Federace identitaneb spolčení totožností

Daniel Kouřil, Martin Kuba,Martin Osovský, Radim Peša, Michal Procházka, ÚVT MU

Masarykova univerzita, stejně jako většina organizací, provozuje své interní webové informační systémy. Uživatelé, tj. zaměstnanci a studenti organizace, se do těchto aplikací přihlašují svými autentizačními údaji, kterými jsou obvykle jméno a heslo. Jedná se o standardní léty ověřená řešení, která v rámci jedné organizace svou funkcionalitou vyhovují.

Avšak v případě, že překročíme hranice jedné organizace, záhy narazíme na limity těchto řešení. Například pokud chceme provozovat webovou aplikaci dostupnou právě vybraným uživatelům různých vysokých škol, obvykle nezbude než pro všechny zúčastněné uživatele založit nové uživatelské účty včetně nového jména a hesla, u nichž nemáme možnost nijak využít žádné z údajů, které o uživatelích vedou jejich mateřské instituce. Nemluvě o tom, že nešťastným uživatelům přibude do sbírky další dvojice přihlašovacích údajů. Pokud se jedná o malý počet zúčastněných uživatelů, účty se jim metodou hrubé síly zřídí, protože jiná cesta prostě neexistuje. Ale pokud bychom chtěli například provozovat aplikaci dostupnout právě všem studentům medicíny v České republice, jednalo by se o úkol prakticky neřešitelný. A právě mimo jiné takovouto třídu úloh je velmi vhodné a ve výsledku i snadné řešit pomocí *federací identit* (anglicky *identity federation*, podle slovníku *spolčení totožností*).

V tomto článku popisujeme model federativních mechanismů pro autentizaci (ověření totožnosti) a autorizaci (povolení přístupu), který umožňuje oddělit správu uživatelů a jejich autentizaci od vlastní aplikace a standardizuje sdílení informací o uživatelích mezi organizacemi ve federaci. Aplikace tak mohou být jednodušší a zároveň poskytovat uživatelům pohodlné použití, protože uživatelé se mohou ve všech aplikacích autentizovat jedinou domovskou sadou přihlašovacích údajů. Zároveň mohou implementovat autorizaci založenou na aktuálních informacích o uživatelích, které jsou poskytovány z jejich domovských institucí. Údaje o uživatelích nejsou duplikovány pro účely jednotlivých aplikací a o jejich aktuálnost se stará ten nejpovolanější tj. domovská instituce.

Současné systémy nejčastěji řeší správu uživatelů a řízení jejich přístupu k poskytovaným službám každý zvlášť a nepočítají s jejich využitím v dalších systémech ani s možností využít data o uživatelích ze stávajících systémů provozovaných jinými organizacemi. 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 určené 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.

Ve větších institucích si potřeba správy většího množství uživatelů a systémů vynutila využití nějakého systému pro centrální správu uživatelů, nejčastěji ve formě webového Single Sign-On řešení (WebAuth, CoSign, CAS, atd.). Na MU je možnost využití databáze uživatelů a hesel IS MU pomocí vlastního SSO řešení zvaného BCA Autentizace.

Obecnou nevýhodou těchto systémů je orientace výhradně na autentizaci (navíc v případě MU vždy řešenou na aplikační úrovni). Tyto systémy obvykle neposkytují standardní cestu pro přístup k dalším informacím o uživateli, které mohou být potřebné pro autorizaci (např. pří-

slušnost ke konkrétní fakultě, předmětu, zda je student, učitel, neakademický zaměstnanec).

Dalším omezením je omezení působnosti pouze na lokální prostředí organizace. Uživatelé, kteří chtějí používat aplikaci provozovanou mimo MU, musí být vždy registrováni v koncovém systému a dostat (a spravovat) tak další autentizační data, například v naduniverzitních projektech. Podobně, pokud s aplikacemi na MU chce pracovat uživatel, který není registrován v IS MU, je nutné uživatele buď zavést do systému (se stejným problémem pro uživatelské pohodlí jako výše) nebo v horším případě řešit jeho přístup ad-hoc způsobem. Navíc v tomto případě nemáme reálnou možnost, jak ověřovat, že uživatelská data jsou pravdivá, případně aktuální po celou dobu jejich existence.

1 Federační model

Hlavní myšlenka federačního 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. Federační 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 uživatelích – „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 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.

Pro ustavení federace je nutné, aby se zúčastněné organizace dohodly na jednotném rozhraní, kterým budou získávat informace z institucí. Toto rozhraní (tzv. *Identity Provider*, IdP, poskytovatel identit) pak nabízí každá zapojená instituce poskytující data o svých uživatelích, zpravidla ve formě specializované služby běžící nad vnitřním systémem správy uživatelů. Identity Provider nabízí data o uživatelích, která jsou využívána koncovými službami ve federaci (*Service Providers*, SP, poskytovatelé služeb). Tímto standardizovaným způsobem mohou koncové služby získávat informace o svých klientech, které lze použít pro následné řízení přístupu. Takto poskytované *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. Autorizace na těchto atributech lze s výhodou použít např. na straně poskytovatelů digitálních knihoven s placeným přístupem. 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.). Řada poskytovatelů těchto zdrojů proto nabízí napojení na federační infrastrukturu, která umožňuje přístup k atributům o konkrétním uživateli, což je výhodnější pro obě strany.

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 přinášejí 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 zavážou dodržovat při implementaci. Přesná podoba politik závisí na zamýšleném zaměření federace. Politiky mohou být specifikovány neformální dohodou zúčastněných stran, ale také to mohou být velmi podrobné dokumenty popisující přesně procedury, které jsou systémy používány pro provoz. Z definice federačního prostředí musí organizace při zapojení do federace souhlasit s tím, že bude informace o svých uživatelích zpřístupňovat všem poskytovatelům služeb ve federaci.

Federované prostředí je velmi příjemné pro uživatele, protože jim stačí jediná sada přihlašovacích údajů 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 zprvu 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 přihlašovacích údajů 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.

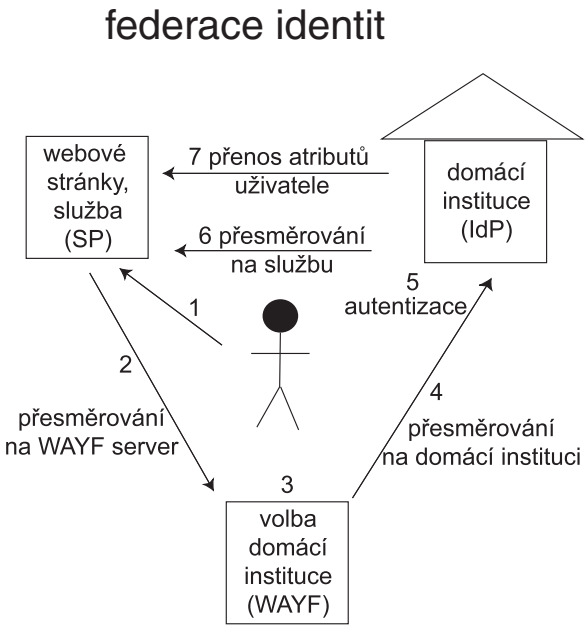
1.1 Shibboleth

Mezi nejpoužívanejší systémy implementující federační model patří middleware Shibboleth[1], který se používá pro zabezpečení přístupu k webovým aplikacím a podpoře SSO ve webovém prostředí. Shibboleth vyvíjí aktivita Internet2 a jsou na něm založeny akademické federace ve Švýcarsku (SWITCH), USA (InCommon), Velké Británii (UK Federation) a jinde.

Schéma systému Shibboleth je znázorněno na obr. 1. Na počátku je uživatel, který použije webový prohlížeč pro přístup k webové službě zabezpečené systémem Shibboleth (krok 1). Jelikož uživatel dosud není autentizovaný, jeho prohlížeč je přesměrován na službu WAYF (krok 2),

[1] `http://shibboleth.internet2.org/`

která uživateli nabídne seznam institucí a jejich poskytovatelů identit. Po výběru své domovské instituce je uživatelův prohlížeč přesměrován na příslušnou stránku instuce (kroky 3 a 4), kde se autentizuje pomocí svého běžného jména a hesla, které používá pro přístup k lokálním systémům (krok 5). Po úspěšné autentizaci je prohlížeč nakonec přesměrován zpět na původní webovou aplikaci (krok 6), která tak dostane informaci o uživatelově úspěšné autentizaci a může také požádat uživatelovu instituci o poskytnutí dodatečných atributů. Tyto atributy jsou poskytnuty ve formě dokumentu v jazyce SAML (Security Assertion Markup Language, založen na XML) a dočasně uloženy na straně poskytovatele služby. Na základě těchto informací a lokální politiky pak služba rozhodne o povolení přístupu uživatele. Explicitní autentizační mechanismus složený z kroků 2 až 6 uživatel absolvuje pouze při přístupu k první službě v rámci jedné seance, všechny další přístupy k dalším službám jsou již autentizovány implicitně, a uživatel tak nemusí opakovaně zadávat své přihlašovací údaje.



Obrázek 1: Postup při přihlašování ve federaci

2 Federace CZTestFed

V České republice byly základy národní akademické federace identit položeny v dubnu 2007 propojením dvou institucí CESNET a ČVUT FEL. Tím vznikla testovací federace czTestFed využívající middleware Shibboleth. Později se postupně do federace czTestFed zapojili poskytovatelé identit dalších akademických institucí. V současné době jsou členy federace METACentrum, Masarykova univerzita, Karlova univerzita, Západočeská univerzita a již zmíněný CESNET a ČVUT FEL. Mimo těchto poskytovatelů identit je do federace zapojeno také několik aplikací (poskytovalů služeb), zatím převážně testovacího charakteru. Jejich seznam a další podrobnosti o federaci czTestFed jsou uvedeny na www stránkách federace[2]. V současné době se připravuje přechod federace z testovací fáze do fáze pilotního provozu se skutečnými údaji o uživatelích, a příprava na zapojení reálných aplikací.

Masarykova univerzita je do federace czTestFed zapojena od června 2007, kdy byl zprovozněn poskytovatel identit pro osoby z MU. V průběhu měsíce října byla na MU zprovozněna i první aplikace využívající federační autentizační mechanismy. Jedná se o aplikaci pro zřizování guest účtů, která je blíže popsaná na konci článku v části 4.3.

V budoucnu se očekává využití federativních mechanismů především pro přístup k placeným elektronickým informačním zdrojům, ale je pravděpodobné, že najdou využití i v řadě dalších aplikací.

3 Konfigurujeme poskytovatele služeb

Jak již bylo řečeno, Masarykova univerzita má zprovozněného svého poskytovatele identit. Co je tedy dalšího potřeba pro využití autentizační a autorizační infrastruktury na bázi Shibboleth v konkrétní webové aplikaci? Je potřeba nainstalovat a zkonfigurovat softwarovou komponentu poskytovatele služeb (Shibboleth Service Providera, SP) pro příslušný server. SP existuje pro www servery Apache a IIS. Skládá se z Apache modulu, démona shibd (respektive ISAPI filtru a služby shibd v případě IIS) a souvisejících konfiguračních souborů.

Klíčovou částí Shibboleth SP je Apache modul (resp. ISAPI filtr), který zpracovává požadavky

[2] `https://cztestfed.feld.cvut.cz/`

na přístup do chráněných oblastí webové aplikace. Pokud není uživatel autentizován, modul přesměrovává jeho požadavek na WAYF stránku, případně přímo na stránky poskytovatele identity. Poté co se uživatel na stránkách svého poskytovatele identit autentizuje, je přesměrován zpět do oblasti chráněné webové aplikace. Modul prostřednictvím démona shibd kontaktuje poskytovatele identit a získá dostupné uživatelské atributy. Díky tomu získává modul k dispozici informace jak o autentizaci uživatele, tak o uživatelských atributech potřebných k autorizačnímu rozhodnutí.

Instalace Shibboleth Service Providera není náročná. Pro Windows je instalace připravena v podobě balíku Microsoft instaleru (msi), pro Debian Linux je připraven debiánovský balíček, pro Red Hat balík RPM atd. Samozřejmě jsou k dispozici i zdrojové kódy k případné kompilaci pro zvolenou platformu. Po instalaci a základní konfiguraci je potřeba informovat ostatní členy federace o existenci nového poskytovatele služeb. To se provede přidáním informací o poskytovateli služeb do *federačních metadat*, což je seznam všech poskytovatelů identit a služeb ve federaci.

Po ukončení instalace a zapojení poskytovatele služeb do federace můžeme začít řídit přístup k chráněným souborům. To můžeme provést například pomocí direktiv v souboru `.htaccess`. Přímočarost konfiguraci si můžeme ilustrovat následujícím příkladem:

```
AuthType shibboleth
ShibRequireSession On
require affiliation student@muni.cz
require user tonda@cuni.cz
require user helena@cesnet.cz
```

Uvedený příklad povoluje přístup k chráněnému adresáři všem uživatelům, kteří jsou studenty na Masarykově univerzitě, a dále uživateli s identifikátorem `tonda` z Karlovy univerzity a uživatelce `helena` ze sdružení CESNET.

Využití direktiv souboru .htaccess je jednou z možností jak definovat autorizační nastavení. Přistupová práva mohou být definována také ve speciálním xml souboru. Výhodou těchto dvou způsobů je to, že nevyžadují žádné zásahy do aplikace samotné. Autentizace a autorizace je ošetřena prostředky webového serveru. Pokud je to však vhodné, může autorizační rozhodnutí provádět samotná aplikace, které Shibboleth modul předá informace o přistupujícím uživateli prostřednictvím systémových proměnných.

Zpravidla jsou předávány informace jako jméno a příjmení, e-mail, zda se jedná o zaměstnance nebo studenta atd. Množina předávaných údajů závisí především na dohodě jednotlivých organizací, které jsou členy federace.

Takovéto předávání údajů o uživatelích mimo vlastní organizaci může vyvolávat obavy v souvislosti s ochranou osobních údajů. Proto jsou v systému Shibboleth implementovány mechanismy pro ochranu osobních údajů uživatelů. Na úrovni každeho poskytovatele identit se definuje jaké údaje mohou jednotlivé aplikace (poskytovatelé služeb) o uživatelích získávat. Aplikaci může být například předávána pouze informace, že přistupující uživatel je student či zaměstnanec bez toho, že by aplikace byla schopna osobu identifikovat nebo získat osobní údaje dotyčné osoby. Existují nadstavby, které samotným uživatelům umožňují ovlivňovat rozsah informací o jejich osobě předávaných poskytovatelům služeb.

Při zájmu o bližší informace o možnostech využití autentizačních a autorizačních mechanismů federovaných identit ve vaší www aplikaci kontaktujte prosím `idp@ics.muni.cz` nebo některého z autorů tohoto článku.

4 Aplikace

Při převodu webové aplikace na využívání federace je nejdříve třeba si rozmyslet, zda do aplikace budou moci pouze přihlášení uživatelé, nebo i nepřihlášení. Oba přístupy jsou možné, například známý software MediaWiki má rozšíření pro přihlašování se pomocí systému Shibboleth, kdy stránky může prohlížet kdokoliv, ale pro jejich editaci je nutné se nejdříve přihlásit. V aplikaci se pak pohybují zároveň jak přihlášení, tak nepřihlášení uživatelé, a je nutné mezi nimi rozlišovat. Naopak v jiných aplikacích musí být všichni uživatelé přihlášení.

Dále je třeba rozmyslet, zda autorizaci provádět na úrovni webového serveru nebo aplikace.

Informace o přihlášeném uživateli se z Apache dostávají do webové aplikace ve formě speciálních HTTP hlaviček, jejichž názvy a mapování na atributy je možné konfigurovat. Případně lze nastavit, aby byl v jedné z hlaviček i celý dokument s údaji o uživateli poskytnutý Identity Providerem v jazyce SAML.

Obvykle je jeden z atributů (např. `eduPersonPrincipalName`) mapován na proměnnou `REMOTE_USER`, aby bylo možné využít standardní mechanismy pro kontrolu přístupu uživatelů a zapisovat identitu uživatele do logů Apache.

Přenos informací o uživateli ve speciálních HTTP hlavičkách je natolik obecný, že samotná aplikace může být vytvořená na libovolné platformě, např. PHP, Java servlety, Perl a další.

V následujících odstavcích jsou uvedeny příklady služeb, které budou zavedeny do české federace.

4.1 Online elektronické zdroje

Oblast poskytování online elektronických zdrojů počítá s největším využitím konceptu federací. V současné době je přístup k těmto zdrojům většinou řešen na základě rozsahu IP adres. Federace umožní poskytovatelům precizně definovat, kdo může ke kterým zdrojům přistupovat. Zároveň uživatelé budou moci ke zdrojům přistupovat odkudkoliv. Poskytovatelé obsahu jako je Elsevier, Ovid, SilverPlatter a EBSCO umožňují přístup přes federaci. V ČR jsme zatím ve stádiu jednání o připojení.

4.2 Patologický atlas

Ve stádiu příprav je také zpřístupnění patologických atlasů[3] přes federaci. Tyto atlasy poskytují tisíce klinických a histologických obrazů kožních chorob, vývojových poruch a dále obsahují výukové materiály pro studenty medicíny. Nyní je pro práci s atlasy nutná registrace a obržení přístupových údajů. Po zapojení do federace budou moci studenti medicíny ze všech škol zapojených v české federaci přistupovat k těmto atlasům přímo.

[3] `http://atlases.muni.cz`

4.3 Aplikace pro zřizování guest účtů

Jako příklad již existující aplikace, která využívá federativní autentizační middleware Shibboleth je možné uvést aplikaci pro zřizování tzv. *guest účtů* na MU. Tato aplikace umožňuje zřizování a údržbu tzv. guest učtů pro přístup k vybraným službám počítačové sítě MU. Guest účty jsou zřizovány pro osoby, které nejsou v přímém vztahu k MU a nevzniká jim tudíž automaticky nárok na využívání služeb dostupných v rámci sítě MU, nicméně je v zájmu MU jim na určitou dobu přístup poskytnout. Může se jednat o učastníky konferencí, osoby spolupracující na společných projektech, návštěvníky univerzitních knihoven atd. Na straně služeb se jedná například o přístup do VPN, do wifi sítě počítačových studoven. Jádrem aplikace pro vytváření guest účtů je webová služba, která operuje nad databází a adresářovou službou. Tato služba poskytuje metody pro vytvoření účtu, pro editaci údajů o uživatelích těchto účtů, a také pro povolování a zakazování časově omezených přístupů k různým zdrojům, jako jsou počítačové studovny, virtuální privátní síť, wifi síť. S touto službou pak komunikují webové aplikace, které zpřístupňují její funkcionalitu uživatelům pomocí grafického uživatelského prostředí.

V současné době mohou guest účty zřizovat pouze vybrané osoby v rámci MU. Tyto aplikace používají federativní autentizaci Shibboleth, takže bude výhledově možné aplikaci zpřístupnit osobám z dalších institucí zapojených do národní federace a v odůvodněných případech umožnit samoobslužné zřízovaní přístupu k službám počítačové sítě MU.

4.4 Testovací aplikace

V rámci testování vzniklo několik demonstračních aplikací, například Wiki s možností editace pouze pro členy federace a „chat pro vyvolené”[4], kde lze vytvářet místnosti s přístupem omezeným na osoby s určitými atributy, například místnost jen pro osoby se jmény Martin nebo Michal. Seznam aplikací v testovací federaci je uveden na stránkách federace czTestFed[5]

[4] `https://meta.cesnet.cz/shibchat/`

[5] `https://cztestfed.feld.cvut.cz/wiki/cztestfed/members/`

4.5 Aplikace bez webového rozhraní

Jak již bylo zmíněno, současné middlewary podporující federace jsou orientovány pouze na prostředí webových aplikací. Ne všechny aplikace však poskytují webový přístup, proto bylo nutné najít řešení jak do federace zapojit poskytovatele služeb, kteří nemají webový přístup. Jednou z možností je využít překladové služby, která převede informace od poskytovatele identit do formátu jiného autentizačního a autorizačního mechanismu. Další možností je „obalit" atributy jiným autentizačním mechanismem. Pro testování jsme využili druhou možnost, kde ukládáme atributy od poskytovatele identit ve formě rozšíření do osobního certifikátu. Experimentálně jsme nasadili tzv. Online-CA. Jedná se o certifikační autoritu, jak je definovaná v konceptu PKI, která vydává osobní certifikáty, ve formátu X.509, uživatelům, kteří se úspěšně autentizovali přes federaci. Tímto způsobem jsme schopni do federace zapojit služby, které umí pracovat s certifikáty. Samotný certifikát slouží jako autentizační mechanismus a atributy uložené uvnitř certifikátu jsou využity k autorizaci.

5 Závěr

Mechanismus federací identit vypadá velmi nadějně pro řešení problému ověřování totožnosti velkého množství uživatelů, protože po uživatelích vyžaduje nulové množství práce, což je přesně to množství práce, které jsou sami ochotni vynaložit pro zabezpečení přístupu k aplikacím. Dále dramaticky snižuje počet hesel, které si uživatelé musí pamatovat.

Z hlediska poskytovatelů služeb federace odbourávají nutnost implementovat vlastní systém pro správu uživatelů, a zároveň zajišťují aktuálnost dat o uživatelích.

Zkušenosti z již existujících federací ukazují, že se jedná o životaschopný koncept a lze očekávat jeho rozšíření v následujících několika letech.