

Nasazení federací ve velkém distribuovaném prostředí: systém pro správu interakcí léků

DANIEL KOUŘIL, MARTIN KUBA, MICHAL PROCHÁZKA

Masarykova univerzita a CESNET
{kouril,makub,michalp}@ics.muni.cz

23.10.2007

Abstrakt

Koncept federací zavádí nový přístup ve správě přístupu uživatelů ke službám. Samotné služby již nemusejí spravovat uživatelské účty, tuto zodpovědnost přebírají domovské instituce uživatelů. Tím se celý systém stává decentralizovaný a není omezena jeho škálovatelnost. Uživatelé mohou využít paletu služeb za použití pouze jedné přihlašovací údaje, které navíc poskytují pouze své domovské instituci. Koncept federací jsme využili pro řešení problému jak zabezpečit přístup k systému pro správu interakcí léků, která musí být veřejně dostupná, ale zápis do ni mohou provádět pouze lékaři.

Klíčová slova: federace, shibboleth, radius

1 Úvod

Doba, kdy na Internetu byly dostupné pouze bezplatné služby a dostupné všem je se vzrůstající penetrací Internetu pryč. Placené a personalizované služby změnily pohled a požadavky na služby jako celek. Autentizace a autorizace uživatelů se stala nezbytnou součástí.

Absence jednotného standardu pro autentizaci a autorizaci zapříčinila situaci, kdy služby implementují vlastní bezpečnostní mechanismy. Případ, kdy několik služeb využívá stejný autentizační nebo autorizační mechanismus ještě neznamená, že uživatel bude mít k těmto službám přístup pomocí jedné přihlašovací údaje. Služby by musely sdílet správu uživatelů a to je samozřejmě u služeb, které provozují cizí subjekty velice nepravděpodobné.

Současný stav, kdy je uživatel nucen spravovat několik jednotek, ale i desítek přihlašovacích údajů je neudržitelný. Uživatelé si ve většině případů přihlašovací údaje zaznamenávají do souborů nebo na papírky a tím samozřejmě oslabují bezpečnost služeb.

Řešení, která předpokládala centrální správu uživatelů se ukázala jako nepoužitelná. Se vzrůstajícím počtem uživatelů se staly tyto systémy nespravitelnými.

Federace umožňují řešit výše zmíněné problémy. Jsou založeny na decentralizované správě uživatelů, kde každý uživatel má svého správce identity. Zároveň federace zvyšují bezpečnost autentizačního mechanismu tím, že uživatel vždy zadává své přihlašovací údaje pouze u své domovské instituce, i když přistupuje ke vzdáleným službám. Jelikož se uživatel autentizuje u své domovské instituce, ta může po úspěšné autentizaci předat službě atributy, které poskytují o uživateli dodatečné informace nutné k autorizačnímu rozhodnutí.

2 Model federovaných systémů

Informační systémy zpracovávají informace, které zpravidla nebývají veřejné a přístupné, ale přístup k nim je povolen jen specifikovaným uživatelům. Příkladem mohou být firemní systémy spravující vnitřní agendu organizace, databáze státních organizací se soukromými údaji občanů nebo systémy digitálních knihoven, které umožňují svým předplatitelům přístup k plným textům spravovaných dokumentů. Nedílnou součástí takových systémů samozřejmě musí být zajištění patřičné úrovně bezpečnosti, zejména spolehlivé autentizace a autorizace uživatelů. Správa uživatelů v takových systémech je zpravidla zcela autonomní a nepočítá s využitím v dalších systémech, ani s možností využít data o uživatelích z jiných stávajících systémů pro správu uživatelů, které obsluhují jiné organizace. Důsledkem této nezávislosti je nutnost registrovat všechny uživatele v databázi, která je součástí informačního systému. Pokud uživatel potřebuje využívat více takto nezávislých systémů, tak se musí zaregistrovat do všech. Ke každému systému samozřejmě obdrží samostatné přihlašovací údaje, které jsou určeny pouze pro přístup k tomuto systému a nelze je použít pro autentizaci k dalším systémům. Tato situace může vést až k faktickému oslabení bezpečnosti. Např. v případě, že autentizace je založena na použití hesla, lze předpokládat, že běžný uživatel bude používat stejné heslo pro přístup ke všem systémům. V případě kompromitování jednoho takového systému a prozrazení uživatelského hesla budou zranitelné i všechny systémy, které daný uživatel takto používá. Situace bude o to horší, že systémy jsou autonomní, nevědí o sobě a administrátoři nejsou informováni ani o kompromitaci jiného systému ani o tom, že byl používán také jejich uživatelem a že tedy může být potřeba nasadit nějaká ochranná opatření.

I když odhlédneme od těchto potenciálních bezpečnostních problémů, stále zůstává pro uživatele nutnost registrace do používaných systémů. Tato registrace často představuje administrativní zátěž jak pro uživatele, tak i pro správce systému. Nežádá se nutně, aby se uživatel dostavil osobně na kontaktní místo, případně doručil nějaká papírová potvrzení apod. Po registraci je navíc nutné údaje udržovat a kontrolovat, že odpovídají skutečnosti. Každá změna údajů se musí promítnout do všech informačních systémů, ve kterých je uživatel zaregistrován. Vzhledem k nezávislosti systémů je nahlášení změny zpravidla výhradně odpovědností samotného uživatele, což nemusí být příliš spolehlivé. Uživatel

může buď zapomenout na některý ze systémů nebo změnu dokonce úmyslně zatajit.

Popsaný stav je možné zvládnout pokud se jedná o několik málo jednotlivých samostatných systémů. Situace se ale rapidně zhoršuje se zvyšujícím se počtem systémů, do kterých je uživatel takto zapojen. V následujících letech lze očekávat, že spíše poroste počet systémů, které nabízejí služby autentizovaným uživatelům, a proto se hledají cesty pro efektivnější správu uživatelských informací. Slibný pokrok v této oblasti nabízí model federací, který umožňuje oddělit správu uživatelů od vlastního přístupu k informacím v systému a umožňuje sdílení informací o spravovaných uživateli s dalšími informačními systémy ve federaci.

Hlavní myšlenka federacíního uspořádání je založena na faktu, že zpravidla každý uživatel spadá pod nějakou „domovskou“ organizaci, která o něm spravuje informace ve svém systému. Takovou organizací je např. škola v případě studentů nebo zaměstnavatel v případě zaměstnanců. Domovská organizace ve vlastním zájmu pečuje o to, aby spravovaná data byla aktuální, protože to potřebuje pro zajištění své provozní agendy (výplaty mezd, organizaci studia, apod). Organizace také zpravidla pro své uživatele provozují informační systémy, včetně sekcí s řízeným přístupem, kam se uživatelé musí přihlásit pomocí autentizačních mechanismů a údajů získaných od své instituce. Federací model umožňuje využít informací spravovaných domovskou institucí i informačními systémy, které nejsou s touto institucí přímo propojeny, ale které jsou zapojeny v infrastruktuře pro výměnu dat o uživateli – „federaci“. Systémy zapojené do federace jsou schopné získat informaci o uživateli přímo z jeho domovské instituce, kde je největší záruka toho, že informace jsou aktuální a není tedy potřeba aby si udržovaly vlastní systémy spravující uživatelské záznamy. Takové uspořádání navíc usnadňuje práci i samotným uživatelům, protože ti se vždy prokazují pouze autentizačními údaji, které používají pro přístup do svého domovského systému. Infrastruktura federace pak zajistí, že systémy si mezi sebou předávají potřebné údaje, tato komunikace je však pro uživatele transparentní.

2.1 Založení a provoz federace

Ustavení federace probíhá v několika krocích. Z technického pohledu je potřeba, aby se zúčastněné organizace dohodly na jednotném rozhraní, kterým budou získávat informace z institucí. Toto rozhraní (tzv. *Identity Provider*) pak nabízí každá zapojená instituce poskytující data o svých uživateli, zpravidla ve formě specializované služby běžící nad vnitřním systémem správy uživatelů. Identity Provider nabízí data o uživateli, která jsou využívána koncovými službami ve federaci (*Service Providers*). Tyto informace lze rozdělit do dvou kategorií, jednak je to binární informace o tom, zda daný uživatel prošel autentizačním mechanismem na domácí instituci a jednak je to množina *atributů*, které poskytují upřesňující informace o uživateli. Atributy mohou určovat např. kategorii poměru uživatele k instituci (např. zda se jedná o studenta, akademického pracovníka nebo pracovníka administrativy), zpřesňovat kategorii zaměstnání (lékař, uklízečka), určovat vztah k vnitřní struktuře organizace (člen konkrétní

fakulty), apod. Pomocí těchto atributů pak koncové služby mohou provádět komplexní řízení přístupu. Dnes je například obvyklé, že fakulta zakoupí pro své zaměstnance a studenty přístup k odborným textům v nějaké digitální knihovně. V současné době je řízení přístupu v této oblasti založeno na síťových IP adresách, kdy je přístup povolen, pokud uživatel přistupuje ke knihovnímu systému z předem specifikovaného rozsahu IP adres. Samozřejmě tento přístup není ideální ani pro provozovatele knihovny (protože přístup tak mohou mít i uživatelé, na které se licence nevztahuje), ani pro uživatele (protože jsou buď omezeni na práci ze své organizace nebo musí složitě konfigurovat různé síťové tunely apod.). Pokud by poskytovatel knihovny a příslušná fakulta byly součástí federované infrastruktury, mohl by poskytovatel obsahu povolit přístup jen pro uživatele, kteří mají ve svých atributech specifikovanou příslušnost k dané fakultě, resp. i pracovní zařazení (např. s požadavkem, že se musí jednat pouze o studenty, či akademické pracovníky).

Dále je potřeba dohodnout způsob předávání atributů, kdy existují dva základní přístupy. Prvním je tzv. push model, ve kterém klientská část zajistí získání potřebných dat o uživateli, která následně pošle na server spolu s požadavkem na přístup k aplikačním datům. Druhou možností je pull model, ve kterém je aktivní server, který kontaktuje uživatelský domovský systém poté, co obdrží požadavek od klienta. V současné době existuje několik nástrojů implementujících tyto modely a na základě vyhodnocení konkrétních požadavků na funkci federace, lze z těchto nástrojů vybrat nejvhodnější řešení. Do oblasti vzájemné komunikace mezi systémy patří samozřejmě problematika bezpečnosti, protože systémy s uživatelskými informacemi často obsahují data podléhající předpisům o ochraně osobních údajů a přístup k nim by tedy měl být omezen pouze na vybrané služby. Je tedy často nutné zajistit i šifrování těchto dat během přenosu. I v případě, že předávaná data nejsou citlivého charakteru, je nutné zajistit minimálně jejich integritu tak, aby příjemce mohl ověřit, že data nebyla během přenosu změněna. Opět existuje několik mechanismů pro implementaci požadovaných bezpečnostních kritérií. Většina federací využívá elektronické podpisy a infrastrukturu veřejných klíčů [1], která je velmi dobře škálovatelná i s velkým počtem zapojených institucí.

Přistupuje-li uživatel ke službě, musí nějakým způsobem poskytnout informaci, kde je jeho Identity Provider. K tomuto účelu slouží služba WAYF (*Where Are You From*). Tato služba je předřazena přístupu ke každé službě v rámci federace, uživatel zde vybere ze seznamu všech Identity Providerů celé federace toho, kdo provede jeho ověření. Služba WAYF je pevně svázána s federací, protože musí pracovat s aktuálním seznamem Identity Providerů.

Další oblastí, kterou je potřeba definovat během zakládání federační infrastruktury je tzv. schéma atributů, které specifikuje jaké atributy popisující uživatele jsou pro danou federaci zajímavé a potřebné. Je potřeba dohodnout syntax těchto atributů i jejich přesnou sémantiku. Praktické zkušenosti ukazují, že zejména tato druhá část je velmi problematická, protože každý zapojený člen federace má trochu odlišnou interpretaci atributů. Příkladem může být atribut `eduPersonAffiliation` ze schématu `eduPerson`, které vzniklo pro popis atributů

člena akademické instituce. Atribut `eduPersonAffiliation` popisuje zařazení v rámci organizace, např. student, zaměstnanec, učitel. Zde vyvstávají otázky typu „je učitel zároveň zaměstnanec?“, apod. Zatím neexistuje shoda na mezinárodní a často ani na národní úrovni o přesné sémantice jednotlivých atributů.

Federace přináší možnost efektivního přístupu k uživatelským záznamům, ale také zavádějí nový model důvěry, kdy služba (Service Provider) přestává nést zodpovědnost za správu uživatelů, kteří ji využívají. Tato zodpovědnost je delegována na domovské instituce uživatelů a služba tak ztrácí přímý vliv na fungování této složky. Nezbytnou součástí každé produkční federace tedy musí být specifikace politik, které se všechny jednotlivé organizace zavází dodržovat při implementaci. Přesná podoba politik závisí na zamýšleném zaměření federace. Politiky mohou být specifikovány neformální dohodou zúčastněných stran, ale také to mohou velmi podrobné dokumenty popisující přesné procedury, které jsou pro provoz systémy používány. Z definice federálního prostředí musí organizace při zapojení do federace souhlasit s tím, že bude informace o svých uživateli zpřístupňovat všem poskytovatelům služeb ve federaci.

2.2 Federace z uživatelského pohledu

Federované prostředí je velmi příjemné pro uživatele, protože jim stačí jediná sada přihlašovacího údaje pro přístup ke všem systémům zapojeným ve federaci. Přístup k dnešním informačním systémům je často založen na protokolu HTTP, který podporuje mechanismus přesměrování, kdy server může odkázat klientský prohlížeč na jinou adresu, kterou je nutné navštívit před použitím samotné služby. Díky tomuto mechanismu může Service Provider odkázat uživatele nejprve na stránku jeho domovské organizace, kam se uživatel nejprve přihlásí. Po úspěšné autentizaci je opět jeho prohlížeč přesměrován na původní Service Provider s tím, že jako součást přesměrování je předána informace o uživateli. Tuto informaci použije Service Provider pro řízení přístupu k poskytované službě.

Uživatelé na tomto mechanismu ocení zejména to, že se vždy autentizují pomocí své domovské webové aplikace, na kterou jsou zvyklí, a to i v případě, že požadují přístup ke službě, která není provozována jejich domovskou organizací. Mají tak pouze jednu sadu přihlašovacího údaje pro přístup ke všem systémům, které jsou zapojené ve federaci. Vedle toho, že takové uspořádání je uživatelsky příjemné, poskytuje i větší bezpečnost. Uživatelé si totiž zvyknou zadávat údaje vždy na jediné aplikaci, která má stálý vzhled. Po náležitém proškolení tak vzrůstá pravděpodobnost, že uživatelé nebudou automaticky zadávat přihlašovací údaje do všech aplikací, které od nich tyto údaje mohou vyžadovat. Pěstování těchto „hygienických návyků“ je velice užitečné, zejména v době, kdy vzrůstá počet phishingových útoků, které lákají z uživatelů citlivá data.

Víceméně jako vedlejší efekt poskytují federace možnost anonymizace, kdy Identity Provider nezpřístupňuje službám jméno uživatele, ale předává pouze jeho atributy, případně jednoznačný identifikátor uživatele, který však nenese informace o jeho skutečné identitě. Uživatel tak nadále může přistupovat ke službám, které omezují přístup jen na určitou množinu uživatelů (definovanou

jejich atributy), ale koncová služba se přímo nedozví identitu konkrétních klientů.

3 Implementace federací

Výše jsme zmínili, že existuje několik přístupů k implementaci federací. V oblasti přístupu k počítačovým sítím je hojně používána služba Radius [2]. Naopak v oblasti webu je nejčastěji používán middleware Shibboleth [3].

3.1 Radius

Radius server (Remote Authentication Dial In User Service) je určen k ověřování identity uživatelů, dále provádí autorizaci uživatelů a accounting. Radius protokol umožňuje vzdálené ověření uživatele, identitu uživatele nejčastěji ověřují síťové prvky jako jsou bezdrátové přístupové body nebo síťové switche.

Radius servery využívané k vytvoření federace jsou seskupeny do hierarchie, kde na nejvyšší úrovni jsou definovány top-level radius servery, dále každá větší organizační složka provozuje vlastní radius servery a samozřejmě je má i každá koncová instituce. Radius servery v cílových organizacích zajišťují ověření identity vlastních uživatelů. Národní a top-level radius servery se starají o předávání autentizačních požadavků. Pokud na jakýkoliv radius server přijde požadavek na ověření identity uživatele, je z jeho uživatelského jména vyextrahován realm, který určuje uživatelskou instituci. Jedná se tedy o implicitní WAYF, kdy je domovský server uživatele specifikován transparentně bez uživatele explicitního zásahu. Pokud není požadavek schopen ověřit tento radius server, pak je přeposlán na nadřazený server.

V případě, že chce uživatel přistoupit k síti připojí se k přístupovému bodu nebo switchi, který kontaktuje lokální radius server. Radius server ověří identitu uživatele proti databázi uživatelů, pokud se jedná o domácího uživatele, v opačném případě je požadavek přeposlán dále do federace radius serverů až k jeho domácímu radius serveru. Mezi uživatelem a domácím radius serverem se vytvoří zabezpečený tunel přes infrastrukturu radius serverů, kterým jsou poslány přihlašovací údaje. Domácí radius server výsledek ověření uživatele pošle zpět přístupovému prvku, který na jeho základě uživatele vpustí nebo nepustí do sítě.

3.2 Shibboleth

Systém Shibboleth je primárně určen do webového prostředí, tzn. přístup k webovým stránkám a webovým službám. Federace postavená na middleware Shibboleth se sestává z jednoho centrálního místa, které udržuje tzv. metadata nesoucí informace o všech poskytovatelích identit (Identity Providers) a služeb (Service Providers) a zároveň poskytuje službu WAYF.

Identity Providers stejně jako v případě Radius ověřují identitu uživatelů, ale zároveň poskytují v autentizační odpovědi atributy o uživateli. Hodnoty atributů jsou čerpány z databáze uživatelů udržované domovskou organizací, hodnoty

atributů mohou být také generovány až ve chvíli autentizace uživatele a mohou se lišit i podle toho, ke které službě uživatel přistupuje.

Autentizační proces systému Shibboleth sleduje model popsany v kapitole 2., včetně použití přesměrování na úrovni protokolu HTTP. Současná implementace Shibboleth také nepodporuje Single Sign-On (SSO), tuto funkcionalitu musí zajistit externí služba, která je provozována současně s IdP.

3.3 Existující federace

Nejznámější federací, která je provozována nadnárodně (v současné době zahrnuje skoro celou Evropu spolu s Japonskem a Austrálií) je Eduroam [4]. Tato federace je budována za účelem podpory mobility akademických pracovníků a usnadnění připojení k počítačové síti během jejich cest. Nejčastěji je EduRoam využíván pro přístup k bezdrátovým sítím. Celá federace je stavěna na recipročním principu, kdy instituce, která umožní svým uživatelům využívat služeb federace musí poskytnout pro uživatele ostatních institucí přístup do počítačové sítě ve svých prostorách. Z konceptu federací využívá Eduroam pouze decentralizovanou správu uživatelů a autentizaci. Ve federaci Eduroam se nepřenáší žádné atributy o uživateli, poskytovatele služeb (přístup do sítě) pouze zajímá, zda uživatel patří do nějaké instituce v rámci federace. Eduroam middleware používá infrastrukturu Radius serveru (viz 3.1).

Federace, které umožňují i autorizaci na úrovni služeb a jsou orientovány na prostředí webu, dnes existují pouze na národní úrovni. Příkladem může být akademická federace ve Švýcarsku – SWITCH¹. Tato federace byla založena jako jedna z prvních a podařilo se do ní zapojit valnou většinu švýcarských vysokoškolských institucí. V současné době provozují třináct služeb v rámci federace, převážně se jedná o e-learningové programy. Další významnou federací je americká InCommon², která zastřešuje 36 vysokoškolských institucí. V Evropě existuje ještě několik úspěšných federací, ve Finsku provozují federaci pro vysoké školy Haka³, ve Velké Británii UKFederation⁴. Výše zmíněné federace využívají jako middleware Shibboleth (viz kap. 3.2). Další velká a produkčně nasazená federace je norská FEIDE⁵, ta oproti ostatním využívá jako middleware Sun Federation Manager⁶. Oba middlewary budou v nových verzích využívat protokol pro předávání informací SAML 2.0 [5], což zajistí vzájemnou interoperabilitu, která je dnes zajišťována pomocí pluginů a specifických úprav v obou systémech. Ve všech zmíněných federacích jsou nejčastěji zastoupeny služby pro přístup k elektronickým zdrojům a různým informačním systémům. V současné době se správci národních federací nejvíce zabývají rozšířením, integrací nových poskytovatelů služeb a tvorbou dokumentů, které definují politiky a postupy.

V České republice vzniká federace akademických institucí, která je založena

¹<http://www.switch.ch/aa1>

²<http://www.incommonfederation.org>

³<http://www.csc.fi/english/institutions/haka>

⁴<http://www.ukfederation.org.uk/>

⁵<http://feide.no/index.en.html>

⁶http://www.sun.com/software/products/federation_mgr/index.jsp

na systému Shibboleth. V současné době je k dispozici ověřovací implementace této federace pod názvem CZTestFed⁷, která poskytuje IdP šesti institucím a devět služeb, které slouží primárně k demonstračním a testovacím účelům.

3.4 Problémy federací

Federace jako každý koncept má i své problémy. Shoda na definici atributů patří k nejvíce diskutovaným problémům. Problém s atributy ve schématu eduPerson již byly zmíněny, proto v rámci Trans-European Research and Education Networking Association (TERENA) vznikla skupina, která se zabývá harmonizací významu atributů mezi akademickými institucemi a zajišťuje definici postupů pro registraci nových atributů.

S atributy je svázán také problém požadavků na atributy od poskytovatelů služeb. Se vzrůstajícím počtem poskytovatelů obsahu a jejich různorodosti vznikají požadavky na další atributy zasílané od IdP pro možnost větší granularity autorizace. Tyto požadavky vedou k neškálovatelnému řešení, kdy IdP má definována pravidla pro vydávání atributů pro různé poskytovatele.

Decentralizace na úrovni správy identit a autentizace je velkou výhodou federací, bohužel i toto schéma má své negativní stránky. Pokud uživatelé nepřistupují ke službám z kontrolovaného prostředí, pak nemají jistotu, zda přihlašovací údaje zadávají své domovské instituci.

4 Federace v medicínském prostředí

V rámci projektu MediGrid⁸ jsme narazili na problém, který je současnými nástroji takřka neřešitelný, ale který lze elegantně vyřešit pomocí federovaného uspořádání. Tímto problémem je správa přístupu k informačnímu systému, který udržuje informace o interakcích mezi léky a který je nutné neustále rozvíjet a přidávat k němu nově objevené interakce. Současná legislativa přikazuje každému lékaři hlásit nově objevenou interakci tak, aby byla dostupná všem ostatním lékařům i veřejnosti. V současné době však není k dispozici informační systém, který by uživatelům dovozoval taková data udržovat a vyhledávat v databázi známých interakcí. Primárním důvodem proč takový systém neexistuje je absence mechanismů, které by umožňovaly poznat lékaře mezi všemi uživateli, kteří k systému přistupují. Systém z principu svého fungování musí fungovat jako obecně dostupná služba, odkud informace může číst kdokoli, ale pouze lékaři jsou oprávněni data vkládat a měnit. Veškeré změny musí samozřejmě být auditovatelné tak, aby bylo možné dohledat uživatele, který změnu provedl. Jak jsme diskutovali v předchozí části příspěvku, není samozřejmě reálné vybavit všechny lékaře jménem a heslem nebo jinými autentizačními údaji, které budou určeny pro přístup k takovému systému.

Správa interakcí není jediným systémem, ke kterému je potřeba řídit přístup na základě profesních atributů. Lékařská komunita například využívá služeb

⁷<https://cztestfed.feld.cvut.cz>

⁸www.medigrid.cz

portálu www.mediclub.cz, který ale obsahuje informace, které by měly být přístupné pouze lékařské veřejnosti. V současnosti se problém omezení přístupu řeší čestným prohlášením uživatele, při prvním přístupu na stránku, což samozřejmě není nijak spolehlivá metoda ověření.

Současné technologie tedy neposkytují dostatečné nástroje pro spolehlivou realizaci řízení přístupu k těmto lékařským systémům. Na druhou stranu se ovšem přímo nabízí využít federační technologie a na nich založených mechanismů pro správu uživatelů a řízení přístupu.

4.1 Budování systému pro správu interakcí

V rámci projektu MediGrid jsme se tedy rozhodli vybudovat experimentální systém založený na federačním modelu, který bude nabízet manipulaci s informacemi o interakcích léků. Tato aktivita má sloužit třem hlavním cílům:

1. lékařům umožní vyzkoušet systém pro správu informací o interakcích
2. seznámí uživatele (tj. především lékaře) s mechanismy federací
3. poskytne potřebnou zpětnou vazbu, kterou budeme moci využít pro návrh dalších systémů, založených na federačním uspořádání

Vzhledem k tomu, že cílem je primárně demonstrovat použitelnost federačních technik, je funkcionální vlastnosti aplikace poměrně jednoduchá. Jejím primárním úkolem je umožnit lékařům zadávat interakce ke dvěma lékům a takto zadané informace spravovat v databázi, jejíž obsah je veřejně přístupný. V současné době je hotová ověřovací implementace této služby, která realizuje popsanou funkcionálníitu přes webové rozhraní⁹. V současné době jsou informace o lécích a jejich interakcích dynamicky stahovány z veřejné databáze Státního ústavu pro kontrolu léčiv (SÚKL). Pomocí webového formuláře uživatel nejprve zadá názvy dvou léků o jejichž vzájemnou interakci se zajímá. Protože zpravidla existuje více léků stejného jména (např. od různých výrobců), aplikace nabídne uživateli seznam všech registrovaných léků, které mají stejný název a uživatel si zvolí požadovaný lék podle jeho kódu. Následně aplikace zobrazí ke každému léku popis jeho interakcí. Pro léky, které nemá aplikace ve své databázi se zobrazí informace získané z veřejně dostupných informací na SÚKL.

Pro zobrazení těchto informací nejsou potřeba žádná specifická oprávnění a informace jsou veřejně přístupné. Pokud si však uživatel přeje změnit stávající popis interakce nebo přidat nový, musí prokázat, že je lékařem. K tomuto účelu jsme naši aplikaci napojili na federaci CZTestFed, která spravuje informace o uživateli ze zapojených institucí. Napojení na federaci CZTestFed je realizováno pomocí softwarového vybavení, které nabízí projekt Shibboleth. Zejména se jedná o démon `shibd`, který je zodpovědný za komunikaci s IdP uživatele a získávání jeho atributů. Pomocí těchto nástrojů jsme realizovali proces přihlašování k naší aplikaci, který je aktivován, pokud uživatel chce měnit interakce. Autentizace tak odpovídá standardnímu procesu ve federačním

⁹<https://www.medigrid.cz/interakce/>

prostředí, kdy je uživatel nejprve přesměrován na svou domovskou instituci, kde se autentizuje a poté je jeho prohlížeč přesměrován zpět na aplikaci. Aplikace si poté vyžádá atributy o uživateli od jeho domovského IdP a provede rozhodnutí o poskytnutí přístupu ke službě. Jelikož právo měnit záznamy mají pouze lékaři, aplikace musí vyhodnotit, zda daný uživatel je lékařem. Přesná podoba vyhodnocování není ještě ustálená a může se také lišit pro jednotlivé IdP. V současné době za lékaře považujeme držitele titulu MUDr., tj. uživatele v jehož attributech je položka „titul“ obsahující řetězec MUDr.

Pro nasazení v lékařském prostředí samozřejmě musíme mít IdP na každé instituci, která lékaře organizačně spravuje. V pilotní fázi aktivity usilujeme o ustavení takové služby u nemocnic, které se účastní projektu MediGrid. Každá z těchto institucí spravuje svůj informační systém, ke kterému poskytuje autentizovaný přístup svým uživatelům a ve kterém spravuje informace o uživateli, zejména o tom, zda pracují jako lékaři. Vedle tohoto systému lze postavit samostatný IdP, který bude přebírat část dat z hlavního systému a zpřístupňovat je poskytovatelům služeb ve federaci. V současné době je v ověřovacím provozu IdP Masarykovy nemocnice v Ústí nad Labem, od jehož provozu očekáváme získání zkušeností pro nasazení IdP i v jiných lékařských zařízeních.

Díky federační infrastruktuře bude služba pro správu interakcí otevřena všem lékařům ze zapojených institucí. Vzhledem k autentizaci bude možné provádět audit změn, tj. sledovat kdo provedl kterou změnu v seznamu interakcí. V pilotní fázi bude systém otevřen pro uživatele, jejichž organizace poskytuje IdP kompatibilní se systémem Shibboleth. Pro uživatele, kteří nejsou pokryti takovou službou poskytneme nezávislý IdP umožňující uživatelům přístup k omezené funkcionalitě aplikace tak, aby mohli lépe pochopit jak její principy, tak i základy federačních mechanismů. Tato služba bude založena na IdP, který provozujeme pro účastníky projektu METACentrum.

5 Závěr

V příspěvku jsme představili model federací, který lze využít pro efektivní správu uživatelů v rozsáhlém distribuovaném prostředí. Popsali jsme problém správy interakcí léků, který nelze reálně řešit současnými prostředky a popsali aktivitu pro implementaci takového systému nad federačním modelem.

Poděkování

Tento výzkum je podporován z prostředků výzkumného záměru "Optická síť národního výzkumu a její nové aplikace" (MSM6383917201) a výzkumného projektu "MediGrid - metody a nástroje pro využití sítě Grid v biomedicíně" (Akademie věd ČR, grant T202090537).

Annotation

Deployment Federations in Large Distributed environment: a System for Drugs Interaction Management

We provide an overview of the federalization model and describe how federations can be used to address problems that cannot be solved using current tools. Then we describe a system for management of drugs interactions allowing physicians to maintain information on drugs. The systems demonstrates how federations can be used to implement an easy-to-use application without the need distribute new sets of credentials.

Reference

- [1] R. Housley, W. Polk, W. Ford, D. Solo. “Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile”. IETF RFC 3280. April 2002.
- [2] C. Rigney, S. Willens, A. Rubens, W. Simpson. “Remote Authentication Dial In User Service (RADIUS)”. IETF RFC 2865. June 2000.
- [3] S. Cantor. “Shibboleth Architecture – Protocols and Profiles”. 10 September 2005.
<http://shibboleth.internet2.edu/shibboleth-documents.html>
- [4] L. Florio, K. Wierenga. “Eduroam, providing mobility for roaming users”. In *Proceedings of the EUNIS 2005 Conference*, Manchester, 2005.
- [5] S. Cantor, J. Kemp, et al. “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0”. Organization for the Advancement of Structured Information Standards (OASIS), Billerica, MA, 2005.
<http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>