Digital Identity Management

Ing. Petr Grolmus[1]
Ing. Michal Švamberg[2]

5. února 2006

[1]grolmus@civ.zcu.cz
[2]svamberg@civ.zcu.cz

Obsah

Závěrečná zpráva projektu Fondu rozvoje sdružení CESNET pro rok 2004. Tento projekt je zařazen do oblasti **II**, tématického okruhu **B**. Řešitelem projektu je Ing. Michal Švamberg.

1 Struktura dokumentu

Struktura tohoto dokumentu je v souladu s podklady pro závěrečné oponentní řízení Fondu rozvoje CESNET, z.s.p.o. rozčleněna následujícím způsobem:

- Dosažené cíle
- Přínosy projektu
- Konkrétní výstupy
- Výkaz hospodaření s finančními prostředky poskytnutými projektu z fondu

2 Dosažené cíle

Předmětem tohoto projektu byla zahraniční cesta, které se podle předpokladu zúčastnili dva pracovníci Centra informatizace a výpočetní techniky při Západočeské univerzitě v Plzni – Ing. Michal Švamberg (řešitel) a Ing. Petr Grolmus (spoluřešitel). Plánovaná zahraniční cesta proběhla v období 28.4.2005-2.6.2005. Místo pobytu v kalifornské oblasti Bay Area u San Francisca nebylo zvoleno náhodně. Výhodou této oblasti je poměrně silné zastoupení institucí zabývajícími se informačními technologiemi: hlavní sídlo firmy Oracle, University of California Berkeley, Lealand Stanford Junior University, celá oblast Silicon Valley, ...

Pobyt byl mimojiné naplnánován také s ohledem na termín konference "DIDW 2005" (Digital ID World 2005)[1], která se konala v San Franciscu ve dnech 9.-12. května v místním hotelu Hyatt Regency na ulici Embarcadero.

Od doby původního podání projektu do podepsání smlouvy došlo k několika významným změnám. Prvními ovlivňujícími faktory byly odchod spoluřešitele Martina Chlumského z řad pracovníků Západočeské univerzity v Plzni a pověření původního řešitele Luboše Kejzlara jinými úkoly. Dalším ovlivňujícím faktorem bylo přijetí projektu se snížením příspěvku. Tyto okolnosti v důsledku vedly k podání žádosti o změnu projektu 087/2004 zaslané dne 21. září 2004 a její upřesnění na žádost Rady Fondu rozvoje zaslané dne 11. listopadu 2004. Schválenými změnami byla změna řešitelského kolektivu a zúžení cílů projektu o komplexní analýzu a zmapování problematiky bezpečné správy elektronické identity. Hlavní důraz zůstal nadále v souladu s původním záměrem na iniciativy a technologie, které jsou prakticky použitelné v prostředích akademických sítích – zejména Liberty Aliance, Shibboleth a WebISO iniciativy Internet2/MACE (Middleware Committee for Education).

Jako další cíle tototo projektu je možné označit návázání kontaktů s předními pracovníky a vývojáři v oblasti identity management a identity federation systémů a výměna informací o těchto systémech, za účelem jejich dalšího možného využití.

Za dobu našeho pobytu se nám podařilo uskutečnit několik významných schůzek s vývojáři projektů Liberty Aliance, Shibboleth, WebAuth a SignIt. Bohužel, s ohledem na snížení příspěvku projektu nebyl v rámci grantu dostatek finančních prostředků na pokrytí nákladů spojených s přímou účastí na výše uvedené konferenci DIDW'2005, které činily cca 3.500 USD

[1] `http://conference.digitalidworld.com/2005/`

pro 2 osoby. Přesto se nám přes dříve realizované kontakty podařilo ve dnech konání konference uskutečnit schůzky s lidmi, kteří byli jinak zcela mimo dosah naší působnosti po dobu pobytu.

V následujícím seznamu jsou uvedeny projekty diskutované po dobu našeho zahraničního pobytu; seznam také obsahuje významné kontakty v rámci uváděných projektů.

2.1 Liberty Aliance

Projekt Liberty Aliance je dnes sdružení více než 160 ziskových, neziskových a vládních oranizací, které dohromady reprezentují více než miliardu zákazníků. Mezi jinými jsou zde zastoupeni také firmy známých jmen: MasterCard, Visa, Sun, Vodafone, Hewlett&Packard, Sony a mnoho dalších. Cílem tohoto projektu (ostatně stejně tak i např. projektu Shibboleth) je zajistit princip Single Sign-On přihlášení přes velkou skupinu aplikací tak, aby uživatel pro přístup mohl použít autentizaci bežnou v jeho domovské organizaci. Jde tedy o vybudování architektury tzv. federativní identity, která s sebou přináší výhody jednoduchého (a jednotného) přihlašování uživatelů ke zdrojům, ke kterým mají přístup. Nevyžaduje ovšem mít osobní informace uživatelů uložené centrálně.

Celá architektura je založena na kruhu důvěry mezi poskytovateli zdrojů (aplikací do kterých se uživatelé hlásí) a poskytovateli identit (udržovateli autentizačních, resp. autorizačních údajů o uživatelích), kteří mají obchodní vazby založené na architektuře Liberty. Komunikace mezi jednotlivými subjekty v kruhu důvěry se odehrávají prostřednictvím protokolu SAML (Security Assertion Markup Language), který je navržený speciálně pro přenos identity a pověření přistupujicích uživatelů.

Detailnější popis architektury Liberty zdaleka přesahuje rámec této závěrečné zprávy. Proto si případného zájemce dovolujeme odkázat přímo na stránky projektu[2].

Kontatkní osoba:
Jeff Hodges (e-mail: `Jeff.Hodges@neustar.biz`) – protocol architect.

2.2 Shibboleth

Shibboleth je projekt obdobný výše uváděnému systému Liberty Aliance s tím rozdílem, že na jeho vývoji se podílí především konsorcium Internet2, které tvoří více než 200 univerzit spolupracujících na partnerských projektech. Lze tedy říci, že zatímco projekt Liberty Aliance je komerčním produktem, tak projekt Shibboleth je produktem akademickým.

V poslední době lze v projektu Shibboleth pozorovat výrazný posun směrem k Liberty Aliance a nová verze Shibbolethu již používá protokol SAML v2.0. Přijetím SAMLu v2.0 i druhým nejsilnějším zástupcem Identity Federation došlo tedy k posílení tohoto protokolu na úroveň standardu. Toto přiblížení obou projektů bylo možné realizovat pouze díky vzájemné spolupráci hlavních vývojařů obou systémů. Jejich cílem je definovat jednotný standard, místo zavádění dvou nekompatibilních pseudostandardů. V budoucnu by tedy neměl být problém provázat mezi sebou organizace jejichž informační prostředí bude používat libovolný produkt z obou těchto systémů.

Detailní informace o Shibbolethu je možné získat na stránkách projektu[3].

[2] `http://www.projectliberty.org/` – domovská stránka sdružení Liberty Aliance
[3] `http://shibboleth.internet2.edu/` – domovská stránka projektu Shibboleth

Kontaktní osoby:
Bob "RL" Morgan (e-mail: `rlmorgan@washington.edu`),
Scott Cantor (e-mail: `cantor.2@osu.edu`)

2.3 WebAuth (Stanford)

Jde o jeden z projektů odkazovaných iniciativou Internet2, resp. její pracovní skupinou WebISO (Web Initial Sign-on). Tato skupina se zabývá výzkumem softwarových produktů vhodných pro autentizaci (příp. autorizaci) uživatelů v prostředí WWW za použití běžných WWW prohlížečů tak, že uživatelova identita je vyžadována pouze při prvním přístupu ke kterékoliv aplikaci v rámci množiny aplikací podporovaných daným systémem.

V rámci Internet2/WebISO jsou uváděny dva různé systémy se shodným názvem WebAuth, proto v záhlaví této sekce je kladen důraz na skutečnost, že zde diskutovaný systém je vyvíjen na univerzitě ve Stanfordu.

Systém WebAuth [1] je tvořen třemi nezávislými moduly webového serveru Apache 2.x. První z modulů `mod_webkdc` běží na samostatném serveru označovaným jako WebKDC. Jeho funkcí je komunikovat s aplikačními servery, zpracování jejich požadavků a ověření identity nově přistupujícího uživatele. Podobnost s názvem KDC (Key Distribution Center) systému Kerberos není náhodná. WebAuth je primárně na systému Kerberos založen. I komunikace mezi aplikačními servery a WebKDC je velmi podobná protokolu Kerbera a samotné aplikační servery se serveru WebKDC prokazují vlastním KRB principalem, na základě kterého WebKDC vyhodnotí, zda stanice smí požadovat ověření přistupujího uživatele. Při úspěšném ověření uživatele vystaví WebKDC cookie s kryptovanými informacemi, kterými se uživatel prokazuje při přesměrování z dalšího aplikačního serveru.

Další dva moduly serveru Apache slouží pro autorizaci uživatele při přístupu k webové aplikaci. Autorizaci lze (stejně jako v případě *Basic authentization*) řídit pouze nad vyjmenovaným adresářem. První z modulů `mod_webauth` umí ověřit buď všechny uživatele `require valid-user` nebo vyjmenované uživatele `require user indy svamberg`. Druhý z modulů `mod_webauthldap` umožňuje provádět autorizaci uživatelů proti skupinám definovaným ve struktuře LDAPu: `Require privgroup lps civ`.

Kontaktní osoby (hlavní vývojáři systému WebAuth):
Tim Torgenrud (e-mail: `torg@stanford.edu`),
Russ Allbery (e-mail: `rra@stanford.edu`)

2.4 SignIt

Jde o další z projektů konsorcia Internet2. Jeho hlavním cílem je zavedení standardu do správy a distribuce autorizačních údajů mezi spolupracujícími organizacemmi. Bohužel narozdíl od projektu Shibboleth od stejného konsorcia, je projekt SignIt zatím ve fázi překotného vývoje a výsledky či možnost testovaní (resp. zdrojové kódy) jsou zatím přístupné výhradně členům konsorcia. V konečné fázi by mělo jít o další dílek do mozaiky dílčích řešení v rámci Shibbolethu.

Kontaktní osoba:
Lynn McRae (e-mail: `lmcrae@stanford.edu`)

3 Přínosy projektu

Neoddiskutovatelným přínosem zahraniční cesty je zcela jistě získání informací "z první ruky" – tedy převážně přímo od hlavních vývojařů jednotlivých projektů. Také navázání osobních kontaktů s lidmi určujícími další směr vývoje Identity federation je možné označit za obrovský přínos.

Kontaktovat vedoucí projektu Shibboleth (tj. Mr. Scott Cantor, Mr. Bob "RL" Morgan) bylo možné právě díky vhodnému naplánování zahraniční cesty s ohledem na termín pořádání konference "DIDW 2005" v San Franciscu. Oba výše uvedení byli na této konferenci zvanými řečníky. Za jiných okolností by tyto význačné kontakty byly zcela mimo náš dosah - Scott Cantor pracuje na Ohio State university a Bob "RL" Morgan je pracovníkem University of Washington.

Sbližování projektů Shibboleth a Liberty Aliance bylo patrné také z faktu, že schůzku s těmito předními odborníky nám pomohl zorganizovat Mr. Jeff Hodges, který je jedním z hlavních pracovníků konkurenčního projektu Liberty. Ze setkání bylo patrné, že skupiny pracovníků obou projektů mezi sebou mají vřelé přátelské vztahy.

Díky možnosti osobně konzultovat zkušenosti s projektem WebAuth přímo s hlavními vývojáři na stanfordské univerzitě, bylo možné v průběhu prázdnin překonat některé drobné problémy a přejít s nasazením tohoto produktu na ZČU z testovacího provozu do provozu produkčního. Z tohoto přechodu je možné zdůraznit jako největší úspěch převod ověření webového rozhraní pro elektronickou poštu (konkrétně produktu Horde) z běžného ověření proti IMAP serveru právě na Single Sign-On ověření pomocí produktu WebAuth. Webové rozhraní pro přístup k elektronické poště využívá běžně přibližně 60-70% našich uživatelů. SSO řešení WebAuth je nyní provozováno již na více jak 20 WWW aplikacích na ZČU.

Na základě informací získaných osobní návštěvou se také podařilo zprovoznit autentizovanou webovou proxy chránenou WebAuthem i pro aplikace, kde by změna z důvodu absence práv pro modifikaci nebo pro nestandardní provozní platformu byla více než problematická.

Na rok 2006 plánujeme zprovoznění několika ověřovacích serverů systému WebAuth do farmy tak, aby se případné odpojení jednoho z ověřovacích serverů (např. z důvodu HW poruchy) nestalo příčinou kolapsu přístupu na všechny chráněné WWW aplikace.

V průběhu roku 2006 také připravujeme v součinnosti s Cesnetem, resp. pracovní skupinou *AAI and Mobility* (Authentication and Authorization Infrastructure and Mobility) vedenou Milanem Sovou, nasazení systému Shibboleth pro základní testování. Výsledky této spolupráce budou koncem roku 2006 přístupné v podobě technické zprávy Cesnet, z.s.p.o. všem členům sdružení.

Díky faktu, že Západočeská univerzita v Plzni je jedním z hlavních pořadatelů konference EurOpen[4], pokusíme se na některou z nich v průběhu roku 2006 (konference se konají dvakrát ročně + jednou mezioborový seminář) přizvat některého předního odborníka z projektů Shibboleth nebo Liberty Aliance, se kterými jsme se setkali v době našeho pobytu v USA. Předběžně možnou účast přislíbili Mr. Scott Cantor a Mr. Jeff Hodges. Že toto přání není nereálné může dokazovat účast Richarda Stallmana coby hlavního řečníka na konferenci EurOpen v roce 1994, příp. právě výše jmenovaného Jeffa Hodgese v roce 2004.

V návaznosti na změny HelpDesku na Západočeské univerzitě jsme zjišťovali také organizaci uživatelské podpory na tamních univerzitách. Nejvíce jsme se zajímali o strukturu a mechanismy podpory na Stanfordské univerzitě, protože má obdobnou strukturu poskytovaných

[4] `http://www.europen.cz/` – sdružení pro podporu svobodného softwaru

služeb a to včetně jejich rozsahu. Získané poznatky jsme předali odpovědným vedoucím za projekt reorganizace HelpDesku na ZČU.

4 Konkrétní výstupy projektu

Konkrétní výstupy projektu lze shrnout v těchto bodech:

4.1 Publikace

Výsledky grantu, přípravy a zhodnocení získaných informací byly doposud prezentovány následujícími publikacemi:

Grolmus P., Švamberg M.: *Identity federation nejen v univerzitním prostředí*
vyšlo v Data Security Management, 2005, ročník 9, č. 1, ISSN 1211-8737, s. 14-17

Grolmus P., Švamberg M.: *Single Sign-On řešení pro webové aplikace*
Sborník příspěvků z XXVII. konference EurOpen.CZ, Srní 23.-26. října 2005, EurOpen.CZ, 2005, s. 87-100 , ISBN: 80-86583-09-0

Grolmus P.: *WebISO - Single Sign-On řešení pro WWW*
technická zpráva č. 7/2005, Cesnet z.s.p.o., Praha

4.2 Semináře

Pro zaměstnance a studenty jsme připravili následujicí informační semináře:

Čížek J., Švamberg M.: *Bezdrátové sítě na ZČU a jednotné webové přihlášení*
informační seminář pořádaný pro studenty a zaměstnance ZČU v Plzni, 23. listopad 2005

Grolmus P., Švamberg M.: *Shrnutí poznatků z pracovní cesty*
interní seminář CIV, 9. červen 2005

4.3 Softwarová řešení

Zde jsou vyjmenovány významné změny v IT infrastruktuře Západočeské univerzity v Plzni, které byly provedeny na základě získaných informací v rámci tohoto grantu.

- převod z testovacího režimu Single Sign-On řešení do produkčního stádia
- přihlašování do webového rozhraní k elektronické poště přes Single Sign-On
- zavedení autentizované webové proxy
- testování load balancingu pro WebKDC servery
- příprava `lbnamed`[5], tak aby byla zajištěna tolerantnost vůči jednotlivým výpadkům WebKDC serverů

[5] **TODO:** `doplnit URL` – **Bind server s možností testování dostupnosti**

5 Výkaz hospodaření s finančními prostředky poskytnutými projektu z fondu

Na projektu se podílely dva subjekty a to Fond rozvoje CESNETu a Západočeská univerzita v Plzni. Z prostředků fondu rozvoje bylo hrazeno cestovné pro jednoho účastníka, Západočeská univerzita hradila cestovné druhého účastníka pracovní cesty a ostatní náklady.

Vyúčtování pracovní cesty provedlo ekonomické oddělení Západočeské univerzity v Plzni dle platných předpisů. Doklady o pracovní cestě jsou uloženy taktéž na ekonomickém oddělení ZČU. Drobné náklady (benzín, městská doprava, parkovné či tuzemské cestovné) byly hrazeny z kapesného účastníků zahraniční cesty.

Položka / Náklady	Celkem	Hrazeno ZČU	Hrazeno FR Cesnet
Zahraniční cestovné	251 082,51	175 452,26	75 630,25
Kurzové ztráty	1 682,40	1 682,40	
Celkem	252 764,91	177 134,66	75 630,25

Tabulka 1: Tabulka nákladů v Kč, výpis vyúčtování lze nalézt v příloze A.

Celkem bylo čerpáno 252 758,91 Kč, z toho z Fondu rozvoje Cesnet 75 630,25 Kč (90tis. Kč bez DPH), ostatní náklady v hodnotě 177 134,66 Kč byly hrazeny Západočeskou univerzitou v Plzni, čímž spoluúčast z původně plánovaných 35% narostla na cca 70%. Tento nárust byl způsoben zejména přijetím projektu se snížením příspěvku.

Oproti předpokladům v zadání byl rozpočet překročen o cca 13tis. Kč, což lze přikládat dvěma faktorům. Prvním neovlivnitelným je vývoj ekonomiky (inflace, vývoj ceny ropy, kurzu dolaru, ...) v době delší než jeden rok; od podání žádosti (březen 2004) až do doby uskutečnění pracovní cesty (květen 2005). Druhým faktorem byla nabídka volných letů s ohledem na nasmlouvané termíny pracovních schůzek. Tím bylo způsobeno, že délka pobytu byla o 4 dny delší než původně plánovaný měsíc.

Reference

[1] Stránka projektu WebAuth na Stanfordské univerzitě
`http://webauthv3.stanford.edu/`

[2] Stránka sdružení Liberty Aliance
`http://www.projectliberty.org/`

[3] Stránka projektu Shibboleth od Internet2
`http://shibboleth.internet2.edu/`

[4] Stránka neziskové organizace EurOpen.CZ na podporu svobodného softwaru
`http://www.europen.cz/`

A Výsledovka vyúčtování pracovní cesty

TODO: kopie vysledovky z magionu