



# Shibboleth és Drupal alapú SSO

**HBONE Workshop 2008**

**Márton Iván, NIIF Intézet**

*[martoni@niif.hu](mailto: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?

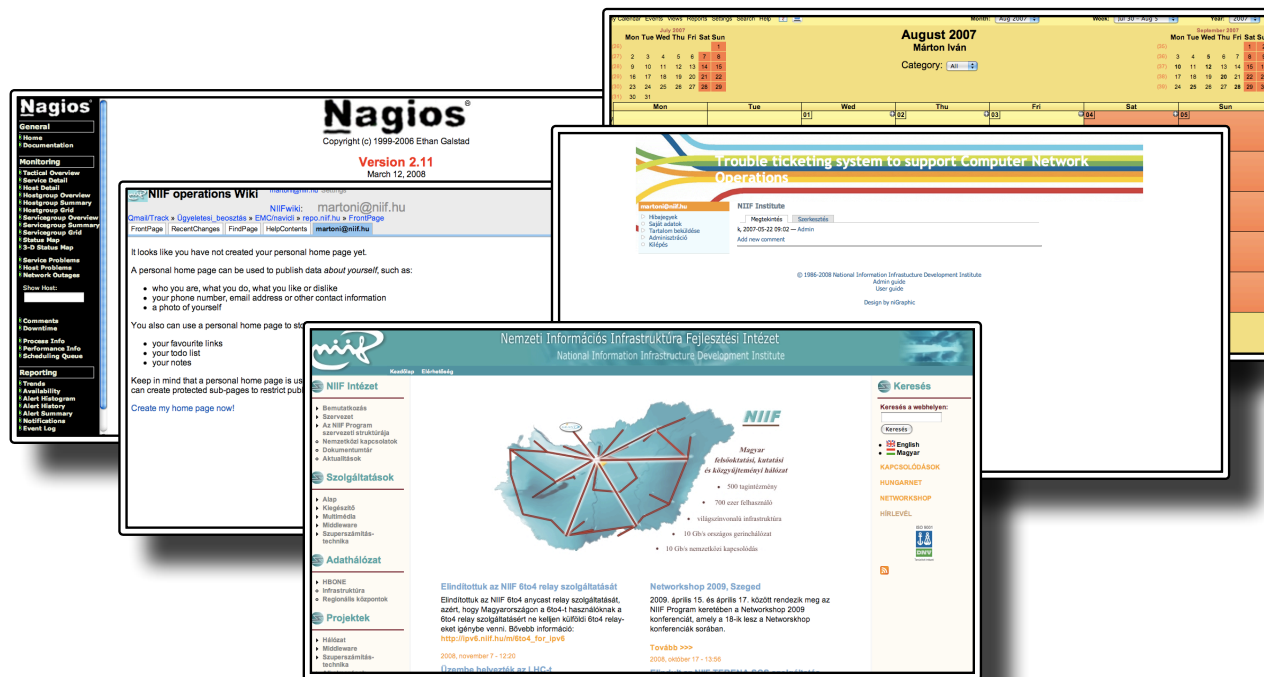
- **Single-Sign On**

Mi az?

Központi autentikáció, azonosítás, felhasználó nyilvántartás

Központi autorizáció, jogosultság kezelés (?)

Egyszeri bejelentkezést tesz lehetővé



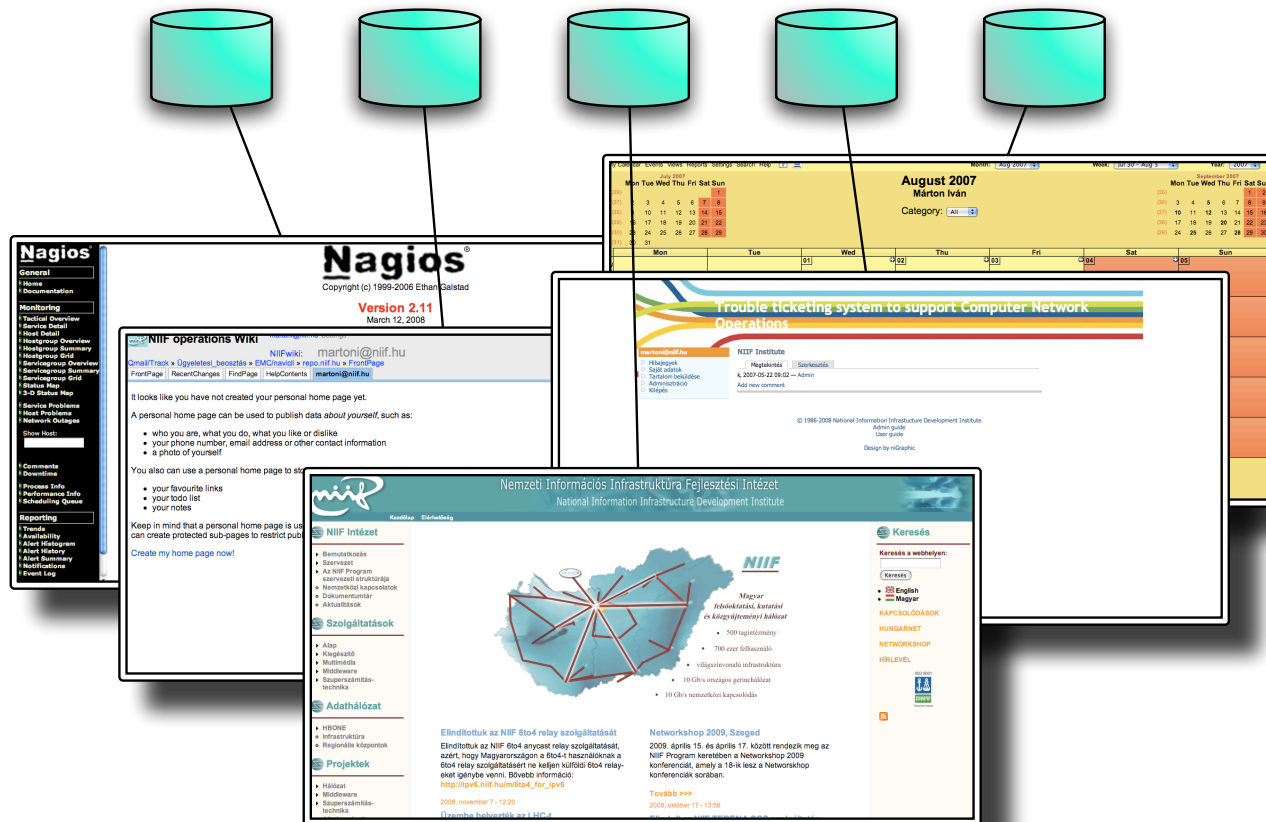
NIIF – <http://www.niif.hu>



# CMS és SSO?

- Lokális adatbázisok

Mindenhol különálló nyilvántartás



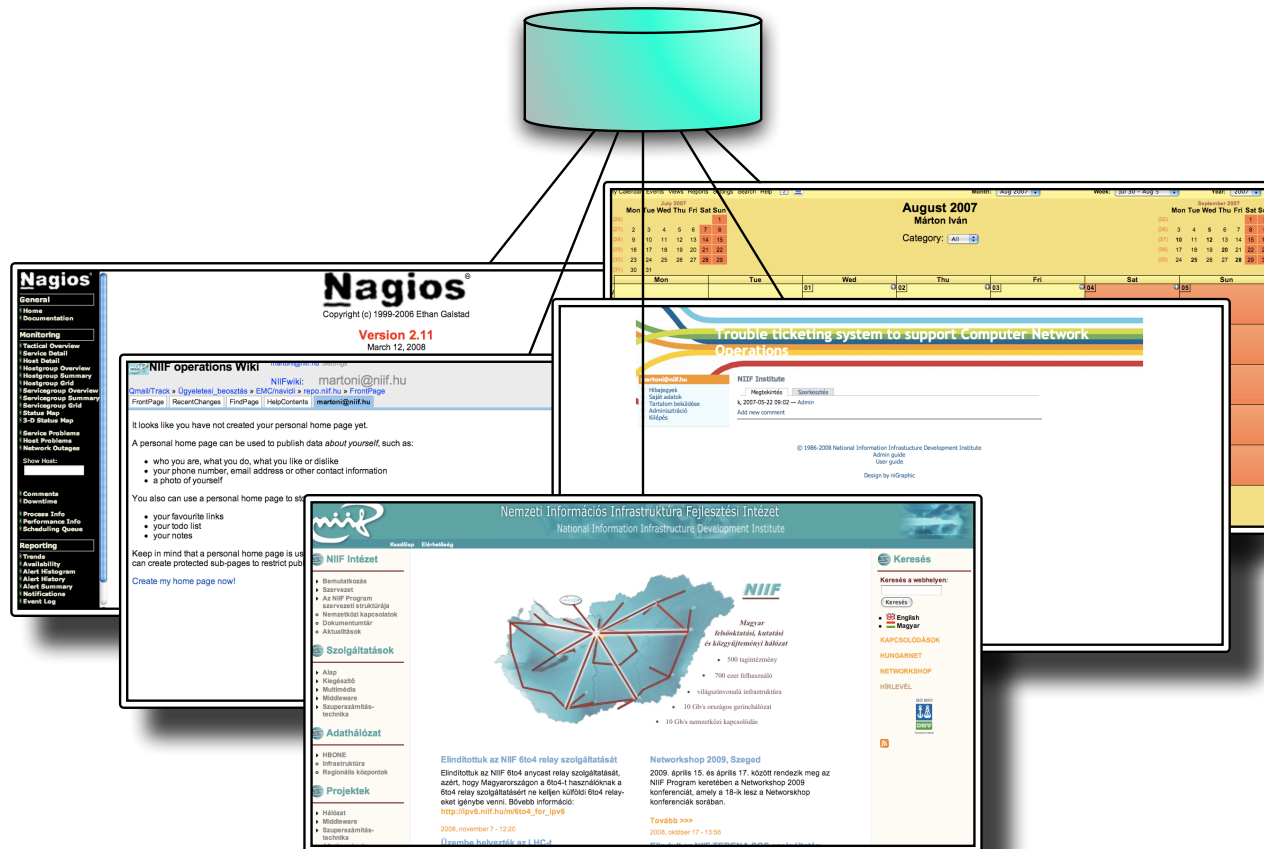
NIIF – <http://www.niif.hu>



# CMS és SSO?

- Központi adatbázis

Mindenhol külön külön bejelentkezés

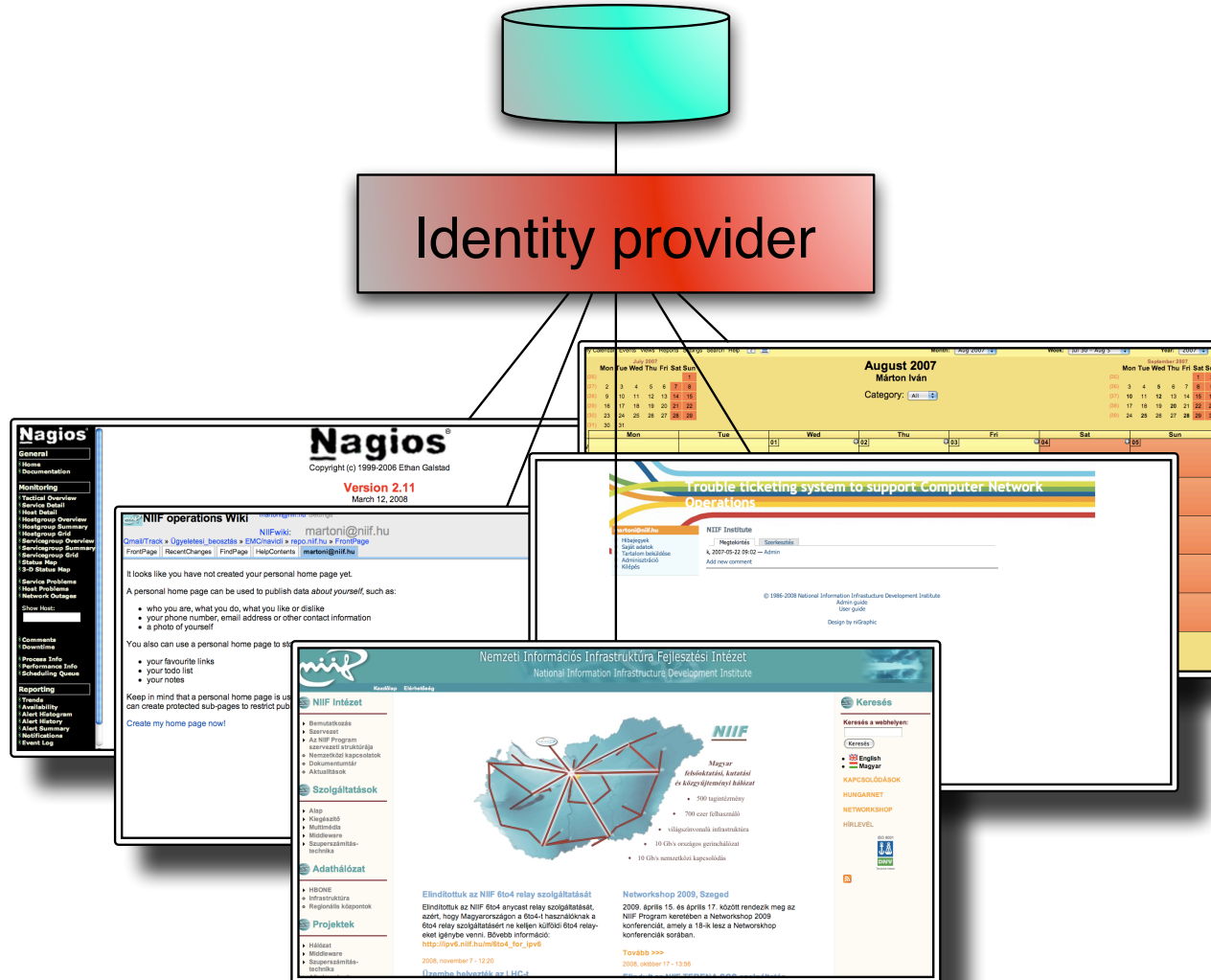


NIIF – <http://www.niif.hu>



# CMS és SSO?

## •Single-Sign On



NIIF – <http://www.niif.hu>



# Shibboleth

- **Biztonságos**

A felhasználó nem adja ki az adatait ismeretlen félnek

- **Egyszerű**

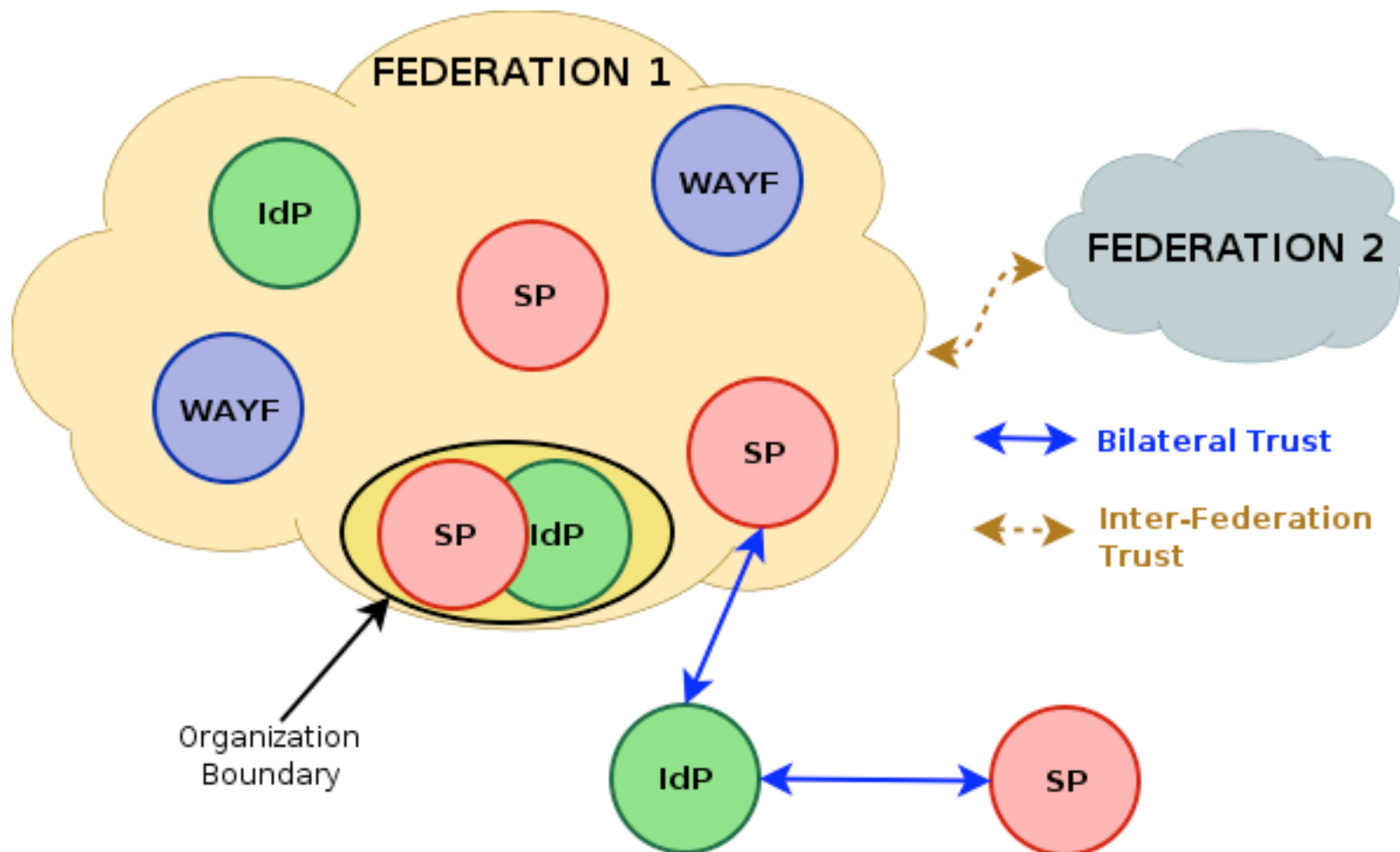
Elég egyetlen entitás

- **Egységes, mégis elosztott felhasználó menedzsment**

Föderatív alapú felhasználó menedzsment

Fontos egy szabályozott, bizalom alapú föderáció

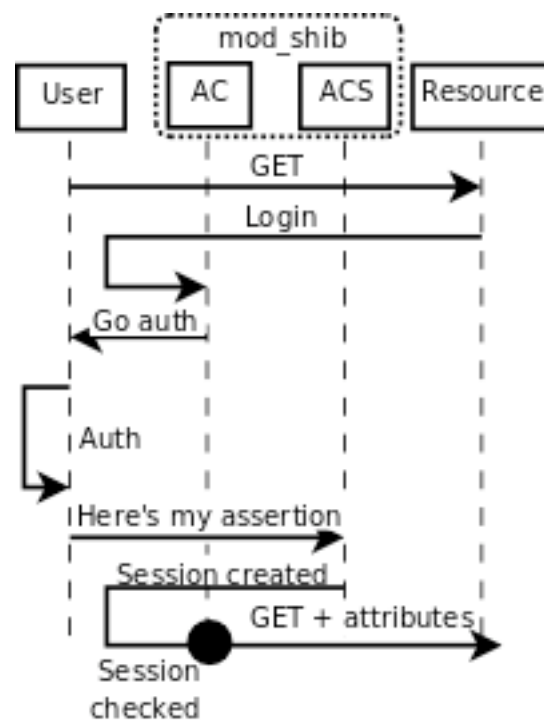
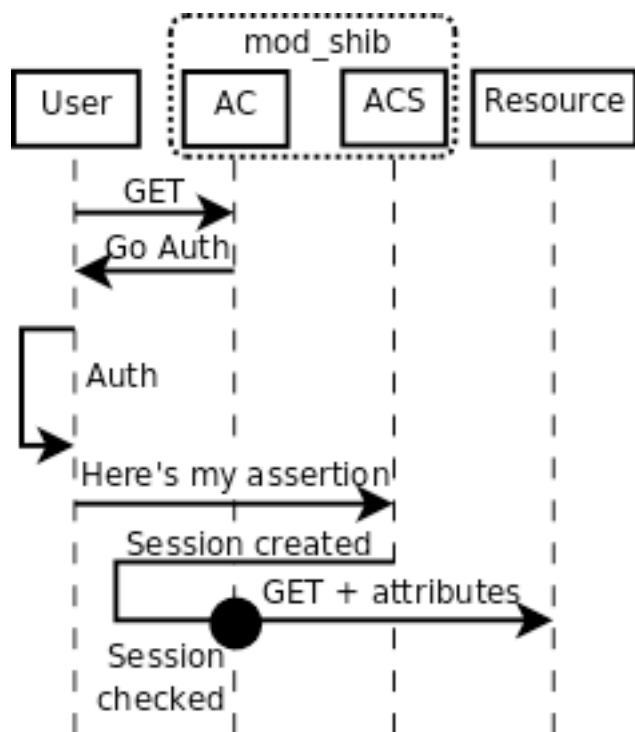
# Shibboleth



**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 infrastruktúra (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 autentikáció **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 settings   **General settings**   Shibboleth group rules   Add new rule

Shibboleth handler settings

**Shibboleth handler URL:**  
  
The URL can be absolute or relative to the server base url: <http://www.example.com/Shibboleth.sso>; /Shibboleth.sso

**Shibboleth handler protocol:**  
   
This option will be effective only if the handler URL is a relative path.

**WAYF location:**

Attribute settings

**Server variable for username:**

**Server variable for e-mail address:**

Enable DEBUG mode.



# Shibboleth modul a gyakorlatban

Shibboleth settings

General settings

Shibboleth group rules

Add new rule

## Shibboleth attribute name:

More properly: `$_SERVER` field name; enable DEBUG mode to list available fields.

Note that it might differ from your users' fields.

## Value (regexp):

## Roles:

authenticated user

Add rule



# Shibboleth modul a gyakorlatban

Shibboleth settings

General settings

Shibboleth group rules

Add new rule

Attribute	RegExp	Role(s)	Actions
affiliation	^staff@niif.hu\$	staff	<a href="#">Clone</a>   <a href="#">Edit</a>   <a href="#">Delete</a>



## Kérdések - Válaszok

[\*martoni@niif.hu\*](mailto:martoni@niif.hu)

[\*http://drupal.org/project/shib\\_auth\*](http://drupal.org/project/shib_auth)

[\*http://wiki.aai.niif.hu/index.php/Drupal\\_Shibboleth\\_module\*](http://wiki.aai.niif.hu/index.php/Drupal_Shibboleth_module)



## Kérdések - Válaszok

[\*martoni@niif.hu\*](mailto:martoni@niif.hu)

[\*http://drupal.org/project/shib\\_auth\*](http://drupal.org/project/shib_auth)

[\*http://wiki.aai.niif.hu/index.php/Drupal\\_Shibboleth\\_mod\*](http://wiki.aai.niif.hu/index.php/Drupal_Shibboleth_mod)