Digital Identity Management

(Analýza moderních trendů a technologií.)

L. Kejzlar

Západočeská univerzita v Plzni
Centrum informatizace a výpočetní techniky
e-mail: kejzlar@civ.zcu.cz

24. března 2004

Abstrakt

Předkládaný projekt se zabývá analýzou moderních trendů a technologií využívaných při řešení problematiky bezpečné identifikace a řízení přístupu k elektronickým službám a informačním zdrojům. Důraz je kladen na komplexní a bezpečnou správu elektronické identity v rozsáhlých výpočetních systémech s distribuovanou administrativou a s přihlédnutím ke specifickým potřebám akademického prostředí.

Projekt je zařazen do oblasti II, tématického okruhu B.

1 Současný stav řešeného problému

Jednou z dlouhodobých priorit a oblastí odborného zájmu řešitelského kolektivu Centra informatizace a výpočetní techniky (CIV) Západočeské univerzity v Plzni (ZČU) jsou teoretické i praktické aspekty návrhu a implementace komplexní *bezpečnostní AAA infrastruktury* (autentizace, autorizace a audit) v prostředí rozsáhlých a heterogenních výpočetních systémů s oddělenými administrativními doménami.

Na základě spolupráce s předními akademickými pracovišti v USA (UCSC, Standford, ISU, MIT) navrhl řešitelský kolektiv koncepci a pilotně implementoval infrastrukturu distribuovaného výpočetního prostředí (DVP) ZČU ORION. Navržená infrastruktura je bez podstatných změn využívána již několik let v produkčním prostředí. Základními stavebními kameny architektury ORION jsou otevřené a dobře škálovatelné technologie založené na průmyslových standardech s vysokou úrovní bezpečnosti. Mezi nejvýznamnější patří:

- distribuovaný souborový systém AFS/OpenAFS,
- autentizační systém MIT Kerberos V5,
- PKI-light infrastruktura (KX.509, KCT),

- adresářové služby OpenLDAP.

Stávající produkční prostředí je průběžně inovováno a doplňováno o nové komponenty a technologie. V současnosti jsou např. realizovány pilotní projekty PKI infrastruktury, portálového řešení na technologii J2EE aplikačního serveru či Single Sign-On pro webové aplikace.

Lze konstatovat, že v rámci DVP ORION byla implementována většina klíčových „low-level" technologií (často v „nadstandardní" konfiguraci zahrnující několik vzájemně spolupracujících autonomních domén), nezbytných k vybudování moderní komplexní bezpečnostní infrastruktury.

Z našeho pohledu však stále chybí řada podstatných komponent (vlastností) „střední" vrstvy služeb, umožňující integraci nových technologií (WS-stack, XML Security, SAML) a především *reflektující* nové bezpečnostní paradigma úlohy *elektronické identity a jejího managementu*. Podrobnější popis této problematiky přesahuje rámec textu[1]. Je však zřejmé, že v procesu zprostředkování informací (či jiné elektronické komodity) vystupují různé role (např. *uživatel*, instituce (*identity provider*), poskytovatel služby (*resource provider*) a elektronický zdroj (*resource*)), které mají protichůdné (mnohdy diametrálně) potřeby a požadavky na ochranu elektronických zdrojů a identity (resp. některých jejích atributů) uživatelů. Celá problematika se podstatně komplikuje, přísluší-li elektronický zdroj a uživatel do vzájemně oddělených administrativních domén (v praxi je tento případ stále častější). Jedním ze slibných řešení nastíněných rozporů jsou technologie umožňující vytváření *důvěryhodných domén (circle of trust)* (pokud možno standardizovaným a co nejjednodušším způsobem) na základě sdílené (resp. společné) identity (*federated identity*) a jejího managementu.

2 Cíle řešení

Předkládaný projekt se zaměřuje na zmapování a analýzu komplexní problematiky bezpečné správy elektronické identity a její aspekty související se specifickými požadavky akademického prostředí. Důraz je kladen na moderní technologie a utvářené standardy řešící sjednocování identity (*identity federation*), její bezpečné předávání a ochranu před zneužitím. Podstatná je také otázka otevřenosti a vzájemné kompatibility vznikajících standardů a možnosti jejich integrace se stávajícími bezpečnostními protokoly a subsystémy.

Hlavním cílem projektu je rozvoj znalostního potenciálu členů řešitelského kolektivu v uvedené oblasti, výměna know-how, exkluzivní přístup ke state-of-art technologiím a jinak nenahraditelná možnost bezprostřední a osobní konfrontace pracovních tezí s předními „vizionáři" špičkových vývojových pracovišť USA v rámci plánovaného studijního pobytu.

Naše pozornost bude primárně zaměřena na vybrané iniciativy a projekty, které hrají podle našeho názoru klíčovou roli při formování nových otevřených standardů a zároveň disponují dostatečným implementačním potenciálem

[1] Hlubší rozbor bude součástí výstupů v případě realizace projektu.

a podporou širší akademické komunity. Cílem tedy není prezentovat vyčerpávající výčet existujících produktů, aktivit a technologií, ale spíše se pokusit o hledání „Svatého grálu“.

Neméně podstatným předpokladem úspěšnosti celého projektu bude i následné utřídění, zpracování a analýza získaných poznatků, tak aby mohly být v případě potřeby efektivně a opakovaně využity nejen řešitelským kolektivem, ale i ostatními zájemci z řad odborné veřejnosti.

Řešitelský kolektiv si také klade za svůj cíl další prohloubení a rozšíření neformální spolupráce mezi kontaktovanými vývojovými pracovišti a ZČU resp. ostatními členy sdružení CESNET. Jsme přesvědčeni, že obdobná forma aktivní odborné spolupráce je při řešení projektů výzkumného charakteru nenahraditelná.

Strategickým cílem, který však *značně přesahuje* rámec řešeného projektu, by bylo ideální zúročení získaných zkušeností a následných analýz vedoucí ke strategické volbě a implementaci technologií podporujících např. řešení typu *federated Single Sign-On*[2]. Není těžké ukázat, kolik duplicitní, neefektivní, nekompatibilní a v konečném důsledku nesmyslné práce by vhodně zvolené řešení odstranilo. Stejně snadno však nahlédneme, že komplexní řešení problematiky má řadu různorodých aspektů, jejichž těžiště neleží v technologické části.

3 Způsob řešení

Řešení projektu bude probíhat ve třech na sebe navazujících etapách zahrnujících *přípravnou fázi, studijní pobyt* a *vyhodnocení a analýzu získaných poznatků.*

Úkolem *přípravné fáze,* která již de-facto probíhá[3], je pokus o zmapování a zpřehlednění významu a úlohy „bezpečnostních funkcí“[4] ve vztahu k současným potřebám a trendu rozvoje informačních technologií[5].

Z hlediska dalších aktivit je zásadní ujasnit si postavení, význam, vzájemné vztahy, potřeby a požadavky jednotlivých rolí vystupujících v procesu zprostředkování elektronické informace a to jak z hlediska současných potřeb, tak i koncepčního výhledu.

Neméně podstatnou fází přípravy je výběr technologií a iniciativ, na jejichž rozbor bude zaměřen studijní pobyt. Z našich dosavadních závěrů vyplývá, že klíčové iniciativy představují:

- Internet2/MACE (Middleware Architecture Committee for Education):
  - *Shibboleth*[6],

[2] Tj. zjednodušeně řečeno: Single Sign-on fungující mezi nezávislými administrativními doménami a podporující vlastnosti federated identity.

[3] Úkol zorientovat se v dané problematice a provést „re-design“ požadavků na charakter bezpečnostní architektury výpočetního prostředí a poskytovaných služeb je z našeho pohledu natolik zásadní a obecný, že jej neváženeme na řešení předkládaného projektu.

[4] „Bezpečnost (ochrana identity) se stává podstatnějším faktorem pro uživatele, než jejich pohodlí.“, studie Gartner Group, 2002

[5] A to nejen obecně, ale především na konkrétních podmínkách ZČU a dalších univerzit.

[6] `http://middleware.internet2.edu/shibboleth`

  - *WebISO (Web Initial Sign-On)*[7],

- *Liberty Alliance Project*[8],
- *OASIS SAML (Security Assertion Markup Language)*[9],
- *WS-Security (Web Services)*[10].

Vlastní *studijní pobyt* v USA je plánován pro dva členy řešitelského kolektivu na dobu jednoho měsíce. Pobyt bude z převážné části realizován na Stanford University (dlouhodobé pracovní kontakty a výhodná „strategická“ poloha) a v současné době je již dohodnut jeho hrubý harmonogram. V rámci pobytu proběhnou pracovní jednání jak s kolegy z ITSS (Stanford), tak i ostatních institucí, s nimiž spolupracujeme nebo jsme navázali kontakt (především Liberty Alliance, OASIS SSTC, Sun Microsystems, UCSC a IBM Research). V souvislosti s naším pobytem se také jedná o uspořádání speciálního workshopu na téma „Digital Identity Management“ za účasti předních odborníků, které by jinak nebylo v našich silách (z časových či finančních důvodů) kontaktovat (mezi nejvýznamnější z nich patří předseda pracovní skupiny Internet2/MACE – Shibboleth, Bob Morgan z University of Washington).

Vybrané příklady potvrzení deklarované spolupráce a navázaných kontaktů jsou uvedeny v příloze tohoto projektu.

Utřídění, *vyhodnocení a analýza* získaných poznatků bude probíhat za účasti „širšího“ řešitelského kolektivu po zbývající dobu trvání projektu. Výstupy této fáze budou průběžně vhodnou formou prezentovány zájemcům a odborné veřejnosti.

4 Prezentace výsledků

Všechny odborné materiály, zdrojové texty a analýzy související s řešením projektu budou zájemcům dostupné v elektronické formě prostřednictvím WWW stránek CIV, ZČU v Plzni.

Klíčové výstupy projektu budou prezentovány na pravidelných odborných seminářích CIV–LPS, pořádaných pro studenty a zaměstnance a na národních konferencích zabývajících se danou problematikou (např. EurOpen.CZ).

Vzhledem k zaměření projektu do infrastrukturální oblasti, se nabízí potenciální využití získaných výsledků v širokém spektru výzkumných a vývojových aktivit jak v rámci ZČU (např. e-Univerzita, PKI, Single Sign-On, podpora $n-$tier architektury, autorizační infrastruktura, WiFi a mobilita), tak i sdružení CESNET (Port@l, autorizační infrastruktura *METACentra*, ID karty apod.). Řešitelský kolektiv se bude aktivně podílet na „popularizaci“ výstupů projektu a podpoře jejich dalšího zhodnocení.

[7] `http://middleware.internet2.edu/webiso`
[8] `http://www.projectliberty.org`
[9] `http://www.oasis-open.org`
[10] `http://www.oasis-open.org/committee/wss`

5 Charakteristika řešitelského kolektivu

Užší řešitelský kolektiv je složen ze zkušených pracovníků Laboratoře počítačových systémů (LPS) CIV a člena vrcholového managementu IT ZČU v Plzni. Na přípravě, a především zpracování a vyhodnocení výsledků projektu, se však bude podílet (přímo či nepřímo) řada dalších kolegů ze ZČU i spolupracujících univerzit (MUNI, ČVUT).

Řešitelský kolektiv má dlouhodobé zkušenosti s úspěšným řešením obdobně koncipovaných projektů, na jejichž základě byla mj. navržena a implementována infrastruktura distribuovaného výpočetního prostředí ORION a *META Centrum*.

Řešitelský kolektiv tvoří:

Ing. Luboš Kejzlar (hlavní řešitel) je absolventem Fakulty elektrotechnické Vysoké školy strojní a elektrotechnické v Plzni v oboru Automatizované systémy řízení. Od roku 1989 je v různých funkcích členem Laboratoře počítačových systému (LPS) Centra informatizace a výpočetní techniky (CIV) ZČU v Plzni.V rámci své pracovní náplně se podílel na řešení řady rozsáhlých projektů z oblasti návrhu síťové infrastruktury a implementace distribuovaného výpočetního prostředí (WEBnet, Cassiopea, ORION). S několika přestávkami se od počátku podílí na realizaci projektů Superpočítačová centra VŠ a návazně *META Centrum*. Mezi jeho profesní zájmy patří problematika bezpečnostní infrastruktury a distribuovaných výpočetních prostředí. Od roku 2002 řídí ve funkci vedoucího LPS výjimečný kolektiv cca. dvaceti spolupracovníků, kteří se aktivně podílejí na tvorbě koncepce, implementaci a provozu komplexního výpočetního prostředí ZČU. Z povahy své funkce v současnosti řídí a podílí se na řešení řady střednědobých infrastrukturálních projektů v oblasti PKI, AAA, mobility, SSO, MOM (Message Oriented Middleware) apod.

Dr. Ing. Jan Rychlík (spoluřešitel) je absolventem Vysoké školy strojní a elektrotechnické v Plzni v oboru Automatizované systémy řízení. V roce 1998 ukončil doktorandské studium, obor Informatika a výpočetní technika. V období 1978 – 1997 působil na ZČU jako odborný asistent na Katedře informatiky a výpočetní techniky (KIV). V letech 1997 – 1999 jako vedoucí Střediska informačních systémů (SIS), CIV ZČU. V období 1999 – 2001 zastával funkci technického ředitele PNS a.s.. Od roku 2001 je prorektorem pro IT na ZČU. Nadále působí jako vyučující na katedře KIV FAV a současně vede kolektiv SIS na CIV ZČU. Podílel se a podílí na řešení mnoha projektů v oblasti analýzy, návrhu a realizace informačních systému (IS dispečinku pro rozvoz tepla TEZA Plzeň, IS a DŘ rozvodu vody VaK Kroměříž, Evidence zařízení pro rozvod el. energie ZČE Plzeň, IS ZČU Studijní agenda STAG, IS pro rozvoj a výstavbu v ZČE, IS pro evidenci události v distribuci ZČE, zavedení systému pro předplatné tisku). Z titulu své funkce je zodpovědný za oblast IT, koncepci a budování komplexního

IS na ZČU. V oblasti výuky se dlouhodobě věnuje databázovým systémům základům operačních systémů.

Ing. Martin Chlumský (spoluřešitel) je absolventem Fakulty aplikovaných věd Západočeské univerzity v oboru Informatika a výpočetní technika. Od roku 1994 pracuje v Laboratoři počítačových systému Centra informatizace a výpočetní techniky, kde napomáhal při budování počítačové sítě WEBnet a distribuovaného výpočetního prostředí ORION. Po několik let spolupracoval při realizaci projektu *METACentrum*. Jeho pracovní náplň tvoří správa distribuovaného souborového systému AFS, správa UNIXových operačních systémů a vedení oddělení Internetových a síťových služeb. Aktivně se podílí při tvorbě koncepce a rozvoji rozsáhlého výpočetního prostředí ZČU.

Ing. Jiří Sitera (spoluřešitel) je absolventem Fakulty aplikovaných věd Západočeské univerzity v Plzni, od roku 1996 působí na CIV ZČU, přesněji LPS (Laboratoř počítačových systémů). V současné době pracuje jako vedoucí oddělení distribuovaných a operačních systémů. Podílí se na řešení projektů z oblasti distribuovaných výpočetních prostředí a GRIDů, jmenovitě projektu *METACentrum* a některých s ním souvisejících projektů (distribuované datové sklady) a je řešitelem projektu EU DataGrid (EGEE). K hlavním specializacím patří adresářové služby a management distribuovaného výpočetního prostředí, což se tématicky odráží v publikační činnosti.

6 Navrhovaná doba trvání projektu

Navrhovaná doba trvání projektu byla stanovena na 12 měsíců.

7 Finanční rozvaha

V rámci grantu požadujeme pouze neinvestiční prostředky nezbytné na pokrytí hlavních nákladů spojených se studijním pobytem, které činí 239 000,– Kč.

Z prostředků fondu rozvoje budou čerpány neinvestiční prostředky ve výši 154 000,– Kč, zbylou částku 85 000,– Kč (tj. 35%) včetně dalších nákladů spojených s projektem hradí řešitelská organizace.

Celková částka na pokrytí hlavních nákladů byla stanovena následovně:

cestovné (letenky a doprava)	85 000,–
stravné a kapesné	110 000,–
ubytování	44 000,–