Zkušenosti s nasazováním Identity Managementu na VŠB-TUO

Martin Lasoň

Vysoká škola báňská - Technická univerzita Ostrava

Počáteční stav

- LDAP server zajišťující přístup pomocí jediného hesla
  - Platforma Novell Netware,
  - Platforma Unix (Linux, AIX, ...),
  - Poštovní server (Linux),
  - Přístup do školní sítě přes VPN,
  - Publikační systém OBD Pro,
  - ...

Počáteční stav

- LDAP server zajišťující přístup pomocí jediného hesla
  - Platforma Novell Netware,
  - Platforma Unix (Linux, AIX, ...),
  - Poštovní server (Linux),
  - Přístup do školní sítě přes VPN,
  - Publikační systém OBD Pro,
  - ...
- Personální agenda (SAP)
- Současná studijní agenda (Student)
- Nová studijní agenda (EDISON)
- Kartové centrum (kiosky)

Požadavky

- Zajištění aktuálnosti dat mezi jednotlivými systémy.
- Potřeba automatizace správy uživatelských identit.
- Nastavování expirace účtu podle nejdelšího vztahu.
- Rozdělení uživatelů do skupin odrážejících organizační strukturu.
- Podpora aplikačních rolí.
- Zabránit anonymním přístupům studentů na počítače některých učeben.

Navržené řešení

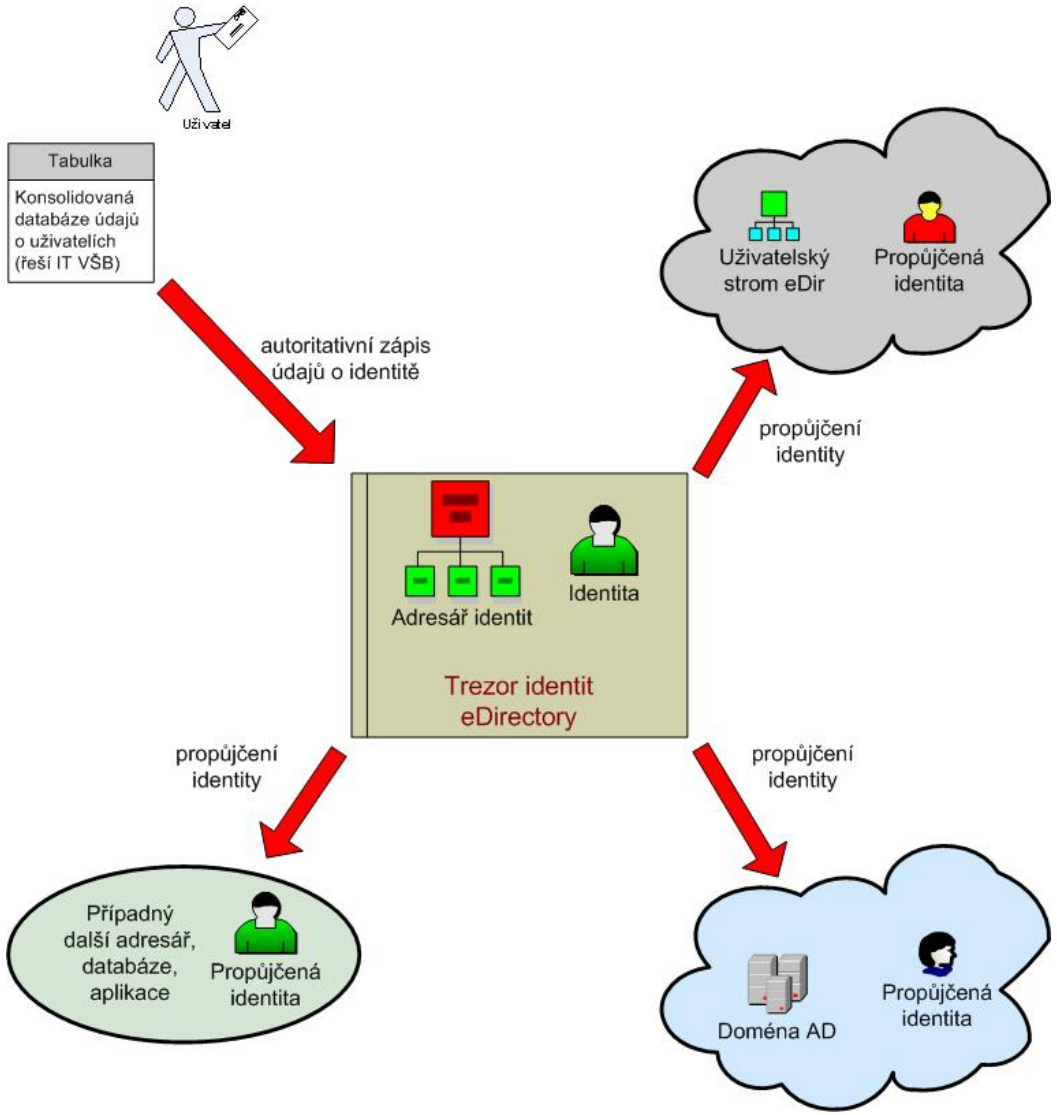
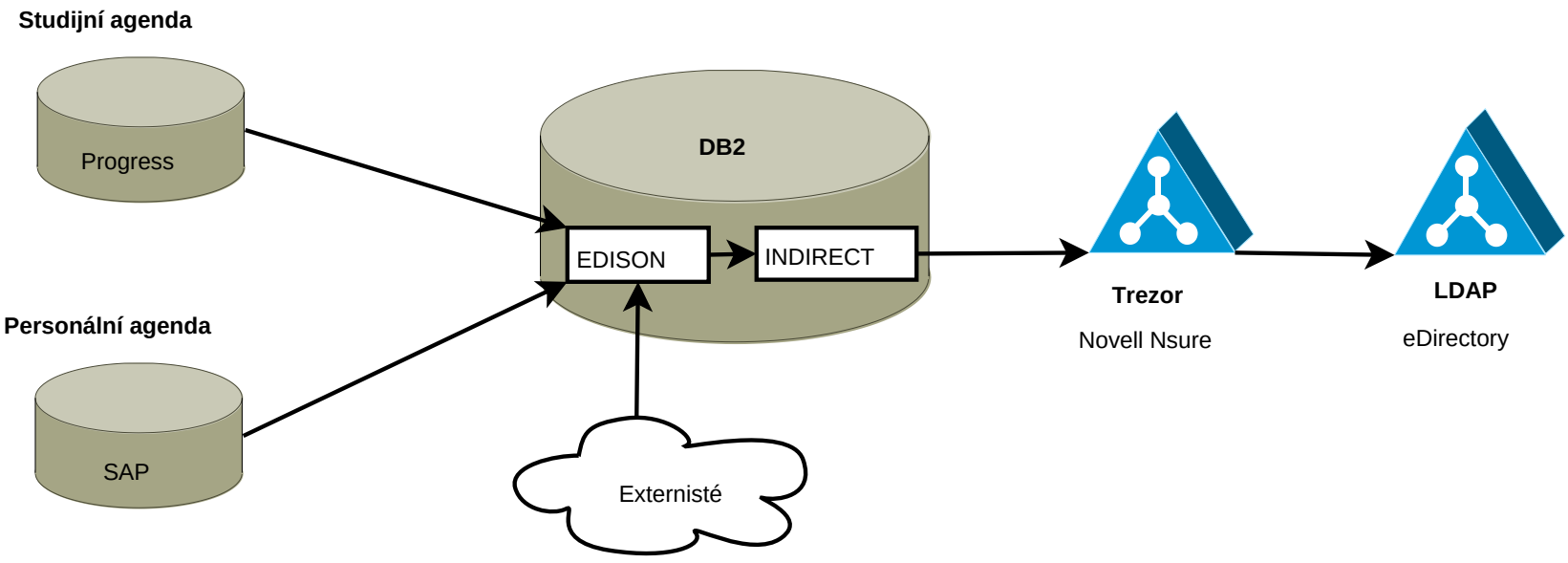


Schéma toku dat – aktuální stav



Osobní čísla

Problém – osobní čísla

- Zaměstnanci – formát 3 + 2 (las03).
- Studenti – formát 3 + 3 (bon007).
- Existence dvou účtů v případě studujícího zaměstnance.

Osobní čísla

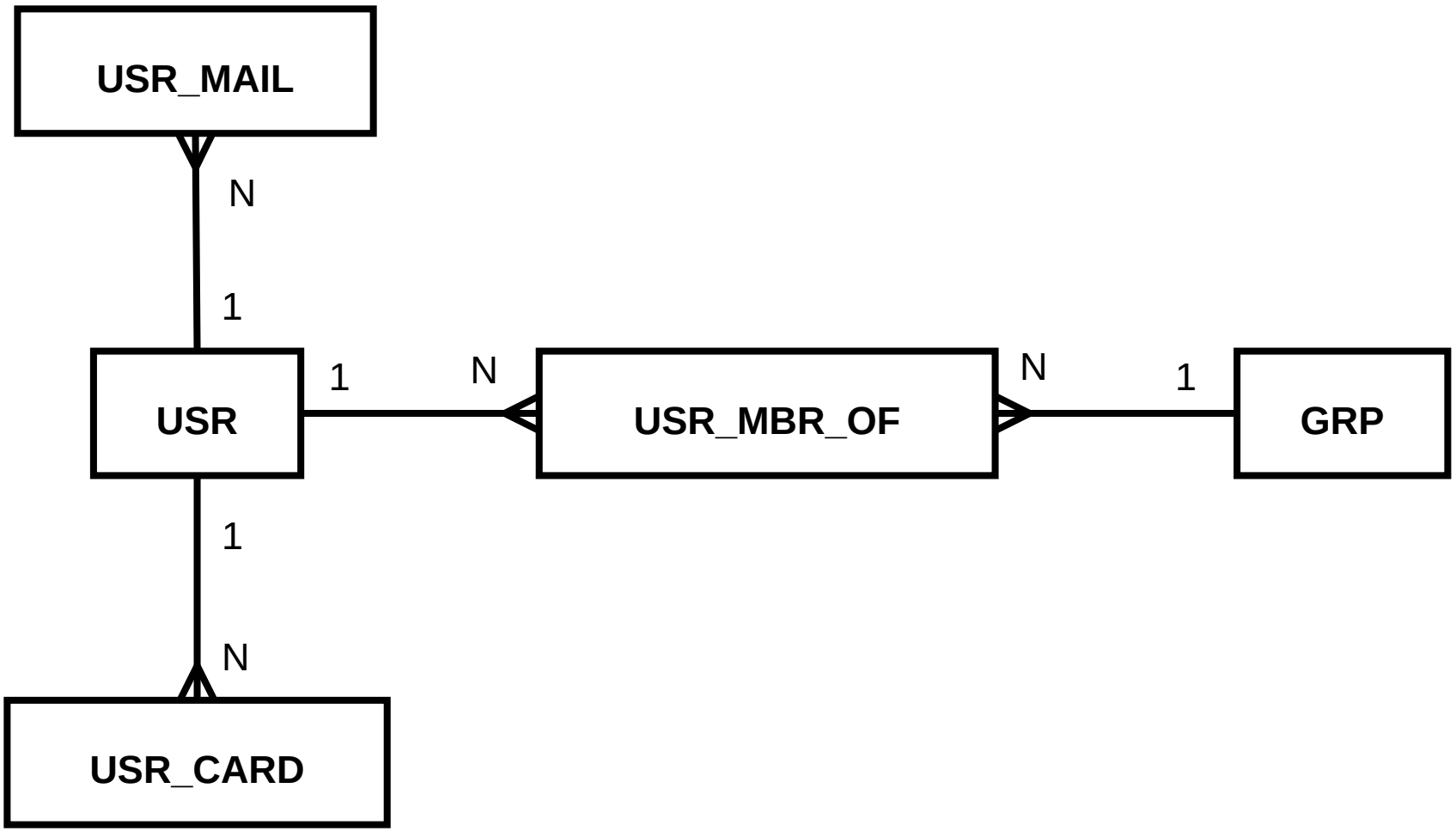
Problém – osobní čísla

- Zaměstnanci – formát 3 + 2 (las03).
- Studenti – formát 3 + 3 (bon007).
- Existence dvou účtů v případě studujícího zaměstnance.

Řešení

- Nové osobní číslo 3 + 4 pro nové uživatele.
- Stará osobní čísla zůstávají.
- Zavedení hlavního osobního čísla (priorita).
- Rušení duálních účtů.

DB2 - struktura tabulek



Uspořádání uživatelů v adresáři

Problém – umístění uživatelů v adresáři

- Zaměstnanci mohou pracovat na více útvarech.
- Nelze automaticky rozpoznat hlavní pracovní poměr.
- Studenti mohou studovat na více fakultách.

Uspořádání uživatelů v adresáři

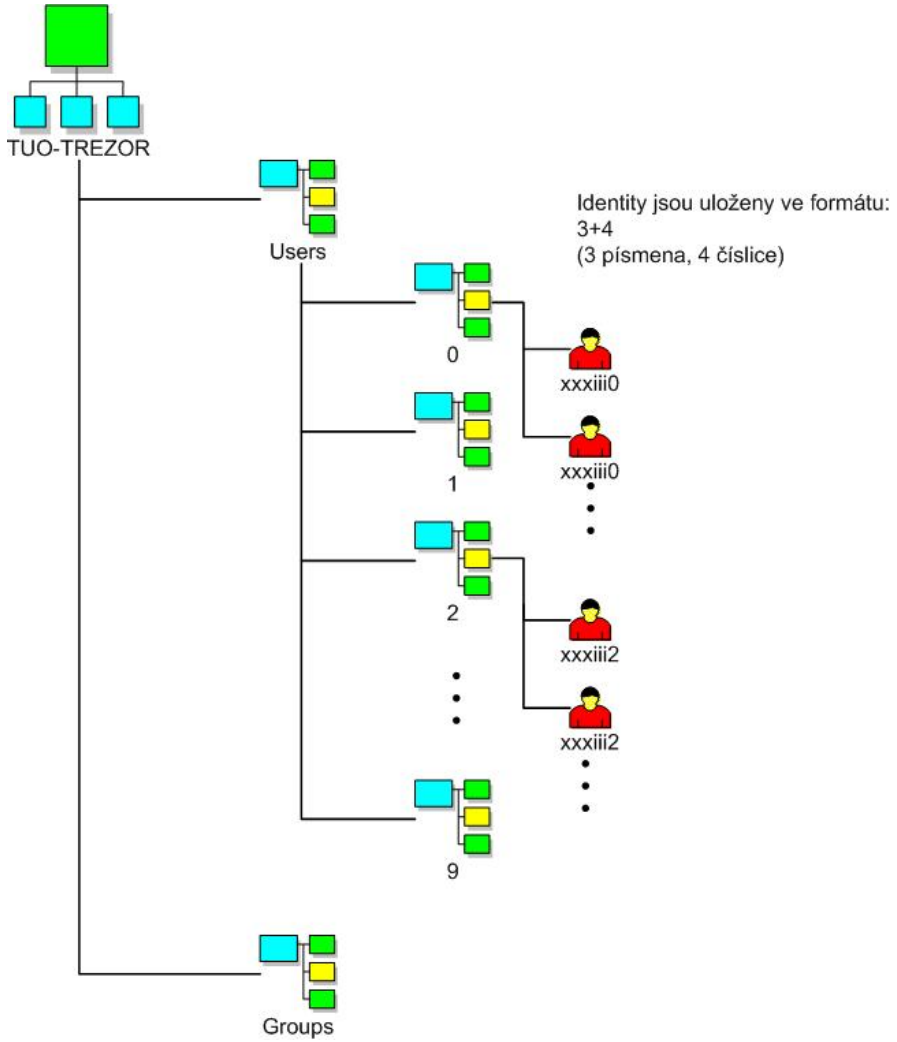
Problém – umístění uživatelů v adresáři

- Zaměstnanci mohou pracovat na více útvarech.
- Nelze automaticky rozpoznat hlavní pracovní poměr.
- Studenti mohou studovat na více fakultách.

Řešení

- Rozdělení do 10 kontejnerů podle poslední číslice osobního čísla.
- Příslušnost k útvarům a fakultám podle členství ve skupinách.

Struktura trezoru



Skupiny

Problém – generování skupin a rolí

- Vygenerování skupin podle organizační struktury.
- Udržování členství podle vztahů s univerzitou.
- Přiřazování uživatelů do aplikačních rolí.

Skupiny

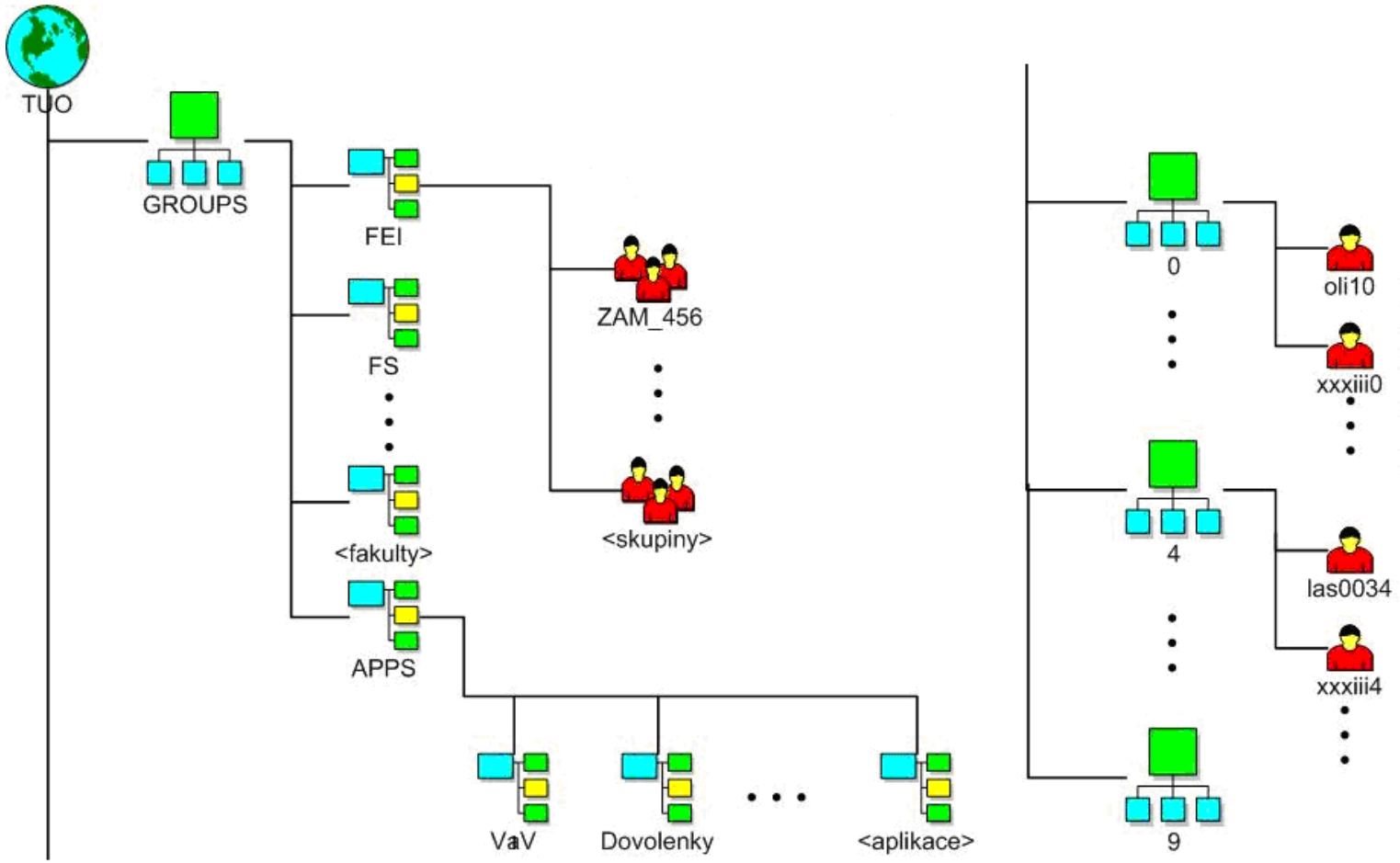
Problém – generování skupin a rolí

- Vygenerování skupin podle organizační struktury.
- Udržování členství podle vztahů s univerzitou.
- Přiřazování uživatelů do aplikačních rolí.

Řešení

- Skupiny ZAM_fakulta, ZAM_číslo útvaru, STU_fakulta.
- Agregované skupiny ZAM_x vs. ZAM_x_KMEN.
- Přiřazování uživatelů do aplikačních rolí v DB2
  1. přímo
  2. prostřednictvím funkcí

Struktura produkčního stromu (LDAP)



Zachování původních dat

Problém – zachování informací v provozním stromu

- Zachování uživatelských hesel.
- Zachování existujících skupin.

Zachování původních dat

Problém – zachování informací v provozním stromu

- Zachování uživatelských hesel.
- Zachování existujících skupin.

Řešení

- Hesla se budou přenášet do trezoru až po změně.
- Provozní strom bude doplněn o nové skupiny.

Mapování atributů I.

DB2 (indirect.usr)	IDM (class user)	LDAP (class user)
uid	uidNumber	uidNumber
givenName	Given Name	givenName
sn	Surname	sn
		fullname
	Group Membership	groupMembership
		securityEquals
		loginDisabled
cn	CN	cn
mail	EMail Address	mail
TUOCardMD5	TUOCardMD5	TUOCardMD5
loginExpirationTime	Login Expiration Time	loginExpirationTime
o	O	
ou	OU	
		uid (uniqueID)
		gidNumber
		homeDirectory
		loginShell

Mapování atributů II.

DB2 (indirect.grp)	IDM (class group)	LDAP (class group)
gid	gidNumber	uidNumber
cn	CN	givenName
o	O	sn
ou	OU	fullname
	Group Membership	groupMembership

DB2 (indirect.usr_mbr_of)	IDM (class group)	LDAP (class group)
uid	Members	member
gid	Group Membership	groupMembership

Životní cyklus identity

1. **Vznik**
   - Zaměstnanec – po zavedení na personálním oddělení do SAPu.
   - Student – po zápise ve studijní agendě.
   - Externisté – po obdržení žádosti zavedeni do DB2.
2. **Život**
   - Dokud trvá alespoň jeden důvěryhodný vztah s univerzitou, probíhá aktualizace všech atributů podle DB2.
3. **Zánik**
   - Po vypršení expirace účet zůstává ještě 6 měsíců v trezoru.
   - Po 6 měsících je smazán z DB2 a zablokován v LDAP.
   - Zakázaní uživatelé jsou pravidelně promazáváni z LDAP i s domovskými adresáři.

Další práce

- Napojení Active Directory.
- Synchronizace hesel mezi LDAP a AD.
- Podpora e-mailových skupin.
- Přechod na stálé osobní číslo.