Správa identity

Petr HANÁČEK[1], Jan STAUDEK[2]

[1]*Ústav inteligentních systémů,FIT VUT Brno*
Božetěchova 2, 612 66 Brno
hanacek@fit.vutbr.cz
[2]*Katedra počítačových systémů a komunikaci, FI MU Brno*
Botanická 68a, 602 00 Brno
staudek@fi.muni.cz

Abstrakt. Vesměs všechny konceptuální modely užívání služeb digitálního světa jsou ve své podstatě založeny na pragmatickém ideji, podle které uživatel konkrétní aplikace, systému, služby, apod. funguje pouze jako koncový konzument nebo producent služby a jednoznačná identita se přisuzuje identifikátoru (ID) uživatele. Správa uživatelů je tedy plněna z valné části správou (digitální) identity. Pokrývá celý životní cyklus uživatelovy identity, od jejího vzniku až do jejího zániku, její náplní jsou správní úkony související s udělováním a s modifikacemi výsad, práv a omezení digitálním identitám uživatelů.

Klíčová slova: správa uživatelů, správa identity, autentizace, synchronizace hesel, SSO, federování správ identit, aktivace prostředí, XNS, Kerberos, PKI, SOAP, SAML, SPML, DSML, WDSL, LDAP, UDDI, OASIS, W3C

1 Úvod

Tutoriál nabízí možnost se zevrubněji seznámit s cíli, prostředky a implementačními mechanismy *správy identity* uživatelů systému, jejímž posláním je poskytování služeb potřebných pro *identifikaci* osob působících v nějakém systému a pro *řízení přístupu* identifikovaných k těm komponentám takového systému, ke kterým je přístup nějakou formou omezený. Zúžení chápání pojmu „systém“ na „systém vybudovaný na bázi IT“ je neodůvodněně restriktivní, systémem může být stát, orgán státní správy, metropolitní akademická síť, obchodní společnost, … Zajímavým problémem s netriviálním řešením se stává správa identity tehdy, když systém není vnitřně homogenní, když je sestaven z technologicky, funkčně a výkonově odlišných dílčích systémů vytvářejících distribuovaný systém. Například pro účastníka konference konané v jiné státu (kontinentu) než právě pobývá by bylo efektivní, kdyby si na základě jednou prokázané identity např. na www stránce aerolinií, u kterých si objednává letenku, mohl rovněž v cílovém místě důvěryhodně najmout auto, zajistit si ubytování apod.

Tomáš Hruška (ed.), DATAKON 2005, Brno, 22.-25. 10. 2005, pp. 1-23.

2 Správa identity

Pojmem *správa identity* označujeme komplex služeb, který poskytuje na základě definovaných politik bezpečné a automatizované řešení správních úkonů efektivně řešících přístup „obrovské“ a vesměs trvale rostoucí komunity uživatelů (zákazníků, zaměstnanců, partnerů, …) k omezeným a mnohdy citlivým informačním zdrojům. *Identitou* entity (osoby, místa, věci, … obecně jistého objektu) se obecně rozumí vyjádření její totožnosti ve smyslu vztažnosti, tj. jejího vymezení vůči jiným entitám. *Identifikací* se rozumí určení, kterou entitu určuje jméno udané v jistém *kontextu*, a jaký má tato entita v udaném kontextu *profil* (vlastnosti, práva, privilegia, …). Pokud hovoříme o *digitální identitě* (entity, objektu), chápeme pod tímto pojmem elektronický záznam atributů určujících identitu – jméno, jednoznačné ID, adresa, doklady vlastností / udělených výsad apod. Správa identit (*IDM*, *Identity Management*) je pak souborem nástrojů pro definování identit entit, bezpečné a v daném prostředí efektivní uchovávání relevantních identitních informací o entitách (jmen, dokladů, …), zpřístupňování těchto informací pomocí standardizovaných rozhraní a pro poskytování odolné distribuované a výkonné infrastruktury pro provozování správních procesů, tj. při správě vztahů zdrojů a entit v daném kontextu.

2.1 bázové rysy správy identity

Mezi bázové rysy správy identity se v současné době zahrnuje:

- Centralizovaná administrace pomocí www aplikace
- Možnost delegování administrativních úkonů na bázi definovaných rolí a pravidel
- Možnost provádět manipulace s hesly uživateli samoobslužně, bez intervence centrální administrativou
- Dostupnost inteligentního směrování schvalovacích postupů při vyřizování žádostí o přístup ke zdrojům
- Automatizované aktivování prostředí jednotlivých uživatelů
- Dostupnost auditních mechanismů a mechanismů pro automatické generování přehledových zpráv (kdo má k čemu přístup)

Při správě identity hrají klíčovou roli funkce související s řízením přístupu uživatelů k informačním zdrojům. Pro efektivní implementaci této klíčové role správy identity musí být vybudovaná odpovídající podpůrná infrastruktura (adresářové služby, autentizační služby, workflow procesů souvisejících se správou identity apod.).

Software podporující správu identity podporuje vzhledem k nejrozšířenějším způsobům zajišťování služby autentizace uživatelů systému především automatizaci správních procesů souvisejících s péčí o hesla. Aby se důvěryhodnost hesel udržela po delší dobu, doba platnosti konkrétního hesla musí být významně omezená, hesla se musí po uplynutí doby platnosti inovovat. V distribuované systému se přitom musí zajistit synchronizovaná úprava hesel ve všech částech celého systému. K těmto účelů lze využít např. technologie označované termínem *single-sign-on* (*SS0*), viz 3.2.

V institucích (v podnicích) se využitím služeb správy identity dosahuje jak vyšší úrovně bezpečnosti tak i produktivity a na tvorbu aplikací, jejich zavedení a provoz se přitom často vynakládá méně peněz a úsilí. Správa identity na úrovni podniku je

v současnosti podporovaná standardizačními procesy, jejichž zevrubnější rozbor je náplní kap. 4.

Industriální zájmové skupiny, jakou je např. *World Wide Web Consortium* (*W3C*), vyvíjejí standardy, které jsou cíleny na globálně chápanou správu identity, ve které je každý jednotlivec identifikovaný jednoznačně. Podle programového prohlášení W3C, [13], správa identity musí vyhovovat požadavkům na:

- *Přenositelnost a interoperabilitu.*
  Vlastník průkazu identity musí mít možnost tento průkaz použít ve všech aplikacích, službách a doménách. Pro globálně použitelný ID uživatele je vhodným vyjádřením např. textový zápis v XML. Musí existovat služba zobrazující obecně používané identifikátory (jména a příjmení, rodná čísla, telefonní čísla, e-mailové adresy, …) na globálně použitelné ID uživatelů. Tato služba musí používat pro předávání tvrzení o identitě a autentizaci univerzálně použitelný protokol podporující jak hierarchické prověřování v neformálních systémech s obecně strukturovaným delegováním prověřovacích práv a povinností, tak i modely „p2p registrace“ v organicky uspořádaných komunitách.
- *Rozšiřitelnost.*
  Výčet atributů podporujících správu identity není nijak omezený a proto se činí závěr, aby protokoly a služby byly z hlediska potřeb univerzální reprezentace dat a definice potřebných schémat založeny na XML a na konceptu XML Schemat. Slovníkovým výčtem být definovatelné jak identitní atributy pro služby správy identity tak i řídicí struktury protokolů správy identity vč. autentizace, sdělení výsledku a slovníku dojednávání řízení. Musí se podporovat distribuovanost lokálních slovníkových definic, aby mohli definice dat a definice zpráv ve speciálních případech rozšiřovat všichni vlastnící identity.
- *Dohodnutelnost úrovně soukromí a bezpečnosti*.
  Služby správy globální identity musí být funkční při působnosti mezi všemi jurisdickými a důvěrnostními doménami. Genericky stanovit všechny relevantní požadavky na soukromí a bezpečnost je tudíž nemožné. Požadovaná úroveň soukromí a bezpečnosti musí být v každém jednotlivém případu vyjednatelná. Služba musí vlastníkům identity povolit pracovat s jejich informačními subjekty výhradně podle omezení daných jejich právním systémem. Služba musí používat dojednávací protokol, který uživatelovu agentu umožní ovlivňovat úroveň soukromí a bezpečnosti, ve které si přeje prosazovat svoji identitu, resp. které požaduje pro výměnu informací. Aby se zaručila ochrana osobních dat a práv, musí takový protokol podporovat anonymitu a pseudonymitu. Zavedení jedinečné celosvětově platné identity jednotlivce se nepožaduje a není to ani žádoucí.
- *Zodpovědnost.*
  Pokud mají reprezentovat identitu uživatelů automatizovaní agenti, musí se pro dosažení potřebné úrovně důvěry a důvěrnosti poskytnout pro služby správy globální identity infrastruktura, která podpoří dosažení potřebné úrovně zodpovědnosti (alespoň takové, jaká se udržuje v systémech mezinárodního bankovnictví a platebních systémů na bázi karet). Vlastníci identity

a poskytovatelé služeb se musí dohodnout na formách, kterými jejich agenti budou prokazovat zodpovědnost za zastupování, za dojednávání a za výkon své činnosti. Prostředí pro řádné naplňování zodpovědnosti musí vycházet ze všeobecně platných právních principů v maximálně možné míře uznávaných mezinárodní legislativou. Kdykoliv je praktické a efektivní použít pro řešení sporů standardní mechanismy, je žádoucí takové mechanismy použít.

– *Distribuovanost registračních autorit*.

  Služby správy globální identity mají mezi-jurisdickou podstatu, nemohou se tudíž spoléhat na existenci jedné centrální registrační autority, musí umožnit pomocí odpovídajících protokolů a podpory kooperačních prostředí spolupůsobení nijak neomezovaného počtu registračních autorit. Služby musí v neformálních systémech s obecně strukturovaným delegováním prověřovacích práv a povinností podporovat hierarchické modely registrace, v organicky uspořádaných komunitách p2p modely registrace. V hierarchickém modelu musí všechny registrační autority používat obecně platné normy a protokoly, aby entity, které je splňují a používají, nebyly nijak omezované, diskriminované. Aby agenti vlastníků identity mohli rozhodovat o změně poskytovatele služby, musí být registrace mezi registračními autoritami přenositelné.

– *Distribuovanost certifikačních autorit*.

  Služby správy globální identity se nemohou spoléhat díky své mezi-jurisdické podstatě na jedinou síť důvěry, musí umožnit používat rozšiřitelný protokol a rozšiřitelné prostředí pro uplatnění více sítí důvěry. V systémech s hierarchiemi delegování důvěry musí podporovat hierarchické modely certifikace, pro organicky uspořádané sítě důvěry musí podporovat p2p modely certifikace. V hierarchickém modelu musí všechny certifikační autority používat obecně platné normy a protokoly, aby vlastníci identity mohli důvěřovat službě jako celku a cítili se bezpeční i při změnách domén důvěry. Standardy musí podporovat chápání důvěry jako fenoménu uspořádatelného do vrstev, aby jednoduché transakce se nezesložiťovaly a aby se vlastníci identity mohli certifikovat pouze na té úrovni důvěry, která je potřebná pro transakce, ve kterých působí. Musí být rozšiřitelné o nové atributy, aby se mohly pro specifická prostředí a aplikace vyvíjet specifické modely důvěry.

– *Nezávislost vládnoucí autority*.

  Každá služba správy globální identity, která vyhovuje výše uvedeným požadavkům, je principiálně neřešitelná jedinou entitou. Tím pádem musí existovat nezávislé uskupení, které rovnocenně, bez jakékoliv diskriminace, reprezentuje všechny entity – lidi, byznys, nevládní organizace, státní správu apod. Taková autorita musí být schopna vystupovat jako mezinárodní nezisková organizace, ze všech možných hledisek nezávislá na průmyslu, obchodu a státních správách. Poněvadž technická řešení a provoz služeb jsou spolu těsně souvisí, musí se definovaná jak technickými tak i provozními normami. Mezi její povinnosti patří i správa vývoje globálního slovníku univerzálních identitních atributů a globálních řídicích struktur, definice forem a způsobů zajišťování zodpovědnosti všech agentů vč. registračních a

certifikačních autorit. Musí sloužit jako nestranná kořenová autorita v hierarchických modelech registrace a certifikace

Mezi cíle správy identity se řadí vytvoření zřejmé a jednoznačné identity pro každého uživatele relevantního systému, poskytnutí nástrojů pro jednoduchou a racionální definici kontextu pro takovou identitu a umožnění definovat politiky a bezpečnost na bázi stanovení profilů definovatelných tříd uživatelů. Aby správa identity splnila své poslání, plní úkoly mnohdy symbolicky označované jako *4A*:

- Dokazování kdo uživatel je – *Authentication*
- Určování práv a výsad uživatelů – *Authorization*
- Správa nástrojů pro řízení přístupu – *Access Control*
- Zpravodajství a auditní činnost – *Audit, Reporting*

Úkoly *4A* musí splnitelné i bez centralizace skladů digitálních identit uživatelů, možnost sdílení digitálních identit mezi partnerskými systémy se označuje pojmem *federování* správ identit. Federovaná správa identit umožňuje kooperaci více nezávislých autorit na pojmenovávání a autentizaci uživatelů.

2.2 Funkční pohled na správu identity

Generický profil funkcionality správy identity lze charakterizovat následujícím výčtem funkčních celků:

- *Správa životního cyklu účtu uživatele*
- *Řízení přístupu a autorizace*
- *Zpravodajství a auditní činnost*

Jako nadstavbovou funkcionalitu správy identity pak zařazujeme

- *Federování identity*
- *Integrace webovských služeb*
- *Prosazování politik a podpora managementu řízeného politikami*

Správa životního cyklu účtu uživatele

Do funkčního celku *Správa životního cyklu účtu uživatele* patří

- *Správa profilů* – vlastní práva identit v užším slova smyslu, a jejich distribuce do externích databází, adresářů, aplikací, … organizace a jejich partnerů, podpora samoobslužnosti uživatelů při správě profilů a podpora automatických replikací informací z profilů uživatelů systémům. Workflow engine správy životního cyklu účtů uživatelů podporuje monitoring procesů správy změn identity a distribuce změn identity, sledování, zda jsou dodržované stanovené politiky, řešení anomálií např. i manuálními zásahy zvláště pak v případech, kdy se vyžaduje schvalování práv přístupu uživatele k jistým zdrojům, určení jak postupovat, když není dodržený standardní časový limity pro schválení, apod.
  Jako typické funkční komponenty správy profilů lze uvést funkce pro vytváření a správu jedinečných uživatelských profilů, pro podporu samoobslužnost definic identitních informací v uživatelských profilech a funkce zajišťující automatické replikace identitních informací z uživatelských profilů do podporovaných systémů.

- *Aktivace a deaktivace prostředí uživatele* – Proces zpřístupnění (znepřístupnění) informačních zdrojů zaměstnancům, smluvním partnerům, zákazníkům atd. Jde tedy např. o zřízení e-mail účtu, povolení přístupu k portálům organizace, povolení přístupu k vybraným službám typu CRM a ERP (Customer Relationship Management, Enterprise Resource Planning), zpřístupnění vzdálených služeb, korekce pravidel na firewallu, získání iniciálních oprávnění, zaslání certifikátů uživateli, zanesení digitální identity uživatele do aplikací, vytvoření jmenovky / ID karty. Aktivace a deaktivace prostředí uživatele zajišťuje změny identitních dat při změně role zaměstnance a likvidaci identity a účtů při rozvázání pracovního poměru. Jejím základním cílem je snížení ceny a doba aktivace / deaktivace účtu uživatele a zvýšení zaručitelné bezpečnosti.
- *Delegování administrace* – poskytuje možnost definovat, ze kterých účtů lze provádět manažerské akce typu zřízení nového účtu, změna privilegií, změna hesla, obnova hesla atd. Musí se zajistit, aby v prostředích účtů s delegovanými právy administrace bylo vytvořené a po dobu akce udržované bezpečné prostředí a aby se manažerská akce provedla řádnou formou. Všechny akce, které se odehrají v systému musí být protokolované, zálohované a auditovatelné.
- *Samoobslužnost uživatelů* – jedná se o extrémní až absolutní delegace administrace na uživatele, kdy z individuálního účtu lze upravovat profil držitele účtu bez intervence Help Desku a/nebo administrátora. Typicky se jedná o možnost úpravy hesla v jiném systému a o obnovu zapomenutého hesla pomocí vhodného protokolu typu výzva / odpověď.
- *Správa hesel a synchronizace hesel* – se řeší vesměs pomocí mechanismů *SSO*, *Single Sign-On* pomocí vhodné front-end aplikace, agentem nebo službou, která operuje s dokumenty jménem (za) uživatele, dodává požadované doklady systému, ke kterému přistupuje a organizuje změny hesel tak, aby byla, podle zvolené politiky, zachována konzistence identity v celém systému. Správu hesel a synchronizace hesel lze řešit pomocí aplikace s webovským rozhraním rozesílající změny nebo centrální pamětí (adresářem), případně doplněnou o synchronizaci pomocí meta-adresářů, případně kombinací obou takových technologií.

Řízení přístupu a autorizace

Řízení přístupu a autorizace se v současnosti téměř výhradně řeší nějakou vhodnou variantou systému typu SSO. Generickým cílem je realizace byznys činnosti ve více systémech (ve více uzlech sítě) bez opakovaného přihlašování (udávání jména, hesla). Snížením počtu přihlašování se zvyšuje efektivita práce uživatele. Dosahuje se vyšší bezpečnosti snadnějším dodržováním bezpečnostní politiky přijaté pro práci s hesly. Nejsou kladeny vysoké nároky na inteligenci přihlašovacích nástrojů pro vzdálené přihlašování. Je potřeba ale počítat s tím, že centrální řešení SSO zvyšuje se riziko dopadu napadení autentizačního nástroje, jedním úspěšným útokem se zpřístupněný celý propojený systém.

Princip SSO lze implementovat aplikací zajišťující synchronizace hesel, službami, které poskytují některé operační systémy (NOS SSO, Network OS SSO, Passport),

kerberizací aplikací, podnikovým řešením na bázi síťového proxy serveru, nástroji SSO implementovanými na straně klienta a nebo nástroji SSO řešenými formou webovského správce přístupu.

2.3 Typické stavební bloky správy identity

Aktualizace hesel

Cílem funkční modulu *aktualizace hesel* je snížení ceny a administrativy vynakládané na prosazování autentizační politiky založené na používání důvěryhodných hesel. Eliminuje potřebu explicitní starosti správce systému o prosazování takové politiky. Uživatelům umožňuje inovovat svá hesla a případně odblokovávat své účty zablokované kontrolními mechanismy prosazované autentizační politiky pokud možno bez kontaktu nebo s minimálně nutným kontaktem s *help desk*. Uživateli umožňuje inovovat své heslo např. aplikací zpřístupněnou standardním www prohlížečem, klientem běžícím pod operačním systémem jeho koncového počítače nebo interaktivně hlasovou službou poskytovanou vhodným *call centrem*. Autentizace uživatele se v takových případech řeší typicky principem *něco znám*, odpověďmi na otázky, které může znát pouze příslušný uživatel (např. dotazy na hodnoty čtené z *grid karty*).

Synchronizace hesel

Cílem funkčního modulu *synchronizace hesel* je umožnit uživatelům, aby při interakci s více aplikacemi (systémy) mohli používat stále jediné heslo a usnadnilo se jim dodržovat zásady stanovené autentizační politikou. Modul *synchronizace hesel*, na rozdíl od řešení pomocí dále popsaného funkčního modulu *single sign-on* (*SSO*), požaduje zadávání ID uživatele a hesla pro každý přístup ke každé aplikaci (systému). Zavedení modul *synchronizace hesel* do infrastruktury správy uživatelů nevyvolává drastické změny v existující infrastruktuře IT organizace. Jeho zavedení si vyžádá vynaložení méně nákladů než zavedení principů typu SSO nebo inteligentního koncového řízení přístupu na úrovni aplikací. Příslušný software pro synchronizaci hesel typicky běží na některém serveru organizace a přes API je navázán na podporované databáze, na systémy zajišťující bezpečnost aplikací, na help deska pod.

Single sign-on (SSO)

Funkční modul *SSO* lze chápat jako další, propracovanější krok navazující na prostou *synchronizaci hesel* ve vývojové linii směřující k optimální správě uživatelů. Uživatel se přihlásí ke svému počítači nebo do sítě pouze jednou a k aplikacím (systémům) spoléhajícím z hlediska prosazování autentizační politiky na zavedený princip SSO přistupuje bez nutnosti opakování autentizace. Tuto službu poskytují např. produkty *eTrust Single Sign-On* od Computer Associates (www.ca.com), *v-GO® Single Sign-On™* od Passlogix (www.passlogix.com), *Web Single Sign-On* od Blockade Systems (www.blockade.com) apod. V prostředí podporovaném SSO se uživatel autentizuje při přihlášení a na obrazovce se mu prezentují dostupné aplikace. Jakmile si uživatel vybere konkrétní aplikaci, agent SSO dodá autentizační informace uživatele zvolené aplikací „na pozadí“, bez explicitně vyžádané interakce s uživatelem. Zavedení technologie SSO požaduje implementovat speciální infrastrukturu, ve které se typicky nachází autentizační server, který dříve než se uživateli umožní přístup k požadované

aplikaci identitu uživatele a jeho přístupová práva ověří. Systémy SSO jsou při srovnání se systémy provádějícími pouze synchronizaci hesel vesměs finančně nákladnější, náročnější na zavedení a implementaci a také náročnější na vlastní administrativní správu.

Inteligentní koncové řízení přístupu

Typickými reprezentanty inteligentního koncového řízení přístupu uživatelů jsou produkty, vesměs používající webové rozhraní, jako *Policy direktor* z IBM Tivoli (www.tivoli.com), *SiteMinder* od Netegrity (www.netegrity.com), *AssureAccess* od Entegrity Solutions (www.entegrity.com), *ClearTrust* od RSA Security (www.rsasecurity.com), *NetPoint* od Oblix (www.oblix.com), *SelectAccess* od Baltimore Technologies (www.baltimoretechnologies.com) nebo *GetAccess* od Entrust (www.entrust.com). Jsou zabudovány do komplexu aplikací a umožňují řešit správu uživatelů on-line, souběžně s provozováním koncových byznys aplikací. Vesměs umožňují používat více autentizačních metod, vč. hesel, digitálních certifikátů, hardwarových nástrojů apod. Umožňují správcům prosazovat politiku přístupu uživatelů k aplikacím centrálně. Jejich součástí bývá server prosazující politiku přístupu na bázi principu SSO. Integrální vlastností těchto nástrojů je, že umožňují řízeně delegovat správu přístupových práv uživatelů na byznys manažery a partnery. Administrátoři těchto nástrojů mohou rovně odvolávat individuální a skupinová přístupová práva k různým zdrojům. Další součástí řešení na bázi těchto nástrojů bývá funkcionalita, která efektivně podporuje *aktivace prostředí a podpůrné infrastruktury* pro uživatele dynamicky požadované v jeho životním cyklu v systému.

2.4 Aktivace prostředí a podpůrné infrastruktury pro uživatele

Každá aplikační aktivita uživatele se odehrává v nějakém prostředí tvořeném potřebnými technologickými (IT) nástroji a podpůrnou infrastrukturou. Prostředí a infrastrukturu je potřeba pro řádné plnění aktivity konkrétním uživatelem pro tohoto uživatele připravit. Nesystematičnost a z toho plynoucí nízká důvěryhodnost přípravy prostředí a infrastruktury snižuje kvalitu a spolehlivost poskytovaných služeb. Přípravu prostředí a podpůrné infrastruktury pro uživatele nazýváme *aktivací* (*provisioning*).

Aktivaci lze zhruba charakterizovat jako definici, správu a automatizaci všech procesů, které řídí životní cyklus uživatelů. Implementace aktivačních postupů a principů se v detailech případ od případu v různých organizacích liší, cíl však mají společný – řeší problém snížení administrativních ztrát a bezpečnostních rizik souvisejících se správou repositářů účtů.

Pro nového zaměstnance se mnohdy musí podle popisu jeho práce založit několik účtů v různých aplikacích a operačních systémech. V průběhu je zaměstnávání se při změnách pracovní náplně zaměstnance a při změnách jeho odpovědností musí vlastnosti účtů měnit. Při rozvázání pracovního poměru je nutné relevantní účty revokovat, případně plně odstranit. Aktivační postupy ve valné většině individuálně provozovaných systémů zahrnují mnohé aspekty, které se zahrnují pod pojem správa identity (uživatelů) – správu hesel, správu přístupových práv apod. Tyto postupy byly dosud řešeny ad hoc, bez zavedení všeobecně uznávaného standardu. Jednotlivé systémy jsou vybaveny proprietárními API, interoperabilita je vesměs silně omezená, pokud je vůbec možná. Navíc, v blízkém časovém horizontu se rýsuje nutnost přechodu od

aktivace uživatelů, resp. od *aktivace účtů* (*User provisioning*, *Account Provisioning*) k zajišťování v šířeji chápaném kontextu, k *aktivaci služeb* (*Service Provisioning*) díky vizi informačního světa, ve kterém spíše než jednotliví uživatelé vystupují identifikovatelní žadatelé služeb, poskytovatelé služeb a zprostředkovatelé služeb využívající obecné, standardizované, účinné, bezpečné a škálovatelné prostředí pro zajišťování žádostí o poskytnutí služeb.

Z pozice soudobých představ o řešitelnosti takto chápaného zajišťování hraje roli adekvátního standardu značkovací jazyk *SPML* **(***Service Provisioning Markup Lanaguage*), viz 4.5. Princip aktivací podle standardu SPML nejlépe objasní jednoduchý příklad, jehož řešení v prostředí SPML je uvedeno v 4.5: Personalista má zřídit nový e-mailový účet pro nového zaměstnance. Klasický postup by mohl být např. následující. Personalista zavolá správce e-mailového serveru a optá se ho co on jako správce potřebuje vědět, aby novému zaměstnanci zřídil e-mailový účet. Dozví se, že musí dostat jméno a příjmení nového zaměstnance, preferovaný ID zaměstnance v e-mail adrese, pracovní funkce zaměstnance, jaké odpovědnosti z takové funkce plynou a např. na kterém projektu/úkolu bude nový zaměstnanec pracovat. Personalista správci požadované informace poskytne a požádá správce, aby ho zpětně informoval, až bude účet zřízený a aby ho rovněž informoval o omezeních, která budou na zřízený účet aplikovaná.

2.5 Federování správ identity

Federovanou správou identity se rozumí systém, který používá v rámci jedné transakce stejné jméno (ID) uživatele, stejné heslo a příp. další osobní identifikační charakteristiky pro prokázání identity téhož uživatele ve více sítích více organizací. Partneři participující v sytému federované správy identity, *Federated Identity Management* (*FIM*) při autentizaci svých případných uživatelů jsou mezi sebou logicky sdruženi do korporace, která si vnitřně vzájemně uznávají positivní autentizace u uživatelům potvrzují z toho plynoucí právo přístupu např. ke službám. Marketingovému řediteli pracujícímu v jistém okamžiku v síti dodavatele např. dovolí korigovat vnitřní prognózy natažením informací z dodavatelovy databáze. Organizace např. mohou sdílet aplikace aniž by musely adoptovat stejné technologie pro plnění adresářových služeb, pro prosazování bezpečnosti, autentizaci apod. Uvnitř spolupracujících organizací se umožní, aby pro adresářové služby typu Active Directory nebo pro produkty používající Lightweight Directory Access Protocol rozpoznávaly své uživatele jedinou identitou. Požadovat, aby všechny spolupracující organizace používaly shodné technologie nebo aby udržovaly účty pro všechny zaměstnance všech svých partnerů je v praxi efektivně neřešitelné. Použití FIM umožní, aby si jednotlivé organizace udržovaly své vlastní adresáře a přitom, aby si mezi nimi informace vyměňovaly bezpečně.

Pokud organizace používá FIM, musí při atestaci uživatelů svých partnerů těmto partnerům důvěřovat. Musí si důvěřovat vzájemně, pokud jeden partner autentizuje identitu některého uživatele, musí positivní autentizaci respektovat i druhý partner. Potřebují proto nějaký standardizovaný kanál pro výměnu zpráv mezi sebou. Takovým nástrojem, mj. vhodným pro potřeby FIM, je např. soubor konvencí definovaných pomocí *Security Assertion Markup Language* (*SAML*, viz 4.4). Zpráva zapsaná v SAML umožní bezprostřední rozpoznání, zda eventuální uživatel je osoba nebo stroj a jaká má tento potenciální uživatel přidělená přístupová práva. Zprávy zapsané

v SAML lze při komunikaci mezi systémy (počítači, sítěmi) partnerů potřebné např. pro Web services (viz 0) předávat pomocí zpráv protokolu *Simple Object Access Protocol* (*SOAP*, viz 0).

Mezi pionýrské organizace z hlediska adaptace principů FIM patřily např. American Express, Boeing, General Motors, Nokia a nebo Proctor & Gamble.

Při adoptování federovaných správ identity je nutné si uvědomit, že důvěřovat partnerovi z hlediska autentizace jeho uživatelů lze pouze tehdy, když partner uplatňuje bezpečnostní politiku s potřebnou zárukou bezpečnosti, tj. když má zavedeny a uplatňuje bezpečnostní praktiky a praktiky správy uživatelů s potřebnou zárukou bezpečnosti. Dále je nutné počítat se faktem, že ne všechny webovské produkty pro řízení přístupu podporují SAML. Pak implementace technologie FIM si nutně vyžádá individuální řešení integrace aplikací a individuální vývoj uživatelských rozhraní.

Zavádění FIM se úzce váže na používání aplikačních služeb, *Web services*, viz 0. FIM a aplikační služby na sobě vzájemně závisí a obě technologie jsou perspektivním řešením letitých problémů efektivní implementace bezpečnosti (e-comm transakce, přihlašování k portálům, jednotné řízení přístupu, …).

Tradiční řešení těchto problémů vycházející např. použití technologie SSO předpokládá centralizaci informací pro řízení přístupu na jednom serveru s vestavěnými Plutony (web agenty) pro získávání informací. Aplikace se musí pro SSO přizpůsobit naprogramováním styku s proprietárními API, které se pravděpodobně v jednotlivých organizacích liší. Tradiční řešení SSO není z tohoto důvodu praktické pro zavedení v rámci extranetů a nevyhovuje ani pro použití *Web services*, nelze předpokládat používání unifikovaných databází. Kopírování citlivých dat zaměstnanců mezi databázemi byť i partnerských organizací nemusí vyhovovat legislativním omezením, obchodním politikám apod.

Místo programování prioprietárního agenta, který musí používat pro komunikaci s partnerovým serverem správy identity proprietární protokol), lze z aplikací zadávat pomocí např. protokolu SOAP, viz. 0, požadavky na autentizaci uživatelů a na autorizaci transakcí pomocí webovských služeb. Místo integrace speciálních knihoven s agenty pro komunikaci s centrálním autentizačním serverem do aplikací, jak to požaduje tradiční SSO, mohou lokální aplikace a organizace udržovat své vlastní repositáře autentizačních dat, která dávají odpovědi s bezpečnostními tvrzeními definujícími vlastnosti, role a práva uživatele jak lokálním, tak i vzdáleným aplikacím. Dominantním standardem pro přizpůsobování webovských služeb potřebám FIM je bezesporu SAML, viz.4.4. Navíc data vyměňovaná pomocí SAML zpráv mohou obsahovat i evidenční informace použitelné jako důkazový materiál kdo, kdy, k čemu přistoupil a kdo to povolil, což výrazně zvyšuje úroveň zaručitelnosti za bezpečnost v takto implementovaných systémech FIM.

Při popisu principů FIM nelze nezmínit *Liberty Alliance Project*[1], který vychází z téze, že sice není nedostatek praktických architektur SSO, ale tyto se špatně přenášejí do světa WEB. Proto Liberty Alliance Project řeší SSO na bázi SAML tvrzení použitelné mezi členy partnerské skupiny. Partnerskou skupinou, *Circle of Trust* je družení poskytovatelů služeb (PS) a poskytovatelů identity (PI) svázaných dohromady byznys vztahy. PI potvrzuje autentizaci uživatele PS a ostatním PI. Federovanou identitou je množina lokálních identit (uživatel, poskytovatel), se kterou lze pracovat

[1] http://www.projectliberty.org/

pomocí Liberty protokolů. Cílem není mít jedinou identitu, ale mít možnost federovat více identit.

3 Vybrané typické techniky autentizace pro správu identity

Autentizace patří mezi fundamentální *bezpečnostní opatření*. Bezpečnostní opatření jsou funkční nástroje systému podporující dosažení stanoveného bezpečnostního cíle. Autentizační opatření potvrzují věrohodnost identity deklarované nějakým subjektem a tím snižují rizika související s hrozbou falšování identity útočníkem na systém. Za předpokladu, že uživatelé systému mají správně definovaná práva přístupu ke zdrojům systému, stávají se autentizační opatření klíčovými nástroji i pro oblast řízení přístupu ke zdrojům systému.

Necháme bez povšimnutí notoricky známé autentizační pravdy (autentizace = *něco znám, něco mám, něco jsem* apod.) a změříme se přímo na výklad principů fungování a mechanismů implementace těch autentizačních mechanismů, které se nepominutelně uplatňují při správě uživatelů heterogenního distribuovaného systému budovaného na bázi IT.

3.1 Autentizační systémy SSL a TLS

Technologie SSL/TLS je uváděna jako referenční příklad standardního, v současné době už klasického, řešení autentizace a důvěrnosti v síťovém prostředí. Pro dosažení cílů požadovaných komplexním řešením správy uživatelů sama o sobě nedostačuje.

Secure Sockets Layer (*SSL*) je internetovský bezpečnostní protokol, který poskytuje ochranu proti kompromitaci privátních dat, narušení jejich integrity a falšování. V systémech typu klient–server umožňuje mezi klientem a serverem ustanovit bezpečný spoj v internetovské síti nad transportními spojem, který zajistí důvěrnost, autenticitu a originalitu dat. *Transport Layer Security* (*TLS*) je následnickým řešením SSL (vychází z definice SSL 3.0 fy Netscape). Sestává ze dvou komponent: *TLS Handshake Protocol* umožňuje klintu a serveru se vzájemně autentizovat, domluvit se na kryptografickém algoritmu pro zajištění důvěrnosti přenášených data a bezpečně si vyměnit odpovídající kryptografické klíče. *TLS Record Protocol* zajišťuje pomocí domluvené kryptografické metody (např. DES) požadovanou úroveň bezpečnosti. Umožňuje rovněž přenášet data v otevřené, nešifrované formě. Většina současných www prohlížečů protokoly TLS podporuje.

3.2 Systémy SSO, Single Sign-On

V aplikačních architekturách budovaných na bázi klient–server se pojmem SSO označuje autentizační proces, který uživateli, jenž chce v rámci jedné relace přistupovat k více aplikacím, umožňuje zadat jméno a heslo pouze jednou. Provedení procesu SSO se vyžádá při zahájení relace. Proces autentizuje uživatele pro přístup ke všem aplikacím, ke kterým mu byla na serveru vydáno právo přístupu a eliminuje tím všechny budoucí výzvy k autentizaci, které by jinak byly aktivovány kdykoliv by se uživatel v rámci relace přepojil mezi aplikacemi.

V e–com aplikacích se pod pojem SSO zahrnuje komplex služeb navržený za účelem centralizovaného udržování zákaznických finančních informací na jednom serve-

ru. Cílem není pouze pohodlí zákazníka, k tomuto řešení vede snaha o zvýšení bezpečnosti – omezuje se počet případů, kdy zákazník musí při placení udávat číslo platební karty nebo jinou citlivou informaci. Jako příklad WWW SSO systému lze uvést Microsoftí *Passport* (http://www.passport.net/), pokrývající více než 40 miliónů uživatelů a řešící typicky 400 autentizací/s. Po vyplnění přihlašovacího formuláře je uživatel zaregistrován na serveru *.NET Passport Web Site* a v rámci služby *Microsoft® .NET Passport*. Účet služby .NET Passport mu umožní použít zadanou e-mailovou adresu a heslo pro přihlášení k libovolnému serveru obsahujícímu tlačítko pro přihlášení k účtu služby .NET Passport.

Systémy SSO jsou vesměs budovány na bázi předávání pověřovacích dokladů (tokenů) a aplikace participující v doméně podporované takovým systémem SSO musí z tohoto hlediska tvořit homogenní systém, musí shodně pověřovacímu dokladu rozumět. I když se použije jako pověřovací doklad standardizovaný certifikát a systém SSO je vybudovaný na bázi PKI, stále se jedná o homogenní systém, všechny aplikace musí být schopny spolupracovat s PKI.

3.3 Kerberos

Kerberos je autentizační systém, který podporuje princip SSO, viz [2], [3]. Byl navržený a vyvinutý pro řízení přístupu ke službám s řízeným přístupem poskytovaných v uzlech sítě. Uživatele autentizuje při jeho počátečním přihlášení bezpečným způsobem (bez přenosu hesla sítí). Autentizovaný uživatel obdrží od *autentizačního serveru* potvrzení své autenticity a na základě tohoto potvrzení dostává od *řídícího serveru SSO* potvrzení jeho přístupových práv ke službě, ke které chce přistupovat. Software které chce služeb Kerbera využívat, musí být „kerberizovaný“, tj. musí se naučit komunikovat s Kerberem pomocí jeho API. Autentizační server Kerberova systému musí být provozován důvěryhodně, s minimalizovanými riziky napadení, výpadků apod. Princip činnosti Kerbera popsat následujícími kroky:

1. Uživatel chce použít službu poskytovanou serverem běžícím v jiném uzlu sítě (bude se k ní přihlašovat). Klientský software ví, že přístup k požadované službě mu bude povolený až po předložení Kerberovského potvrzení svého uživatele autenticity a hodnoty jeho přístupových práv k požadované službě, *tiketu*.
2. Uživatel se musí nejprve ohlásit svým jménem *autentizačnímu serveru*, *AS*. AS připraví na základě udaného jména uživatele a základě hesla uživatele, uchovávaného v důvěryhodně spravované databázi AS, potvrzení identity uživatele a zároveň oprávnění k důvěryhodné komunikaci uživatele s řídicím serverem SSO, tzv. *ticket-granting server* (*TGS*). Tento doklad vrátí AS uživateli důvěrně, je šifrované klíčem odvozeným z hesla uživatele. Uživatel použije své heslo pouze lokálně, z hesla si odvodí dešifrovací klíč a získá tak oprávnění komunikovat s řídicím serverem SSO – *ticket-granting ticket.* Důvěryhodnost oprávnění pro TGS se prokazuje tím, že AS toto oprávnění šifruje klíčem, který zná jenom AS a TGS.
3. Nyní se uživatel s oprávněním komunikovat s TGS obrátí na TGS. TGS může ale nemusí fyzicky být ten stejný server jako AS. Jeho role je ale odlišná. Vypracuje pro server požadované služby oprávnění přístupu uživatele,

ticket. Důvěryhodnost oprávnění pro službu se prokazuje tím, že TGS toto oprávnění šifruje klíčem, který zná jenom TGS a server služby.

4. Pokud služba akceptuje *ticket*, provede se.
5. Oprávnění získané z TGS má omezenou časovou platnost, po celou dobu jeho platnosti může uživatel danou službu používat opakovaně, aniž by si musel vyžadovat vždy nové oprávnění od TGS, resp. Aniž by se opakovaně autentizoval. Časové omezení platnosti, typicky na jednotky hodin, zvyšuje bezpečnost celého systému.

Skutečná procedura v Kerberu je poněkud komplikovanější, popis je pouze orientační. Lišívají se i některé implementace Kerbera.

3.4 PKI

Infrastruktury *PKI* (*public key infrastructure*) umožňují v podstatě ne bezpečnou veřejnou síť (Internet) používat pro bezpečnou komunikaci pomocí technik založených na využití asymetrické kryptografie. Potřebné soukromé a veřejné klíče se získávají a sdílí pomocí služeb poskytovaných důvěryhodnou autoritou. Zásadní roli v systému podporovaném PKI hrají digitální certifikáty generované v PKI, které identifikují jednotlivce nebo instituci a případně uvádí hodnoty některých jejich vlastností, a adresářové služby, které mohou certifikáty uchovávat a pokud je to nutné i revokovat. Forem implementací PKI je mnoho, profesionálních řešení se světovým renomé jsou desítky. Na internetovském standardu PKI pokrývajícím celou infrastrukturu se stále pracuje. Typická PKI sestává z komponent:

- Certifikační autorita (CA), která certifikáty vydává a ověřuje. Certifikáty obsahují potvrzení identity, hodnoty veřejného klíče, definici použitého kryptografického algoritmu apod. Certifikát je certifikační autoritou digitálně podepsán.
- Registrační autorita (RA) je podřízená komponenta CA, která pro svoji CA funguje jako ověřovací úřad před vydáním certifikátu
- Jeden nebo několik adresářů, ve kterých jsou se certifikáty uchovávají
- Správní systém a protokoly pro manipulaci s certifikáty, se žádostmi o jejich vydání či revokaci, s dotazy na platnost certifikátů apod.

Certifikát může hrát roli potvrzení identity uživatele a jeho přístupových práv a jeho rolí.

4 Technologická a standardizační základna implementace správ identity

4.1 Relevantní standardizační organizace

Vzhledem k výrazné orientaci technologií používaných k implementaci správ identity na XML hraje hlavní roli *OASIS*, *Organization for the Advancement of Structured Information Standards*[2]. OASIS je celosvětové neziskové konsorcium, které v oblasti e-byznysu řídí vývoj, konvergenci a přejímání standardů na bázi XML, např. dále

[2] http://www.oasis-open.org/

zmíněné standardy SAML, XACML, DSML, SPML, tj. standardy autentizace, řízení přístupu, adresářových a aktivačních služeb. OASIS vznikla v r. 1993, má asi 4000 individuálních i institucionálních členů z více než 100 zemí.

Významnou roli hraje *WS–I, Web Services Interoperability*[3], „open" industriální organizace pro prosazování interoperability a Web Services v různých platformách, OS a programovacích jazyků. Stojí např. za standardem protokolu *SOAP, Simple Object Access Protocol* .

Vzhledem k výrazné orientaci na použití webovských rozhraní vstupuje do hry rovněž mezinárodní konzorcium *W3C, World Wide Web Consortium* [4] administrované v USA z MIT a v Evropě z ERCIM. Posláním W3C je tvorba standardů a směrnic pro užívání webovských technologií. Plní roli fóra pro výměnu informací, vedení obchodu, komunikace a pro fóra pro vzájemné porozumění. V oblasti správy identity se stará např. o standard *WSDL*, *Web Services Description Language*.

IETF, *Internet Engineering Task Force*[5] podporuje rozvoj adresářových služeb na bázi protokolu *LDAP*.

Historické kořeny správy identity vycházejí z iniciativ *ITU–T, ITU Telecommunication Standardization Sector*[6] v oblasti podpory doporučení X.500, prakticky veškeré iniciativy v oblasti certifikované identity využívají pro definici certifikátů jeho standard X.509.

4.2 Standardy adresářových služeb

X.500

X.500 je morálně překonanou technologickou bází adresářových služeb, v současnosti má význam hlavně dílčí standard X.509 využívaný pro definici certifikátů většiny PKI.

LDAP – Lightweight Directory Access Protocol

LDAP je prakticky nejrozšířenější soudobá technologie adresářových služeb. Lightweight Directory Access Protocol, LDAP, [5] je jméno, které zavedl IETF pro síťový protokol vybudovaný na bázi TCP/IP určený pro zpřístupňování to serverů poskytujících adresářové služby. *Adresářové služby* (LDAP nevyjímaje) umožňují uživatelům vyhledat objekty (lidi, zdroje) podle specifikovaných podmínek. Například jsou určeny pro zodpovídání dotazů typu „hledám uživatele a znám jeho e-mail" nebo „hledám tiskárnu formátu A4, která umí tisknout barevně". Adresářové služby mohou samozřejmě sloužit také k získávání informací o konkrétních objektech, tj. zná-li dotazující konkrétní specifikaci objektu (například jméno tiskárny), může se dotázat na její vlastnosti.

Adresářová služba LDAP je specializovaná aplikace pro ukládání dat, jejich organizaci a přístup k nim. Data se ukládají ve formě záznamů, kde každý záznam obsahuje několik položek – atributů. Atributům se přidělují hodnoty. Každý záznam má

[3] http://www.ws-i.org/
[4] http://www.w3.org/
[5] http://www.ietf.org/
[6] http://www.itu.int/ITU-T/

jedinečné jméno (primární klíč) v rámci množiny záznamů a každý atribut má unikátní jméno v rámci záznamu. Záznam je složený z hierarchicky uspořádaných položek. Záznamy adresářových služeb jsou logicky rozmístěny v *adresářovém stromu* (DIT – Directory Information Tree). Adresářová služba LDAP sloužící jako centrální strukturované úložiště informací může udržovat např. úložiště identifikačních a autentizačních parametrů uživatelů, konfiguračních údajů systémů a aplikací apod.

Adresářová služba LDAP může hrát roli centrálního zdroje dat – do serveru LDAP se zadávají všechna data coby do centrálního skladu dat. Ze serveru LDAP jsou data distribuována jednotlivým systémům na požádání. Adresářová služba LDAP může ale hrát také roli kolektoru dat – pro LDAP server se definují důvěryhodné zdroje dat (např. telefonní ústředna jako zdroj informací o telefonních číslech, mail server jako zdroj informací o e-mailových adresách a personální systém jako zdroj personálních dat), LDAP tato data automaticky importuje pomocí importních scriptů a ukládá je do příslušných záznamů. Celá databáze je pak k dispozici všem systémům na požádání. V obou případech je hlavním úkolem při navrhování adresářové služby správné určení zdrojů dat a definice profilů jednotlivých záznamů a jejich atributů.

Záznamy se uspořádávají do hierarchie – *DIT* (*Directory Information Tree*). DIT definuje uspořádání záznamů takovým způsobem, aby ke každému záznam v hierarchii vedla pevně daná logická cestu a aby se záznam v celém stromě vyskytoval pouze jednou. Jeden server LDAP může pracovat s více DIT. Kromě základního adresářové služby, která zajišťuje vyhledávání, přidávání a modifikaci záznamů a schématu, se poskytují jako adresářové služby LDAP další volitelné služby. Například služba pro sběr dat z jiných adresářových služeb pomocí tzv. *konektorů* běžících přímo v prostředí jiné adresářové služby (např. Active Directory, Novell Directory Services, apod). LDAP Proxy je konfigurovatelné LDAP rozhraní umožňující nastavovat na celou strukturu bezpečnostní filtry nebo vytvořit jiný stromový pohled na existující uspořádání adresářové struktury.

LDAP nachází uplatnění v roli centrální databáze uživatelů pro aplikace a systémy, v podpůrných systémech SSO (Single-Sign-On) pro podporu přihlašování uživatele k relaci pomocí jednoho autentizačního místa, v systémech PKI jako distribuční služba pro diseminaci a prezentaci CRL a veřejných klíčů, používá se jako centrální registr parametrů pro konfiguraci systémů a aplikací, může plnit roli meta-adresáře, tj. sjednocení adresářových informací v rámci informačního systému apod.

DSML – Directory Services Markup Language

DSML – Directory Services Markup Language, [1], je aplikace XML, která umožňuje vyjádřit jedním společným a mnoha adresáři sdíleným formátem odlišné formáty různých síťových adresářů. DSML definuje rovněž dokument, který lze použít pro zobrazení obsahů každého z adresářů a pro vyměňování adresářových dat transportními protokoly.

DSML je nástroj pro reprezentaci informace o struktuře adresáře formou XML dokumentu. Definuje dokument, který lze použít pro zobrazení obsahů každého z adresářů. Jde o aplikaci XML, která umožňuje vyjádřit odlišné formáty různých síťových adresářů jedním společným a mnoha adresáři sdíleným formátem.

Aplikace provozované organizací a založené na XML pomocí DSML mohou zadat profil a zdroj informace z adresáře jim přirozeným způsobem. LDAP informace

lze zpřístupňovat jako XML data, DSML přidává XML funkcionalitu do adresářových služeb. V DSML vzniká XML dokument pro publikování schémat adresářů a pro vyměňování adresářových dat transportními protokoly

DSML je nástroj definice XML schematu, které umožňuje adresářům prezentovat základní profil informace formou XML dokumentu, takže tato může být sdílena nativními Internetovskými protokoly (HTTP, SMTP) a používaná i jinými aplikacemi

Cílem DSML není a nebylo ani specifikovat atributy, které musí osahovat všechny adresáře, ani metody, kterými se informace z adresáře dostává.

DSML vznikl na popud praxe jako klíčová komponenta e-com a webovských aplikací, která váží do jednoho celku byznys procesy. Byl definovaný v r. 1999, inovace definice se provedla v r. 2002

Rozvoj DSML podporuje IBM, Microsoft, Novell, Oracle a Sun-Netscape Alliance. Propagátoři DSML zdůrazňují, DSML synergisticky pracuje s LDAP adresáři, umožňuje informace z LDAP adresářů zasílat přes tradiční firewally apod.

Další snahy o vývoj systémů nad klasickými adresáři např.

DSML a LDAP nejsou jedinými iniciativami v oblasti rozvoje adresářových služeb. Vedle rozvoje DSML existují snahy o vývoj podobných systémů nad klasickými adresáři např. *Directory Interoperability Forum* (*DIF*)[7], nebo *Directory Enabled Networking* (*DEN*)[8],

4.3 Standardy z oblasti WEB Services, SOA

Jde o standardy světa *WS*, *WEB Services*, tj. o standardy úzce související s filozofií *SOA*, *Service Oriented Architecture,*jejíž podstata vychází z myšlenky, že aplikace volají funkcionality jiných aplikací přes síť. Role a infrastukturní funkcionality v SOA tvoří:

- *Volající strana* – klient – *WS Requestor*, která hledá / objevuje – find / discovery službu u zprostředkovatelů.
- *Zprostředkovatel – WS Broker* volající stranu navazuje – *bind* – na hledanou službu, dává jí potřebné navigace. Zprostředkovatel provozuje adresář (*Registry*) *UDDI*, *Universal Description, Discovery, and Integration* tj. databázi kde se pamatuje kde je jaká WS a jak se volá.
- Službu zveřejňuje – *publish* – u zprostředkovatele *poskytovatel WS – WS Provider*, aby zprostředkovatel uměl klienta na WS navázat tak, aby klient nalezenou službu u poskytovatele mohl vyvolat. Publikační data o WS se zapisují ve *WSDL*, *Web Services Description Language*. WSDL soubory uchovává zprostředkovatel v UDDI adresáři.

Klient po navazuje kontakt s WS výměnou zpráv řízenou protokolem *SOAP*, *Simple Object Access Protocol*. SOAP zprávy jsou přenášeny protokolem http, aby se umožnil průchod přes firewally apod. A vše je postaveno na technologické bázi XML.

[7] http://www.opengroup.org/directory/

[8] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/diren.htm

Web Services

Webovské služby, nazývané rovněž *aplikační služby*, jsou služby, které mnohdy reprezentují jak algoritmickou logickou aktivitu, tak i daty a nebo i činnosti lidských činitelů, jsou dostupné webovským uživatelům a programům napojených na webovské prostředí na aplikačních webovských serverech. Poskytovatelé webovských služeb se často označují jako poskytovatelé aplikačních služeb. Škála webovských služeb je široká a různorodá, objevují se mezi nimi služby jak z oblasti získávání a ukládání dat a nebo z oblasti *customer relationship management* (*CRM*), tak i mnohem úžeji orientované služby jakými je např. správa skladových zásob nebo aukce. Škála webovských služeb se rychle rozšiřuje.

Uživatelé si mohou webovské služby zpřístupňovat nejen jejich aktivací na centrálním serveru, ale rovněž ve vhodném p2p uspořádání. Webovské služby mohou mezi sebou komunikovat, potřebná výměna procedur a dat bývá podporována software, který bývá zvykem označovat jako *middleware*. Je zřejmý výrazný trend standardizace těchto služeb. Standardizace formátů dat a výměn dat vesměs vychází tou či onou formou z technologické báze representované XML. XML je základnou, ze které byl vyvinut *Web Services Description Language* (*WSDL*), [17]. Součinnost WSDL s principy SOAP komunikace a UDDI vyhledávání přehledově popisuje např. [18].

Dobrým studijním materiálem pro získání vjemu do problematiky tvorby webovských aplikací je přehledový článek [16] i diplomová práce [4]. Článek [11] umožní si dát svět webovských služeb do souvislosti s pojmy jako jsou komponentní architektury, vícevrstvé architektury apod.

SOAP – Simple Object Access Protocol

SOAP [SOAP] je platformově (OS) a jazykově nezávislý jednoduchý a snadno rozšiřitelný protokol, pro řízení komunikace mezi aplikacemi běžícími v síti Internet, tj. v decentralizovaném, distribuovaném prostředí, založený na XML. Předpisuje formáty vyměňovaných zpráv – v obálce se popisuje co obsahuje vlastní zpráva a jak se má její obsah zpracovat, pomocí pravidel se vyjadřují instance aplikačních datových typů a konečně se ve zprávách reprezentují podpory pro vzdálená volání procedur a odpovědi na ně, messaging apod. Na rozdíl od protokolů typu RPC (Remote Procedure Calls), jimiž řízený provoz je normálně blokován ve firewallech a proxy serverech, SOAP zprávy přes firewally procházejí. SOAP byl navržen pro komunikaci realizovanou na bázi protokolu HTTP, který je podporován všemi internetovskými prohlížeči i servery.

SOAP patří např. mezi klíčové prvky Microsoftí architektury .NET. SOAP je definován jako de facto standard W3C, vedle Microsoftu podporují jeho vývoj také HP, IBM, SAP a další firmy.

WSDL – Web Services Description Language

WSDL umožňuje vyjádření syntaxe programového rozhraní a jejich umístění v XML. WSDL soubor popisuje službu určením zpráv pro komunikaci se službou, operací podporovaných službou, určením jakými protokoly lze službu vyvolat a jak musí být formátovaná příslušná data, port, na kterém se služba poskytuje, síťové adresy, kde se služba poskytuje apod.

WSDL popis se zpřístupňuje na Internetu typicky v UDDI. Publikované WSDL soubory mohou používat programy na straně klienta a vývojové nástroje pro získání informací o dostupných WS a pro budování proxies nebo programových šablon pro zpřístupnění WS.

UDDI – Universal Description, Discovery, and Integration

UDDI (*Universal Description, Discovery and Integration*) je standardní mechanismus umožňující registraci a vyhledávání webových služeb. Ke každé webové službě by měl být k dispozici její formální popis v jazyce WSDL. Z tohoto popisu již jde automaticky vygenerovat požadavek v SOAP. Ve větších systémech nebo přímo v otevřeném prostředí Internetu se popis služby může zaregistrovat do UDDI registru. Ten slouží jako jakýsi telefonní seznam („zlaté stránky"), který umožňuje vyhledávání služeb s určitými parametry. Klient, který chce využít webovou službu, získá buď přes UDDI, nebo přímo její popis. Z něj je jasné, jakou strukturu má mít SOAP zpráva a kam se má webové službě poslat, aby ji rozpoznala.
Hlavními silami stojícími za vývojem UDDI byli Microsoft a IBM, projekt UDDI dnes podporuje více než stovka velkých korporací – American Express, SAP AG, Ford Motor Company a dokonce i Hewlett-Packard, jejíž vlastní řešení adresáře na bázi XML, e-speak, se integrovalo do UDDI. Specifikace UDDI se využívají ve standardech W3C i IETF.

XNS, Extensible Name Service

Koncept XNS (eXtensible Name Service) původně rozšiřoval koncept DNS do oblasti správy identity. DNS umožňuje uzlům sítě Internet přidělit numerické, hierarchicky strukturované *IP adresy* a jim odpovídající symbolická, opět hierarchicky strukturovaná *doménová jména*. Obě struktury, adresní i jmenná přidělují kontaktní identifikaci uzlu jednojednoznačně v celosvětovém pokrytí. DNS je jedinou vazbou mezi oběma formami identifikace uzlů. Přehled standardů definujících koncept DNS uvádí např. http://www.dns.net/dnsrd/rfc/.

Koncept XNS [15] se ale během svého vývoje od DNS hodně vzdálil. XNS je velmi robustní identifikační p2p protokol. Je budován na bázi protokolu SOAP (viz 0), SAML (viz 4.4) a XML jako otevřený protokol a open–source platforma pro univerzální adresování, automatizaci výměn dat a řízení důvěrnosti. Použití XML umožňuje dosažení platformové nezávislosti XNS. Automatizace výměn, vázání a synchronizování informací mezi jejich vydavateli a konzumenty se realizuje pomocí webovských agentů.

Standard XNS 1.0 byl publikován v polovině r. 2002, na jeho vývoji participovaly především reprezentanti finančního průmyslu – Visa International, Gemplus, Nomura Research Institute, Wave Systems apod. Od r. 2003 je XNS součástí iniciativ konsorcia OASIS, viz **Chyba! Nenalezen zdroj odkazů.**, při vývoji *XRI* (*Extensible Resource Identifier*) jako identifikačního schématu kompatibilního s URI (specifikace XRI syntaxe vychází ze specifikace *URI* (*Uniform Resource Identifier*), RFC 3986, a *IRI* (*Internationalized Resource Identifier*, RFC 3987) a odpovídajících identifikačních protokolů. XRI jsou nezávislé na umístění, aplikacích a transportních službách a mohou být tudíž sdílené v libovolných doménách a adresářích. Současně jsou řešeny definice XRI metadat jako identifikátorů pro popis ostatních identifikátorů.

4.4 Bezpečnostní standardy

SAML – Security Assertions Markup Language

SAML [7] je jazyk, který poskytuje XML prostředí pro tvorbu webovských služeb, které partnerům na aplikační úrovni umožňují si vyměňovat autentizační a autorizační informace (assertions, tvrzení). SAML podporuje spolupráci mezi správou přístupu na úrovni www a bezpečnostními produkty – uživatel by se měl být schopný se elektronicky podepsat na některé stránce u poskytovatele, se kterým komunikuje, a pak předpokládat, že se jeho pověřovací bezpečnostní data přenesou automaticky na všechna další místa, spravovaná i jinými poskytovateli, která navštíví. SAML nepodporuje dosažení důvěrnosti. Z hlediska přínosů pro bezpečnost, nepřichází s žádnou novou technikou autentizace. Byl navržen pro řešení transakcí pro B2B a B2C. Velmi dobrý přehled principů použití SAML uvádí [8].

SAML definuje množinu XML formátů pro reprezentaci identity a dalších atributů a pro definici protokolů pro zadávání požadavků na informace z oblasti řízení přístupu a autentizace a pro tvorbu odpovědí. Základem jsou *tvrzení*, výroky, které o někom vydává důvěryhodná strana. Tvrzení a protokolární postupy SAML určují strukturu dokumentů přenášejících bezpečnostní informace – definují způsob výměny autentizačních a autorizačních informací. Komunikující partneři své vnitřní bezpečnostní architektury měnit nemusí. Tvrzení jsou deklaracemi pravd o uživatelích (ať již humánní nebo technologické podstaty) – co prokazuje identitu uživatele, jaké má uživatel vlastnosti a pro co je autorizován. Tvrzení může rovněž obsahovat celý důkazový řetěz použitý pro rozhodnutí o právu přístupu. Důkazový řetěz může sloužit jako doklad prokazující kdo přistoupil ke kterým datům, kdy a kdo to povolil.

Protokol použitý pro výměnu zpráv má charakter *výzva/odpověď*. V současné době SAML podporuje protokol SOAP (viz. 0) nad HTTP, výzvy SAML jsou mapovány do výměn SOAP zpráv běžících nad HTTP. Lze očekávat brzké zabudování i dalších komunikačních a transportních protokolů. Způsob zabudovávání tvrzení a výměn tvrzení lze předepsat pomocí *SAML profilů*. SAML je nástroj pro vyjádření tvrzení o nutných akreditačních datech, žádné autentizace a autorizace uživatelů SAML neřeší. Toto provádí autentizační server využívající adresář *LDAP* (*Lightweight Directory Access Protocol*, viz **Chyba! Nenalezen zdroj odkazů.**). SAML vytvoří spoj na skutečnou autentizaci a tvrzení vypracuje z dat získaných tímto krokem. Způsob použití SAML pro systémy SSO přehledně popisuje např. článek [9].

SAML podporují především firmy RSA Security Inc., Baltimore Technologies, Novell Inc., Sun Microsystems Inc. a Tivoli Systems IBM. Microsoft bude podporovat SAML v operačním systému .Net Server.

XACML – eXtended Access Control Markup Language

XACML je standard řízení přístupu ve sféře WEB Services.

WS-S, Web Services Security

WS–S, standard známý rovněž pod názvem *WS Security Language* umožňuje zadat specifikace pro SOAP, které definují způsob zajištění důvěrnosti a integrity, jak a kam umístit bezpečnostní informaci do obálky SOAP zprávy apod. Do WSS modelu

lze zahrnout definice SAML, volání PKI, Kerberos, SSL. O standard WS–S se stará *WS–I*[9], *Web Services Interoperability*, organizace, která se stará i o SOAP.

4.5 Standard aktivaci prostředí, SPML – Service Provisioning Markup Lanaguage,

Standard značkovacího jazyka *SPML*, *Service Provisioning Markup Lanaguage* [SPML, SPLMIBM] se zaměřuje na dosažení dvou met – automatizace úloh plnících aktivaci prostředí a podpůrné infrastruktury pro plnění služeb a interopoerabilita různých aktivačních systémů. V konceptuálním modelu aktivací pomocí SPML hrají významnou roli tři základní komponenty – požadující autorita (*RA*, *Requesting Autority*), aktivační server (*PSP*, *Provisioning Service Point*) a aktivovaná služba (*PST*, *Provisioning Service Target*).

Princip aktivace podle standardu SPML nejlépe objasní jednoduchý příklad zmíněný při obecném popisu aktivací (viz 2.4). Personalista má zřídit nový e-mailový účet pro nového zaměstnance. Klasický postup by mohl být např. následující: Personalista zavolá správce e-mailového serveru a optá se ho co on jako správce potřebuje vědět, aby novému zaměstnanci zřídil e-mailový účet. Dozví se, že musí dostat jméno a příjmení nového zaměstnance, preferovaný ID zaměstnance v e-mail adrese, pracovní funkce zaměstnance, jaké odpovědnosti z takové funkce plynou a např. na kterém projektu/úkolu bude nový zaměstnanec pracovat. Personalista správci požadované informace poskytne a požádá správce, aby ho zpětně informoval, až bude účet zřízený a aby ho rovněž informoval o omezeních, která budou na zřízený účet aplikovaná.

V prostředí SPML se tato konverzace implementuje pomocí SPML zpráv kódovaných pomocí protokolu SOAP (viz 0) a budovaných a vyměňovaných podle pravidel deklarovaných XML schématu služby mezi systémem personalistiky a mail serverem, ve kterém se má zřídit nový e-mail účet nového zaměstnance. Personalistický systém vystupuje v roli RA a pošle na PSP, který je odpovědný za správu mail serveru, který vystupuje v roli PST, žádost o sdělení informací potřebných pro zřízení nového e-mail účtu nového zaměstnance. Oslovený PSP vrátí RA zprávu s popisem informací, které mail server požaduje pro zřízení účtu. Třetí zprávu, nyní už s požadavkem na zřízení nového účtu posílá RA opět na již oslovený PSP. PSP posílá čtvrtou zprávu na PST – zahajuje proces zřízení nového e-mail účtu buďto přímým voláním API mail serveru nebo předáním SPML zprávy s žádostí o zřízení nového účtu. Detaily o zřízení nového e-mail účtu PSP může poznačit v logovacím souboru a na RA vrací specifikace uplatněných omezení (např. horní mez kapacity mailboxu).

PSP mohou při aktivaci služeb spolupracovat, mohou např. hrát roli zprostředkovatele, pokud RA nemá / nezná přímý přístup k PSP cílové služby.

4.6 Standardy workflow pro Web Services

Konečně poslední z oblastí standardizačních iniciativ vhodných pro implementaci správ identity je oblast workflow pro WS. Reprezentativním standardem je *BPEL*, *Business Process Execution Language,* resp. *BPEL4WS*, který vychází z *WSDL* a

[9] http://www.ws-i.org/

z *WSDL Extensions*. Je využívaný hlavně svými původními vývojáři – MS, IBM. Jeho cílem je umožnit popsat byznys procesy složené z více WS plněných více partnery a standardizovat výměny zpráv jak v rámci organizace, tak i mezi partnery. BPEL definuje kroky a pořadí běhu kroků jejich vč. Paralelizace, BPEL nedefinuje co se v jednotlivých krocích děje. Obsah kroků řeší WS. BPEL pokrývá potřeby *instrumentacebyznys procesů* (Orchestration), tj. definice toku byznys procesů z pohledu a pod řízením jednoho koncového bodu. Pro oblast *choreografi byznys procesů,* tj. pro popis výměn zpráv, pravidel interakce a dohod mezi dvěma a více koncovými body byznys procesů se vyvíjejí standardy typu CDL4WS, *Choreography Description Language*.

5 Závěrem několik konkrétních příkladů systémů pro správu identity a řešení SSO

Níže uvedené odkazy si nekladou za cíl být vyčerpávajícím přehledem systémů pro správu uživatelů, řešení SSO a správu identity, pouze upozorňují na některé výrazné reprezentanty, se kterými se autoři setkali při přípravě tutoriálu.

- IBM Tivoli Identity Manager, *Policy direktor* z IBM Tivoli (www.tivoli.com),
- eTrust, *eTrust Single Sign-On* od Computer Associates (www.ca.com),
- RSA Federated Identity Manager,
- *ClearTrust* od RSA Security (www.rsasecurity.com),
- *SiteMinder* od Netegrity (www.netegrity.com),
- *AssureAccess* od Entegrity Solutions (www.entegrity.com),
- *NetPoint* od Oblix (www.oblix.com),
- *SelectAccess* od Baltimore Technologies (www.baltimoretechnologies.com)
- *GetAccess* od Entrust (www.entrust.com)
- *v-GO® Single Sign-On*^{TM} od Passlogix (www.passlogix.com),
- *Web Single Sign-On* od Blockade Systems (www.blockade.com)

Literatura

[1] *Directory Services Markup Language (DSML) v2.0*, http://www.oasis-open.org/specs/index.php#dsmlv2

[2] *Microsoft BizTalk Server 2004, Enterprise Single Sign-On Security*, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/deploying/htm/ebiz_depl_sso_abpo.asp

[3] Mayank Upadhyay, Ram Marti, *Single Sign-on Using Kerberos in Java*, Sun Microsystems, Inc., http://msdn.microsoft.com/library/default.asp?url=/library/en-us/deploying/htm/ebiz_depl_sso_abpo.asp

[4] Jirka Kosek, *Inteligentní podpora navigace na WWW s využitím XML,* 2002, http://www.kosek.cz/diplomka/html/index.html.

[5] *LDAP*, *Lightweight Directory Access Protocol*, RFC 1777, http://www.ietf.org/rfc/rfc1777.txt?number=1777

[6] *OASIS – domovská stránka*, http://www.oasis-open.org/home/index.php

[7] *Security Assertion Markup Language (SAML)*, http://xml.coverpages.org/saml.html

[8] *The "S" in SAML isn't for Simple* http://www.securewebservices.org/archives/16-The-S-in-SAML-isnt-for-Simple.html

[9] Jon Byous, *Single Sign-on Simplicity with SAML* http://java.sun.com/features/2002/05/single-signon.html

[SOAP] *SOAP – Simple Object Access Protocol*, http://www.w3.org/TR/soap/

[SPML] *OASIS Service Provisioning Markup Language (SPML) Roadmap*, http://lists.oasis-open.org/archives/provision/200306/doc00000.doc

[10] Manish Verma, *Manage identities more effectively with SPML*, The objectives, architecture, and basic concepts of Service Provisioning Markup Language http://lists.oasis-open.org/archives/provision/200306/doc00000.doc

[11] Petr Tůma, *Co nového přinášejí moderní softwarové architektury?*, http://www.automa.cz/automa/2004/au060419.htm

[12] *About the World Wide Web Consortium* (*W3C*), http://www.w3.org/Consortium/

[13] *Requirements for a Global Identity Management Service*, A Position Paper from OneName Corporation for the W3C Workshop on Web Services, 11-12 April 2001, San Jose, CA USA, http://www.w3.org/2001/03/WSWS-popa/paper57

[14] E. Kuznetsov, Federated identity management and Web services, January 13, 2005, http://news.zdnet.com/2100-1009_22-5535345.html

[15] *XNS Addressing Specification v1.1*, http://www.oasis-open.org/committees/download.php/1832/xns-addressing-specification-v1.1.doc

[16] Web Services, Program Integration across Application and Organization boundaries, 2003, http://www.w3.org/DesignIssues/WebServices.html

[17] Ecma publishes key Web Services call control standard, ECMA, 2003, http://www.ecma-international.org/news/CSTA-WDSL%20final.htm

[18] Programmatic Access to Web Sites and Applications, 2002, http://www.oracle.com/technology/tech/webservices/htdocs/wsvsm/wshome.html

Annotation:

Identity managment

10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.

Tutoriál

10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.
10 až 15 řádků anglické anotace.