Správa identít v akademickom sektore SR

Identity management in edu sector of SR

Jozef KORICINA

Abstract

An important factor in the further development of information and communication technologies (ICT) at Slovak universities is implementation of Information Security Management System (ISMS). The important part of the ISMS is management user access accounts whose task is to ensure users' access to information systems and services of the University. In the university it comes in a very short time to pick up a large number of students, which is necessary in a very short time to ensure access to the university network and all necessary services. Experience shows that it is in the university environment has automated identity management justified. Some universities have already successfully implemented commercial Identity Management Systems (IDM), and can effectively ensure the life cycle management of user access accounts. The advantages of IDM is a unique identifier of the person, which is a prerequisite for the integration of university and departmental information systems.

Keywords

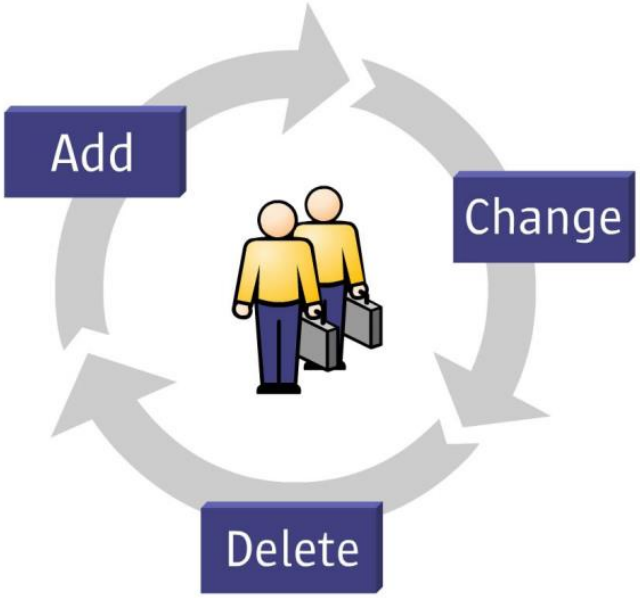
Information and communication technologies, Information Security Management System, Identity Management System.

Univerzity sú už svojou podstatou organizáciami, kde dochádza k pravidelnej a zásadnej obmene používateľov informačných systémov, ako aj k zmenám ich údajov spracovávaných aplikáciami. Rôznorodosť systémov používaných v univerzitnom prostredí zapríčiňuje, že sa správa identít stáva náročnou činnosťou vzhľadom na počty študentov, ktorí na univerzity prichádzajú alebo ich opúšťajú po ukončení štúdia. Náročnou nielen z hľadiska počtu zmien, ale aj z pohľadu procesov a atribútov ich väzby na univerzitu.

Používateľ na univerzite môže byť študentom, zamestnancom alebo externistom, pričom môže jednotlivé stavy plynule meniť alebo nadobúdať súčasne. Ako študent môže mať viac štúdií, ako zamestnanec viac pracovných pomerov. V priebehu životného cyklu môže študent štúdium prerušiť, obnoviť, ukončiť alebo absolvovať, pričom špecifickú množinu tvoria absolventi 1. stupňa štúdia, ktorí väčšinou pokračujú v ďalšom (novom) štúdiu v ďalších stupňoch. Zamestnanec môže prejsť do mimoevidenčného stavu a znovu sa vrátiť do aktívneho pracovného pomeru. Pracovný pomer môže byť interný alebo na dohodu, pričom práve množina pracovných pomerov na dohodu je početná a podlieha častým zmenám. Počas akademického roka tvorí asi 30 až 40% pracovných pomerov. Vyskytujú sa prípady, keď má zamestnanec aj 6 pracovných pomerov, ktoré môžu byť na rôznych fakultách a mnohé z nich sú iba krátkodobé dohody na niekoľko dní.
Primárnymi a autoritatívnymi zdrojmi používateľov sú akademický informačný systém MAIS (študenti) a systém SAP HCM (zamestnanci). Externista je používateľ, ktorý nie je ani v jednom z uvedených systémov, potrebuje však diferencovane prístup do rôznych sekundárnych informačných systémov (e-learning, evidencia záverečných prác, stravovací systém, WIFI, SunRay, ...).

Z hľadiska zložitosti statusu a životného cyklu používateľa na univerzite je potrebné riešiť problémy, ktoré sa v bežnom firemnom prostredí nevyskytujú, ako napríklad zmena stavu používateľa alebo určenie tzv. hlavného štúdia a hlavného pracovného pomeru, ktoré sú rozhodujúce pre import údajov do sekundárnych systémov a môžu sa v čase meniť, či „odklad“ terminácie účtov u absolventov 1.stupňa, ktorí sa po 3 mesiacoch znovu vrátia.

Obr.1 Riadenie životného cyklu identít



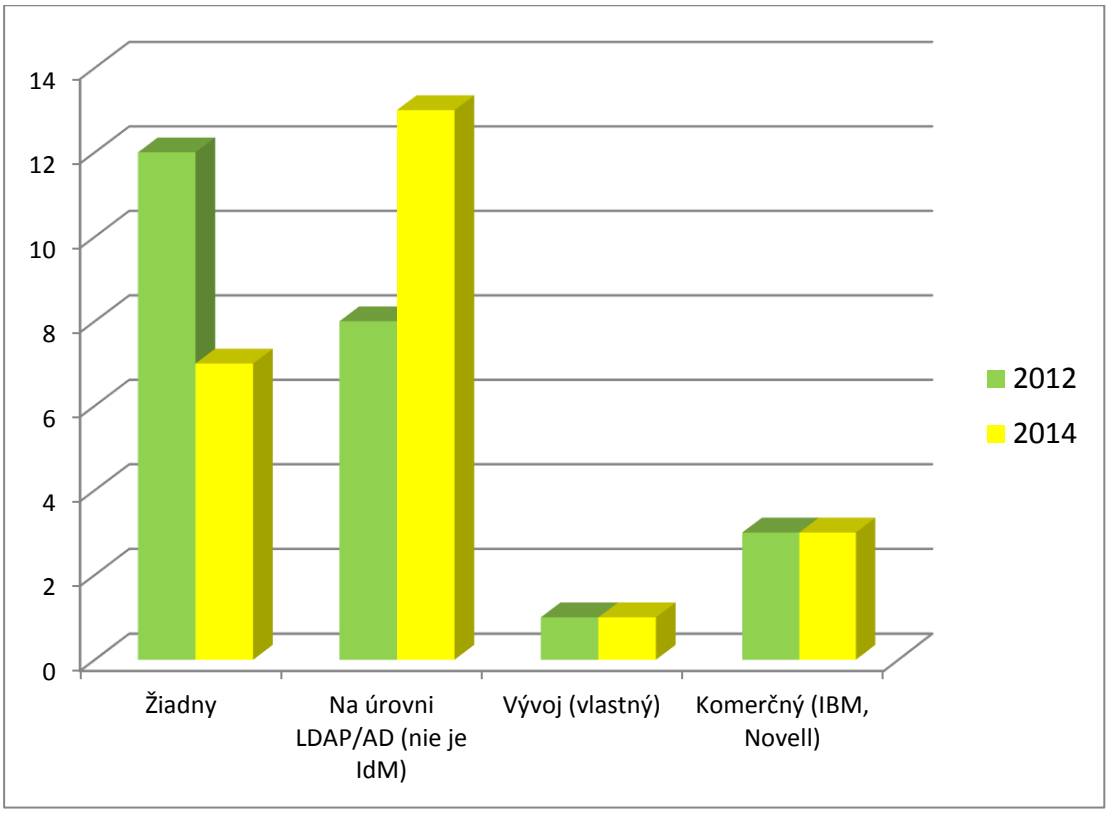
Univerzity musia bezpečne spravovať a optimalizovať heterogénne IT zdroje naprieč fyzickými, virtuálnymi a cloudovými prostrediami. Nutnosťou pre organizácie tohto typu je taktiež získanie inteligentného prehľadu o prístupe používateľov. Tento problém je potrebné vyriešiť centralizovaným poskytovaním používateľských účtov, riadením rolí a bezpečným prístupom ku zdrojom a aplikáciám. Pomocou integrovanej správy rolí a pracovných postupov je možné veľmi efektívne definovať a kontrolovať oprávnenosť prístupov používateľov k univerzitným IT zdrojom.

Riešenie na správu identít a prístupov zabezpečuje, aby zdroje boli prideľované efektívnym spôsobom tým používateľom, ktorí ich potrebujú a zároveň majú oprávnenie k nim pristupovať. Dôležitou črtou je tiež neinvazívnosť riešenia, teda minimálne vyžadované zmeny na strane integrovanej aplikácie. Základné systémy, kde je treba riešiť integráciu a správu používateľov, sú podobné ako v každej bežnej firme, teda napr. SAP, elektronická pošta, stravovací system, prístup do WiFi a samozrejme hlavný informačný systém – v prostredí univerzít ide o akademický informačný systém (AIS).

Združenie EUNIS-SK v rokoch 2012 a 2014 realizovalo prieskum o stave IKT na slovenských univerzitách. V rámci prieskumu univerzity odpovedali na otázku, akým spôsobom spravujú identity, resp. používateľské účty na prístup k informačným systémom a službám univerzity. Vyhodnotenie tejto otázky ukazuje graf č.1. Najviac univerzít (13) využívalo v roku 2014 centrálny LDAP na pridelenie prístupov k univerzitným systémom a na uchovávanie dôležitých atribútov o používateľoch. Riadenie životného cyklu používateľov sa v tomto prípade najčastejšie uskutočňuje pomocou skriptov, ktoré aktualizujú dáta v LDAP na základe zmien v zdrojových systémoch (SAP-HCM, AIS). Potešiteľný je trend zmenšovania počtu univerzít, ktoré nemajú centrálnu správu používateľských účtov.

V roku 2012 i 2014 rovnako štyri univerzity deklarovali plnohodnotnú prevádzku systému na správu identít, pričom tri používajú komerčný systém a jedna univerzita vyvíja vlastný IDM. Je to zrejme tým, že pred nasadením systému na správu identít treba vykonať dôslednú analýzu vnútorných procesov, zdrojových a cieľových informačných systémov (integrovaných s IDM). Ďalším faktorom je, že proces implementácie nie je možné realizovať v krátkom čase. Je potrebné rozdeliť implementáciu na etapy a cieľové systémy integrovať s IDM postupne.

Graf č.1 Spôsob správy identít na slovenských VŠ v rokoch 2012 a 2014



V Koncepcii informatizácie rezortu školstva do roku 2020 sa so systematickým riešením správy identít neuvažuje. Len veľmi okrajovo a nekonkrétne sa spomína v Akčných plánoch digitalizácie a informatizácie rezortu školstva do roku 2020: „Identifikácia a riadenie prístupov je v súčasnosti spravované cez prierezový IS RIAM, Rezortný Identity Access Management“. RIAM je správa používateľov zo stredných škôl, ktorí pristupujú k elektronickému edukačnému obsahu. Univerzity, ktoré majú kvalitnú správu identít by od MŠVVaŠ SR požadovali v tejto oblasti jasne definované ciele:

1) Zaviesť jednotný identifikátor osoby v sektore školstva (edu_ID)
2) Akceptácia univerzitných IDM pri integrácii s rezortnými IS
3) Podpora riešení, ktoré zapoja slovenské VŠ do akademickej federácie identít eduGAIN

Pozitívnym príkladom v tejto oblasti je integrácia univerzitného systému Novell IDM so Zamestnaneckým portálom VŠ (ESS portál SAP-SOFIA). V rámci menšieho rezortného projektu sa podarilo implementovať riešenie, pri ktorom centrálny systém autentifikuje používateľa voči univerzitnému IDM (LDAP):

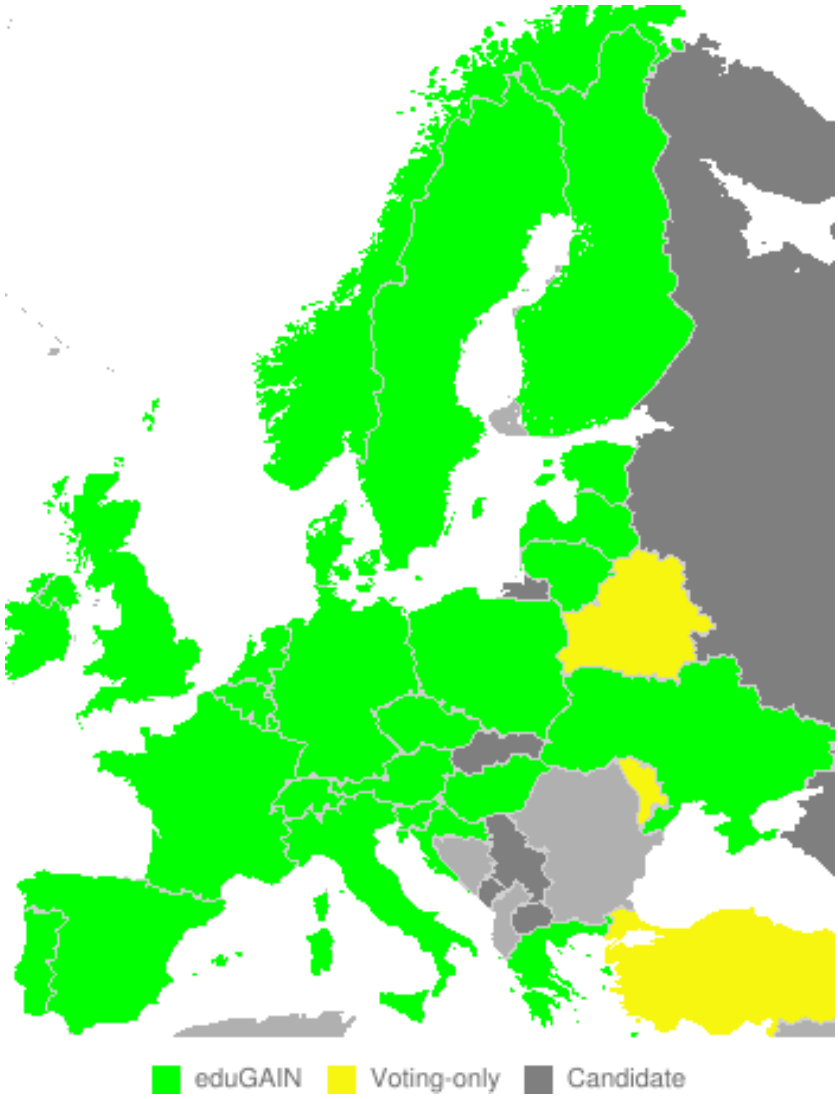
- IDM je master, z ktorého ESS portál preberá heslo
- Prenos hesla realizuje synchrónna webová služba v Process Integration

- Zmena hesla v IDM je udalosť, ktorá spúšťa webservis
- Prenos hesla je notifikovaný do IDM (úspešne/neúspešne)

Zodpovedná správa identít na univerzite je základným predpokladom, ktorý je potrebné splniť, aby mohli používatelia univerzity pristupovať k webovým službám a elektronickým dátovým zdrojom prostredníctvom federácie federácií európskych akademických a výskumných inštitúcií s názvom eduGAIN. Druhým predpokladom je vytvorenie slovenskej akademickej federácie identít s názvom safeID, ktorá bude garantom dodržiavania federačnej politiky a dôveryhodnosti členmi národnej fede- rácie. Výhody safeID:

a) Jednotný prístup k viacerým službám a aplikáciám
b) Správcovia služieb neudržiavajú autentifikačné dáta používateľov
c) Citlivé dáta pri autentizácii neopúšťajú sieť univerzity
d) Federačná infraštruktúra poskytuje bezpečný spôsob výmeny dát o používateľoch

Obr.1: Mapa Európy s vyznačením zapojenia do eduGAIN



Záverom si dovolím vysloviť svoj názor, že implementovanie systému na správu identít môže byť konkrétnym a pozitívnym prínosom k zvyšovaniu kvality každej univerzity v SR.

Abstrakt
Dôležitým faktorom ďalšieho rozvoja informačných a komunikačných technológií (IKT) na slovenských univerzitách je implementácia systému riadenia informačnej bezpečnosti (ISMS). Dôležitou súčasťou ISMS je správa používateľských prístupových účtov, ktorej úlohou je zabezpečiť prístup používateľov k informačným systémom a službám univerzity. V prostredí univerzity prichádza vo veľmi krátkom čase k nástupu veľkého množstva študentov, ktorým je nevyhnutné vo veľmi krátkom čase zabezpečiť prístup k univerzitnej sieti a všetkým potrebným službám. Ukazuje sa, že práve v univerzitnom prostredí má automatizovaný systém správy identít svoje opodstatnenie. Niektoré univerzity už úspešne implementovali komerčné Identity Management Systems (IDM) a dokážu efektívne zabezpečiť riadenie životného cyklu používateľských prístupových účtov. Nespornou výhodou systémov IDM je jednotný identifikátor osoby, ktorý je nevyhnutnou podmienkou pri integrácii univerzitných a rezortných informačných systémov.

Kľúčové slová
Informačné a komunikačné technológie, systém riadenia informačnej bezpečnosti, systém na správu identít.

Kontakt
Ing. Jozef Koricina, Centrum informačných systémov, Hornopotočná 23, 918 43 Trnava, č.t.: 0335939345, E-mail adresa: jozef.koricina@truni.sk

Recenzent: RNDr. Darina Tothová, PhD., SPU v Nitre