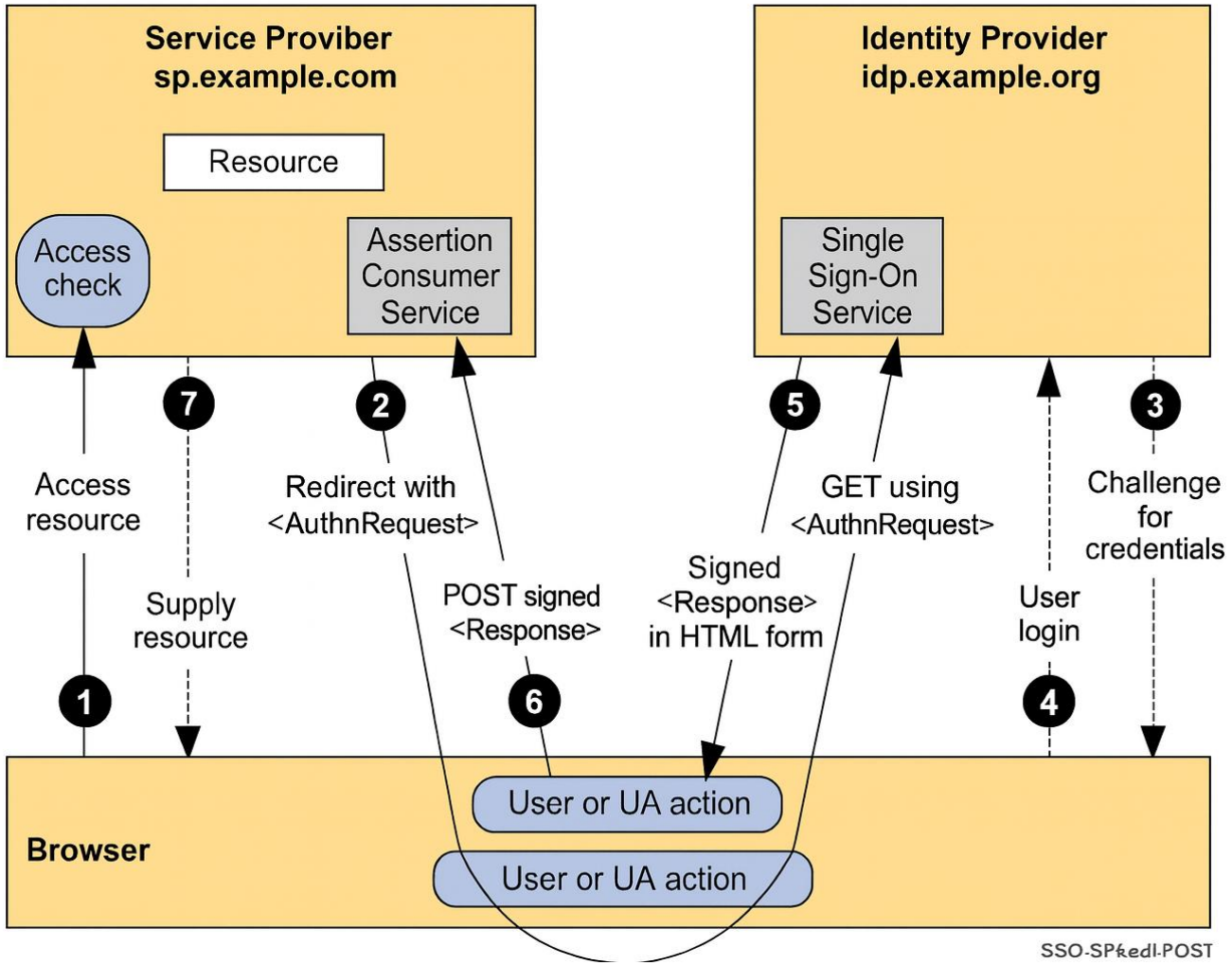
- **Kryptografická ochrana**
  - Každý SAML assertion vydaný IdP je **digitálne podpísaný** (XML Signature).
  - SP má vopred nahratý **verejný kľúč/certifikát IdP**
  - Pri overovaní SP kontroluje:
    - či podpis sedí (nebol token zmenený),
    - či certifikát patrí dôveryhodnému IdP.
- **Overenie parametrov XML assertion**
  - SP okrem podpisu kontroluje aj:
    - **Issuer** – kto vydal token (musí byť správne IdP),
    - **Audience** – komu je token určený (konkrétny SP),
    - **Validity** – čas platnosti (NotBefore, NotOnOrAfter),
    - **Attributes/Claims** – roly, skupiny, e-mail atď.
- **Bezpečný kanál komunikácie**
  - SAML používa **HTTPS/TLS**, aby ho nikto nemohol odchytiť alebo pozmeniť




```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="_req-9f2a2b7c1d"
    Version="2.0"
    IssueInstant="2025-09-27T12:34:56Z"
    Destination="https://idp.example.com/sso"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    AssertionConsumerServiceURL="https://sp.example.com/saml/acs">
  <saml:Issuer>{IDP_OR_SP_ENTITY_ID? → TU
SP!}https://sp.example.com/metadata</saml:Issuer>
  <samlp:NameIDPolicy
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
      AllowCreate="true"/>
  <samlp:RequestedAuthnContext Comparison="minimum">
    <saml:AuthnContextClassRef>

urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
...
```

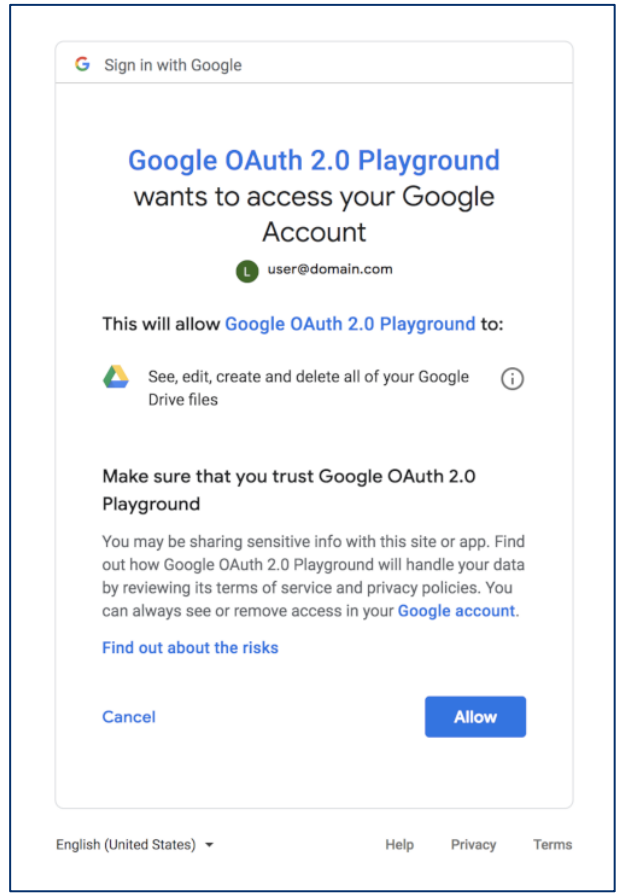
SAML (WEB services)



1. **Používateľ otvorí aplikáciu (SP)**
   Aplikácia vidí, že používateľ nie je prihlásený
2. **Aplikácia pošle používateľa na prihlasovaciu stránku IdP**
   Povie IdP: „potrebujem overiť totožnosť tohto človeka pre túto aplikáciu“
3. **IdP vyzve na prihlásenie**
   Ak už je používateľ na IdP prihlásený, krok sa preskočí
4. **Používateľ sa prihlási (heslo/MFA)**
   IdP teraz pozná, kto to je
5. **IdP pripraví potvrdenie totožnosti.**
   Digitálne „SAML tvrdenie“ určený konkrétne pre túto aplikáciu
6. **IdP odošle** tvrdenie **späť do aplikácie.**
   Prehliadač ho prenesie na špeciálnu adresu aplikácie (ACS) v SP
7. **Aplikácia** SAML tvrdenie **skontroluje a prihlási používateľa**
   Ak je v poriadku, vytvorí lokálnu reláciu a zobrazí požadovaný obsah

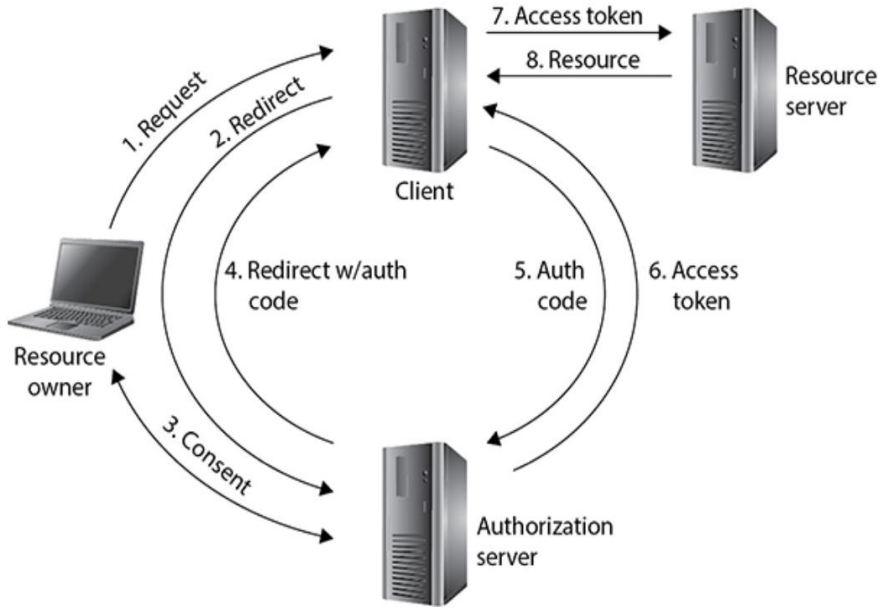
OAuth - Open Authorization

- **Čo je OAuth – Open Authorization?**
  - Otvorený štandard RFC 6749 pre bezpečnú **autorizáciu**
  - Umožňuje prístup k rôznym zdrojom v mene používateľa **bez zdieľania prihlasovacích údajov**
  - Aktuálna verzia **OAuth 2.1** (najpoužívanejší štandard)
  - Primárne autorizácia pre API a mobilné aplikácie
- **Hlavné roly**
  - **Resource Owner (RO)** – používateľ, ktorý vlastní dáta
  - **Client** – aplikácia, ktorá chce k dátam pristúpiť (*LinkedIn, spotify, ChatGPT, mobilná appka*)
  - **Authorization Server (AS)** – vydáva prístupové tokeny (*Google Identity/Authorization server, Okta, Auth0, Azure AD/Entra, Strava OAuth*)
  - **Resource Server (RS)** – chránený zdroj (API, služba - *X/Twitter API, Google Calendar API, GitHub API, StravaAPI*)
- **Princíp fungovania**
  - Používateľ **autorizuje** aplikáciu cez poskytovateľa identity (IdP, napr. Google)
  - IdP vydá šifrovaný access token (a prípadne refresh token) aplikácii
  - Aplikácia použije token na prístup k zdrojom (napr. kontakty sprístupniť na riadenie z Linkedin)
- **Príklady**
  - Prihlásenie cez Google/Facebook → aplikácia získa token a prístup k dátam používateľa
  - Mobilné appky využívajúce API (Spotify, LinkedIn integrácie)




```
! Priklad token - telo
{
  "iss": "https://auth.example.com/",
  "sub": "user-12345",
  "aud": "https://api.example.com/",
  "exp": 1758965787,
  "iat": 1758962187,
  "scope": "tweet:write profile:read",
  "client_id": "client-7890",
  "jti": "a2753cfb-b862-4a78-8f3a-
01118c269a10"
}
```

OAuth proces - Scenár: Garmin → Strava AutoSync (typický pre používateľov hodiniek)



- **Cieľ:** po prepojení účtov sa nové aktivity z Garmin Connect automaticky objavia v Strave.
- **Roly (OAuth)**
  - **Client: Garmin Connect** (mobil/web služba, ktorá nahráva dáta do Stravy)
  - **Resource Owner: ty** (vlastník účtu **Strava**)
  - **Authorization Server (AS): Strava OAuth** (od teba získa súhlas)
  - **Resource Server (RS): Strava API** (koncové body na nahranie/čítanie aktivít)

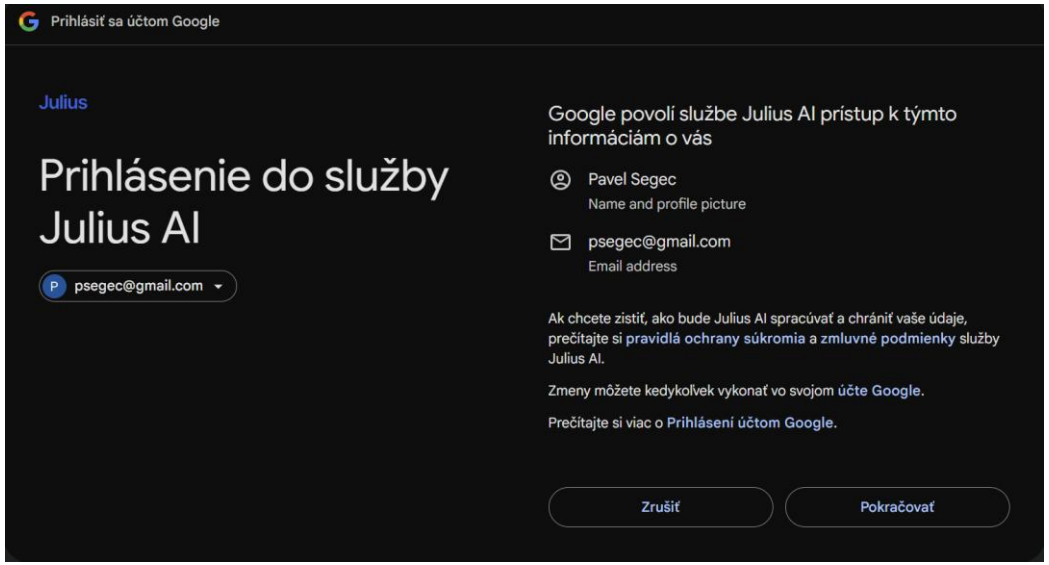
- **1) Request (RO → Client)**
  - V Garmin Connect klikneš Connect with Strava (chcem prepojiť účty)
- **2) Redirect (Client → AS /authorize)**
  - Garmin (Client) pošle používateľa na Stravu (Authorization Server), aby sa prihlásil
- **3) Consent (RO ↔ AS)**
  - Na Strave sa prihlásiš a udelíš Garminu súhlas
  - Consent = proces získania súhlasu používateľa
- **4) Redirect w/ auth code (AS → Client)**
  - Strava vydá kód a pošle ho späť Garminu
- **5) 6) Auth code (Client → AS /token) / Access token (AS → Client)**
  - Garmin vymení kód za access token u Stravy
  - Access token = „digitálny kľúč“, ktorý Garmin používa pri volaní Strava API
- **7) Access token (Client → Resource server)**
  - Garmin pošle dáta (aktivity) do Stravy spolu s tokenom
  - Po každej novej aktivite Garmin volá Strava API
- **8) Resource (RS → Client)**
  - Strava token overí, spracuje upload a vráti stav/ID aktivity → aktivita sa objaví v Strave
- Pozn.: Kroky 1–6 sú jednorazové (prepojenie účtov). Kroky 7–8 sa opakujú pri každej novej aktivite

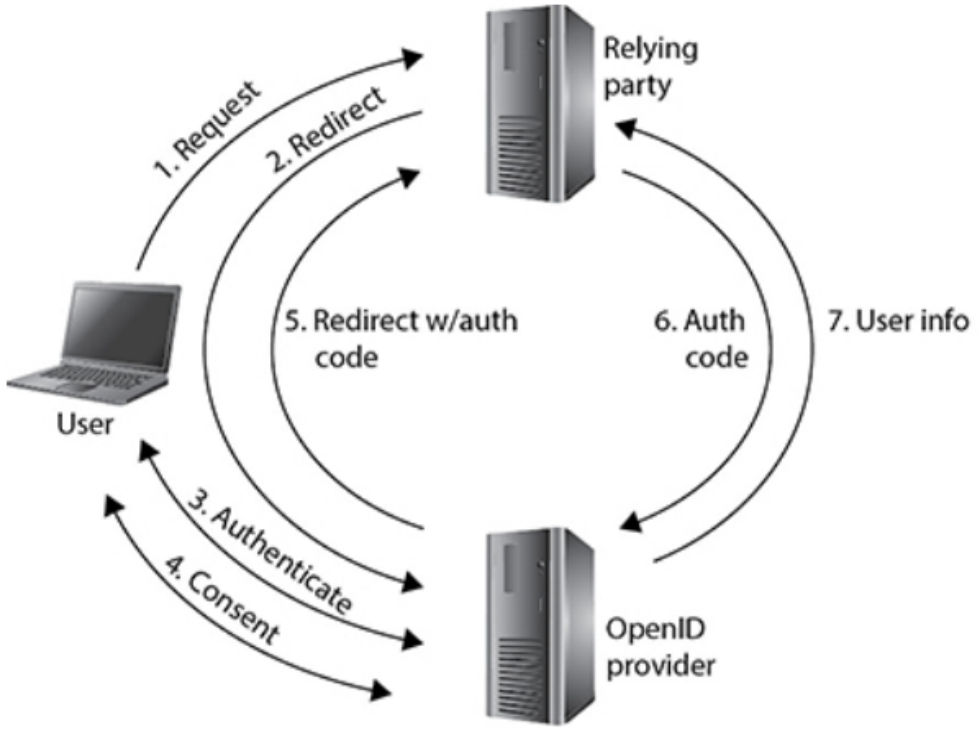
OpenID Connect (OIDC)

- **OpenID Connect (OIDC)**
  - **Otvorený štandard** pre decentralizovanú autentifikáciu (od 2014)
  - Postavený ako autentifikačná vrstva ***nad OAuth 2.0 (autorizácia)***
    - Kombinuje tak autentifikáciu (kto je používateľ) s autorizáciou (čo môže robiť)
- **Autorizácia =>** Používa autentikačný **JSON Web Token (JWT)**
  - Obsahuje informácie o identite používateľa (napr. meno, e-mail, ID)
    - Umožňuje získať info u používateľovi
  - Digitálne podpísaný => integrita a autenticita
  - Časovo obmedzený (typicky minúty)
- **Proces**
  - Používateľ sa prihlási cez IdP (napr. Google, Okta)
  - IdP vydá JWT, ktorý obsahuje overené údaje o identite
  - Cieľová aplikácia (napr. eBay) overí JWT a povolí prístup
- **Určenie**
  - Webové/mobilné aplikácie – jednotné prihlásenie
    - napr. Google login => prihlásenie do eBay cez Google účet (JWT)
    - Cloudové služby (Google login, Microsoft login)

Hlavné entity v OIDC

- **End User (Resource Owner)**
  - Fyzická osoba, ktorá sa chce autentifikovať
  - Zadáva svoje poverenia (heslo, MFA, biometria)
- **Relying Party (RP)**
  - Aplikácia alebo služba, ktorá chce poznať identitu používateľa
  - RP prijíma **ID token** a dôveruje mu
  - Príklady: Spotify, eBay, Slack, SaaS aplikácie
- **OpenID Provider (OP)**
  - Poskytovateľ identity (IdP) – autentifikuje používateľa
  - Vydáva **ID token** a voliteľne aj **Access token**
  - Príklady: Google, Microsoft, Keycloak, Okta, FreeIPA

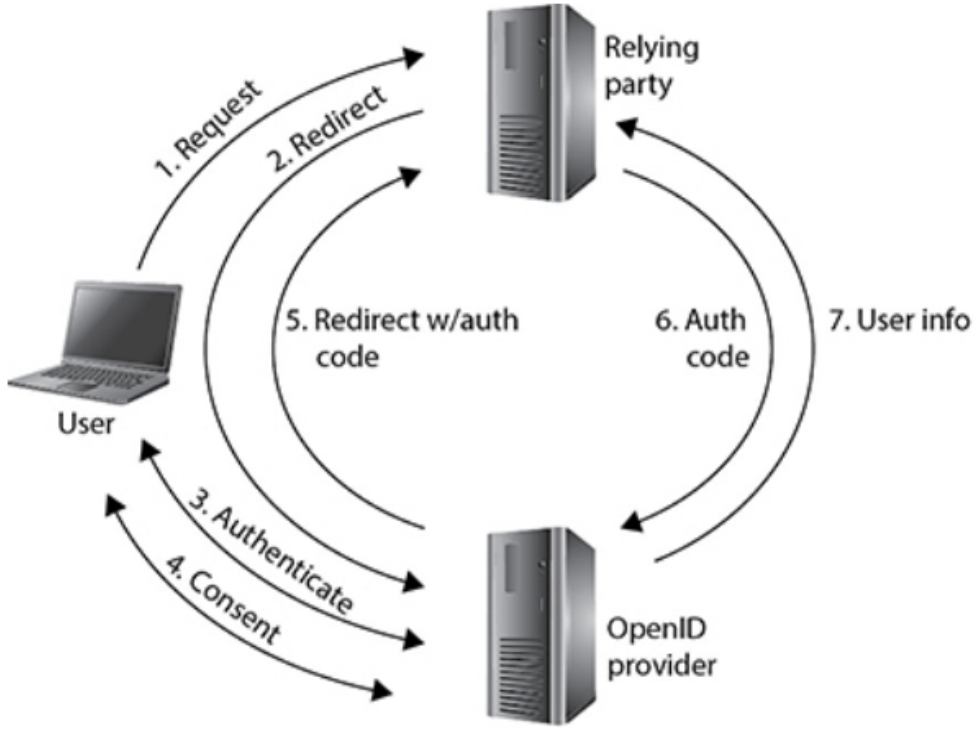




Authorization code flow

OIDC scénar – „Sign in with Google“ do Spotify (OIDC autentifikácia)

- **1) Request (RP → OP /authorize)**
  - Relying Party (aplikácia) presmeruje používateľa na OpenID Provider (IdP)
  - V Spotify kliknem na „Continue with Google“
- **2) Redirect**
  - Spotify ma presmeruje na Google login stránku => Cieľ: získať **authorization code**
- **3) Autentifikácia** (User ↔ Google)
  - Google ma (ak treba) **autentifikuje** – heslo/MFA alebo existujúca relácia
- **4) Consent (User ↔ Google)**
  - OP (IdP) autentifikuje používateľa (heslo, MFA, biometria)
  - Zobrazí sa **súhlas** so zdieľaním identity (e-mail, profil). Potvrdíš.
- **5) Redirect s kódom (OP → RP)**
  - Prehliadač je presmerovaný späť do Spotify .
- **6) 7)** Auth code (Spotify → Google **/token)**
  - Spotify (na serveri) pošle Google **authorization code**
- **7) Validácia ID tokenu (RP)**
  - Google vráti token a RP overí podpis
  - Ak je validný → vytvorí session pre používateľa



Authorization code flow

- **„Cieľ:** prihlásiť/registrovať sa do Spotify účtu cez Google identitu.
- **Roly**
  - **RP (klient):** Spotify
  - **OP / Authorization Server: Google** (OpenID Provider)
  - **Používateľ:** ja/ty/vy

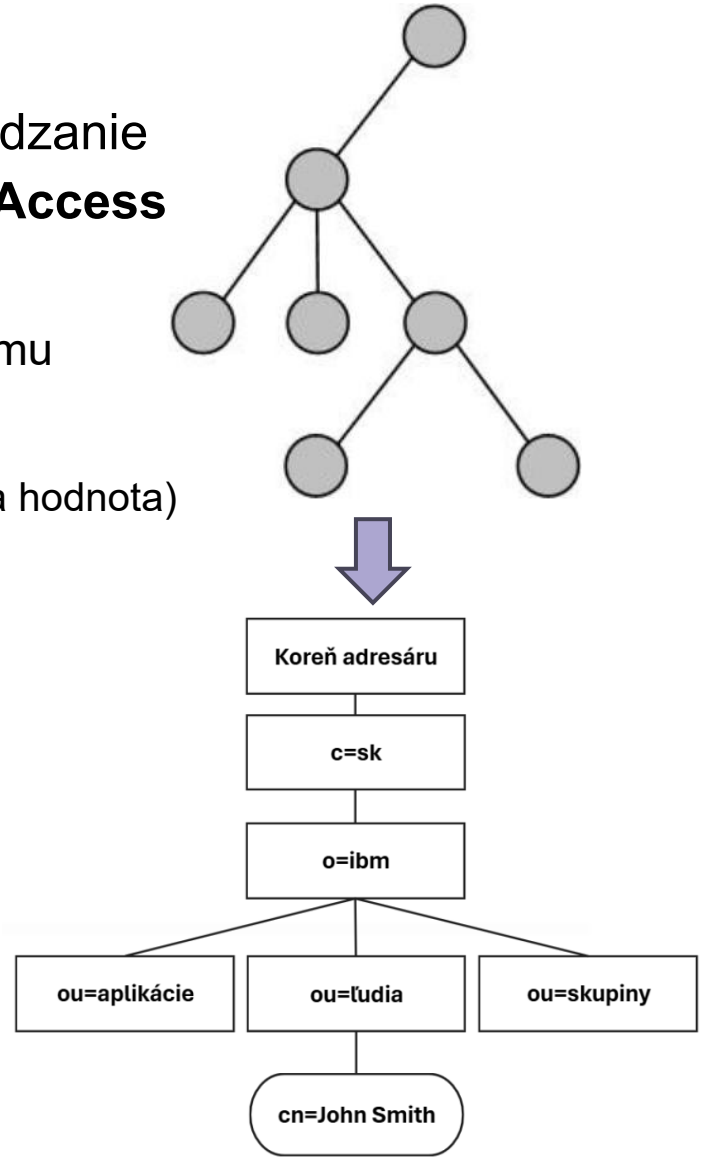
Sumarizácia

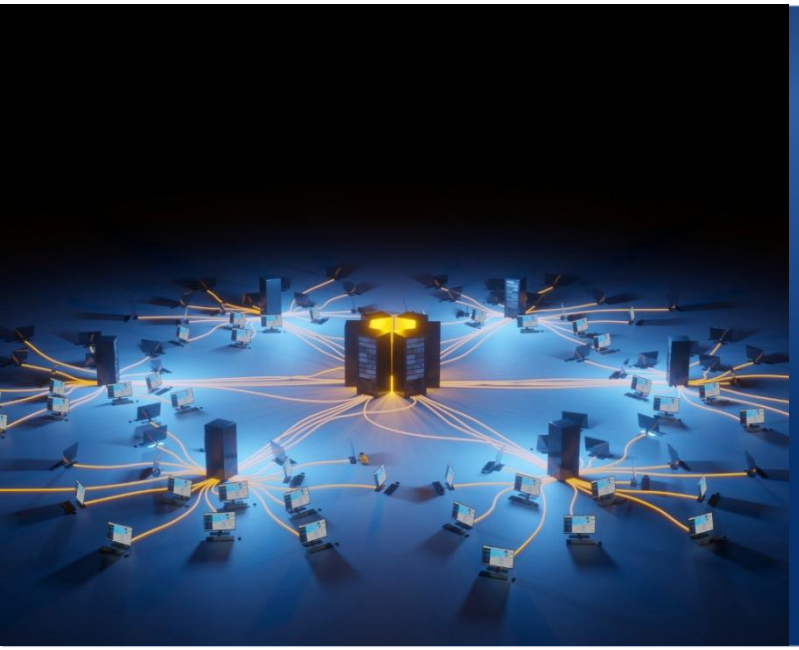
Protokol	Účel	Mechanizmus / Token	Typické použitie	Výhody	Nevýhody
SAML	Autentifikácia & federácia	**SAML Assertion** (XML)	Enterprise, univerzity (eduGAIN, SAP)	Overený a robustný, široká podpora vo federáciách	Ťažkopádny (XML), slabšia podpora mobil/cloud
OAuth 2.0	Autorizácia (API access)	**Access token** (Bearer), Refresh token	API prístup, mobilné appky (Spotify, LinkedIn)	Bezpečný prístup bez hesiel, flexibilný	Nerobí autentifikáciu, komplexná implementácia
OIDC	Autentifikácia + autorizácia	**ID token (JWT)** + Access token	Moderné webové a cloud loginy (Google, Azure AD)	Ľahký formát (JSON), jednoduchšia integrácia, vhodný pre cloud/mobil	Závislosť na OAuth, viac endpointov, riziko pri zlej implementácii

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

LDAP – adresárový protokol

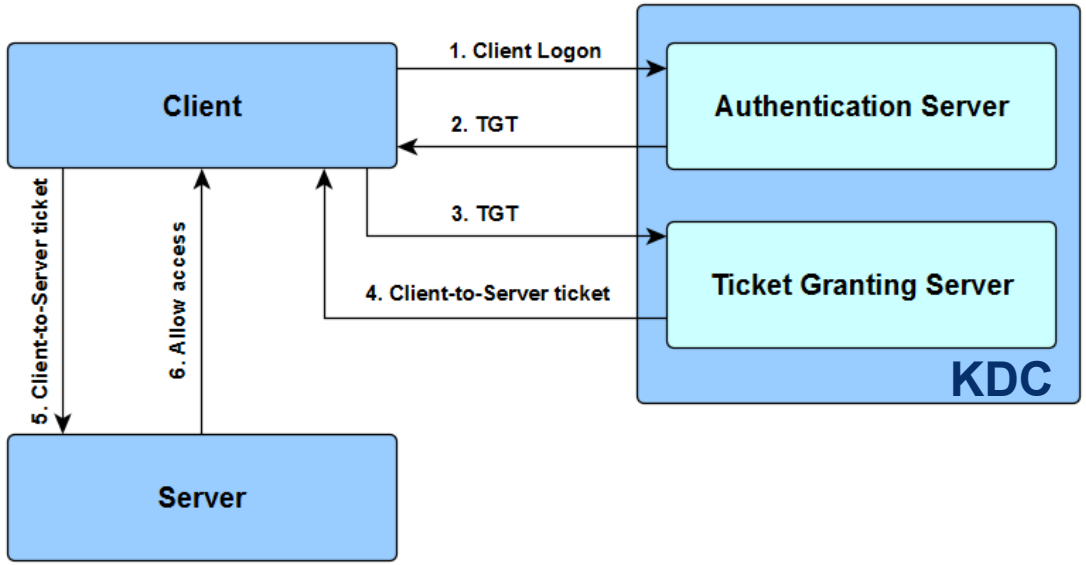
- Adresár = špecializovaná databáza navrhnutá na vyhľadávanie a prechádzanie
- Otvorený štandard pre adresáre (RFC 4510+) – **Lightweight Directory Access Protocol**
  - Základný „zdroj pravdy“ pre IdP a aplikácie
  - **Ukladá** záznamy o identitách (DN, OU) a ich atribútoch do hierarchického stromu
    - DN – distinguished name, OU – organization unit, cn – common name
  - **Typické objekty & dáta**
    - **Users, Groups, OrganizatUnits** + atribúty (napr. e-mail, department, role v tvare typ a hodnota)
    - Odvolávka na objekt cez jeho DN
- **Použitie**
  - **Backend pre IdP** (Azure/AD, OpenLDAP, FreeIPA, Keycloak)
    - Slúži aj ako **PIP** zdroj atribútov pre autorizáciu
  - Integrácie aplikácií: vyhľadávanie používateľov, skupín a rolí
- **Bezpečnosť & prevádzka**
  - **LDAPS/TLS**, princípy „least privilege“ pre bind účty
  - Replikácia a vysoká dostupnosť (HA) pre spoľahlivosť
- **Limity (čo LDAP nie je)**
  - Nie je to SSO ani engine autorizácie - je to **adresár/úložisko** identít a atribútov
- Príklady: MS Actvie Directory, OpenLDAP ...





Technológie pre sieťové riadenie prístupu a SSO

Kerberos: Prehľad



- Sieťový autentifikačný protokol K/S založený na systéme ticketov (symetrická kryptografia)
- Komponenty
  - **Klient**: Používateľ alebo služba, ktorá žiada o prístup
  - **Server služby:** Cieľová služba, napr. súborové úložisko, mail server
  - **KDC** (Key Distribution Center) – centrálna autorita (MS DC)
    - **AS (Authentication Service)** – overuje totožnosť, vydáva TGT (Ticket Granting Ticket)
    - **TGS (Ticket Granting Service)** – vydáva Service Tickets pre jednotlivé služby
- **Login (zjednodušene):**
  - Používateľ sa prihlás do Win => **AS** overí údaje a vydá **TGT**
  - Pri prístupe k službe klient požiada **TGS** o **Service Ticket** (obsahuje session key)
  - Klient predloží **Service Ticket** serveru => server tiket overí (cez KDC) a povolí prístup
- **Poznámka**
  - Vyžaduje **synchronizovaný čas (NTP)**, správne **SPN** a bezpečné kľúče

Kerberos - použitie, výhody, limity

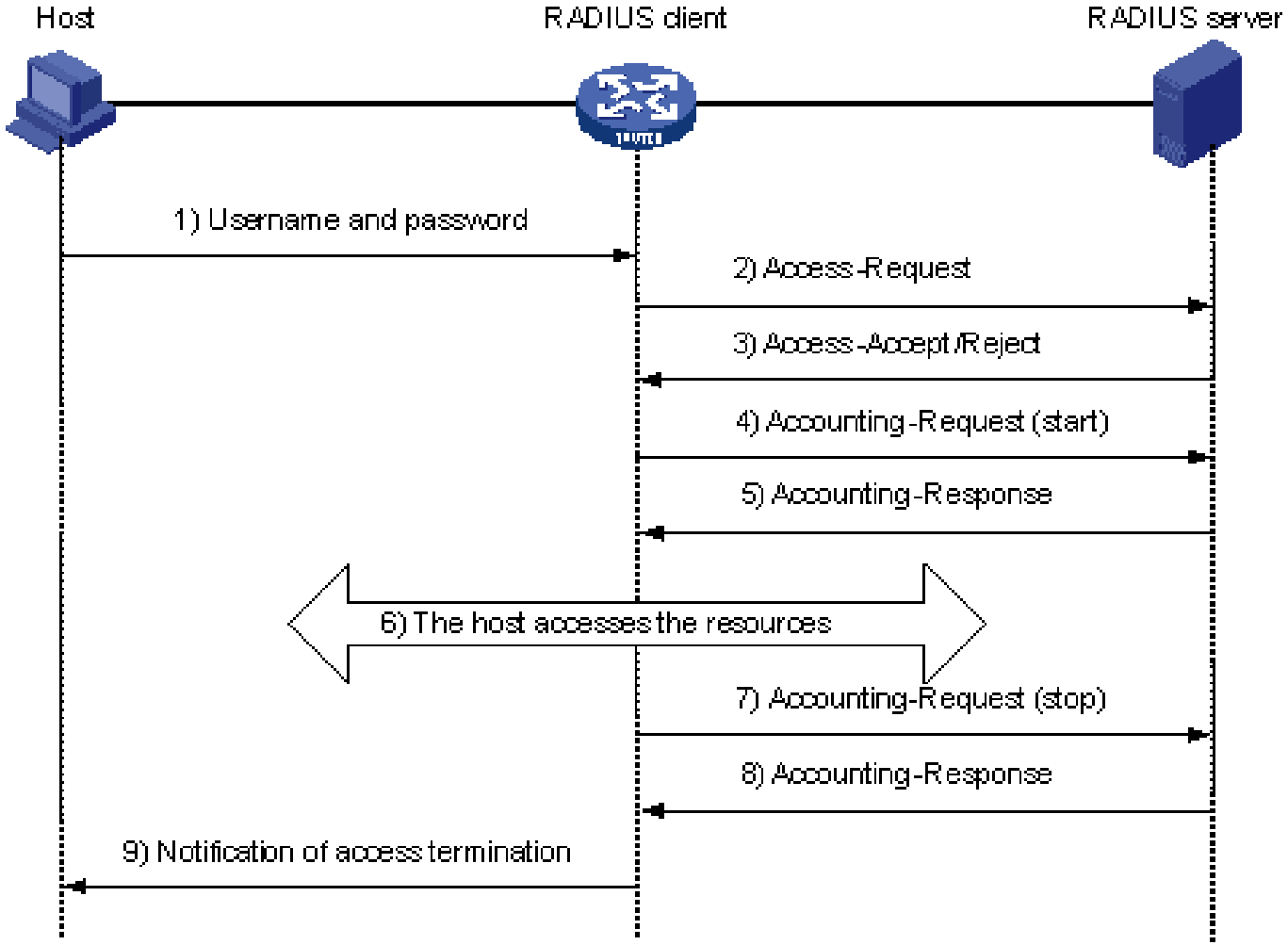
- **Kde sa používa**
  - **Active Directory (Windows domény)** – základ SSO v intranete
  - Integrácia **Linux/UNIX** do AD alebo vlastného KDC
  - Služby: SMB, SQL, SSH (GSSAPI)
- **Výhody**
  - **SSO po úvodnom logine** (žiadne opakované heslá)
  - **Vzájomná autentifikácia** klient↔server; heslo nejde po sieti
  - Overený a zrelý štandard pre **on-prem** prostredia
- **Limity / riziká**
  - Závislosť na **KDC** (HA/redundancia je nutná)
  - Citlivosť na **čas** (NTP)
  - Menej vhodný pre **internet/čistý cloud**; lístky majú obmedzenú **životnosť** (TTL)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

RADIUS (Remote Authentication Dial-In User Service)

- Otvorené klient/server riešenie
- Centralizuje autentifikáciu, autorizáciu a účtovanie (**AAA**) pre prístup do siete (Wi-Fi, VPN, 802.1X/NAC)
- **Ako to zapadá do IAM?**
  - **RADIUS klient (NAS)** => posiela požiadavky na **RADIUS server**, ktorý si berie údaje z adresára/IdP (AD/LDAP)
  - Politiky prístupu a atribúty sa spravujú centrálne (skupiny, role, VLAN, ACL)
- **Kde sa používa**
  - Podnikové/akademické Wi-Fi (WPA2/3-Enterprise s EAP), **VPN brány,** Prístup do káblovej siete (802.1X)
- **Výhody**
  - Široko podporovaný a štandardizovaný
  - Centralizovaná správa používateľských poverení
  - Vhodný pre veľké nasadenia, ako sú ISP a podniky
- **Limity / bezpečnostné poznámky**
  - Tradične negarantuje plnú integritu/šifrovanie celej správy
  - Treba riešiť cez **TLS/EAP-TLS**

RADIUS – základná komunikácia – prístup do siete



- Architektúra RADIUS
  - **RADIUS klient**
    - Zariadenia požadujúce autentifikáciu
  - **RADIUS server**
    - Server vykonávajúci autentifikáciu a autorizáciu
  - **RADIUS databáza**
    - Ukladá informácie o používateľoch
    - AD/LDAP

https://support.hpe.com/techhub/eginfolib/networking/docs/routers/msrv5/cg/5200-2323_security-cg/content/459369118.htm

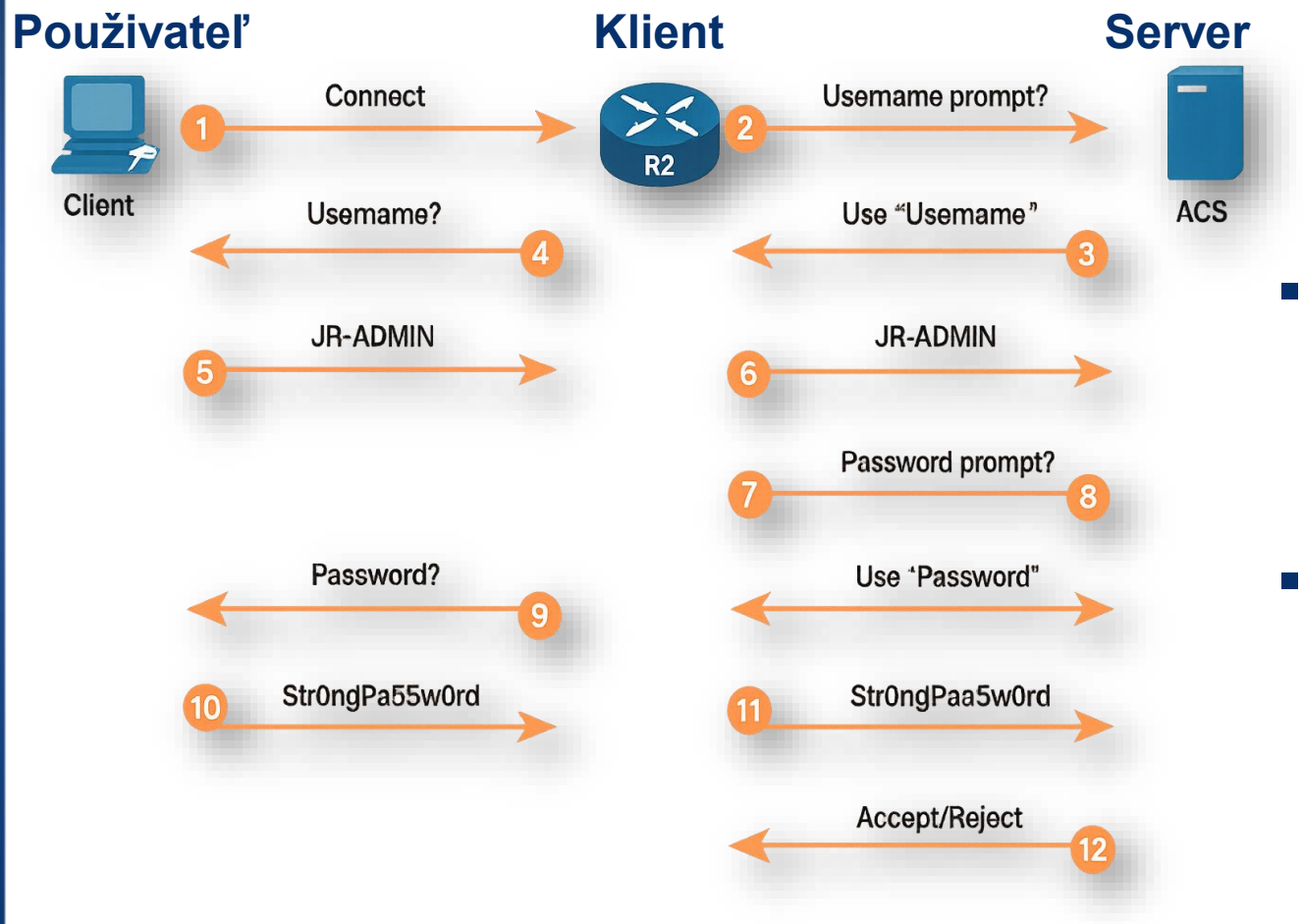
Terminal Access Controller Access-Control System Plus

TACACS+ – administrátorský prístup k sieťovým zariadeniam

- AAA pre **správu sieťových zariadení** (smerovače, prepínače, firewally)
- Ako zapadá do IAM
  - **TACACS+ server** autentifikuje adminov voči **AD/LDAP/IdP**
  - **Autorizácia „per-command“**: profily/role (napr. read-only, net-admin) definujú **povolené príkazy**
  - **Accounting**: detailné logy každého príkazu → audit/forenzika

- **Prečo TACACS+ (vs. RADIUS)**
  - Šifruje **celý obsah správy** a **oddelené kanály** pre A-A-A
  - Granulárna **autorizácia príkazov** (nie len „allow/deny“ služby)
  - Ideálne na **riadenie administrátorských činností**;
    - RADIUS je skôr pre prístup používateľov do siete (Wi-Fi/VPN/802.1X)
- **Politiky a prax**
  - Role/profily, sady povolených príkazov, časové okná; schvaľovanie zmien pre kritické zóny
  - **HA** TACACS+ servery, zasielanie logov do **SIEM**
  - „**Break-glass**“ lokálne účty minimalizovať/rotovať (PAM)

TACACS+ architektúra



- **TACACS+ klient (Sieťové zariadenia)**
  - Smerovače, prepínače, firewally
  - Požadujú AAA službu
  - Autentifikácia používateľov, autorizácia príkazov a zaznamenávanie účtovných informácií
- **TACACS+ Server**
  - Centrálna autorita pre AAA funkcie
  - Spracováva požiadavky od klientov
  - Komunikuje s používateľskými databázami a presadzuje prístupové politiky
- **Databáza (Úložisko používateľov)**
  - Ukladá prihlasovacie údaje používateľov, roly, oprávnenia a účtovné záznamy
  - Môže sa integrovať s externými adresármi:
    - **Active Directory**, **LDAP** alebo lokálne databázy

Porovnanie transportných AAA protokolov

Feature	RADIUS	TACACS+	DIAMETER
Primárne použitie	Sieťový prístup (VPN, Wi-Fi, 802.1X)	Administrátorský prístup na zariadenia (SSH, konzola)	Telco AAA (IMS, LTE/5G)
Transport	UDP 1812 (Auth), 1813 (Acct)	TCP 49	TCP/SCTP 3868
Šifrovanie	Len heslá	Celý payload	Celá komunikácia
AAA funkcie	Auth + AuthZ + Acct v jednej správe	Auth, AuthZ, Acct oddelené	Kombinované + rozšíriteľné
Granularita	Obmedzená (user access, VLAN/ACL)	Vysoká (command-level control)	Vysoká (viac funkcií než TACACS+)
Škálovateľnosť	Veľké enterprise siete	Stredné až veľké siete	Veľmi vysoká – moderné telco
Komplexita	Jednoduchšia konfigurácia	Zložitejšia – oddelené AAA	Najzložitejší, mnoho funkcií
Integrácia	Široká podpora všetkými vendormi	Primárne Cisco & podobné	Telco infra, pokročilé siete
Accounting	Silné účtovanie (VPN, Wi-Fi sessions)	Limitované (skôr admin logy)	Rozšírené, billing v telco

Ako integrovať sieťový aj webový prístup v IAM/SSO

Kľúčová idea:
Technicky sa používajú **rôzne protokoly** (Kerberos, RADIUS, SAML, OIDC), ale všetky sa opierajú o **jednu identitu v centrálnom adresári**. Preto to používateľ vníma ako **SSO**

- **Spoločný zdroj identity (IdP)**
  - Základom je **centrálny adresár (AD/LDAP)** – jedna databáza účtov a atribútov.
  - Všetky systémy (RADIUS, Kerberos, SAML/OIDC IdP) **dôverujú rovnakému adresáru**.
  - Výsledok: používateľ má **jednu identitu** (univerzitný login), ktorou sa autentifikuje všade.
- **Sieťový prístup (RADIUS, 802.1X, VPN)**
  - Wi-Fi ENT alebo VPN používajú **RADIUS server**, ktorý sa integruje s AD/LDAP.
  - Prihlásenie = meno@uniba.sk + heslo → RADIUS overí proti AD.
  - Možné rozšírenie: certifikáty (EAP-TLS), MFA pre VPN.
  - Z IAM pohľadu: RADIUS funguje ako **PEP** (enforcement), AD ako **IdP**
- **Webové aplikácie (SAML/OIDC/OAuth2)**
  - Webové aplikácie (Moodle, AIS, knižnica, cloud služby) používajú **IdP vrstvu** (napr. Shibboleth, Keycloak, Azure AD)
  - IdP je integrovaný s tým istým AD/LDAP
  - Prihlásenie = rovnaké univerzitné konto, IdP vydá token (SAML assertion, OIDC ID token)

- **Spoločný rámec IAM/SSO**
  - Používateľ sa prihlasuje **tou istou identitou**:
    - **Do siete** (RADIUS)
    - **Do Windows domény** (Kerberos ticket)
    - **Do webových aplikácií** (SAML/OIDC tokeny)
  - Pre používateľa to pôsobí ako **SSO**, hoci technicky ide o viac protokolov.
  - IAM systém ich zjednocuje → **jedno meno/heslo, centrálne MFA, centralizovaný audit**
- **Praktické príklady**
  - **Eduroam + Azure AD + Shibboleth**:
    - eduroam Wi-Fi = RADIUS + AD
    - web apps = federácia cez SAML/OIDC (Shibboleth IdP, Azure AD)
    - cloud (M365, Google Workspace) = federácia s tým istým IdP
  - **Firemné prostredie**:
    - VPN = RADIUS/AD
    - intranet = Kerberos/AD
    - SaaS = OIDC tokeny z Azure AD

JWT

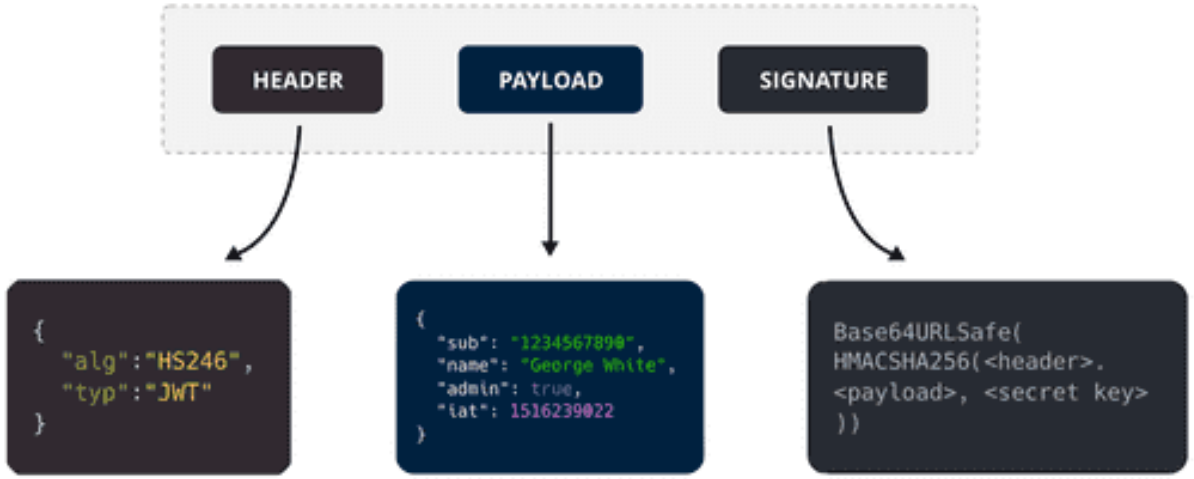
Tokeny

Typy tokenov (Access, ID, Refresh)

- **Token**
  - Krátko platný digitálny „lístok“ (dôkaz identity/práv)
  - Vydáva IdP a aplikácia (SP) verí
  - Nesie v sebe všetky autentifikačné a autorizačné údaje
  - Je digitálne podpísaný a šifrovaný
- **Prečo tokeny**
  - Umožnia **SSO/FIM** bez zdieľania hesiel
  - Zjednodušujú autentifikáciu a autorizáciu
  - Fungujú naprieč web, mobil aj API volania / kompatibilita
  - Stateless / škálovateľnosť
  - Bezpečnosť
- Typy tokenov (pozn. reálne je ich viac)
  - **Access** – čo smiem
    - Krátkodobý „kľúč“ na volania API (autorizácia)(platný minúty–hodiny)
  - **ID (ODC)** – kto som
    - Potvrdzuje identitu používateľa
    - Vydáva IdP (podpísaný JWT, obsahuje claims: meno, e-mail, roly)
  - **Refresh** - obnova
    - Vydá nový access token bez ďalšieho loginu (dlhšia platnosť)
- Životný cyklus
  - **Login** → vznikne **ID + Access**
  - po expirácii **Access** t. sa obnoví cez **Refresh t.**
- Zásady používania tokenov
  - Krátka životnosť (**TTL)**
  - Overovať *iss/aud/exp*
  - Prenos len cez **TLS**
  - Tokeny nevkladať do URL/logov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklad ID tokenu (JWT) – dekódovaná časť *payload*



- **Kľúčové claims:**
  - **iss** – kto vydal token (IdP)
  - **sub** – identita používateľa (unikátne ID)
  - **aud** – aplikácia, ktorej je token určený
  - **exp / iat** – platnosť tokenu
  - **role / scope** – oprávnenia, roly

```
{
  "iss": "https://login.univerzita.sk",    // issuer – kto token vydal
  "sub": "1234567890",                     // subject – unikátne ID používateľa
  "aud": "moodle-app",                     // audience – komu je token určený
  "exp": 1716249022,                       // expiration – čas vypršania
  "iat": 1716245422,                       // issued at – kedy bol vydaný
  "nonce": "xyz123",                       // ochrana proti replay útokom
  "email": "jana.novakova@univerzita.sk", // atribút používateľa
  "name": „Jana Novakova",                 // ďalší claim
  "roles": ["student", "user"]             // role / skupiny
}
```

JWT vs. Opaque token

- **JWT (self-contained)**
  - Token **obsahuje údaje** (claims) + podpis IdP
    - Klient / Resource Server vie token overiť lokálne (claims)
    - Žiadne volanie IdP
  - Vhodné pre distribuované služby, rýchle API, výkon
  - Revokácia je ťažšia
    - krátke TTL + rotácia
- Voľba v praxi, ak…
  - Potrebujem škálovať a nízku latenciu

- **Opaque token (referencia)**
  - Token je len odkaz – app vždy pýta IdP
  - Výhoda
    - centrálna kontrola
    - ľahká revokácia
  - Nevýhoda
    - Potreba online kontroly (záťaž IdP)
    - Závislosť na **dostupnosti IdP**
    - Mierne vyššia latencia
- Voľba v praxi, ak...
  - Chceme centrálnu a prísnu kontrolu
  - Jednoduché odvolanie prístupu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnosť tokenov a relácií

- **Riziká**
  - Únik tokenu = plný prístup (Bearer model)
  - Replay útok (použitie odchyteného tokenu)
  - Phishing na login/consent obrazovky
- **Najčastejšie chyby (a rýchle nápravy)**
  - **Príliš dlhé TTL**
    - Aby ukradnutý token nešlo znovu použiť
    - Skrátiť, zaviesť rotáciu/expiráciu
      - Access na 5–15 min, API token minúty, refresh rotácia, odpojenie pri podozrení
  - **Chýbajúca audience** alebo nevalidovaný issuer
    - Aby sa token nedal použiť pre inú aplik.
    - Služba (SP/API) musí kontrolovať
      - **pre koho (aud)** token je, **kto ho vydal (iss)** a **dokedy platí (exp)**
      - pri JWT je navyše digitálny **podpis**
  - **Token v URL alebo logoch**
    - URL končia v logoch, histórii prehliadača
    - Presunúť token do Authorization header + Secure Cookie + maskuj v logovaní
  - **Bez revokácie**
    - Starý token platí aj pri odobratí prístupu
    - Používaj opaque token, alebo blacklist pre JWT + krátke TTL
- **Ďalšie ochranné opatrenia**
  - Šifrovaný prenos, vždy cez aktuálny TLS (HTTPS)
  - MFA pre kritické prístupy, alebo keď je riziko
  - Viazanie tokenu na klienta (cert or kľuč)
- **Session vs. Token**
  - Session cookies (server-side stav) vhodné pre intranet
  - Tokeny (stateless) vhodné pre cloud a API

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Tokeny – čo má manažér sledovať (KPI)

- Dostupnosť a rýchlosť prihlásenia
  - Uptime IdP/AS (%), p95 čas prihlásenia (< 3 s), p95 latencia autorizácie API
- Úspešnosť prihlásení a MFA
  - Login success rate, MFA challenge rate a MFA drop-off (odpad po výzve)
  - Podiel „step-up MFA“ pri citlivých akciách
- Bezpečnosť tokenov
  - Priemerné TTL access (cieľ 5–15 min) a max age refresh (≤ 30 dní, s rotáciou)
  - Počet revokovaných tokenov / týždeň, detekcie replay a únikov (token v URL/logoch)
- Správnosť validácie na SP/API
  - % služieb, ktoré striktne overujú podpis, iss, aud, exp (cieľ 100 %)
  - Pokrytie TLS (100 % externé) a adopcia MTLS tam, kde dáva zmysel
- Revokácia a kľúče
  - MTTR-R (mean time to revoke) po incidente, čas propagácie rotácie kľúča
  - Podiel endpointov s opaque introspekciou vs. JWT + blacklist + krátke TTL
- Hygiena a compliance
  - % aplikácií na centrálnom IdP/SSO, % privilegovaných s step-up MFA
  - Kompletnosť audit logov (kto/kedy/k čomu), retencia podľa politiky

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zhrnutie a odporúčania – Moderné IAM

- **Konsolidácia identít**
  - Jeden adresár (AD/LDAP) ako „source of truth“
  - Centrálne IdP pre autentifikáciu (OIDC/SAML)
- **SSO a Federácia**
  - SSO pre intranetové a cloud aplikácie
  - Federácia (Circle of Trust) pre medzi-organizačné prostredia
  - Princípy bezpečnosti (Lest privilege, Separation of Duties ...)
- **Protokoly a interoperabilita**
  - SAML pre legacy/univerzitné prostredia
  - OIDC/OAuth2 ako moderný štandard pre web, mobil, API
  - Kerberos / RADIUS pre intranet a sieťové prístupy
- **Tokeny a relácie**
  - Uprednostniť **krátke TTL**, rotáciu a MFA/step-up pri citlivých akciách
  - JWT = rýchle, ale revokácia je náročnejšia; opaque token = jednoduchšia kontrola
- **Trendy**
  - Passwordless (WebAuthn)
  - Zero Trust IAM (kontinuálne overovanie, risk-based policies)
  - Automatizovaný provisioning (SCIM, JIT)

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti

Pavel Segeč

KC KYB UNIZA, https://kc.uniza.sk

Pavel.Segec@fri.uniza.sk