Správa identity

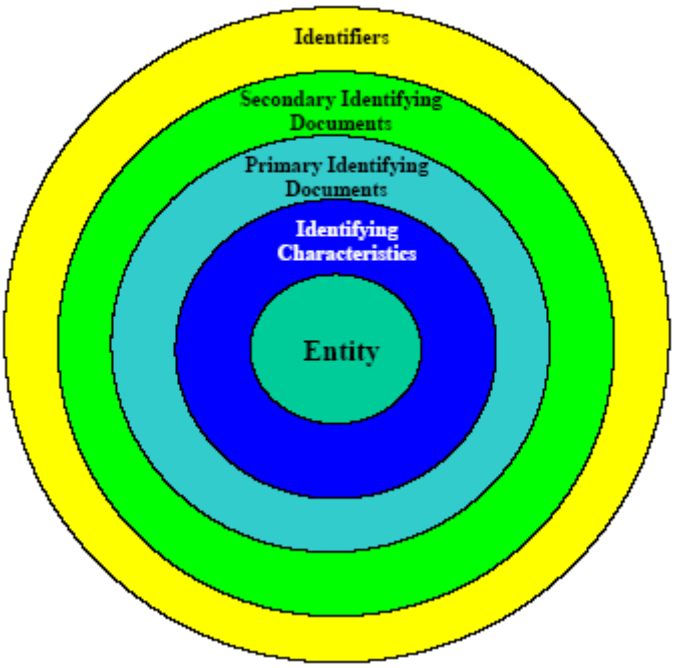
Identifikátory: jméno, userID, rodné číslo

Sekundární identifikující dokumenty: směnka, výplatní páska, permanentka, ...

Primární identifikující dokumentu: občanský průkaz, pas, dokumenty svázané přímo s identifikující charakteristikou (např fotografií, otiskem prstu)

Identifikující charakteristika: biometrika, fotografie, další prostředky rozpoznání jednotlivce

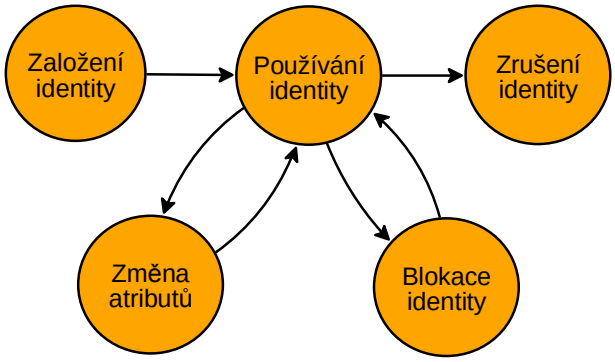
Entita: bytost, místo, věc



Identita uživatele

Rostou nároky na informace udržované o uživateli, prostou identifikaci nahrazuje komplikovaná struktura označovaná jako ***profil***

- userID, heslo
- jméno, příjmení, tituly, ...
- kontaktní informace
- příslušenství ke skupinám, organizačním jednotkám, ...
- certifikáty, klíče
- personalizace
- ...



nejen uživatelé:

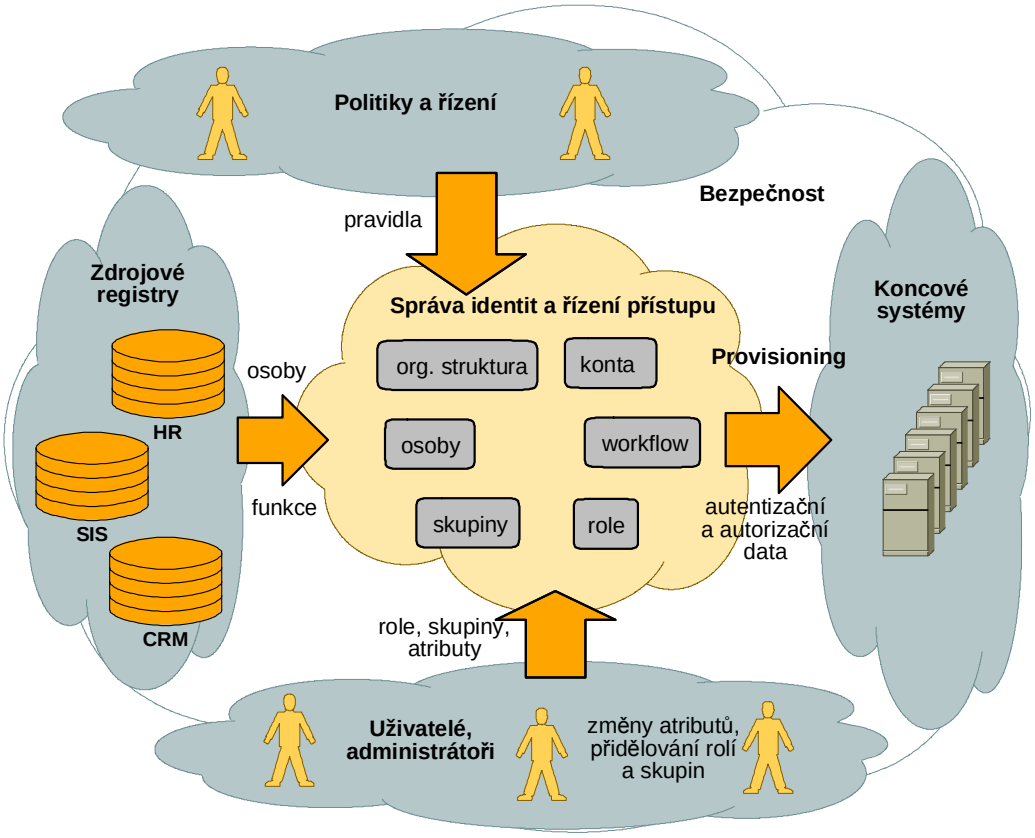
- obchodní partneři
- adresáti a odesilatelé korespondence,
- zájmové subjekty,
- ...

Další příbuzné pojmy:

- alias
- anonymita
- pseudonymita

Federalizace identity

jediná identita uživatele ve všech systémech
konzistentní záznamy o uživateli, změnu záznamů a identifikačních údajů
kredenciály (přenos identity)
může být komplikované vzhledem k technickým omezením jednotlivých systémů
synchronizace vs. externí identita



Řízení přístupu

Na všech úrovních:

- fyzický přístup do chráněných prostor
- přístup do sítě z vnějšího prostředí
- přihlášení k jednotlivému OS, DB, aplikaci
- globální přihlášení k portálu nebo skupině aplikací

Auditování a záznamy o činnosti

persistence identity:

- možnost svázat provedené operace s konkrétní entitou
- potřeba zachování identity dlouhodobě (audit událostí i po zániku přístupu k systému)
- potřeba kontinuity identity (po vypršení kredenciálů)

Technická realizace

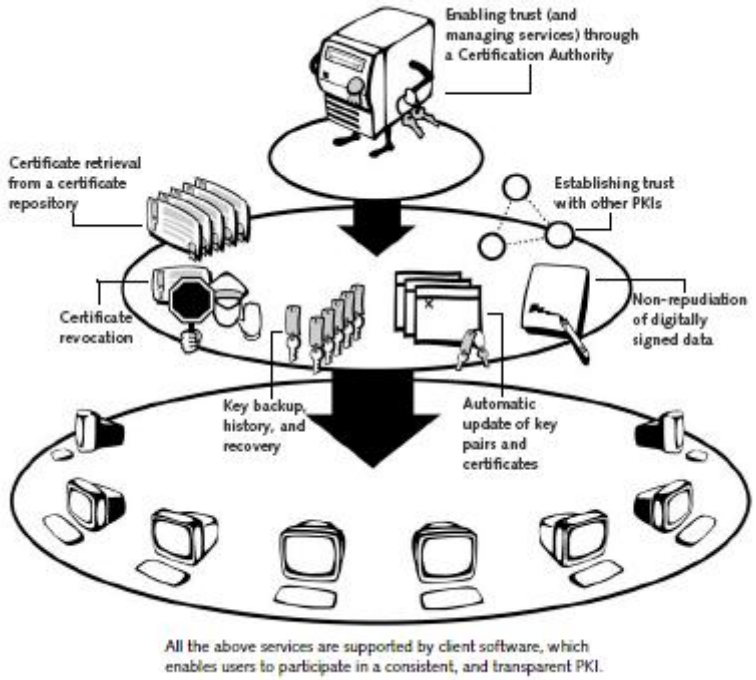
Referenční systém

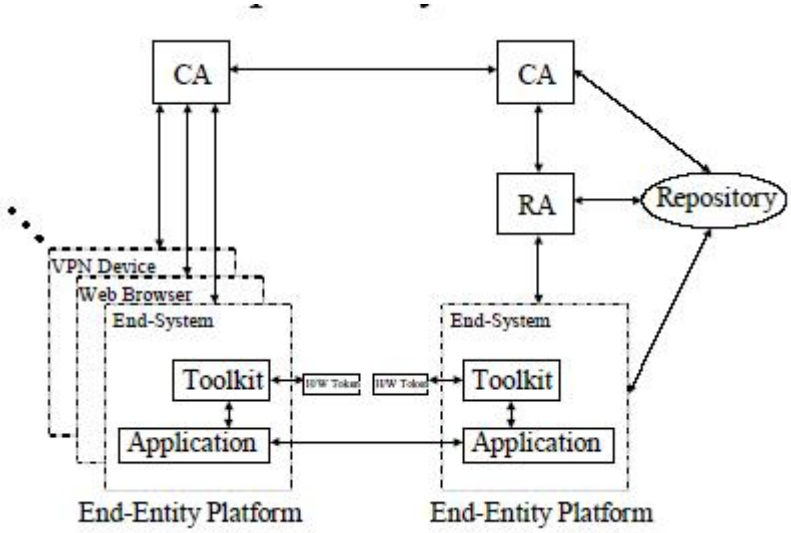
je zvolen jeden systém (zpravidla HR), který udržuje autoritativní informace o uživatelích
správu lze realizovat v rámci správy kmenových dat
uložení v rámci datového skladu

Identity manager

Specializovaný system zahrnující provisioning (vložení centrálních informací do spravovaných systémů), nástroje pro údržbu dat a konsolidaci
samoobsluhu, reporting, …

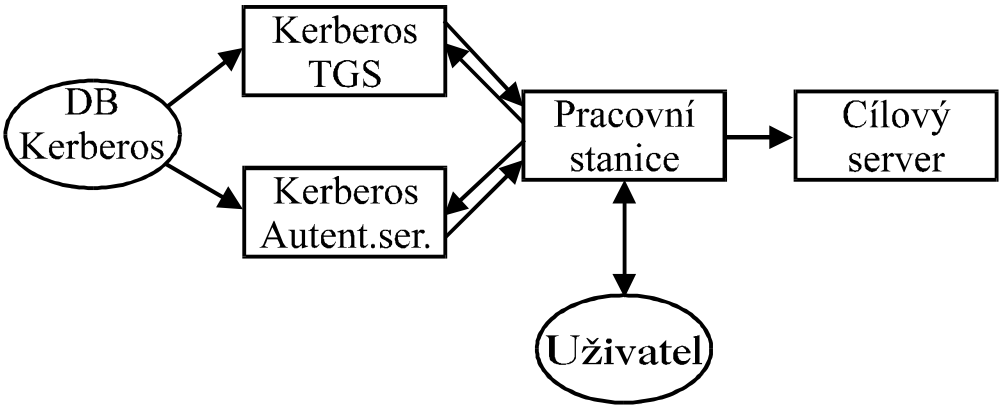
PKI





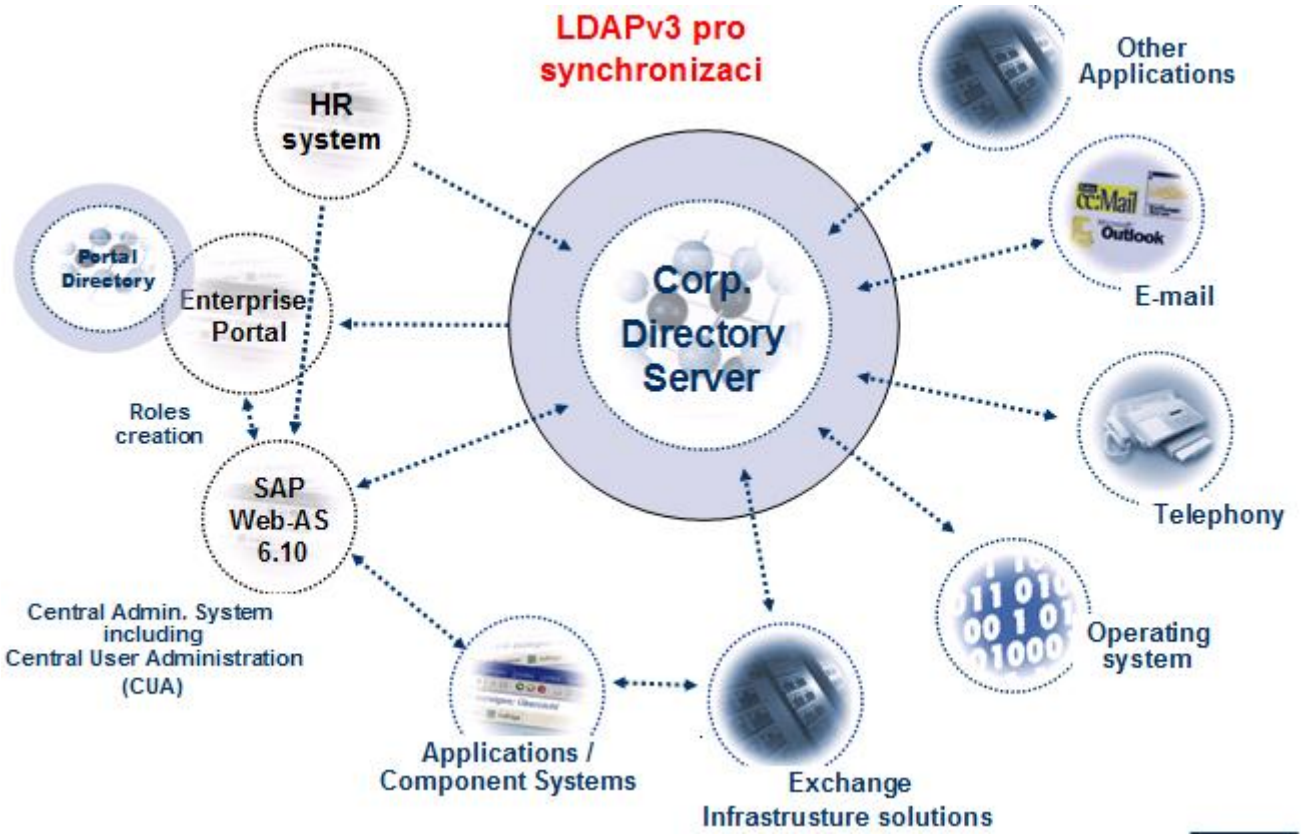
Kerberos

centrální autentizace a autorizace
centrální správa identit



LDAP

stává se tradičním úložištěm kmenových dat a tedy i informací o uživatelích
autentizace možná provedením operace bind jménem uživatele



Autentizace uživatele

synchronizace autentizačních informací vs. externí autentizace
jednotné přihlášení

- Co ví (pouze) dotyčná osoba - heslo, pass-phrase, šifrovací klíč
- Co vlastní - token, schopnost

- Schopnost provést operaci
- Cosi charakteristického - biometriky

Hesla

Charakteristika dobrého hesla:

- Obsahuje kromě velkých a malých písmen též číslice a další na klávesnici se vyskytující značky
- Dostatečná délka
- Nejde o obvyklé slovo nebo známou frázi
- Nepravděpodobné - nelze jej odvodit ze znalosti osoby vlastníka
- Často obměňované
- Není nikde po okolí poznamenáno

Odolnost hesla, předpokládaná rychlost útočníka 1.000.000 pokusů za sekundu.

Délka (znaků)	Bezpečnost	Průměrný čas útoku	Použití
1 až 7	Nízká	Krátká	Nebezpečné
8 až 9	Střední	32 let	Vzdálená přihlášení v organizacích s nízkým rizikem útoku.
10 až 11	Vysoká	217 000 let	Vzdálená přihlášení, externí přístupy do klíčových aplikací, přístupy do VPN.
12 až 23	Velmi vysoká	1 400 000 000 let	Vzdálená přihlášení v prostředích s vysokými nároky na bezpečnost, přístupy do VPN, servisní účty.
24 or more	Extrémí	Přesahuje odhadované trvání vesmíru	Výměny a aktivace důležitých klíčů, vysoce důležité účty.

Skupinová hesla

z různých důvodů občas systémy připouštějí hesla společná skupinám uživatelů - tato hesla jsou málo bezpečná, bývají často vyzrazena

Piny

(personal identiifcation number)
jsou číselné řetězce standardní délky, sloužící k podobným účelům jako hesla
v souvislosti s platebními a kreditními kartami často používány 4-místné piny

Challenge-Response systémy

heslo může být zachyceno v průběhu vkládání, nebo při přenosu cílovému uzlu
časté změny hesla jsou pro uživatele zatěžující
vhodnější je, pokud systém zašle výzvu v podobě náhodné zprávy a uživatel jako heslo vrátí správnou reakci na tuto zprávu - např. její zašifrování tajným klíčem apod.

Vícefaktorová autentizace

kombinace několika autentizačních postupů, např. pin + smart karta
vyšší úroveň bezpečnosti

Asymetrické klíče

Schopnost provádět oper ace tajným klíčem jednoznačně identifikuje držitele (dokazovatel) tohoto klíče:

1. ověřovatel zašle dokazovateli náhodně volený řetězec
2. dokazovatel jej transformuje za použití tajného klíče
3. ověřovatel pomocí odpovídajícího veřejného klíče ověří správnost

Symetrické klíče

protokol běží stejným způsobem jako v případě asymetrických klíčů, pouze v tomto případě může ověřovatel napodobovat (impersonation) dokazovatele

Passphrases

jde vlastně o dlouhá hesla, mohou to být části písní, básniček, části citátů …
pokud použijeme vhodný kompresní algoritmus, lze passphrázi transformovat ve velmi kvalitní heslo
navíc je možné aplikovat různé další měření - např. rytmus stisku jednotlivých kláves, jež bývá pro každého charakteristický

Tokeny, smart cards

token je obecné označení pro předmět, který autentizuje svého vlastníka
musí být jedinečný a nepadělatelný
obvyklá implementace jsou nejrůznější magnetické nebi čipové karty
pokud karta umí reagovat na vnější podněty, má např. vlastní výpočetní kapacitu, paměť, hovoříme o tzv. *smart card*
předložení tokenu bývá často kombinováno s nutností zadat odpovídající heslo

Biometriky

jde o techniky identifikace lidí na základě jejich osobních charakteristik
navzájem se odlišují různou mírou spolehlivosti, ceny a v neposlední řadě i společenské přijatelnosti
hledáme charakteristiky mající dostatečnou mezi-osobní variabilitu při zachování vnitro-osobní reproducibility
kvalitu biometrik lze charakterizovat:

- četnost nesprávných odmítnutí - autorizovaného subjektu
- četnost nesprávných přijetí - útočníka

- Verifikace hlasu
- Verifikace dynamiky podpisu
- Verifikace otisků prstů
- Geometrie ruky
- Obrazy sítnice

Otázkou v současné době je možnost podvrhnout identitu a celková spolehlivost biometrikcých senzorů.