Shibboleth

elegantní technologie pro vzdálený přístup
k informačním zdrojům

Ing. Jiří Pavlík
INFORUM, VŠE, 23-25.5.2006

ÚVT
Univerzita Karlova v Praze

Shibboleth

- "The Gileadites captured the fords of the Jordan leading to Ephraim, and whenever a survivour of Ephraim said, "Let me go over," the men of Gilead asked him, "Are you an Ephraimite?" If he replied, "No," they said, "All right, say 'Shibboleth'." If he said, "Sibboleth," because he could not pronounce the word correctly, they seized him and killed him at the fords of the Jordan. Forty-two thousand Ephraimites were killed at that time." (Judges 12:5-6, NIV)

- http://en.wikipedia.org/wiki/Shibboleth

Shibboleth

- Shibboleth is an Internet2 Middleware Initiative project that has created an architecture and open-source implementation for federated identity-based authentication and authorization infrastructure based on SAML. Federated identity allows for information about users in one security domain to be provided to other organizations in a common federation. This allows for cross-domain single sign-on and removes the need for content providers to maintain usernames and passwords. Identity providers (IdP's) supply user information, while service providers (SP's) consume this information and gate access to secure content.

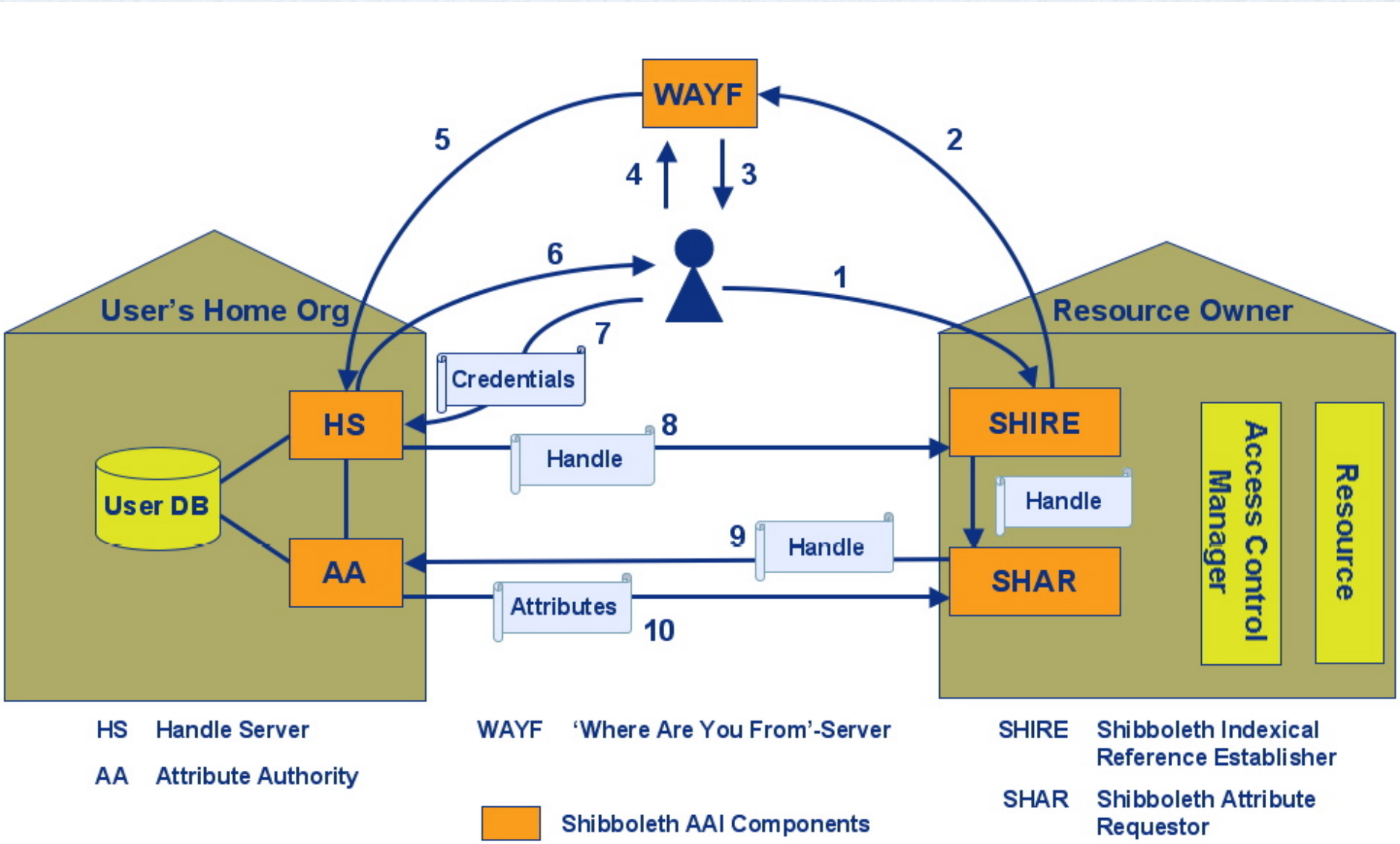
- http://en.wikipedia.org/wiki/Shibboleth_(Internet2)

Proč Shibboleth

- Standardní technologie pro webovou federativní autentikaci
- Snižuje nároky na správu přístupů ke zdrojům s autetikovaným přístupem
- Zvyšuje bezpečnost díky vytvoření Single-Sign-On prostředí
- Jednoduché řešení pro velké i malé instituce

Základní princip

- Každý uživatel má domovskou organizaci, u které je autentikován – Identity Provider IdP
- Provozovatelé služeb – Service Providers – využívají autentikace u IdP
- Zachována anonymita uživatele – uživatel je identifikován dočasným ID
- Bezpečnostní kontext uložený v cookie
- Služba WAYF jako prostředník mezi IdP a SP provozovaná v rámci Shibboleth federace


WAYF
5
2
4
3
6
1
User's Home Org
Resource Owner
7
Credentials
HS
8
Handle
SHIRE
User DB
Handle
9
Handle
AA
SHAR
Attributes
10
Access Control Manager
Resource
HS Handle Server
AA Attribute Authority
WAYF 'Where Are You From'-Server
Shibboleth AAI Components
SHIRE Shibboleth Indexical Reference Establisher
SHAR Shibboleth Attribute Requestor

Typické využití

- Informační zdroje a systémy pro knihovny
- E-learning systémy
- Gridy

Poskytovatelé databází

- Podporují: EBSCO, JSTOR, Elsevier, Thomson Gale, OCLC,
- Připravují podporu: Proquest, CSA, Ovid

Systémy

- Knihovní: MetaLib, SFX, Fedora, EZProxy
- E-learning: Moodle, Blackboard, Digitalbrain, Bodington, WebCT, ILIAS
- Jiné: TWiki

Shibboleth ve světě

- Finsko, USA, Švýcarsko, Velká Británie, Francie, Dánsko

Finsko

- Federace Haka
- Shibboleth 1.2.1
- 8 institucí jako IdP, 8 SP (Nelli portal, Moodle @ Tampere University)

Velká Británie

- JISC plánuje nahradit Athens pomocí Shibboleth do 2008
- Federace SDSS, 10 institucí jako IdP, 17 projektů jako IdP nebo SP, 13 SP

Technologie

- SAML
- LDAP
- Základní sada atributů eduPerson
- Balíky pro IdP a SP pro různé platformy volně ke stažení ze stránek Internet2
- Shibboleth 1.1 (1.2, 1.3), připravuje se 2.0

Ke studiu

- http://shibboleth.internet2.edu/
- https://authdev.it.ohio-state.edu/twiki/bin/view/Shibboleth/WebHome
- http://www.switch.ch/aai/documents/
- http://www.lupa.cz/clanky/shibboleth/
- http://www.cesnet.cz/projekt/09/

- https://authdev.it.ohio-state.edu/twiki/bin/view/Shibboleth/ShibTwoRoadmap

Shibboleth v ČR

- přelom 2005/2006 pracovní skupina při Cesnet (AAI a mobilita, Milan Sova)
- březen 2006 první setkání pracovní skupiny
- plán 2006: zkušební nasazení, založení federace, dohodnutí skupiny atributů, spuštění WAYF na serveru Cesnetu

Vyzkoušejte si

- http://www.switch.ch/aai/demo

Jiří Pavlík
pavlik @ cuni.cz