

# Nasazení federací ve velkém distribuovaném prostředí: systém pro správu interakcí léků

Daniel Kouřil, Martin Kuba, Michal Procházka

CESNET a ÚVT MU

# Na počátku byla otázka:

- Jak můžeme o náhodných návštěvnících webového serveru s jistotou vědět, zda jsou lékaři ?

# Databáze interakcí léků

- potřebovali jsme web, kam mohou psát pouze skuteční lékaři
- v ČR je registrovaných cca 44000 léků (databáze SÚKL)
- účinky jsou známy pro každý zvlášť
- interakce mezi dvojicemi léků jsou obvykle neznámé
- Web 2.0 databáze interakcí léků, příspěvky mohou přidat pouze lékaři

# Ale jak poznat lékaře ?

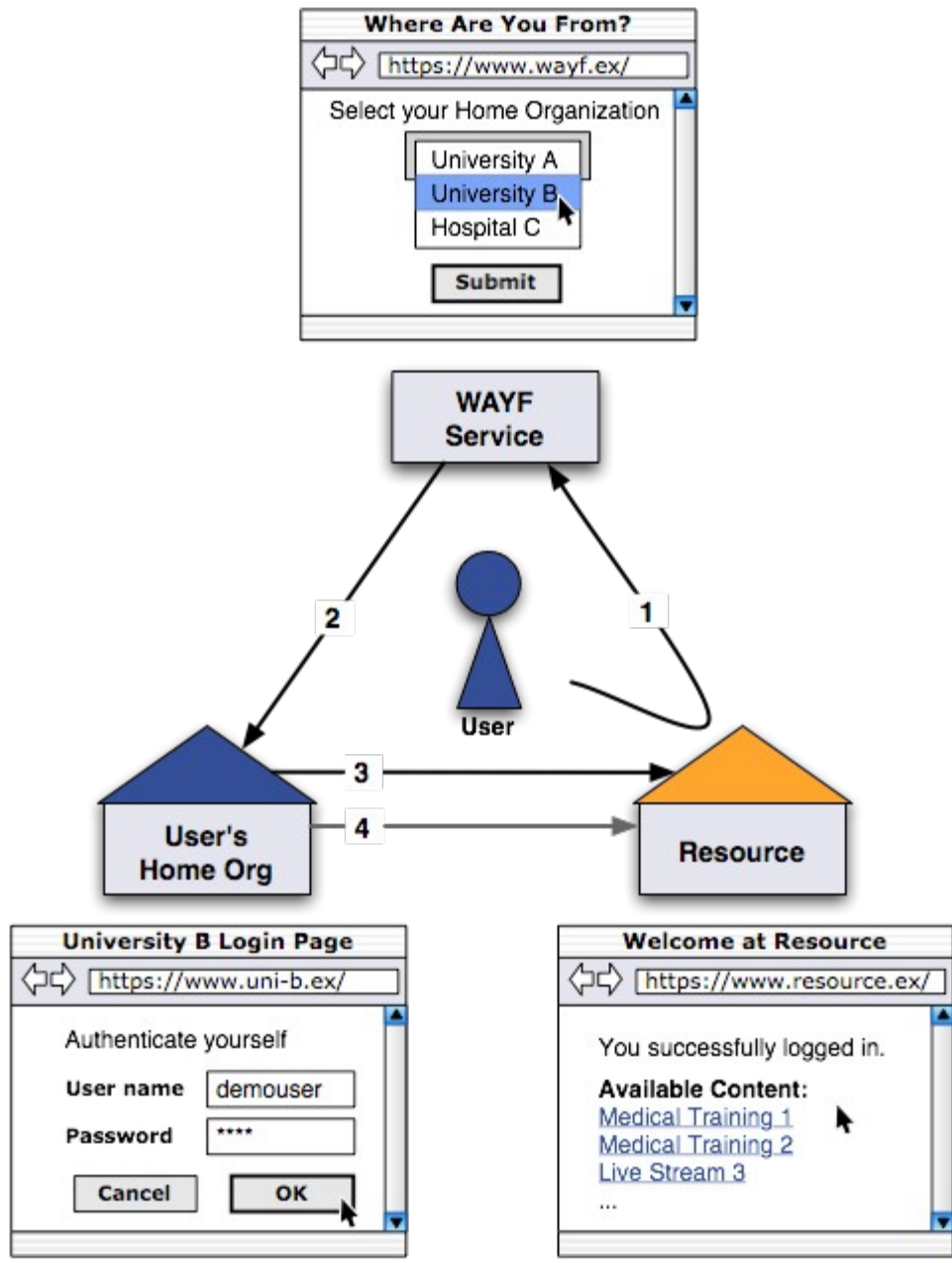
- „na Internetu nikdo nepozná, že jsi pes“
- neschůdné možnosti
  - jména a hesla (hesel je moc)
  - digitální certifikáty (návštěva CA)
  - jakékoliv řešení, kde uživatel musí cokoliv udělat
- existuje řešení, kdy uživatel nemusí udělat nic, a přece můžeme s jistotou znát jeho identitu – federace identit

# Federace identit

- uživatel má zpravidla nějakou domovskou organizaci (škola, zaměstnavatel)
- organizace si obvykle udržuje aktuální data o uživateli
- organizace obvykle již vyřešila autentizaci svých uživatelů
- systémy ve federaci získávají údaje o uživateli z jeho domovské instituce

# provoz federace

- Identity Providers (IdP) – domovské org.
  - autentizují uživatele
  - poskytují o uživateli *atributy*
    - *jméno, vztah k organizaci, zařazení v organizaci,...*
- Service Providers (SP) – koncové služby
  - získávají data o uživateli od IdP
- WAYF (Where Are You From) služba
  - zjistí od uživatele, kdo je jeho IdP
- závazné politiky



obrázek z webu SWITCH AAI

# Výhody federace

- z pohledu uživatele
  - stačí jim jediná sada přihlašovacích údajů
  - vždy se autentizují „doma“
  - odnaučí se zadávat jméno a heslo všude na každé požádání
- z pohledu poskytovatele služeb
  - není nutné jednat s každým uživatelem zvlášť, stačí přimět organizaci k instalaci IdP
  - má vždy aktuální údaje o uživateli od IdP

# Existující federace

- implementace RADIUS
  - pro přihlašování k sítím (WiFi)
  - federace EDUROAM (Evropa, Austrálie, Jap.)
- implementace Shibboleth
  - pro přístup k webovým stránkám
  - akademická švýcarská federace SWITCH AAI
  - americká federace InCommon
  - česká CzTestFed (CESNET)

# CzTestFed WAYF

[O federaci](#) | [Politika](#) | [Kontakty](#)

**Zvolte vaši domovskou organizaci:**

CESNET

Fakulta elektrotechnická ČVUT

**Masarykova univerzita**

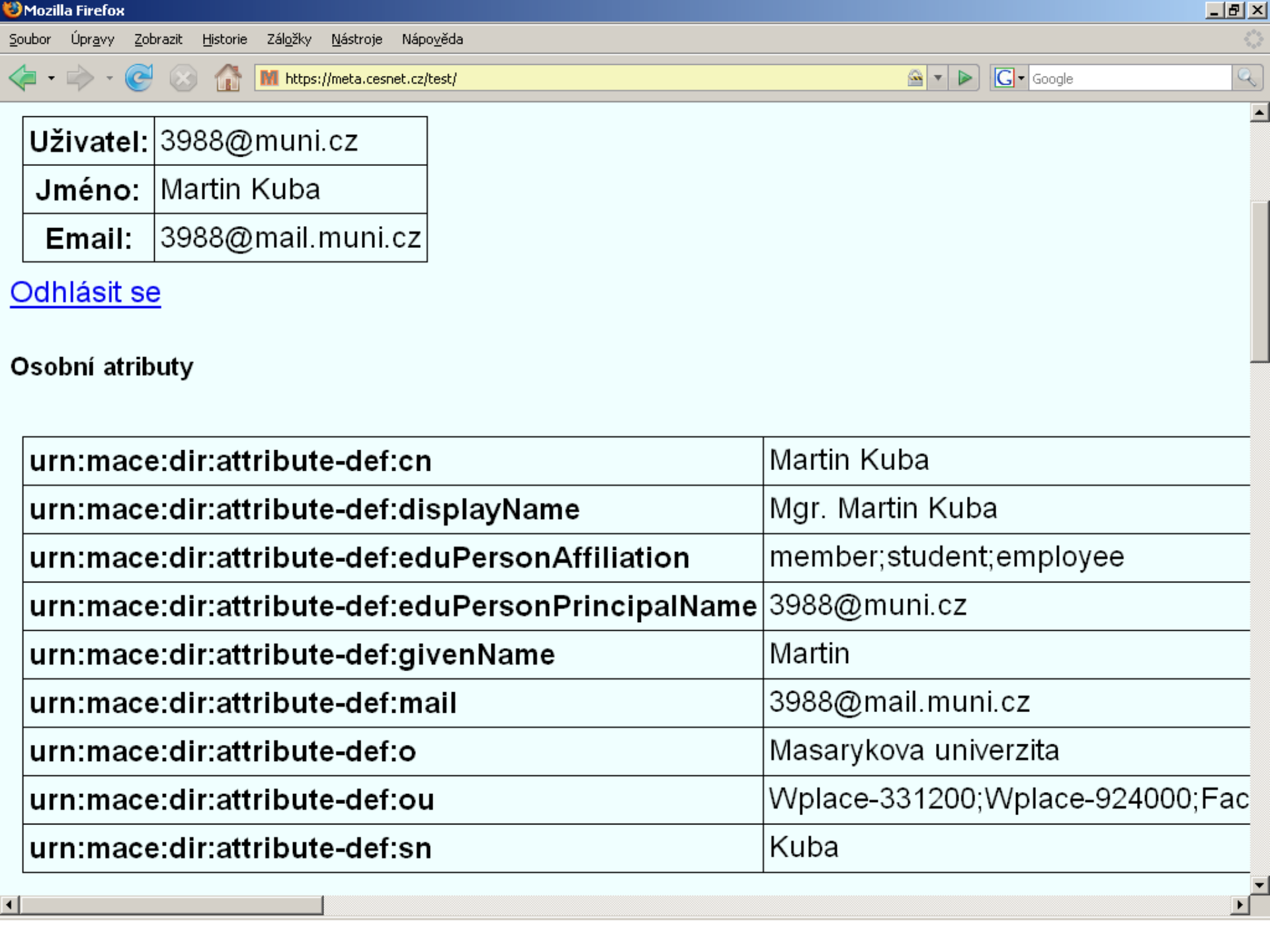
Univerzita Karlova v Praze

Západočeská univerzita v Plzni

METACentrum

Masarykova nemocnice

<h2>Masarykova univerzita AAI - přihlašovací stránka</h2>	
 <a href="#">Nápověda</a> <a href="#">ÚVT</a>	<p>Pokusil jste se přistoupit na stránky, které vyžadují autentizaci. Pro přihlášení použijte UČO a sekundární heslo.</p> <p><b>Uživatelské jméno (UČO)</b> <input type="text" value="3988"/></p> <p><b>Heslo</b> <input type="password" value="*****"/></p> <p><input type="button" value="Přihlásit"/></p>



<b>Uživatel:</b>	3988@muni.cz
<b>Jméno:</b>	Martin Kuba
<b>Email:</b>	3988@mail.muni.cz

[Odhlásit se](#)

### Osobní atributy

<b>urn:mace:dir:attribute-def:cn</b>	Martin Kuba
<b>urn:mace:dir:attribute-def:displayName</b>	Mgr. Martin Kuba
<b>urn:mace:dir:attribute-def:eduPersonAffiliation</b>	member;student;employee
<b>urn:mace:dir:attribute-def:eduPersonPrincipalName</b>	3988@muni.cz
<b>urn:mace:dir:attribute-def:givenName</b>	Martin
<b>urn:mace:dir:attribute-def:mail</b>	3988@mail.muni.cz
<b>urn:mace:dir:attribute-def:o</b>	Masarykova univerzita
<b>urn:mace:dir:attribute-def:ou</b>	Wplace-331200;Wplace-924000;Fac
<b>urn:mace:dir:attribute-def:sn</b>	Kuba

# Naše zkušenosti

- ve federacích je problém dohodnout význam atributů (member, staff, associate)
- preferujeme virtuální organizace uvnitř federací
  - federace zajišťuje jen identifikátor a jméno osoby
  - atributy si dohodnou VO podle potřeb
- za lékaře považujeme osobu s titulem MUDr.
- autorizace na SP je lépe provádět pomocí *entitlement* atributů než znát význam atributů



- vyvinut v rámci projektu Internet2
- SP - moduly do Apache a IIS, shibd démon
- IdP – Java aplikace pro TomCat
- atributy předávány pomocí jazyka SAML
- identita IdP a SP je zajištěna pomocí X509 certifikátů a souboru se seznamem
- na IdP lze nastavit, jaké atributy se kterému SP posílají, a naopak
- podporuje i anonymní přístup

# interakce léků

- prototypová aplikace s webovým rozhraním na platformě JavaEE
- v rámci projektu MediGrid, distribuovaném přes řadu institucí
- pro ověření konceptu federací a demonstraci použití
- technické řešení – Shibboleth SP, Apache
- dohodnuta VO v rámci CzTestFed

# Konec

- Děkuji za pozornost