Shibboleth - elegantní technologie pro vzdálený přístup k dabatázím

Jiří Pavlík
Univerzita Karlova v Praze
pavlik@cuni.cz

INFORUM 2006: 12. konference o profesionálních informačních zdrojích
Praha, 23. - 25.5. 2006

Abstrakt. Shibboleth je middleware navržený konzorciem Internet2 pro zajištění distribuované webové autentikace a Single-Sign-On při přístupu k lokálním i vzdáleným informačním zdrojům. V příspěvku budou představeny principy Shibboleth, stav jeho implemantace v knihovnách ve světě, u významných provozovatelů informačních zdrojů jako Elsevier, EBSCO, JSTOR a postup implementace na univerzitách a v knihovnách v České republice.

Jemný úvod do Shibboleth

Shibboleth je middleware navržený konzorciem Internet2 pro zajištění distribuované webové autentikace a Single-Sign-On. V prostředí knihoven a informačních zdrojů se standard Shibboleth uplatňuje pro řešení tzv. vzdáleného přístupu k lokálním i vzdáleným informačním zdrojům.

Výhoda Shibboleth oproti řešením typu VPN, proxy a oproti portálovým řešením (Han/Netman, Onelog) pro vzdálený přístup k informačním zdrojům je vyšší úroveň zabezpečení, standardizovaný způsob autentikace a Single-Sign-On prostředí.

Nevýhodou Shibboleth je nutnost podpora toho prostředí jak ze strany poskytovatelů obsahu tak ze strany organizací, které pro uživatele zajišťují ověření identity.

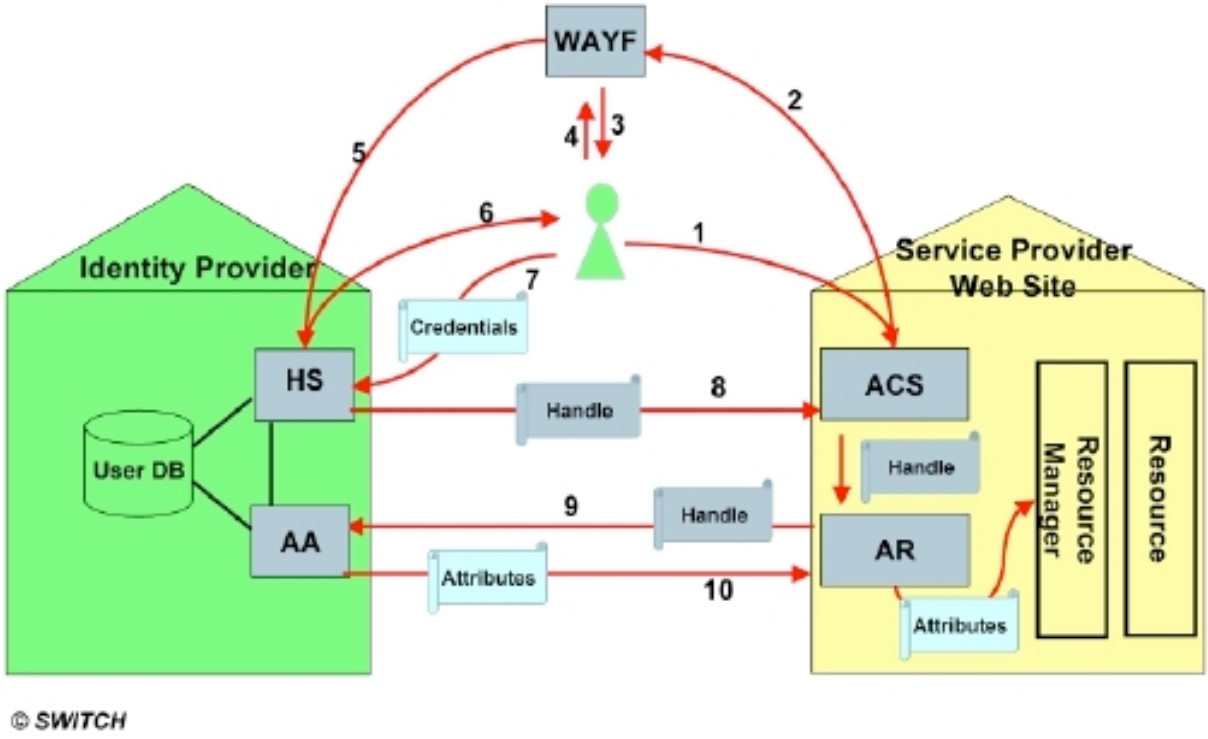
Šikovným řešením pro přechodné období, kdy někteří z poskytovatelů obsahu nebudou podporovat autentikaci prostřednictvím Shibboleth, jsou proxy či portálová řešení, které Shibboleth podporují a poskytují autentikaci na základě IP adresy nebo přihlašovacího jména a hesla pro ty informační zdroje, které Shibboleth nepodporují. Příkladem takového řešení je v současné době EZProxy od firmy Useful Utilities.

Komponenty software pro Shibboleth jsou open source software a jsou volně dostupné pro stažení na stránkách Internet2 pod Apache licencí. Instalační balíčky jsou připaveny pro platformy Linux, Mac OS X, Solaris a Windows. Shibboleth používá protokoly SAML (Security Assertion Markup Language) a LDAP (Lightweight Directory Access Protocol).

Poskytovatelé obsahu, služeb v prostředí Shibboleth vystupují jako tzv. Service Provider (SP). Organizace, které pro uživatele zajišťují ověření identity, vystupují jako tzv. Identity

Provider (IdP). SP a IdP se typicky spojují do tzv. federací. V rámci federace je definován jednotný seznam atributů poskytovaných o uživateli IdP a je provozována služba Where Are You From (WAYF). Služba WAYF zajišťuje přesměrování autentikačního požadavku u SP na příslušného IdP. Při přístupu k SP je uživatel přesměrován na službu WAYF, kde si volí svého IdP a u něj se pak autentikuje. K SP pak putuje informace o výsledku autentikace a minimální sada atributů nutná pro autorizaci pro služby poskytované SP. Federace je typicky provozována na národní úrovni.

Obrázek ilustruje postup autentikace v prostředí Shibboleth:



Implementace Shibboleth ve světě

Na začátku roku 2006 je Shibboleth používán nejvíce ve Finsku, Švýcarsku, Francii, Velké Británii a v USA. V těchto zemích jsou založeny federace. Dále např. v Dánsku, Španělsku, Rakousku se nasazení Shibboleth plánuje.

Ve Velké Británii je autentikace pro vzdálený přístup k informačním zdrojům zajišťována pomocí systému Athens centrálně provozovaného organizací JISC. Proprietání systém Athens plánuje JISC nahradit do roku 2008 pomocí Shibboleth.

Ve Švýcarsku, kde je aplikace Shibboleth jedna z nejpokročilejších, se Shibboleth využívá především pro autentikaci k e-learningovým systémům.

Z poskytovatelů obsahu Shibboleth podporují Blackwell, EBSCO, Elsevier ScienceDirect, JSTOR, OCLC, Proquest, Thomson Gale. Podporu připravují CSA, Ovid Technologie.

Ze systémů pracujících s on-line zdroji Shibboleth podporují systémy od firem Ex Libris (SFX, Digitool, podpora pro Aleph a MetaLib se připravuje), Serial Solutions a Useful Utilities.

Z výukových systémů Shibboleth podporují Blackboard - WebCT, Moodle, OLAT.

Implementace Shibboleth v České Republice

Na přelomu 2005 a 2006 byla při Cesnet založena pracovní skupina pro Federativní AAI (Authentication and Authorization Infrastructure). V březnu 2006 se na semináři Cesnet v Táboře konalo úvodní setkání skupiny. Setkání se zúčastnili zástupci univerzit, které jsou členy Cesnet, a zástupce Státní technické knihovny.

Na rok 2006 byly rozděleny práce - pracuje se na vyhodnocení vhodnosti Shibboleth v českém prostředí, sbírají se zkušenosti s instalací a provozem Shibboleth komponent, vybírá se nejvhodnější seznam atributů používaných při autorizaci. Uvažuje se o nasazení Shibboleth pro autentikaci k informačním zdrojům a e-learningovým systémům.

Zdoje

1. http://shibboleth.internet2.edu
2. http://www.switch.ch/aai/shibboleth/
3. http://www.projectliberty.org/
4. http://www.jisc.ac.uk/index.cfm?name=programme_middleware
5. http://seminar.deff.dk/
6. https://authdev.it.ohio-state.edu/twiki/bin/view/Shibboleth/ShibTwoRoadmap