ATLASES JAKO POSKYTOVATEL SLUŽBY VE FEDERACÍCH

ATLASES AS A SERVICE PROVIDER IN THE IDENTITY FEDERATIONS

M. Procházka[1], J. Feit[2]

[1]CESNET, z. s. p. o., Zikova 4, 160 00 Praha 6,
[2]Masarykova Universita v Brně, Žerotínovo nám. 617/9, 601 77 Brno

Abstrakt

Hypertextové atlasy dermatopatologie, fetální a novorozenecké patologie obsahují velké množství obrázků ve vysokém rozlišení a k nim přidružené popisné informace. V době vzniku byly první atlasy poskytovány na Internetu bez jakýchkoliv omezení. S růstem počtu uložených objektů rostl nejen počet zájemců, ale začali se objevovat i lidé, kteří se snažili atlas bez vědomí autora zkopírovat a následně snímky (ale i popisy) vydávat za vlastní. Byly jsme proto nuceni nasadit autentizaci uživatelů, která nám umožnila auditovat přístupy k atlasům. V příspěvku popisujeme nasazení vybraného autentizačního systému, který využívá národní federace identit. Atlasy se tak staly poskytovatelem služby v národních federacích, kde mohou uživatelé využívat služby za použití autentizačního mechanismu vlastní instituce.

Klíčová slova: atlas patologie, federace identit, autentizace

Abstract

The hypertext atlases of dermatopatology, fetal and neonatal pathology contain a lot of images in very high resolution together with the annotations. The atlases were available on the Internet without any restrictions at the beginning. As the number of images as well as the user base has been grown, unfortunately there were users who tried to mirror the atlases without letting know the author and then publish images and annotations as their own. Therefor we had to deploy an authentication system which allows auditing users' access. In the paper, we describe deployment of an authentication system which uses national identity federations. The atlases thus have become a service provider in a national identity federation, where users can authenticate with the services with their home institution's authentication mechanisms.

Keywords: atlas of pathology, identity federation, authentication

Úvod

Hypertextové atlasy dermatopatolgie, fetální a novorozenecké patologie [1][2] se díky poskytování velice kvalitních informací v podobě snímků ve velmi vysokém rozlišení a doplňkových informací stávají důležitým zdrojem nejen pro studenty medicíny, ale i pro samotné patology. Atlasy jsou od svého vzniku dostupné na Internetu v anglické i české verzi a jsou poskytovány bezúplatně pro kohokoliv, proto jsou denně využívány tisíci uživateli z celého světa. Právě jejich dostupnost bez jakýchkoliv překážek způsobila, že někteří uživatelé vytvářeli kopie atlasů a následně se je snažili vydávat za vlastní dílo nebo je integrovali bez vědomí autora do svých aplikací. Byli jsme proto v první fázi nuceni zavést registraci uživatelů, jejíž součástí bylo mimo jiné vygenerování uživatelského jména a hesla pro přístup k atlasům. Tímto jsme mohli kontrolovat, jak který uživatel atlasy využívá. Technicky jsme sice problém vyřešili, ovšem za cenu vyšší složitosti přístupu pro legitimní uživatele. Ti si teď byli nuceni pamatovat své přístupové údaje.

Snaha minimalizovat administrativní zátěž uživatelů při udržení kontroly přístupu nás přivedla k federacím identit. Federace představují koncept, kde jsou definovány dvě entity a to poskytovatelé identit a poskytovatelé služeb. Uživatelé mohou přistupovat k autentizovaným službám poskytovatelů služeb za použití autentizačního mechanismu jejich domovské organizace (poskytovatel identit). V následujících kapitolách přiblížíme koncept federací a zapojení atlasů do těchto federací. Popsané zkušenosti lze aplikovat i na jiné služby, které mají charakter služby poskytující informace nejen lokální komunitě uživatelů.

Federace identit

Federace identit znamená seskupení poskytovatelů identit a poskytovatelů služeb do jednoho celku, kde si jednotlivé entity věří. Poskytovatel identit je organizace, například universita, která spravuje údaje svých zaměstnanců a studentů. Nutným předpokladem organizace, která se chce stát poskytovatelem identit, je schopnost libovolným způsobem autentizovat své uživatele. Naopak poskytoval služby něco uživatelům nabízí a vyžaduje autentizaci uživatele. Pro přístup ke službě uživatel používá přihlašovací údaje, které běžně používá ve své domovské instituci. Systém je přitom koncipován tak, že uživatelovy přihlašovací údaje nejsou zpřístupněny poskytovateli služby, ale speciální webové službě, provozované jeho domovskou organizací. Poskytovatel služby se dozví pouze výsledek ověření identity -- jedná či nejedná se o osobu, kterou poskytovatel zná nebo nezná -- a případně dostane další dodatečné informace (např. zda se jedná o zaměstnance či studenta), ale nedozví se konkrétní identitu osoby. V případě potíží (např. zneužití služby) je možné konkrétní osoby ve spolupráci s poskytovatelem identit dohledat (nejde tedy o anonymní přístup). Z

pohledu uživatele se proces přihlášení skládá ze 3 kroků. Uživatel přistoupí k poskytovateli služby, pokud je to první přístup uživatele, je ihned přesměrován na webovou stránku nazvanou WAYF (Where Are You From), kde ze seznamu všech poskytovatelů identit v rámci federace vybere vlastní domovskou organizaci. Následně je přesměrován na autentizační stránku své domovské organizace, kde zadá přihlašovací údaje. Pokud se uživatel úspěšně autentizoval, je přesměrován již k poskytovateli služby, ten spolu s potvrzením, že se uživatel úspěšně autentizoval dostává i dodatečné atributy o uživateli. Poskytovatel služby se na základě těchto údajů rozhodne, zda uživatele pustí dál.

Popsaný koncept jasně demonstruje, že uživatel používá jediný typ autentizace pro všechny služby dostupné v rámci federace. Zároveň je zajištěno, že poskytovatel služby nemůže získat přihlašovací údaje uživatele. Tímto se stává systém bezpečnější hned z několika hledisek. První a velice důležitý, přihlašovací údaje nemohou být zneužity třetí stranou. Za druhé, uživatel je nucen spravovat pouze jedny přihlašovací údaje pro všechny služby v rámci federace. Současný stav, kdy si musí udržovat autentizační údaje pro každou službu zvlášť a převážně volí stejné přihlašovací údaje pro více služeb, umožňuje službám tyto údaje zneužít. Třetí důvod se týká používaného autentizačního mechanismu u poskytovatele identit, tento systém může využívat bezpečnější a přísnější mechanismy. Federace jednak využívají systém Single Sign-On, požadující ověření uživatele pouze jednou za určitý časový úsek a ne při každém přístupu, proto uživatel nebude protestovat pokud autentizace zabere více úsílí nebo času. Silnější autentizace může být například heslo delší než 8 znaků a obsahovat nealfanumerické znaky nebo se může skládat ze dvou mechanismů jako je použití digitálního certifikátu a hesla.

Koncept federací využívá některé specifické vlastnosti protokolu HTTP, proto poskytovatelé služeb jsou pouze webové služby, existují však mechanismy jak federace dostat do newebového světa. Jejich popis je nad rámec tohoto článku.

Atlasy jako poskytovatel služby

V akademickém prostředí po celém světě vznikají národní akademické federace, které sdružují akademické instituce jako poskytovatele identit. Poskytovateli služeb jsou nejenom webové služby z akademického prostředí, ale i komerční poskytovatelé. Proto jsme se rozhodli, že nabídneme atlasy jako poskytovatele služeb do těchto federací. Jednak vyřešíme problém s generováním přihlašovacích údajů pro uživatele, ale získáme i ověřenou identitu uživatele třetí stranou. Zapojení do federace přináší výhody nejen provozovateli služby, nemusí vkládat úsilí do správy autentizačních dat uživatelů, ale i samotným uživatelům, protože dostávají jednotný způsob autentizace k více

službám. V neposlední řadě je členství ve federacích i určitým způsobem reklama, protože každá federace publikuje seznam svých poskytovatelů služeb.

Mít všechny uživatele z federací by byl ideální stav, v dohledné době je to však nereálné. Proto musíme podporovat i registraci uživatelů mimo federace, bohužel zde nejsme schopni zjistit, zda pod dvěma různými loginy přistupují dva různí lidé.

Zkušenosti s nasazením

Samotné připojování atlasů do federací ukázalo, že se jedná o natolik nový záměr, že v řadě národních federací jsme byli první přeshraniční služba, což s sebou v řadě případů přineslo další organizační i technické problémy, které bylo nutno vyřešit.

Technické problémy lze rozdělit do dvou kategorií, kompatibilita a sémantika. Ne všechny federace používají stejný middleware, proto bylo nutné sladit konfigurace na obou stranách, abychom byli vzájemně kompatibilní. Atlasy využívají middleware *Shibboleth* [3], který je v akademických federacích nejvíce rozšířen. Někteří poskytovatelé služeb či identit používají middleware *SimpleSamlPHP* [4]. Oba tyto middlewary používají jako komunikační protokol *SAML2* [5]. Druhým problémem bylo porozumění hodnotě atributů, které poskytovatelé identit o uživatelích vydávají. Jelikož standardy jsou v popisu atributů velice vágní a každá federace si je vykládá po svém, bylo nutné sémantiku atributů dojednat přímo s provozovateli, i přesto, že jsme požadovali pouze jeden atribut. Pro provoz atlasů stačí atribut nesoucí tzv. pseudoanonymní identitu, jedná se o náhodný řetězec, který je různý pro každého jednotlivého poskytovatele služeb. Náhodný identifikátor je u poskytovatele identit spřažen s konkrétní osobou, proto je pseudoanonymní.

Organizační problémy představovaly převážnou část problémů a překážek. Obecně největším problém je různá fáze nasazení federací v jednotlivých státech. V době, kdy jsme začali atlasy připojovat do federací, se většinou jednalo o testovací federace, kde nebyly nastaveny postupy zapojování poskytovatelů služeb a nebyly k dispozici smlouvy s vymezením odpovědností a závazků. Proto připojení do federace vyžadovalo netriviální mailovou a telefonní komunikaci. U federací, kde již měli v určité fázi formální kroky specifikovány a smlouvy připraveny jsme naráželi na neexistenci překladu smluv alespoň do anglického jazyka nebo podmínky smluv vyžadovaly podpisy odpovědných osob na úrovni ředitelství organizace, která službu provozuje.

Pro demonstraci rozdílného přístupu k poskytovatelům služeb uvedeme vybrané federace a postup připojování.

WAYF.dk – Dánská akademická federace. Tato federace patří mezi plně ustavené federace. Jsou plně otevřeni přijímat nové poskytovatele služeb. Proces

se iniciuje kontaktováním provozovatele federace přes email. Následuje zapojení služby do testovací federace, kde se provedou testy interoperability a spojení. Po úspěšném otestování je provozovatel služby vyzván k zaslání stručného popisu své služby, který bude dostupný na webových stránkách federace a digitálního certifikátu určeného pro autentizaci a šifrování komunikace mezi službou a federací. Je nutné také dodat seznam atributů, které služba o uživatelích potřebuje znát. Požadavek na každý atribut musí být zdůvodněn, protože se většinou jedná o osobní údaje a v případě přeshraniční služby je to o to striktnější. Po vyjednání výše uvedeného je služba přesunuta do QA federace, kde je nové nastavení opět otestováno. Když vše proběhne dobře je služba přesunuta do produkční federace. Samozřejmostí je podepsání smlouvy mezi provozovatelem federace a služby, kde jsou vymezeny odpovědnosti a povinnosti. Charakterem jsou smlouvy u ostatních federací stejné. Obecně se poskytovatel služby zaváže, že poskytnuté informace o uživateli nebude dále šířit třetím stranám vyjma orgánům činným v trestním řízení. Nesmí také provádět žádné kroky, které by vedly k poškození infrastruktury federace. Provozovatel federace se zavazuje, že bude infrastrukturu udržovat v provozu v režimu best effort a o každé důležité změně bude informovat.

SWITCH AAI – Švýcarská akademická federace. V této federaci atlasy zatím připojeny nejsou, stejně jako ve finské *HAKA* a americké *InCommon*. Obě tyto federace vyžadují organizaci nebo jednotlivce z jejich federace, který o službu projeví explicitní zájem. Připojovací proces tedy musí iniciovat uživatel. Tento systém je dle našeho názoru velice komplikovaný pro provozovatele služby. V případě atlasů se velmi špatně hledá uživatel z konkrétní země, protože nevyžadujeme zadání země původu a také nechceme uživatele zatěžovat organizačními procedurami. V současné době rozmýšlíme, zda umístit informaci na úvodní stránku atlasů, aby se nám uživatelé ze zmíněných zemí ozvali.

SURFfederatie – Holandská akademická federace. Zde jsme se stali součástí běžnou procedurou, kdy jsme prošli testovací fází a nakonec podepsali smlouvy. Tato federace se od ostatních liší způsobem publikování poskytovatelů služeb jednotlivým poskytovatelům identit. Správce federace po připojení nové služby rozešle informaci všem poskytovatelům identit, a pouze těm, kteří explicitně projeví zájem je služba zpřístupněna. Z pohledu poskytovatele služby je takřka nemožné zasáhnout do tohoto procesu.

UPKI – Japonská akademická federace. Tato federace patří k velice otevřeným federacím. Celé připojování spočívalo v iniciálním testu spojení, specifikaci atributů a následnému přechodu do produkční federace. Tento postup, kdy se otestuje spojení a dohodnou atributy a následně se přechází do produkční federace jsme aplikovali i u chorvatské *AAI@EduHr* a italské *IDEM GARR AAI*. Spolu s podepsáním smlouvy jsme tento postup provedli i u španělské federace *Servidor de Identidad de RedIRIS* a německé *DFN AAI*.

Během provozu se ukázali některé úskalí technického provedení konceptu federací. U německé DFN AAI někteří poskytovatelé identit přešli na novou verzi middleware, což znamenalo, že atribut eduPersonTargeteId, který atlasy využívají, změnil svoji hodnotu u každého uživatele. Atlasy na tento identifikátor mapují dodatečné informace o uživateli, proto se museli uživatelé od těchto poskytovatelů registrovat znovu, protože neexistovalo mapování ze staré hodnoty na novou. Daleko větším problémem byla výměna certifikátu u atlasů. Atlasy používají důvěryhodný certifikát vydaný českou certifikační autoritou CESNET CA, který je platný jeden rok. Výměna certifikátu znamenala kontaktovat všechny provozovatele federací a provést výměnu v jejich metadatech. Metadata definují samotnou federaci, obsahují provozní informace o poskytovatelích služeb a identit. Některé federace poskytují nástroj na správu těchto údajů přes webový portál, u ostatních znamenala výměna emailovou komunikaci. Celý proces zabral bezmála 14 dní.

Poslední problém, který patří mezi kurióznější, bylo vysvětlování provozovatelům federace, že nabízíme službu, která je zdarma. Někteří měli ze začátku ke službě nedůvěru, protože pokud se za službu neplatí, nelze nikoho vést k odpovědnosti za obsah.

Současný stav

V současné době jsou atlasy zapojeny do devíti produkčních federací a do čtyř testovacích. Jednání s dalšími federacemi pokračují. Ke dni odevzdání článku bylo v atlasech evidováno přes 8600 uživatelů, z čeho je přes 300 uživatelů z různých národních federací. Relativně malé číslo je způsobeno zatím nedostatečným počtem zapojených lékařských fakult a zdravotních zařízení do národních federací. Situace se ale postupně mění a počet uživatelů přistupujících k atlasu přes federace trvale roste, i díky tomu, že tito uživatelé si nemusí pamatovat nové přihlašovací údaje (ani prozrazovat stávající).

Závěr

V článku jsme přiblížili koncept federací a popsali postupy a problémy, se kterými jsme se potkali při zapojování atlasů do federací. Popsané postupy mohou sloužit ostatním poskytovatelům služeb jako návod pro zpřístupnění své služby netriviálnímu množství uživatelů. Podle ohlasů se atlasy staly velice užitečnou pomůckou při výuce a přístup přes federaci ulehčil uživatelům přístup k informacím a nám lépe zabezpečil poskytovaný obsah.

Literatura

[1] Feit J., Kempf W., Jedličková H., Burg G., „Hypertext atlas of dermatopathology with expert systém for epithelial tumors of the skin“, *Journal of Cutaneous Pathology*, vol. 32/6, pp. 433–437, ISBN 0303-6987, 2005.

[2] Ježová M., Múčková K., Souček O., Feit J., Vlašín P., „Hypertext atlas of fetal and neonatal pathology“, *Diagnostic Pathology*. Vol. 3, p. 59, ISSN 1746-1596, 2008.

[3] Cantor S., „Shibboleth Architecture -- Protocols and Profiles“, 10 September 2005, http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-conformance-200509.pdf.

[4] SimpleSamlPHP, http://rnd.feide.no/simplesamlphp, Listopad 2009.

[5] Cantor S., Kemp J., 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.