Shibboleth és Drupal alapú SSO

HBONE Workshop 2008

Márton Iván, NIIF Intézet
martoni@niif.hu

2008.11.13.

CMS és SSO?

- **Content Management System**

  Mi az?

  Miért kell?

    Sérülékenység

    SQL injection

    Cross Site Scripting (XSS)

    Hibakezelés

  Melyiket válasszuk?

    http://www.cmsmatrix.org/

    Drupal, Joomla, CMS Made Simple, WordPress, stb.

CMS és SSO?

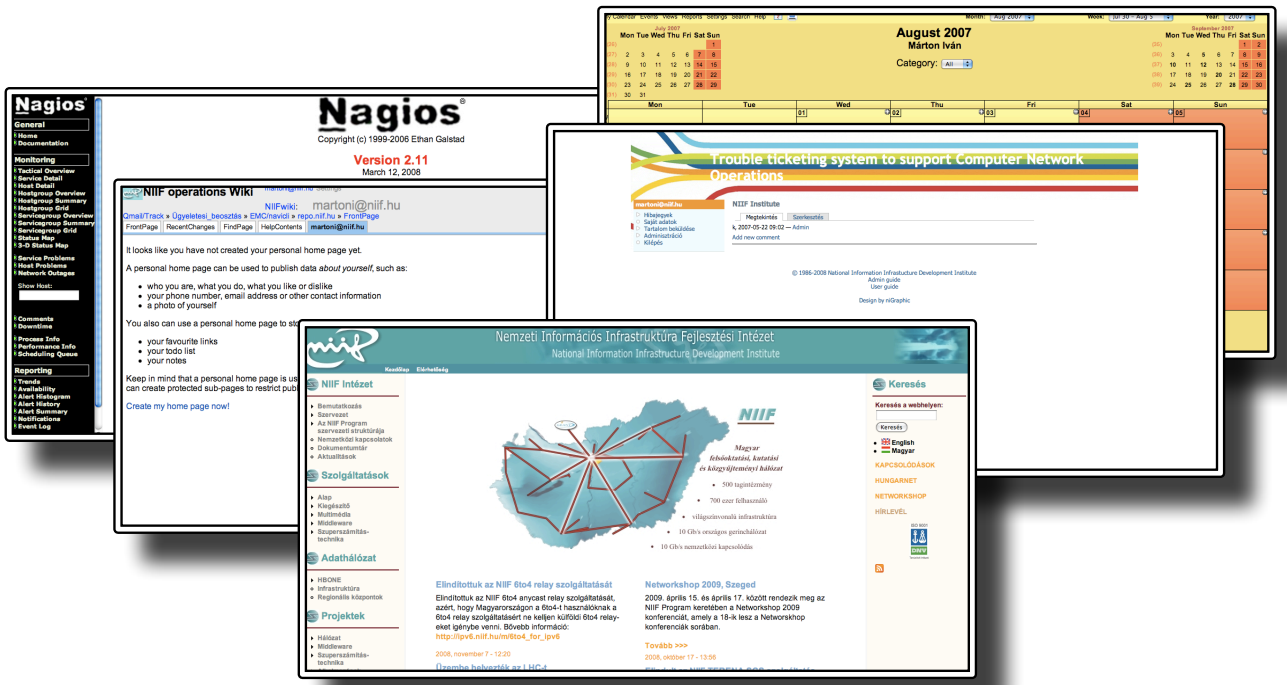
- **Single-Sign On**

  Mi az?

  Központi authentikáció, azonosítás, felhasználó nyilvántartás

  Központi authorizáció, jogosultság kezelés (?)

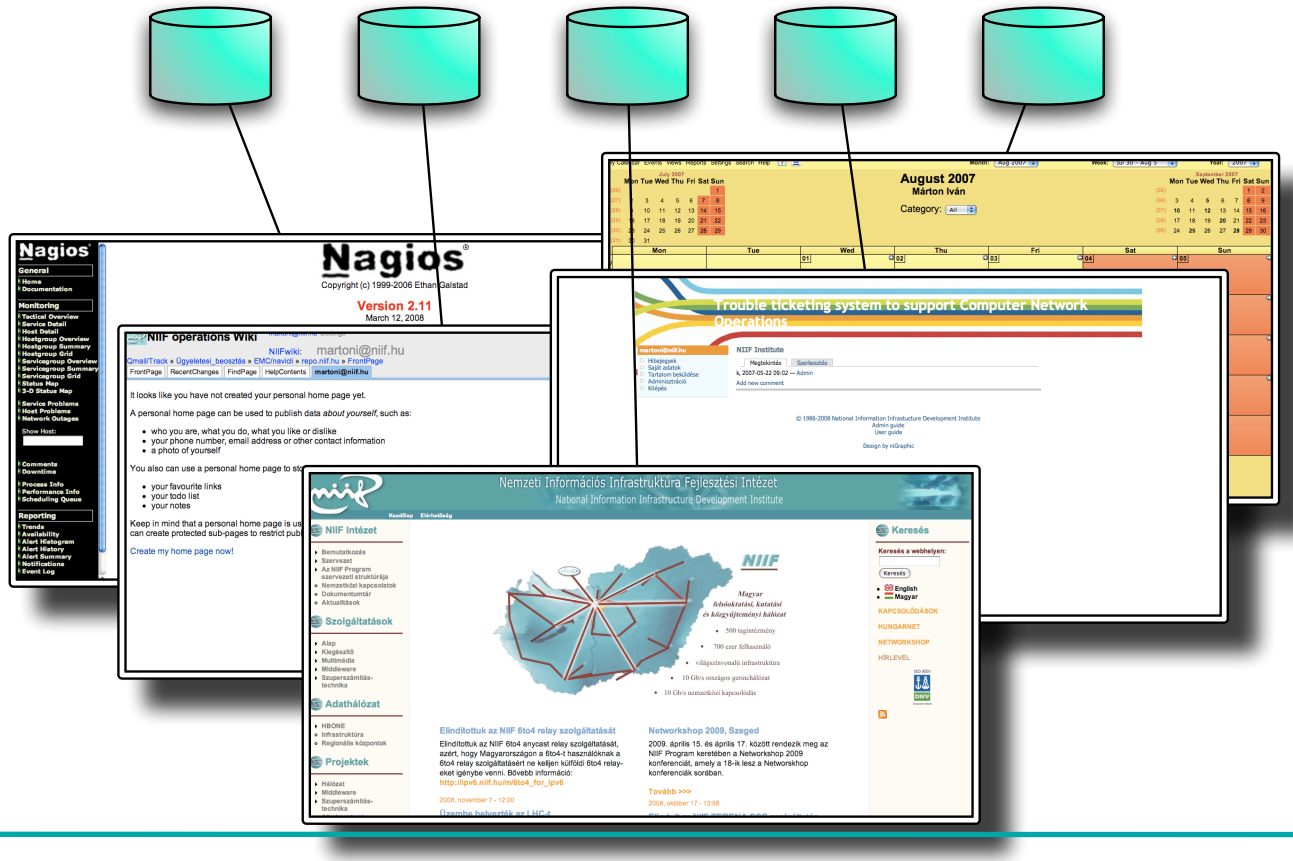
  Egyszeri bejelentkezést tesz lehetővé



CMS és SSO?

- **Lokális adatbázisok**

  Mindenhol különálló nyilvántartás

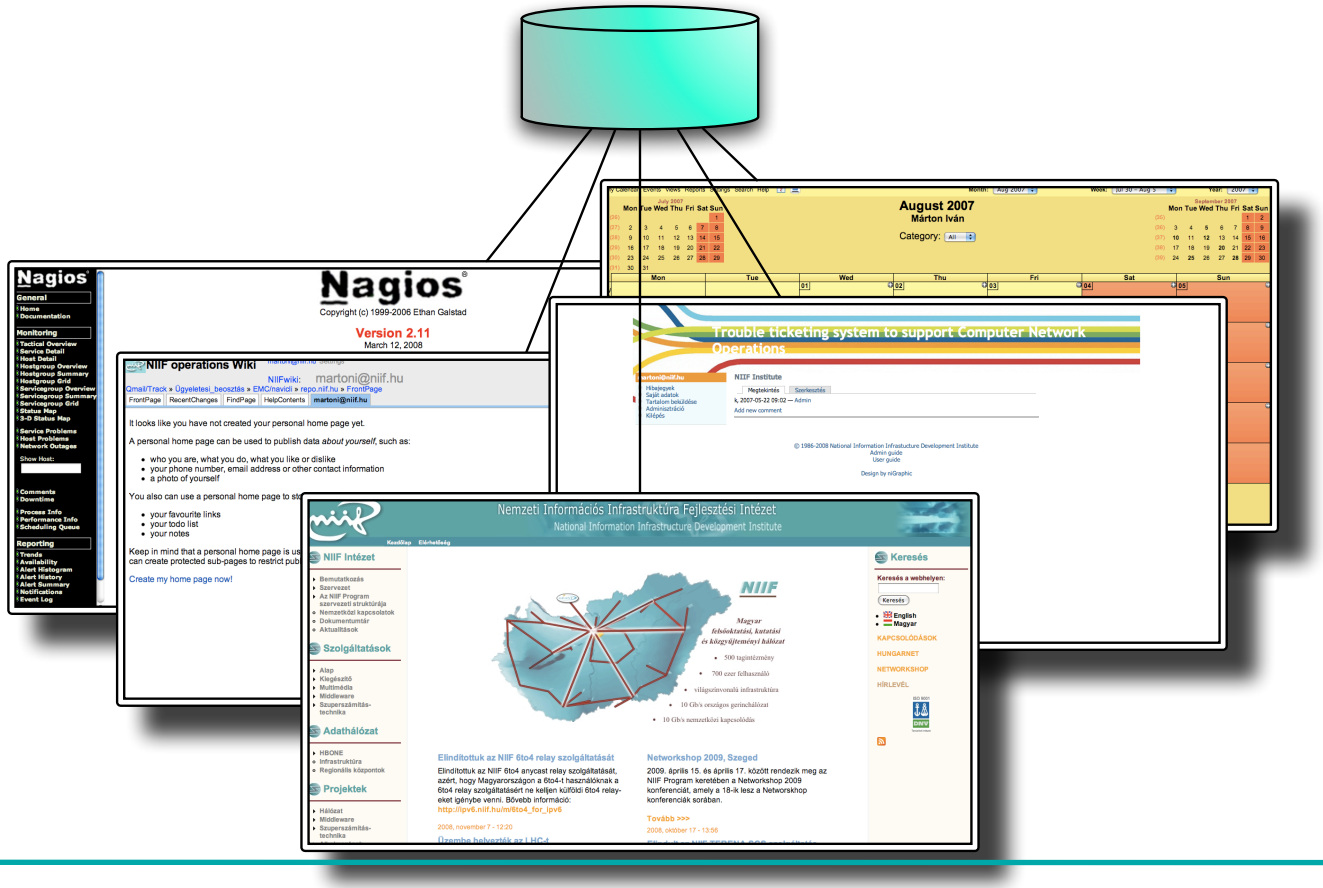


NIIF – *http://www.niif.hu*

CMS és SSO?

- **Központi adatbázis**

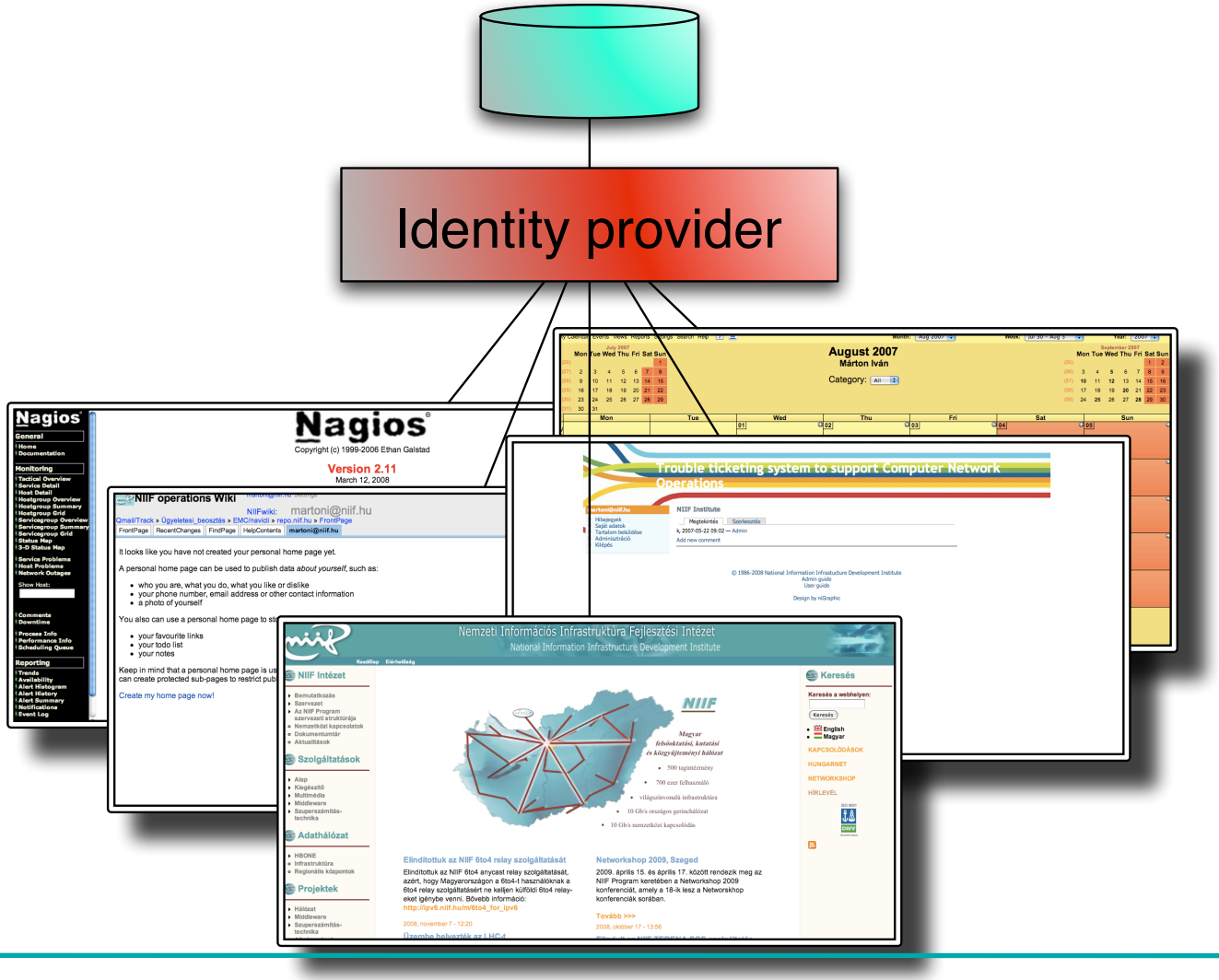
  Mindenhol külön külön bejelentkezés



NIIF – *http://www.niif.hu*

CMS és SSO?

- **Single-Sign On**



NIIF – *http://www.niif.hu*

Shibboleth

- **Biztonságos**

  A felhasználó nem adja ki az adatait ismereten félnek

- **Egyszerű**

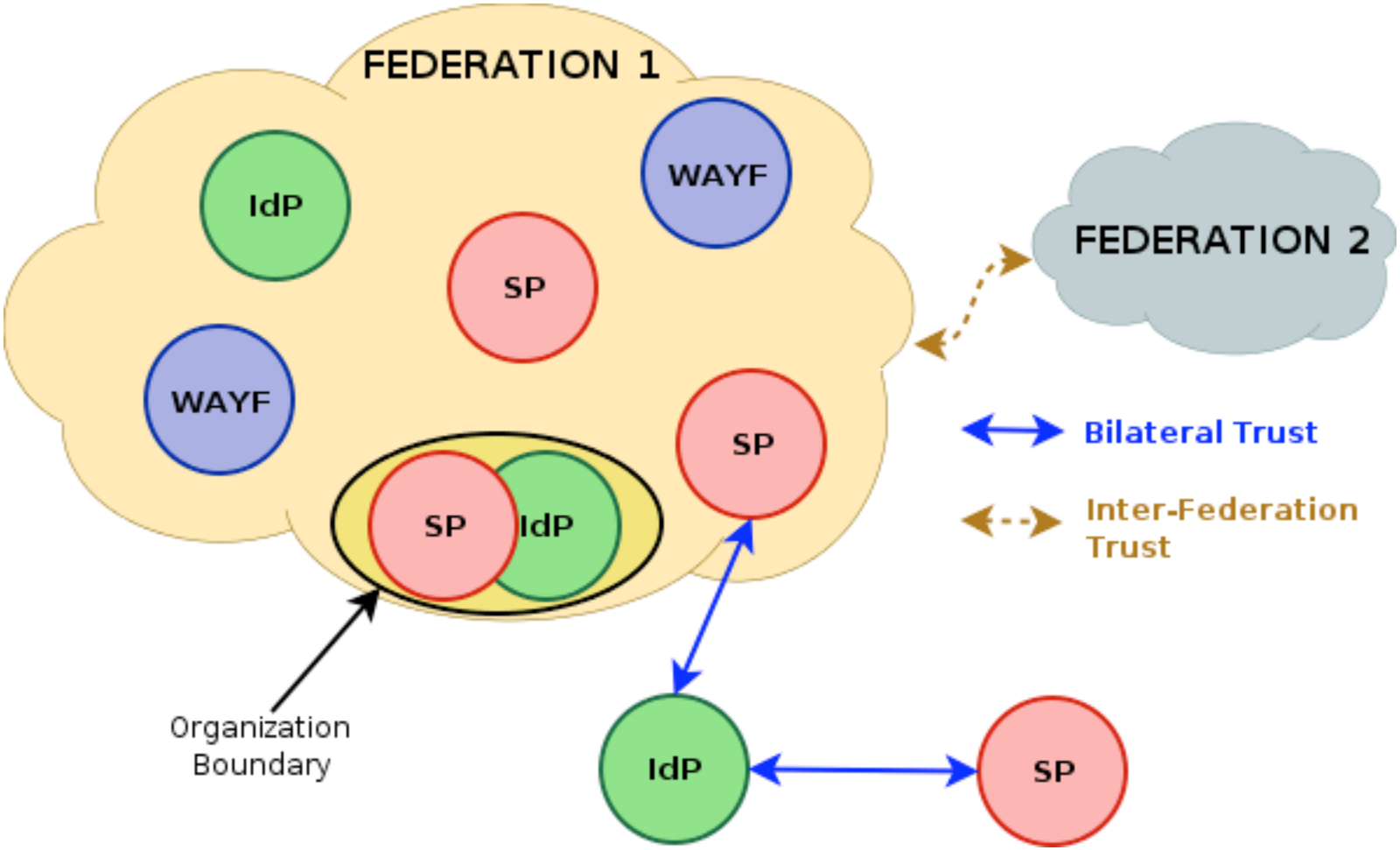
  Elég egyetlen entitás

- **Egységes, mégis elosztott felhasználó menedzsment**

  Föderatív alapú felhasználó menedzsment

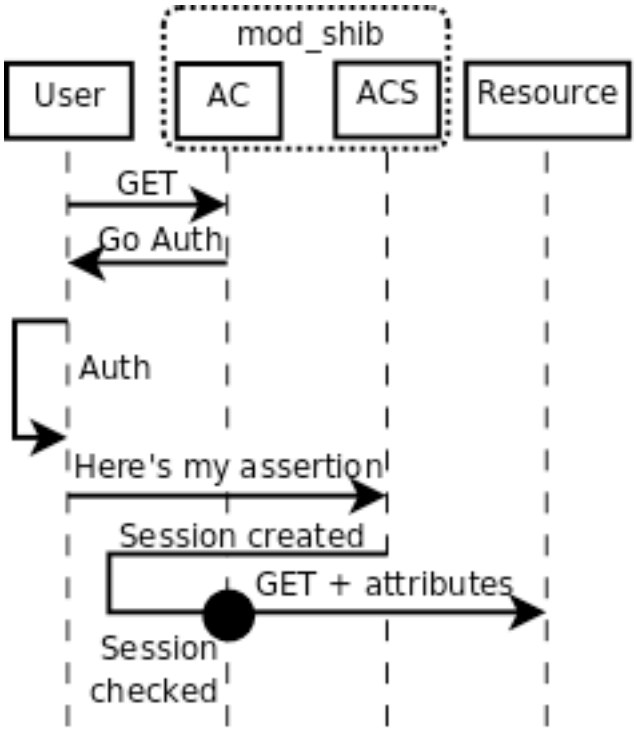
  Fontos egy szabályozott, bizalom alapú föderáció

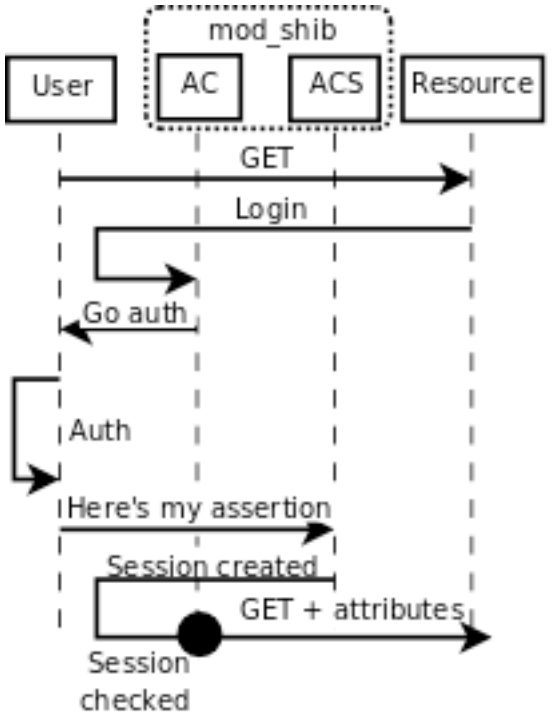
Shibboleth



Az alkalmazást is fel kell készíteni!

Strict & Lazy session





Az alkalmazást is fel kell készíteni!

Drupal SSO

- **OpenID modul**

  https://www.myopenid.com

  Core modul, DE

    nem authorizál

    nem valódi SSO

- **CAS**

  Nálunk hiányzik mögötte az infrastuktúra (USA «-» Európa)

  Automatikus jogosultság osztás (nem konfigurálható)

- **Shibboleth modul**

  Intézetünk fejleszti aktív felhasználói közreműködéssel

  Széles szolgáltatási spektrum

OpenID modul

- **“Identity provider”**

  A felhasználónak rendelkezni kell egy account-tal legalább egy IdP-nél. Az authentikáció MINDENKITŐL elfogadott.

- **SSO**

  Nem valódi Single-Sign On, ugyanis minden oldalon külön-külön be kell jelentkezni.

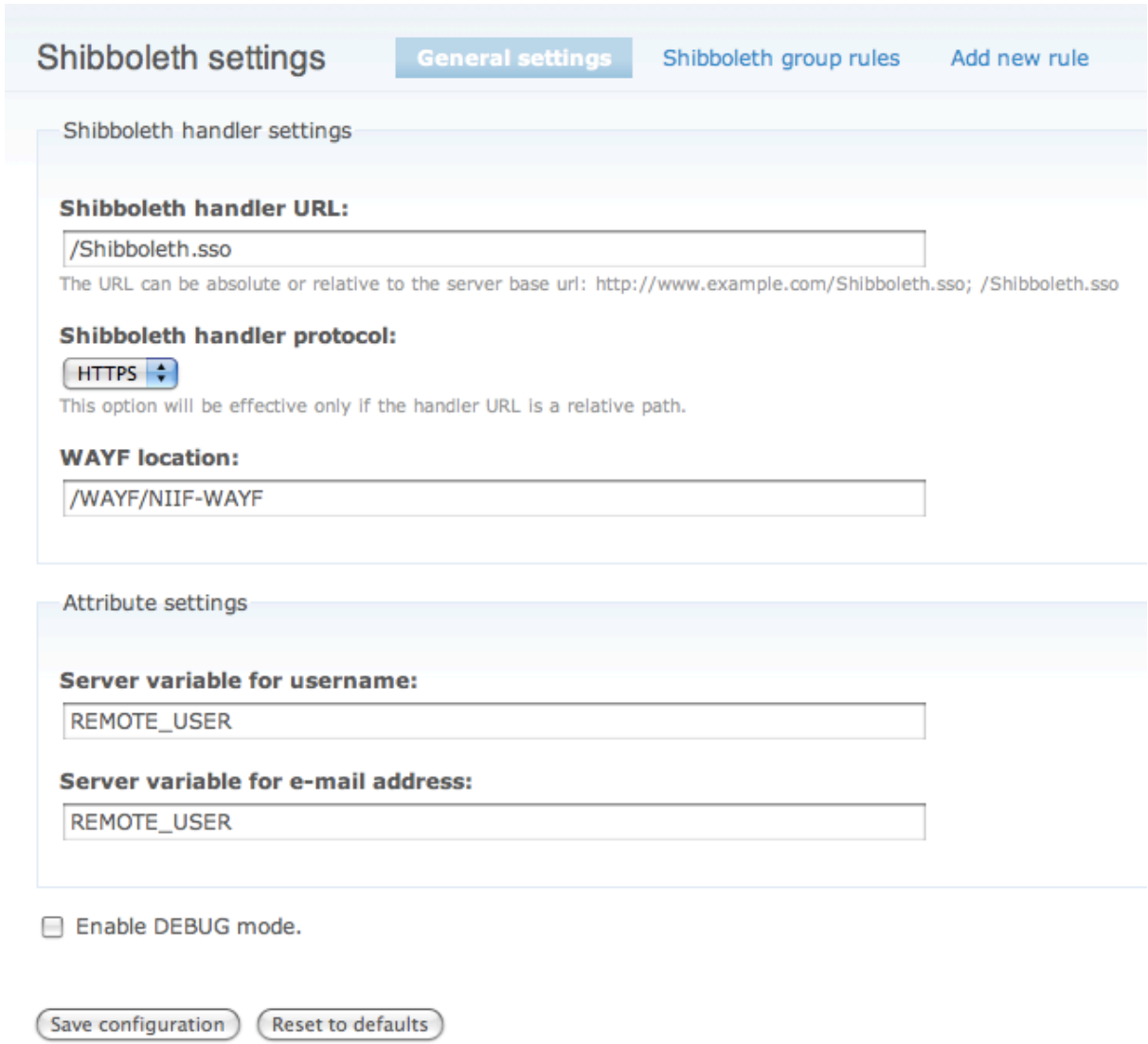
- **Authorizáció**

  Mivel tetszőleges szolgáltató adatai elfogadottak, így KIFEJEZETTEN nem ajánlott ezek alapján az adatok alapján jogokat osztani.

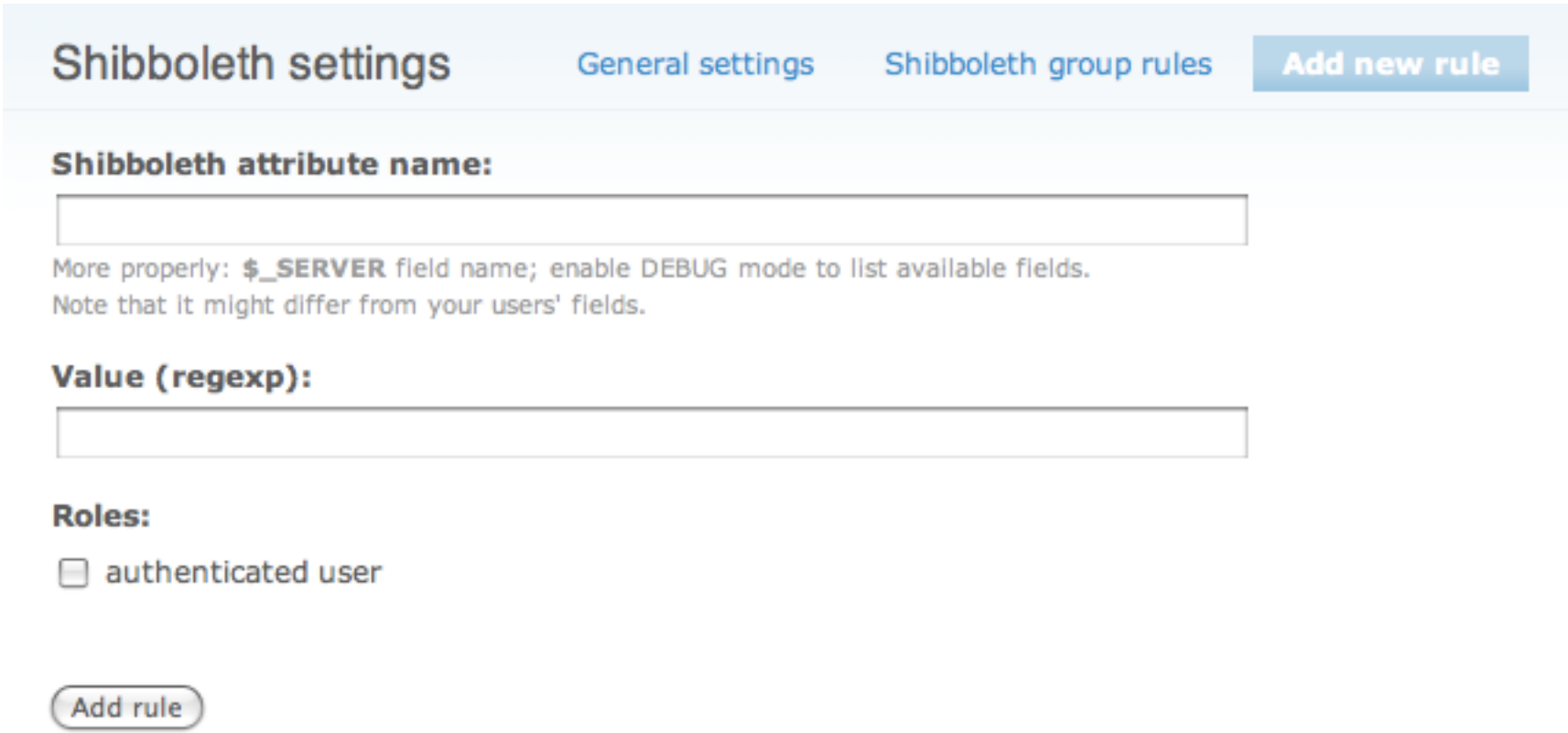
- **Feltétele**

  OpenID szerver, vagy egy már meglévő használata

Shibboleth modul a gyakorlatban



Shibboleth modul a gyakorlatban



Shibboleth modul a gyakorlatban

?

Kérdések - Válaszok

martoni@niif.hu

http://drupal.org/project/shib_auth
http://wiki.aai.niif.hu/index.php/Drupal_Shibboleth_module

?

Kérdések - Válaszok

martoni@niif.hu

http://drupal.org/project/shib_auth

http://wiki.aai.niif.hu/index.php/Drupal_Shibboleth_mod