AMU – Akademie múzických umění v Praze – od zápisu k personifikovaným elektronickým informačním službám za 10 minut!

Radim CHVÁLA
Akademie múzických umění v Praze
radim.chvala@amu.cz

INFORUM 2005: 11. konference o profesionálních informačních zdrojích
Praha, 24. - 26.5. 2005

Abstrakt.

Chceme-li poskytovat uživatelům příjemné a personifikované informační služby, musíme vyřešit snadný a bezpečný přístup k výpočetní technice a jednotnou síťovou identitu.
Počítačovou síť AMU tvoří 11 serverů v 8 lokalitách, vůči kterým se uživatelé přihlašují. Ruční zpracování této agendy přináší problémy v rychlosti, přesnosti, aktuálnosti, bezpečnosti i odpovědnosti.
Řešení přineslo on-line propojení Studijního informačního systému a Personálního systému (Oracle) se síťovým adresářovým systémem (Novell eDirectory) a e-mailovým systémem (GroupWise).
Na základě jména a zařazení ve Studijním nebo Personálním systému, se spouští proces, který uživateli automaticky vytváří: 1) síťový účet a přihlašovací jméno do sítě (ID), 2) domácí adresář na serveru v příslušné lokalitě (home), 3) účet a e-mailovou adresu, 4) prvotní hesla do sítě i do pošty, 5) personifikovanou sadu přístupových práv do aplikací. Účet slouží též pro personifikaci služeb školního portálu. Některé aplikace (např. TinLib) si data přebírají pro svůj provoz. Účty lze nejen vytvářet, ale též podle zadaných pravidel automaticky omezovat a rušit.
Popsané řešení využívá technologie XML a pracuje s „krabicovým produktem" Novell dirXML. (Od verze 2,0 distribuovaným jako NSure Identity Manager). Nasazení spočívalo zejména v analýze a konfiguraci, nevyžadovalo prakticky žádné rozsáhlé programátorské práce.
Každý uživatel tak může za 10 minut po přijetí za studenta nebo zaměstnance, odkudkoli plnohodnotně pracovat s informačními zdroji.

Úvod:

Můj příspěvek trochu vybočuje ze směru většiny příspěvků na konferenci. Nezabývá se způsoby budování nebo využívání konkrétních elektronických informačních zdrojů, nýbrž ukazuje na jednu z nutných podmínek, které musíme splnit, abychom k smysluplnému využívání elektronických informačních zdrojů mohli vůbec přikročit.

Všichni oprávnění uživatelé musí mít snadný, spolehlivý, bezpečný a snadno administrovatelný přístup k informačním technologiím, a to pokud možno ihned po navázání oficiálního kontaktu s institucí – v našem případě uzavření pracovního poměru u pedagogů a zaměstnanců nebo zahájení studia u studentů. Oprávnění musí být dynamické, v závislosti na momentálním studijním stavu uživatele (např. změna přístupů a práv při přerušení studia nebo dlouhodobé stáži).

Výchozí stav:

Práce studentů, pedagogů a ostatních zaměstnanců s informačními technologiemi na Akademii múzických umění v Praze se stala pevnou součástí přípravy budoucích vysokoškolsky vzdělaných umělců. Je umožněna relativně rozsáhlou počítačovou sítí, kterou tvoří vzájemně propojené lokální sítě (100Mb/sec) vybudované ve všech objektech AMU. Ve všech lokálních sítích je nainstalován Novell Netvare 6.5. Celkem je pomocí sítě Pasnet a Cesnet propojeno 11 serverů v 8 lokalitách, z toho 2 mimopražské. Rychlost připojení je typicky 100 Mb/sec. V síti pracuje cca 1500 osob.

Uživatelé pracují jednak na specializovaných pracovištích (například elektronický střih televizního obrazu, elektronická hudba a zpracování digitalizovaného záznamu zvuku, digitální fotografie, grafická pracoviště pro scénografii, manažerské aplikace pro produkční katedry apod.), jednak na volně přístupných počítačích v některém objektu AMU, a konečně ve vzdáleném režimu – z kteréhokoli místa připojeného k Internetu.

Při rozšiřování elektronických informačních služeb a zejména při budování webového portálu AMU, jako nástroje bezpečného, spolehlivého a personifikovaného přístupu ke všem informačním zdrojům, se ukázal jako limitující požadavek zajistit jednotnou síťovou identitu uživatelů.

Historicky vzniklý stav byl takový, že vzájemně se překrývající informace o uživatelích byly roztroušeny jednak v adresářích eDirectory jednotlivých objektů, jednak v několika aplikacích a databázích Oracle. Některé aplikace (například redakční systém SALUKI, knihovní systém TinLib nebo systém hlášení závad a námětů HelpDesk) používaly vlastní adresářové struktury, jejichž údržba byla pouze a zcela v kompetenci obsluhy pracovníků těchto aplikací. Složitá a obtížně koordinovatelná správa systému, (prakticky realizovaná telefonáty, písemnými požadavky a e-maily mezi jednotlivými správci) vedla k mnohým omylům, duplicitám a nekonzistencím. Distribuce informací o identitě uživatelů byla nesystematická a nespolehlivá. Míra bezpečnosti přístupu k jednotlivým zdrojům a aplikacím nebyla standardní. Ruční zpracování a přenos dat mezi jednotlivými systémy byly doprovázeny problémy v rychlosti, přesnosti, aktuálnosti, bezpečnosti i odpovědnosti.

Návrh řešení:

Jelikož tento stav byl neúnosný a stal se limitujícím faktorem pro jakýkoli další rozvoj informačního prostředí školy, bylo rozhodnuto inovovat zásadním způsobem celou tuto oblast, s cílem vytvořit jeden adresář pro všechny osoby přistupující k síti AMU. Na základě analýzy systému a dobrých zkušeností s produkty Novell, bylo rozhodnuto i nadále používat jako bázi jednotné síťové identity adresář eDirectory s průběžně aktualizovanými replikami v jednotlivých objektech. Jako prostředek správy síťové identity a služba sdílení dat byl vybrán produkt Novell dirXML , od verze 2.0 šířený jako Novell NSure Identity Manager.

Odpovědnost za správné a oprávněné zařazení uživatele do struktury AMU bude nadále svěřena výhradně pracovištím k tomu povolaným, která na AMU ošetřují vztah osob ke škole a spravují tak tzv. životní cyklus síťové identity uživatelů. Za studenty jsou to Studijní oddělení jednotlivých fakult (přispívající do společné aplikace Oracle - KOS), za pedagogy a ostatní zaměstnance Personální oddělení (aplikace Oracle – Elanor Global). Hlavním úkolem bylo zajistit, aby do adresáře eDirectory byly z těchto dvou aplikací dodávány vždy aktuální informace o uživatelích. Ostatní aplikace budou data z adresáře eDirectory přebírat, ale nebudou do eDirectory přispívat. Pracovníci, kteří je obsluhují, nevytvářejí nové uživatele, ani neruší staré. Omezí práci s interním adresářem uživatelů pouze na úpravy atributů souvisejících výhradně s provozem aplikace (např. v knihovním systému knihovnice stanovují povolené doby výpůjčky pro jednotlivé kategorie čtenářů, ale nerozhodují o zařazení osoby mezi studenty).

Data přenášená ze zdrojových aplikací obsahují jednak identifikaci osoby jako uživatele oprávněného ke vstupu do sítě AMU, ale též jeho zařazení ve struktuře školy. Informace o pracovišti a pracovním či pedagogickém zařazení zaměstnanců, stejně jako informace o fakultě, studijním oboru a druhu studia u studentů, se promítá do eDirectory jako zařazení do jednotlivých kontejnerů a skupin. To dovoluje nastavit v aplikacích individuální přístup podle toho, jaký uživatel, ze kterého kontejneru a z které skupiny přichází. Hlavně této vlastnosti využívá portál, jehož jednotlivé prvky jsou přiřazeny k objektům v eDirectory.

Zařazení uživatele ve zdrojových aplikacích (Studijní agenda a personální agenda) tak prostřednictvím eDirectory automaticky umožňuje a určuje personifikované chování vůči uživatelům, identifikovaným přihlašovacím jménem a heslem.

Principy synchronizace:

Centrem prostředí s několika adresáři je adresář eDirectory. Ten je synchronizován se zdrojovými aplikacemi a posléze jsou s ním synchronizovány adresáře ostatních aplikací. Například při přijetí nového pracovníka v personální aplikaci Elanor je v první řadě synchronizován eDirectory s Elanor a posléze jsou všechny ostatní adresáře synchronizovány s eDirectory. Změnu tak stačilo

provést jen na jednom místě a příslušné informace jsou automaticky rozneseny do dalších míst. Komunikace mezi eDirectory a adresáři aplikací může být jednosměrná nebo dvousměrná. Pro každý směr je definován kanál. Publisher channel – pro vkládání změn z adresáře do eDirectory a subscriber channel pro opačný směr, tj. z eDirectory do adresáře aplikace. Přidáním vhodných filtrů ke kanálům lze řídit vlastní přenos informací, tedy např. určovat, které změny se mají příslušným kanálem přenášet. Přenášená data lze modulem Join Engine též modifikovat podle předem zadaných pravidel. Rozhraní mezi konkrétní databází (např. Oracle, MySql apod.) a dirXML zajišťují zvláštní drivery (DirXML driver shim).

Celý proces pak například pro kanál subscriber (směr z eDirectory do adresáře aplikace) pak vypadá takto: z eDirectory jsou informace propuštěné filtry převedeny na formát XML, potom jsou na ně v Join Engine aplikována předem definovaná pravidla a XSLT transformace. Nakonec jsou upravená data předána dirXML driveru, ten je převede do příslušného formátu a pomocí odpovídající funkce konkrétního adresáře je vloží do cílového prostředí.

Potřebné drivery dirXML driver shim jsou dostupné prakticky pro všechny běžné databáze.

Konfigurovatelnost pravidel je velmi výhodná. Např. ze zdrojového personálního systému přichází kanálem publisher uživatel Radim Chvála. V eDirectory se potom automaticky vygeneruje (podle algoritmu pro zaměstnance - maximálně 7 znaků z příjmení a jednoho znaku ze jména) uživatel CHVALAR s e-mailovou adresou radim.chvala@amu.cz. Adresa se potom kanálem subscriber předává do adresáře poštovního systému GroupWise. V případě, že by zdrojem byl Studentský informační systém, byl by pro tohoto uživatele vygenerován (podle algoritmu pro studenty) uživatel CHVALA01 s adresou chvala01@st.amu.cz. Nebo změna studijního stavu ze STUDUJE na stav PŘERUŠEN se promítne kanálem subscribe do aplikace TinLib jako změna atributu STATUT ČTENÁŘE, který už si dále mohou dodefinovat knihovníci sami. Lze přidávat i nové vlastnosti, například podle zařazení pracovníka v organizační struktuře mu lze vytvářet kontext. Při předávání dat lze měnit jejich formát (například datum nebo čas). Významné je, že DirXML manipuluje s daty převedenými do moderního univerzálního formátu XML.

Realizace a výsledky:

Zásadní úprava adresářové struktury sítě a aplikací je velmi delikátní operace, která může mít kromě sledovaných pozitivních efektů též silné negativní dopady, pokud není příprava perfektně zvládnuta. Ke spolupráci proto byla přizvána firma DATRON Česká Lípa, která má s prací v prostředí Novell bohaté zkušenosti a jejíž pomoc se ukázala jako naprosto klíčová. Spolupráce byla navázána též s firmou Novell-Praha, která poskytla na své produkty velké EDU slevy, s firmami BBM Písek (Ekonomický systém FIS) a TRIL Kladno (Studijní systém KOS), pro objasnění možností synchronizace adresářů jejich aplikací s eDirectory. Akce byla z velké části hrazena jako součást projektu Fondu rozvoje CESNETu – vytvoření nového portálu AMU.

V rámci podrobné analýzy byly zpracovány zejména tyto úkoly:

- Definice procesů: vytvoření asociace, přesuny objektů, změna vlastností objektu
- Definice klasifikace atributů (povinné, systémové, uživatelské)
- Popis struktury v aplikacích (kontrola na podporovaný datový typ)
- Popis stávajícího adresářového stromu
- Popis replikací eDirectory v lokalitách
- Specifikace atributů v eDirectory
- Specifikace umístění objektu v eDirectory, je-li osoba současně student i zaměstnanec

Byly definovány též jednotlivé procesy jako Přijetí zaměstnance, Změna pracoviště, Ukončení pracovního poměru, Přerušení studia, Konec studia atd.

Byl vytvořen tzv. metastrom, jako kopie eDirectory, ve které se prováděly veškeré operace a teprve po úspěšných kontrolách byla modifikována „ostrá“ databáze.

Rutinní provoz byl spuštěn v listopadu 2004. V současné době systém funguje takto:

Na základě zařazení osoby ve Studijním nebo Personálním systému se spouští sada procesů, které cca do 10 minut uživateli automaticky vytváří:

a) síťový účet a přihlašovací jméno do sítě (ID);
b) domácí adresář na serveru v příslušné lokalitě (home);
c) účet a e-mailovou adresu;
d) prvotní hesla do sítě i do pošty;
e) personifikovanou sadu přístupových práv do aplikací a do portálu.

Účty jsou nejen vytvářeny, ale podle změn ve zdrojových aplikacích a zadaných pravidel též automaticky omezovány, eventuálně rušeny.

Ostatní aplikace si data přebírají pro svůj provoz a jejich operátoři jsou tak zcela zbaveni povinnosti starat se o data uživatelů.

Propojené aplikace:

Aplikace	Název	Databáze
Síťový adresář	eDirectory	Novell
Systém studijních informací	KOS	Oracle
Personální agenda	Elanor Global	Oracle
Finance a evidence majetku	FIS	Oracle
Skupinová práce a e-mail	GroupWise	Novell
Evidence HardWare a SoftWare	Správce	FoxPro
Hlášení a evidence řešení poruch	HelpDesk	MySQL
Rezervace filmové a TV techniky	Dispečer	MySQL
Rezervace počítačů v učebnách	Rezervace PC	Oracle
Řízení e-learningu	Moodle	MySQL
Identifikační karty	(připravujeme)	MySQL?
Knihovní systém	TinLib (dokončujeme)	TinMan

Propojení s knihovním systémem TinLib právě dokončujeme ve spolupráci s Ústavem výpočetní techniky UK Praha. Pro TinLib sice neexistuje driver DirXML, celkem snadno však lze vygenerovat z příslušných atributů eDirectory importní soubor v přijatelném tvaru, který TinLib automaticky naimportuje a aktualizuje si tak svůj adresář.

Popsané řešení synchronizace adresářových služeb je výhodné hlavně tím, že pracuje s „krabicovým produktem“ Novell dirXML (Novell NSure Identity Manager). Nasazení pak spočívalo zejména v analýze a konfiguraci, a vyžadovalo nesrovnatelně méně programovacích prací, než v případě kompletního vlastního vývoje. Jednalo se zejména o balíčky javy pro konverze a počítání datumů a generování prvotních hesel. Po nezbytném odladění se dnes systém jeví jako naprosto stabilní a bezchybně pracující. Uvedení modernizovaných adresářových služeb do života otevřelo pro AMU zcela nové možnosti v inovacích informačního prostředí.

Na závěr můžeme potvrdit platnost tvrzení z počátku příspěvku, že „na AMU může každý uživatel již za 10 minut po přijetí za studenta nebo zaměstnance odkudkoli plnohodnotně pracovat s informačními zdroji.“ Poděkování za to patří pracovníkům Počítačového centra AMU, ale též firmám DATRON s.r.o., Novell-Praha s.r.o. a CESNET z.s.p.o., které se každá svým způsobem o úspěch projektu zasloužily.