

Řekni Shibboleth :-) webové jednotné přihlašování nejen pro vzdálený přístup v knihovnách

*Ing. Jiří Pavlík / Univerzita Karlova v Praze / Cesnet
e-mail: pavlik@cuni.cz, <http://www.pavlik.ruk.cuni.cz>*

Také máte množství přihlašovacích jmen a hesel k e-mailu, k internetovým obchodům a aukcím, k Facebook, LinkedIn, Twitter, k Flickr, YouTube, k PayPal, Netvibes, Mag.nolia, del.icio.us, k blogům, k oblíbeným on-line časopisům, do knihoven, atd.? Dokolečka vyplňujete registrační údaje? Jestli se pohybujete občas na internetu, pak nejspíš dobře víte, o čem je řeč :-)

V červnu roku 2007 vznikla OpenID nadace, která si vzala za cíl propagaci technologie OpenID, která umožňuje v prostředí webu přihlašování jednotným jménem a heslem a je založená na volně dostupných open-source nástrojích. V dnešní době je registrováno přibližně 160 miliónů OpenID, tedy 160 miliónů identit uživatelů, kteří mohou využívat přihlašování pomocí OpenID u téměř 10 tisíc služeb na webu.

V prostředí OpenID je možné si bez schvalování jakékoli organizace vytvořit internetovou identitu. To má své výhody, nicméně v akademickém prostředí je nutné, aby jen tak kdokoli nemohl prohlásit, že je Steve Jobs a studuje Psychologii na Filozofické fakultě Univerzity Karlovy v Praze. Často je také vhodné, aby webová služba nedostala nic více než garantovanou informaci, že se jedná o studenta Univerzity Karlovy – jde o službu, do níž přístup pro své studenty hradí Univerzita Karlova, služba nenabízí personalizované služby a s ohledem na ochranu osobních údajů je tedy optimální, když služba dostane Univerzitou garantovanou informaci, že se jedná o studenta Univerzity Karlovy. Nic více, nic méně.

V akademickém prostředí se využívá technologie Shibboleth, která zajišťuje webové jednotné přihlašování v rámci organizace i napříč organizacemi. Shibboleth patří mezi projekty konsorcia Internet2. Ve Velké Británii, Spojených státech amerických, ve Švýcarsku, Finsku, Německu, Francii, Dánsku, Holandsku, v České republice a v několika dalších zemích je Shibboleth využíván stovkami organizací.

Podobně jako u OpenID je Shibboleth založen na dostupných standardech a volně přístupných open-source nástrojích. Narozdíl od OpenID ale v prostředí Shibboleth platí, že domovská organizace dodává poskytovatelům webových služeb garantované informace o uživatelích. Na základě toho poskytovatelé mohou provádět informovaná autorizační rozhodnutí, mohou nabídnout právě ty služby, ke kterým na základě licenčních smluv mezi organizací a poskytovatelem mají mít uživatelé přístup.

Shibboleth je také navržen s ohledem na ochranu soukromí uživatelů. Poskytovatel služeb typicky dostává od domovské organizace jen nezbytné údaje o uživateli, aby mohl nabídnout příslušné služby. Pokud to není pro zajištění služeb nutné, poskytovatel nedostává ID uživatele. Pokud to nutné je, domovská organizace dodá poskytovateli ID uživatele, které je typicky specifické pro každého poskytovatele.

Shibboleth je často využíván v rámci federací. Federace sdružují domovské organizace uživatelů a poskytovatele služeb. Ve federaci platí pravidla, která definují tvar a význam údajů o uživatelích předávaných domovskými organizacemi poskytovatelům. Federace jsou typicky provozovány na národní úrovni.

Českou národní akademickou federaci eduID.cz provozuje Cesnet. Do ostrého provozu

byla federace spuštěna 1.1.2009. Na webových stránkách eduID.cz jsou zveřejněny: politika, použití atributů, seznam členů, návod na připojení do federace, kontakty, kam se obracet s dotazy. Pro uživatele jsou na stránkách uvedeny také jednoduché návody k přihlášení a odhlášení v prostředí Shibboleth. Pro správce pak potřebné administrativní a technické podrobnosti. V anglické sekci stránek jsou uvedeny informace pro zahraniční poskytovatele služeb.

Souběžně s eduID.cz provozuje Cesnet také federaci czTestFed sloužící pro testování před připojením domovských organizací nebo služeb do produkční federace eduID.cz. K připojení organizace nebo služby do eduID.cz, instalaci shibbolethových komponent Identity Provider a Service Provider připravuje Cesnet školení. V případě zájmu je možné se zúčastnit také skvěle organizovaných školení pořádaných SWITCH. Nejbližší školení SWITCH proběhne v Zurichu 18.-20. května 2009.

Autentizace, ověřování uživatelů pomocí Shibboleth, je využíváno také u CESNET Adobe Connect, Apple iTunes University, Microsoft DreamSpark, Google Apps. Webové jednotné přihlašování na bázi Shibboleth přináší uživatelům výrazně vyšší komfort pro práci a pro studium. Do prostředí knihoven přináší řešení pro tzv. vzdálený přístup k elektronickým zdrojům založené na standardech, volně dostupné, mezinárodně rozšířené, výborně škálovatelné, se zajištěnou podporou a vývojem. Pro správce systémů pro vzdálený přístup přináší významné snížení nároků na správu a podporu, pro kolegy z knihoven odpovědné za zpřístupnění elektronických zdrojů odstraňuje často náročná vyjednávání k IP adresám a provozu systémů nebo technologií typu proxy server, VPN server, terminal server, SSH tunel. Pro poskytovatele služeb spuštění shibbolethové autentizace znamená v současné době také významnou konkurenční výhodu.

Shibboleth je jedním z nástrojů, který knihovnám přináší snížení nároků na provoz, významně zvýšení komfortu uživatelů a pomáhá tak uspět u čtenářů v dnešním vysoce konkurenčním informačním světě.

Zdroje:

Stránky projektu Shibboleth, <http://shibboleth.internet2.edu/>

Stránky české národní akademické federace eduID.cz, <http://www.eduid.cz/>

Stránky projektu OpenID, <http://openid.net/>

Stránky k Shibboleth na Univerzitě Karlově v Praze, <http://kis.is.cuni.cz/KSIS-41.html>

OpenID versus Shibboleth, james@melcoe.mq.edu.au, <http://lists.aarnet.edu.au/piper-mail/middle-l/2007-May/000164.html>

OpenID: Decentralised Single Sign-on for the Web, Andy Powell, David Recordon, <http://www.ariadne.ac.uk/issue51/powell-recordon/>

Shibboleth - Wikipedia, <http://en.wikipedia.org/wiki/Shibboleth>

CESNET Adobe Connect, <https://vidcon.cesnet.cz/app/ac/about>

Achieving Single Sign-on with Google Apps and Shibboleth 2.0, <http://code.google.com/apis/apps/articles/shibboleth2.0.html>

iTunes U: Apple is InCommon-ly Good for Universities, http://www.incommonfederation.org/docs/eg/InC_CaseStudy_iTunes_2008.pdf

Microsoft Provides Students with a Sweet Suite, http://www.incommonfederation.org/docs/eg/InC_CaseStudy_Dreamspark_2008.pdf

SWITCH Shibboleth 2 Install Fests 2009, <http://www.switch.ch/aai/support/presentations/installfest-2009/>

Shibboleth : a project of the Internet2 Middleware Initiative [online]. Washington, DC : Internet2, c2009 [cit. 2009-05-04]. Dostupný z WWW: <<http://shibboleth.internet2.edu>>.

Česká akademická federace identit eduID.cz [online]. Praha : CESNET, c2009 [cit. 2009-05-04]. Dostupný z WWW: <http://www.eduid.cz/wiki/eduid/index#ceska_akademicka_federace_identit_eduid.cz>.

OpenID [online]. San Ramon, CA : OpenID Foundation, 2007- [cit. 2009-05-04]. Dostupný z WWW: <<http://openid.net/>>.

Knihovní služby Univerzity Karlovy – Shibboleth [online]. Praha : Univerzita Karlova, 2009 [cit. 2009-05-04]. Dostupný z WWW: <<http://kis.is.cuni.cz/KSIS-41.html>>.

DALZIEL, James. OpenID versus Shibboleth. In *The Middle L Archives* [online]. Thu May 17 10:39:37 EST 2007 [cit. 2009-05-04]. Dostupný z Internetu: <james@melcoe.mq.edu.au>. Dostupný také z WWW : <<http://lists.aarnet.edu.au/pipermail/middle-l/2007-May/000164.html>>.

POWELL, Andy; RECORDON, David. OpenID : decentralised single sign-on for the web. *Ariadne* [online]. April 2007, iss. 51 [cit. 2009-05-04]. Dostupný z WWW: <<http://www.ariadne.ac.uk/issue51/powell-recordon/>>.

Shibboleth [online]. Wikipedia : the free encyclopedia, 2009 [cit. 2009-05-04]. Dostupný z WWW: <<http://en.wikipedia.org/wiki/Shibboleth>>.

NORRIS, Will. Achieving Single Sign-on with *Google Apps and Shibboleth 2.0*. In *Google Apps APIs – Google Code* [online]. Google, 2008 [cit. 2009-05-04]. Dostupný z WWW: <<http://code.google.com/intl/cs/apis/apps/articles/shibboleth2.0.html>>.

iTunes U : Apple is InCommon-ly Good for Universities. Pilot program tests iTunes U protected access through InCommon. In *InCommon* [online]. Ann Arbor : InCommon, 2008 [cit. 2009-05-04]. Dostupný z WWW: <http://www.incommonfederation.org/docs/eg/InC_CaseStudy_iTunes_2008.pdf>.

Microsoft Provides Students with a Sweet Suite : DreamSpark design and development tools available through InCommon. In *InCommon* [online]. Ann Arbor : InCommon, 2008 [cit. 2009-05-04]. Dostupný z WWW: <http://www.incommonfederation.org/docs/eg/InC_CaseStudy_Dreamspark_2008.pdf>.

SWITCH. *SWITCH* [online]. Zurich : SWITCH, 2009 [cit. 2009-05-04]. SWITCH Shibboleth 2 Install Fests 2009. Dostupný z WWW: <<http://www.switch.ch/aai/support/presentations/installfest-2009/>>.