



Konceptuálne postavenie Identity managementu ako jediného zdroja centrálnneho riadenia prístupov

*e*FOCUS

Tatra banka, a.s. – 27 rokov skúseností



Tatra banka bola založená v roku 1990 a počas svojej existencie získala viac ako 120 ocenení od 27 vyhlasovateľov.

Rok 2016

Global Finance

- The Best Consumer Digital Bank in Slovakia
- Best in Social Media in Central & Eastern Europe (CEE)
- Best Web Site Design in CEE
- Best Private Bank in Slovakia

Euromoney Private Banking and Wealth Management Survey 2016

- Best private banking services overall
- Net-worth-specific services (High Net Worth clients; US\$ 5 million to US\$ 30 million)
- Net-worth-specific services (Super affluent clients; US\$ 1 million to US\$ 5 million)
- Research and Asset Allocation Advice
- Innovative Technology - Client Experience

The Banker

- Best Private Bank in Slovakia
- Bank of the Year in Slovakia

EMEA Finance

- Tatra banka - Best Bank in Slovakia
- Tatra Asset Management - Best Asset Manager in Slovakia

Trend

- Banka roka 2016 (2.miesto)

Android Code

- Brandované aplikácie (**1. miesto**)
- Verejné hlasovanie (**2. miesto**)

Techbox

- Banková aplikácia roka





Tatra banka, a.s. – líder v inováciách



- Mobilná aplikácia **Tatra banka** pre okuliare **Microsoft Hololens** a **AppleWatch**
- Manažment financií – Spending report, Majetok a záväzky, Ciele
- Aplikácia **MobilePay^{TB}** – bezkontaktné platby mobilom s OS Android
- Online manažment kariet – zmena limitov na platobných kartách
- Výber z bankomatu mobilom
- Hlasová biometria
- Internet banking
- **Karta** a čítačka^{TB}, aplikácia **Čítačka**
- Online konzultácia hypotéky
- **Darčeková karta^{TB}**
- Bankomaty pre nevidiacich
- Karta na počkanie
- Digitalizovaný podpis
- ...



Čo je Identity management?



Z pohľadu tejto prednášky definujeme Identity management nasledovne:

- Proces spadajúci pod IT bezpečnosť, ktorého úlohou je zabezpečiť, aby mala správna osoba správne prístupové oprávnenia na správnych systémoch v správnom čase. Získanie privilégií sa deje prostredníctvom jednotného auditovateľného bodu.

Takúto definíciu nám zabezpečuje jeden IDM systém.



Prečo Identity Management

- Neustále narastajúce množstvo aplikácií v banke
- Zvyšovanie prácnosti na strane aplikačných administrátorov
- Zvyšovanie rizika neoprávnených prístupov
- Zabezpečovanie nezlučiteľnosti privilégii



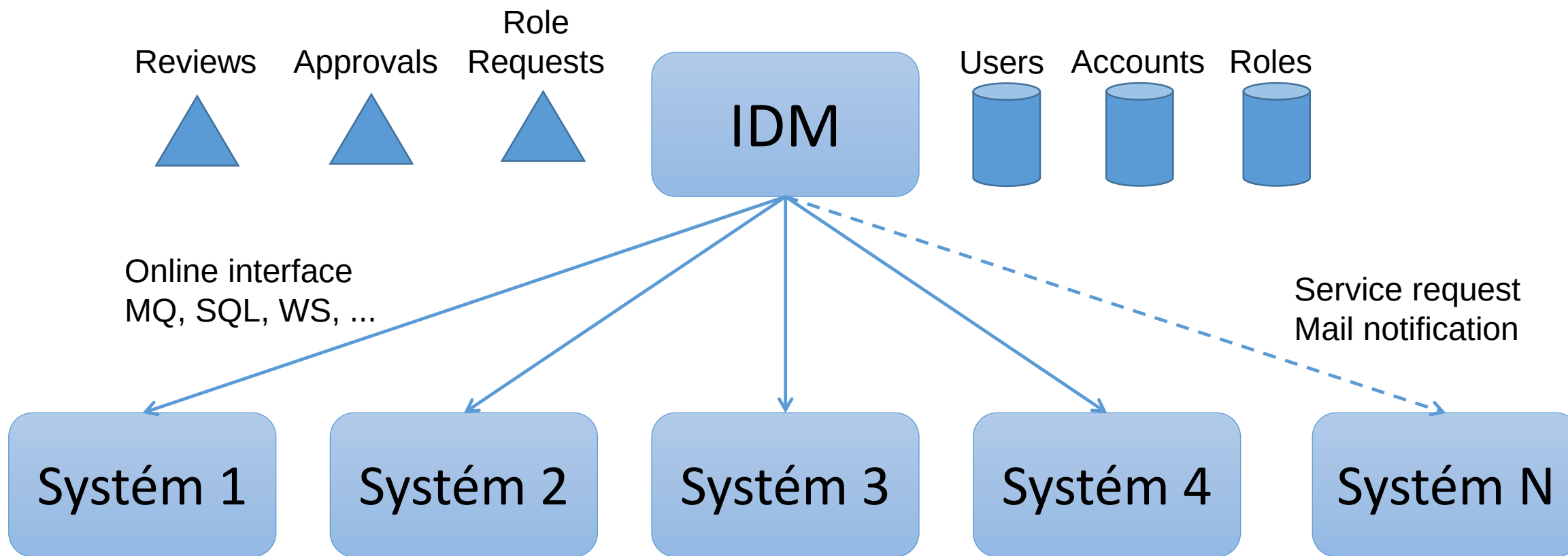


Rozvoj IDM/evolúcia biznis rolí

- Pilotné nasadenie IDM
- Riadenie niekoľkých systémov
- Riadenie stoviek systémov a tisícov rolí
- Potreba spájania do nadrolí
- Pilotné nasadenie BR
- Postupné vytvorenie rolí pre všetky útvary v banke



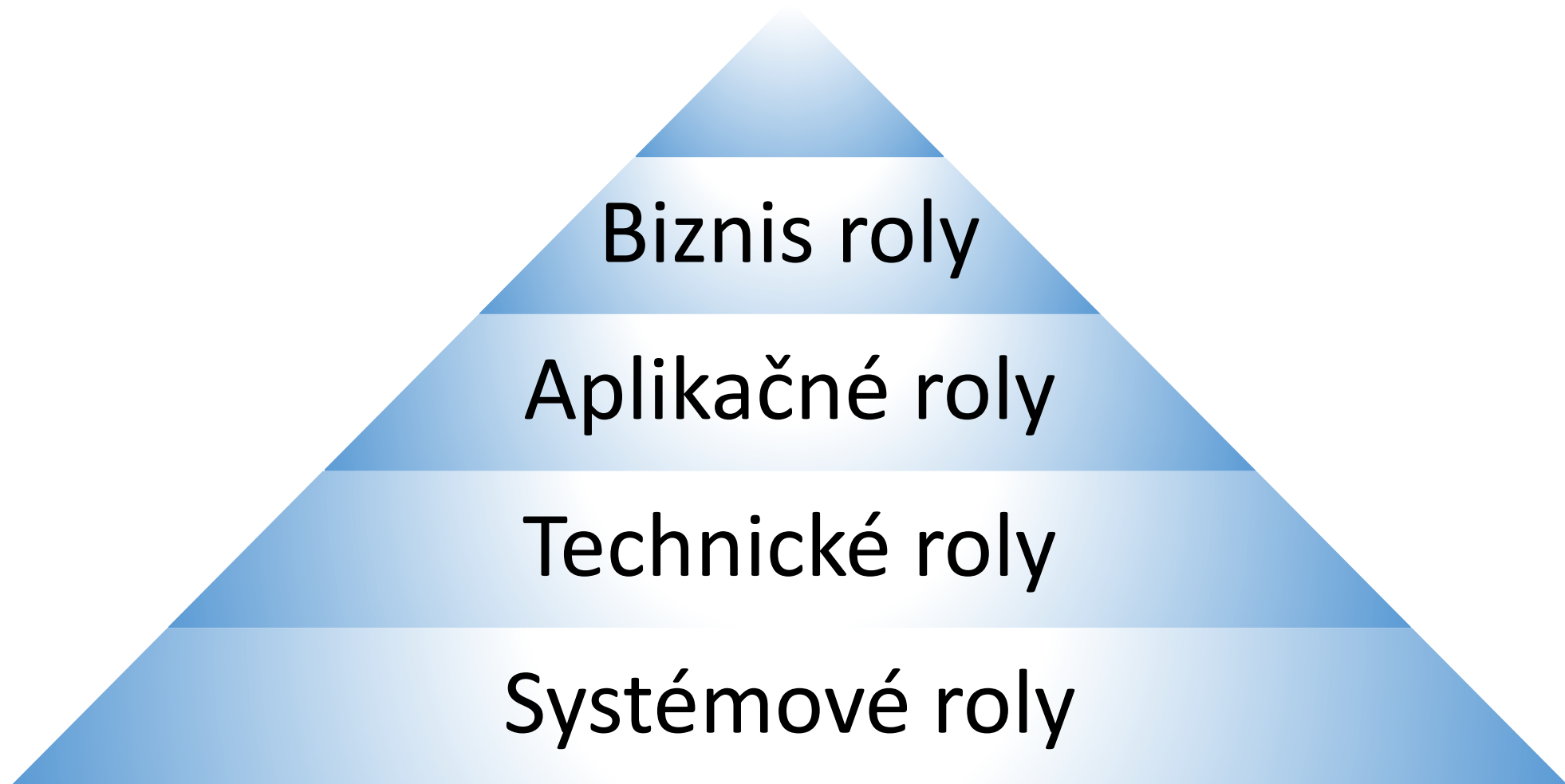
IDM systém



Stovky systémov

Väčšina pripojená online

Všetky pripojené aj v predprodukčných prostrediach ak ich majú





- Rola zabezpečujúca vytvorenie a riadenie účtu na danom systéme.
- Nastavuje všetky potrebné atribúty pre konkrétny systém.
- **Príklad:** Nastavenie mena ...
- **Hint:** Pokiaľ má používateľ priradenú systémovú rolu, je možné mu na takomto systéme na danom účte meniť heslo, blokovať ho a podobne.



- Rola nastavujúca atribúty, potrebné na danom systéme ale s ohľadom na konkrétnu aplikáciu.
- **Príklad:** Nastavenie čísla pobočky, na ktorej používateľ pracuje.



- Rola s konkrétnym privilegiom v danom systéme.
- **Príklad:** Privilegium aplikáciu spustiť, vyhľadať klienta, zadať žiadosť, schváliť žiadosť a podobne.



- Súbor všetkých prístupových oprávnení potrebných pre vykonávanie agendy na konkrétnej pracovnej pozícii.
- **Príklad:** Privilégium A v systéme 1, privilégium B v systéme 2, privilégium C v systéme 3 ...
- Čo všetko obsahuje biznis rola?





Príklad biznis roly

- POBOCKA::LIVE::Servisny poradca
- Obsahuje:
 - POBOCKOVA APLIKACIA::LIVE::Servisny poradca
 - CENTR.BANK.SYSTEM::LIVE::Servisny poradca
 - DOKUMENT.ARCHIV::LIVE::Vyhľadavanie
 - DOKUMENT.ARCHIV::LIVE::Tlac
 - KARTOVY SYSTEM::LIVE::Pobockovy pracovník
 - INTERNET::LIVE::Standardny pristup
 - PODPISOVE OPRAVENENIE::LIVE::Pobocka Samostatne A
 - PLNA MOC::LIVE::Pobockove opravenia
 - FYZICKY PRISTUP::LIVE::Pobocka
- Mimo biznis roly: POBOCKA::LIVE::123 – OC EUROVEA 3



Prínosy zavedeného IDM

- zníženie prácnosti na strane administrátorov
- zrýchlenie vytvorenia účtov a získania privilégií
- zjednotenie systémových atribútov
- zníženie rizika chyby manuálnej práce
- zníženie rizika interného fraudu
- jednotné miesto na zmenu hesla
- jednotné miesto pre žiadanie o privilégiá

Prínosy biznis rolí 1/2



- zníženie nadbytočných privilégií
- zníženie problémov z chýbajúcich privilégií
- zníženie administratívy pri nástupe nového pracovníka a
- zrýchlenie získania prístupov pre nového pracovníka
- zníženie administratívy pri prestupe pracovníka na iný útvar (výmena BR)
- zníženie administratívy pri crossingu (výmena BR, alebo doplnková BR)

Prínosy biznis rolí 2/2



- zjednodušenie vyradovania aplikácií z prevádzky (úprava BR, nie profilu množstva pracovníkov)
- zjednodušenie nasadzovania nových aplikácií do prevádzky (úprava BR, nie profilu množstva pracovníkov)
- zjednodušenie požiadaviek a odporúčaní pri vývoji a úprave aplikácií (definícia privilégií už s ohľadom na BR)
- zabezpečenie nezlučiteľnosti funkcií (SOD)



Čím sa môžeme pochváliť?

- Nový zamestnanec má pri nástupe všetky prístupy
- Manažujeme INT, UAT aj LIVE prostredia
- Fungovanie biznis rolí je bezproblémové
- BR obsahujú IT prístupy, podpisové oprávnenia, plné moci, fyzické prístupy, ...

A čo v budúcnosti:

- TB IDM jediný zdroj prístupov pre všetko



Ďakujeme za pozornosť

