

Správa identit v rozsáhlé organizaci

Kooperativa, pojišťovna, a. s.

Martin Lízner

martin.lizner@anect.com

24. října 2005



www.anect.com



Obsah prezentace

- Kooperativa pojišťovna, a.s.
- Správa identit
- Fáze projektu
- Technické řešení
- Poznátky
- Závěr

Kooperativa, pojišťovna, a.s.

- Centrum v Praze, cca 20 lokalit v ČR
- Sdílení IS pro tři pojišťovací subjekty
- Přístup dalších partnerských subjektů do IS
- Vazba na PKI
- Více než 4000 uživatelů
- Fluktuace 5 % (?)
- Klíčové systémy: SAP, IS Golem, Microsoft, AIX

Správa identit š pšvodní stav

- Roztříštěné databáze uživatelů
- Roztříštěná správa přístupových práv
- Autentizace ke každé službě zvlášť
- Chybějící bezpečnostní politika účtů
- Rozdílné jmenné konvence

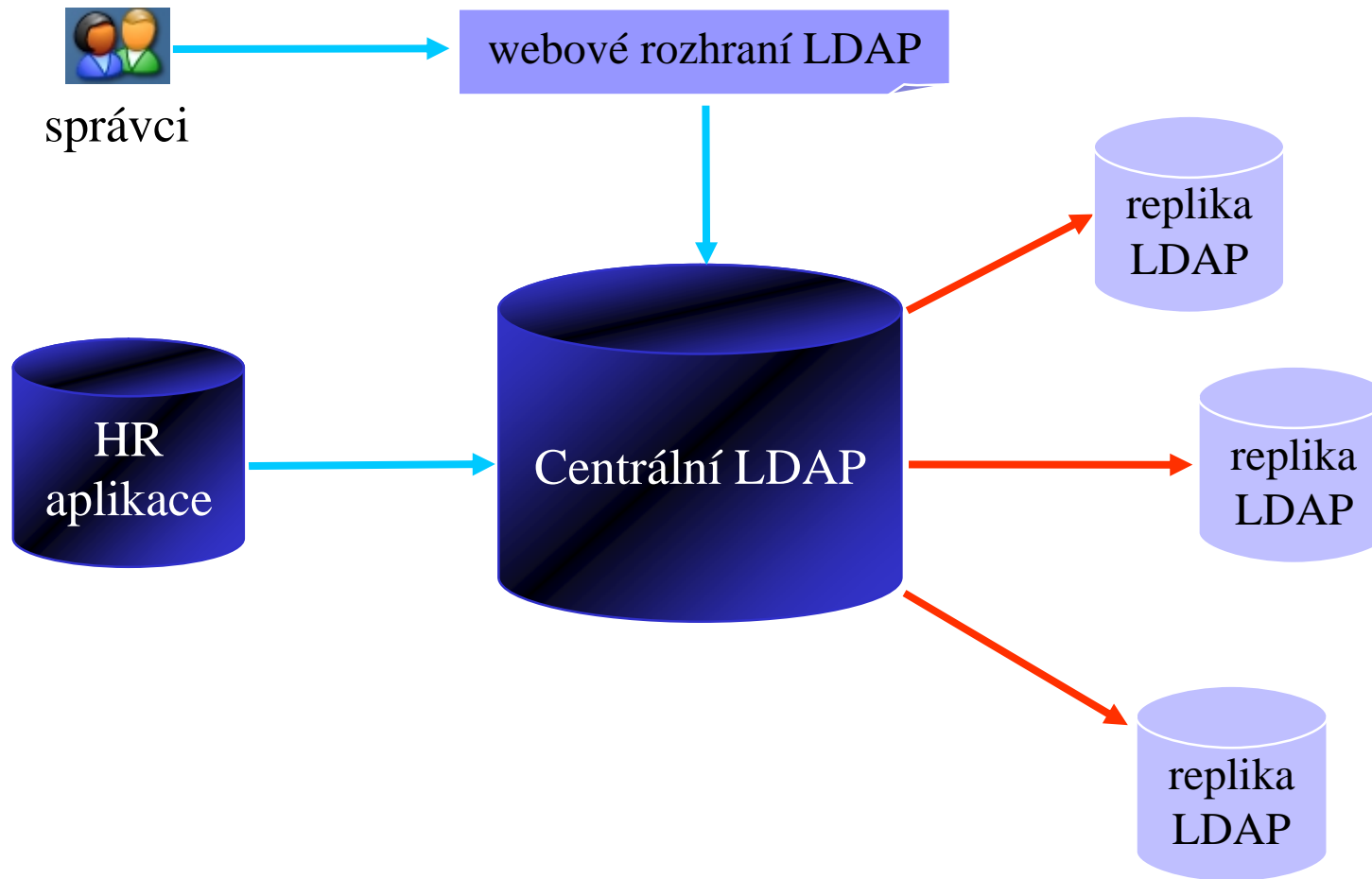
Správa identit š plánovaný stav

- Centralizovaná správa identit
- Zabezpečený prenos identit
- Bezpečnostní politika hesel a účtů
- Sada obecných atributů popisujících identitu
- Identita poskytována všem hlavním systémům
- Zdrojem identit personální aplikace či správci
- Zdrojem rolí personální aplikace
- Otevřené standardy

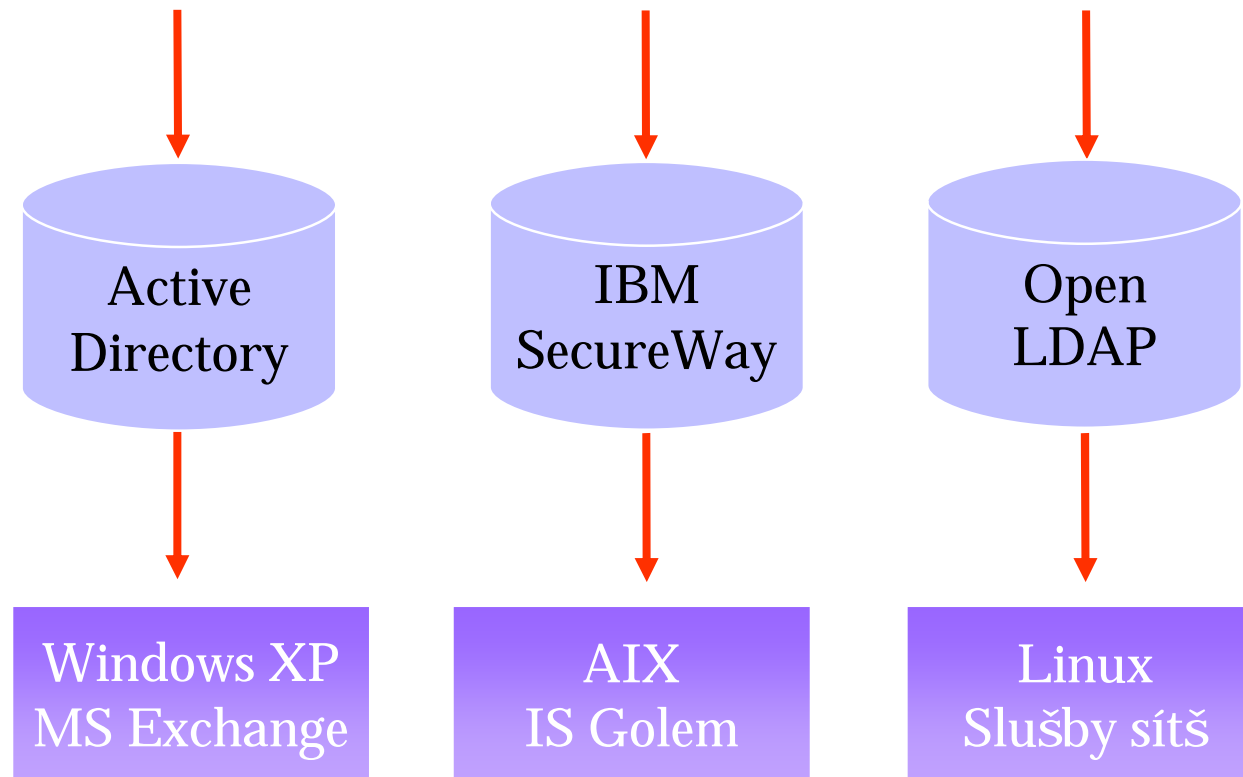
Fáze projektu

- Analýza – aplikace, uživatelé, procesy
- Návrh technologie – LDAP / X509 / Java
- Integrace
 - Vytvoření struktury centrálního LDAP
 - Sloučení uživatelů do LDAP
 - Vytvoření uživatelského rozhraní LDAP
 - Vytvoření soustavy replik
 - Vytvoření konektorů a vazeb na klíčové IS
 - Produkční přenos dat do IS
 - Implementace bezpečnostních politik
 - Navázání zdrojového IS na centrální LDAP
- Zkušební provoz a dokumentace

Technické řešení



Technické řešení - repliky



Technické řešení - platformy

- Personální aplikace – SAP HR / AIX
- Centrální adresář – OpenLDAP / Linux
- Webové rozhraní – Tomcat / Linux
- Mailové systémy - Sendmail / Linux, MS Exchange
- IS Golem – vlastní aplikace / IBM SecureWay / AIX
- IS Microsoft – Active Directory / MS Windows
- Ostatní – MS Windows, Linux

Technické řešení š platformy LDAP

- Struktura adresáře podle lokalit a typu objektu
- Uživatelé, skupiny, mailing listy, role
- Uživatel
 - Unikátní identifikátory (UID a osobní číslo)
 - Základem třídy InetOrgPerson a PosixAccount
 - Doplněny třídami dle navázaných systémů
 - Autentizační atributy (hesla a X509)
 - Autorizační atributy
 - Provozní atributy (např. pro mailové systémy)
 - Ostatní informace (personální údaje)

Technické řešení š rozhraní LDAP

File Edit View Go Bookmarks Tools Help

https://localhost:20000/ad2/admgr/index.jsp?Fcn=&Fuid=Pol*&Fou=ph&Fo=&Fl=&rtn=Zobrazit

Autorizační databáze Kooperativa

[\[Přidej uživatele\]](#) [\[Import SAP uživatele\]](#) [\[Politika hesel\]](#) [\[Správa uživatelů\]](#) [\[Správa skupin\]](#) [\[Správa rolí\]](#) [\[Odhlásit\]](#) [\[Info\]](#) Jste přihlášen jako: mlizner

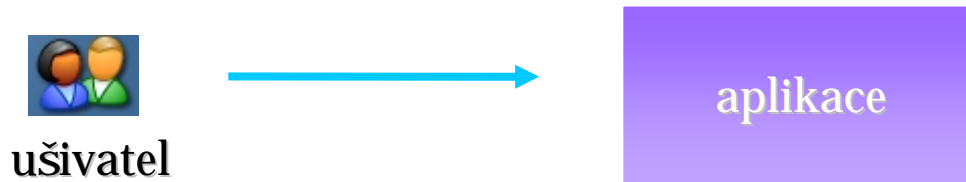
Správa uživatelů

LDAP filtr: (uid=*Pol**)(ou=ph)(objectClass=KoopPortalUser)

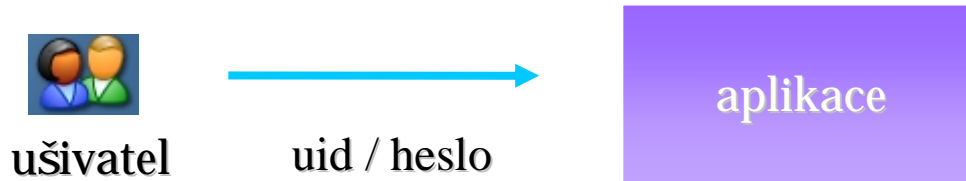
Příjmení	uid	Organizační útvar	Organizace	Lokalita	Zobrazit
<input type="text"/>	<input type="text" value="Pol*"/>	<input type="text" value="ph"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Zobrazit"/>

#	Příjmení Jméno	uid	OU	Organizace	Lokalita	E-mail
1	Dílhopolcek Michal	mdlhopolcek	ph	Kooperativa		mdlhopolcek@koop.cz
2	Polák Vojtěch	vpolak	ph	Kooperativa	Praha GR	vpolak@koop.cz
3	Poláčková Jana	jpolackova	ph	Kooperativa		jpolackova@koop.cz

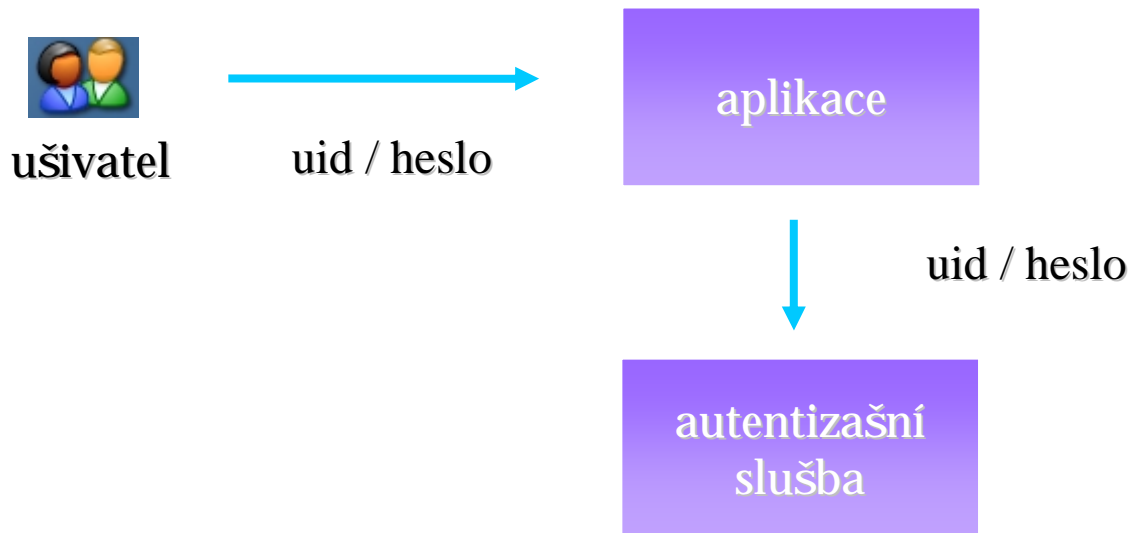
Technické řešení s příklad ověření



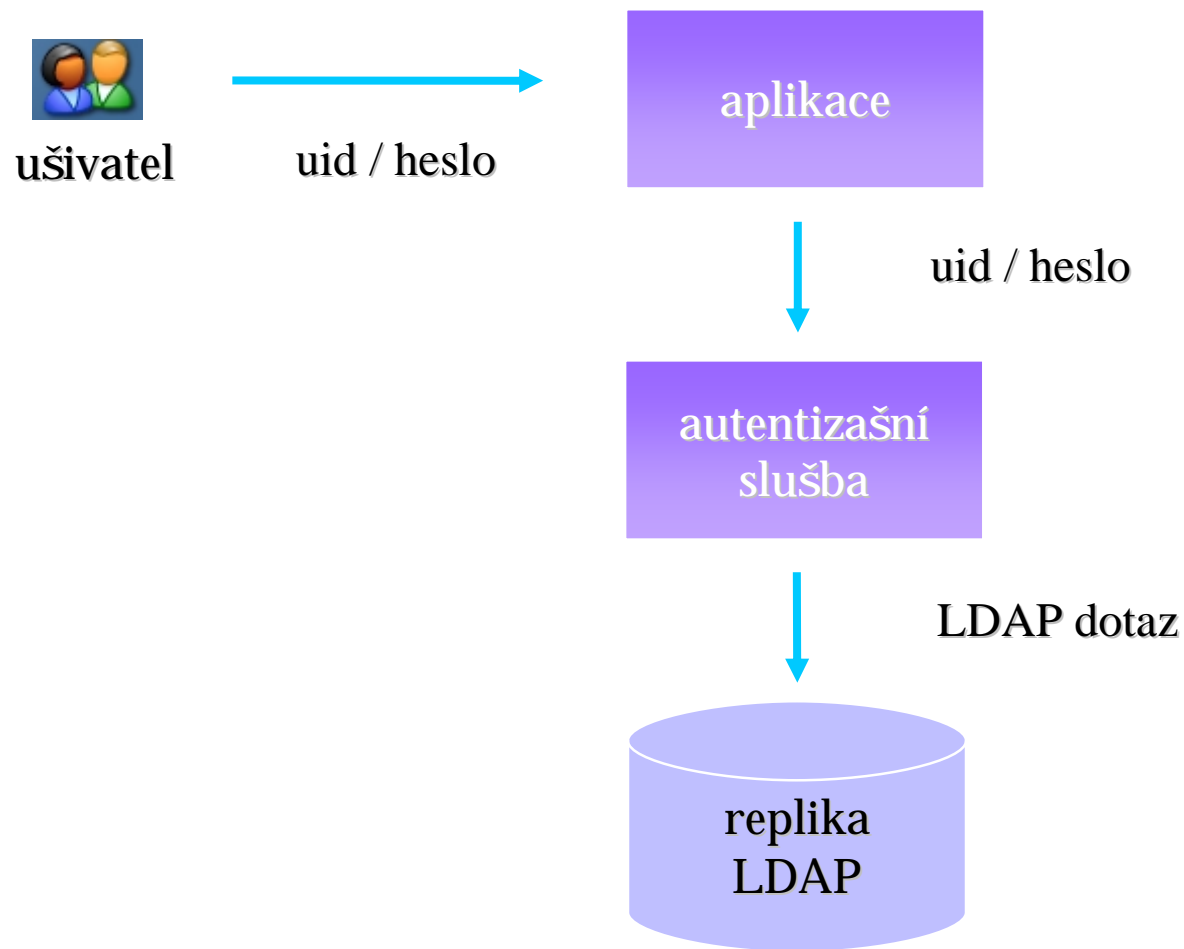
Technické řešení š příklad ověšení



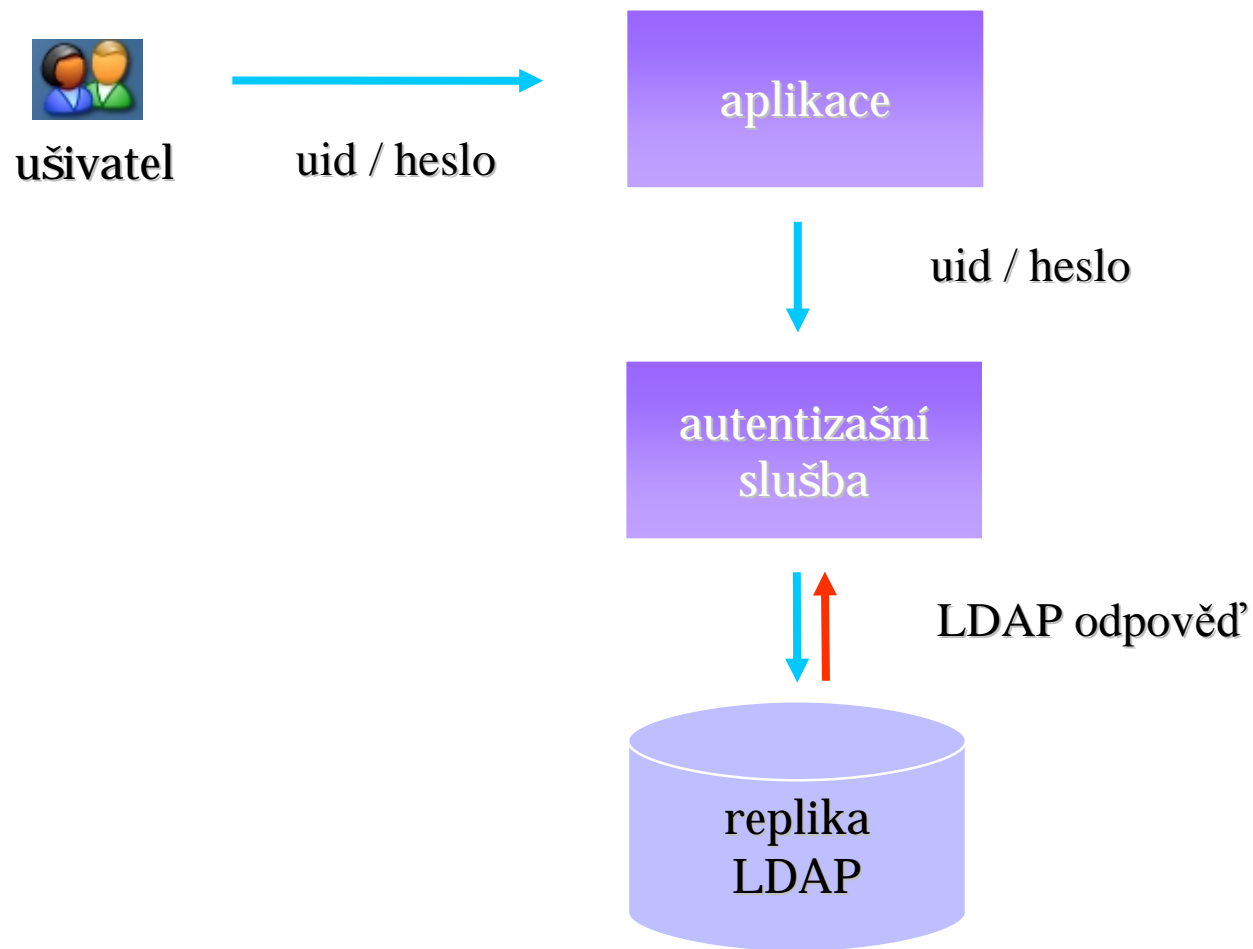
Technické řešení s příklad ověření



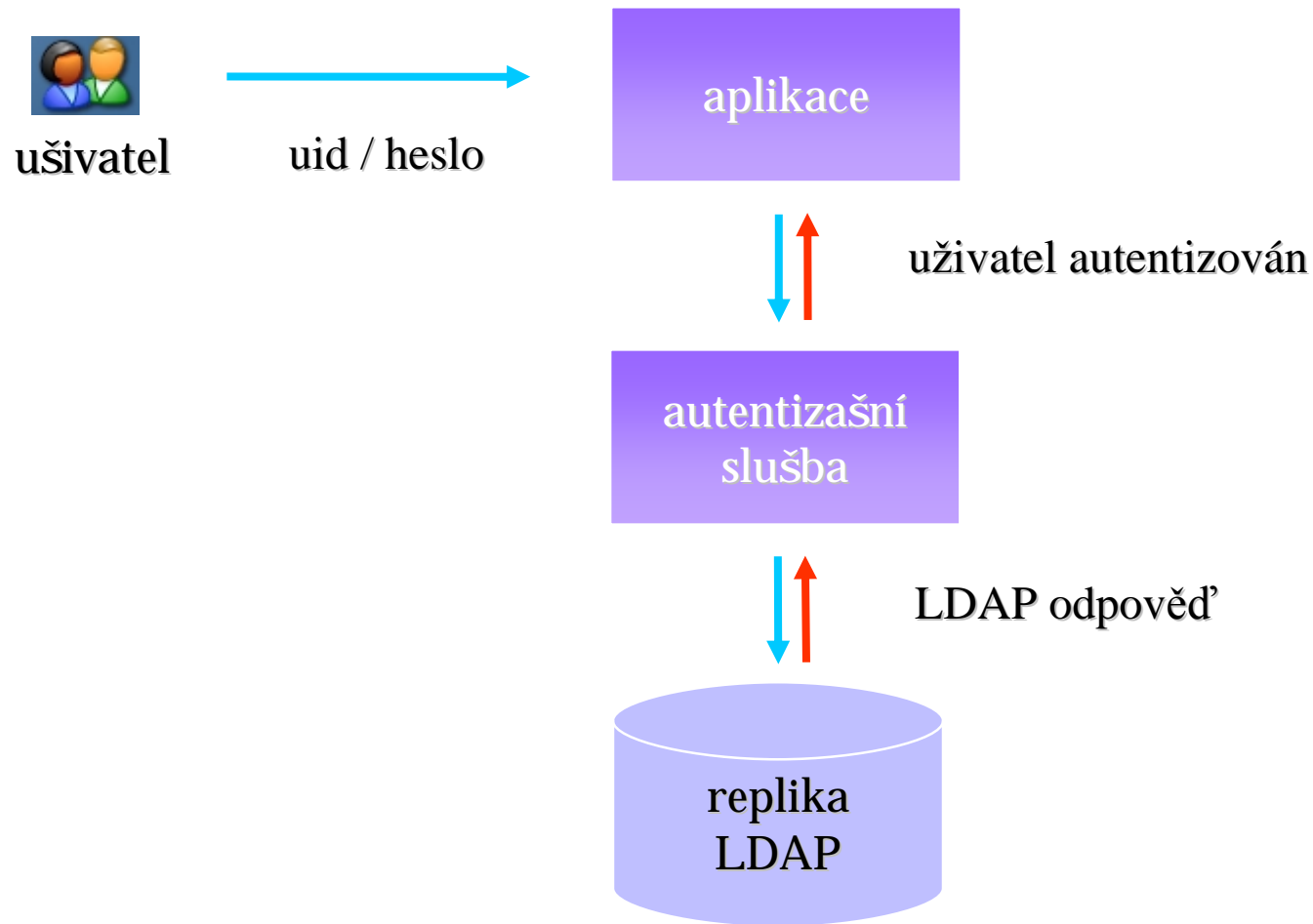
Technické řešení s příklad ověření



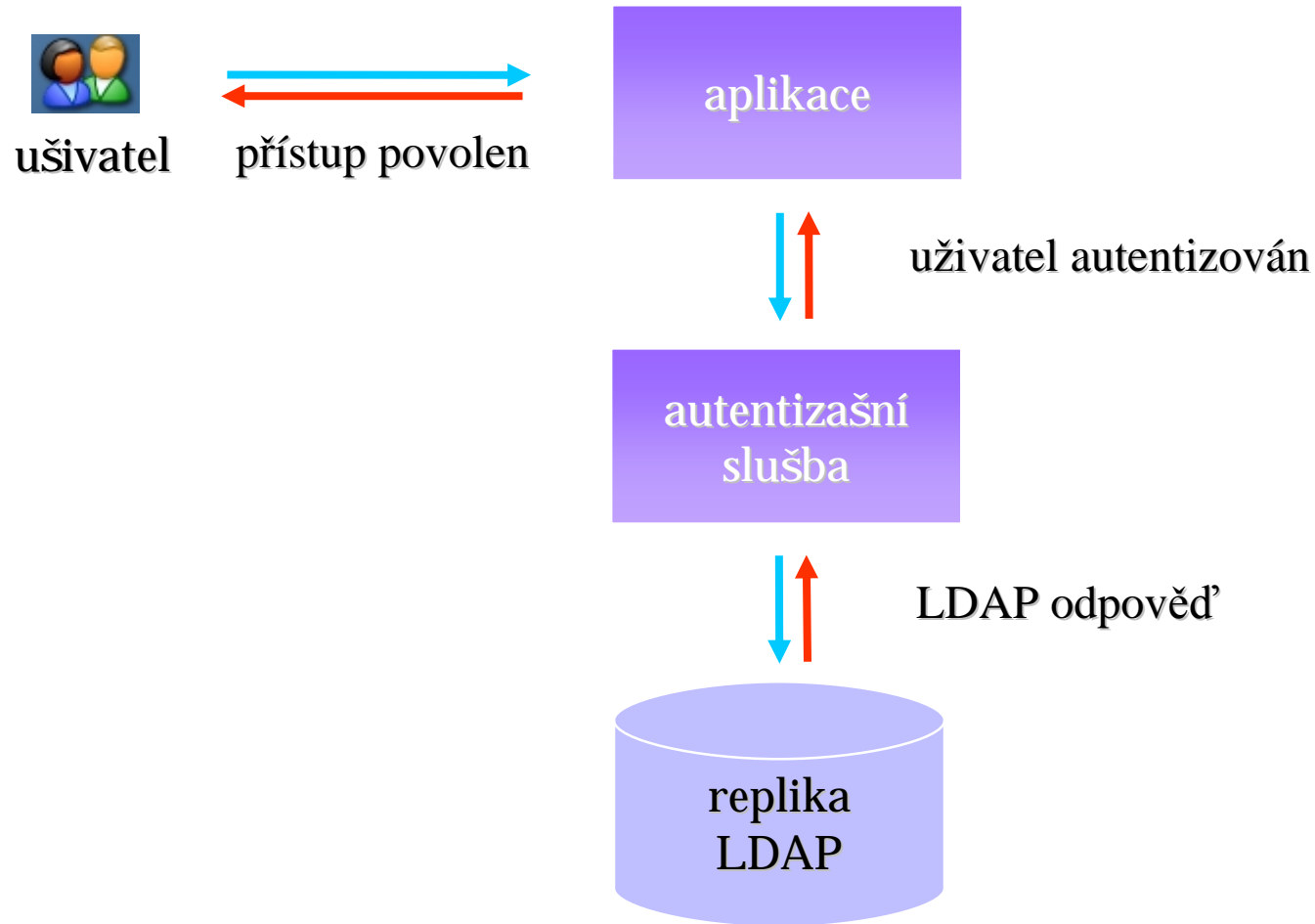
Technické řešení s příklad ověření



Technické řešení s příklad ověření



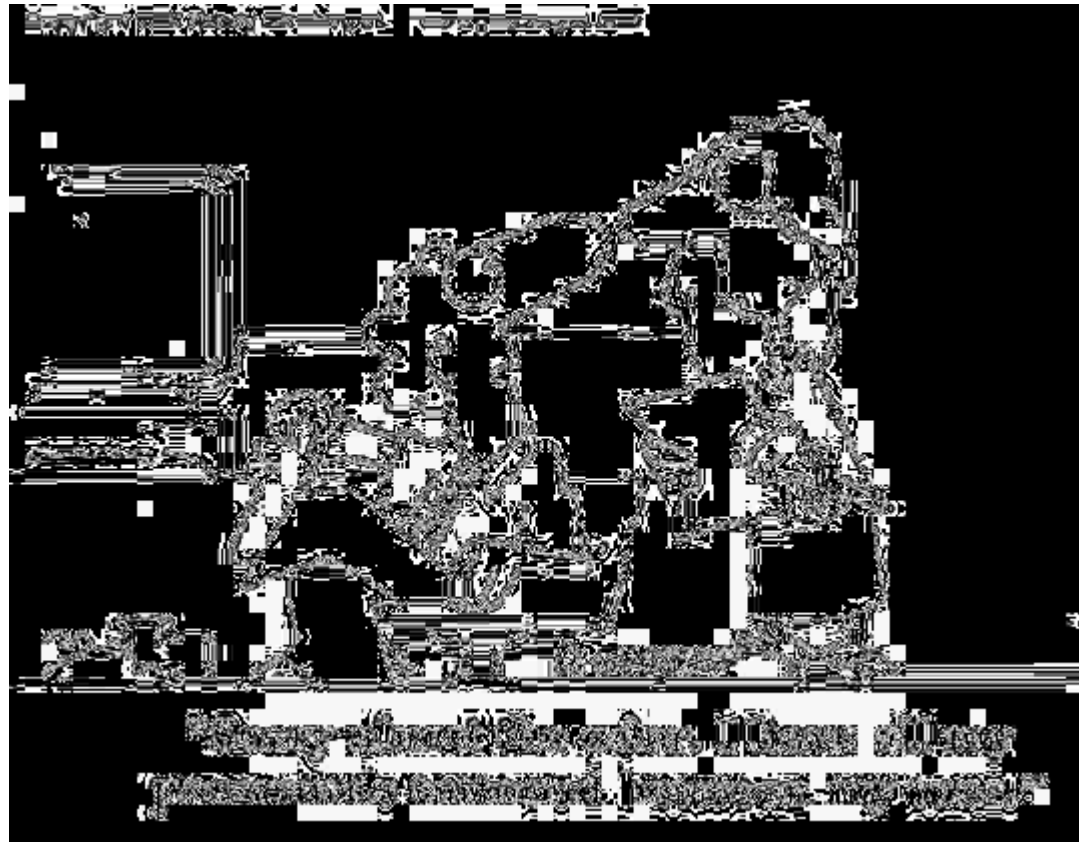
Technické řešení s příklad ověření



Poznátky

- Otevřené systémy - flexibilní integrace
- Uzavřené systémy omezují celé řešení
- Potřeba kvalitních dat synchronizovaných systémů
- Technicky náročnější okruhy:
 - Politiky hesel a účtů
 - Konektory
 - Sdílení dat mezi partnerskými subjekty

Dotazyš



Dokonalý systém byl vytvořen již dávno.

Naším cílem je dodat jej k vám.



www.anect.com

