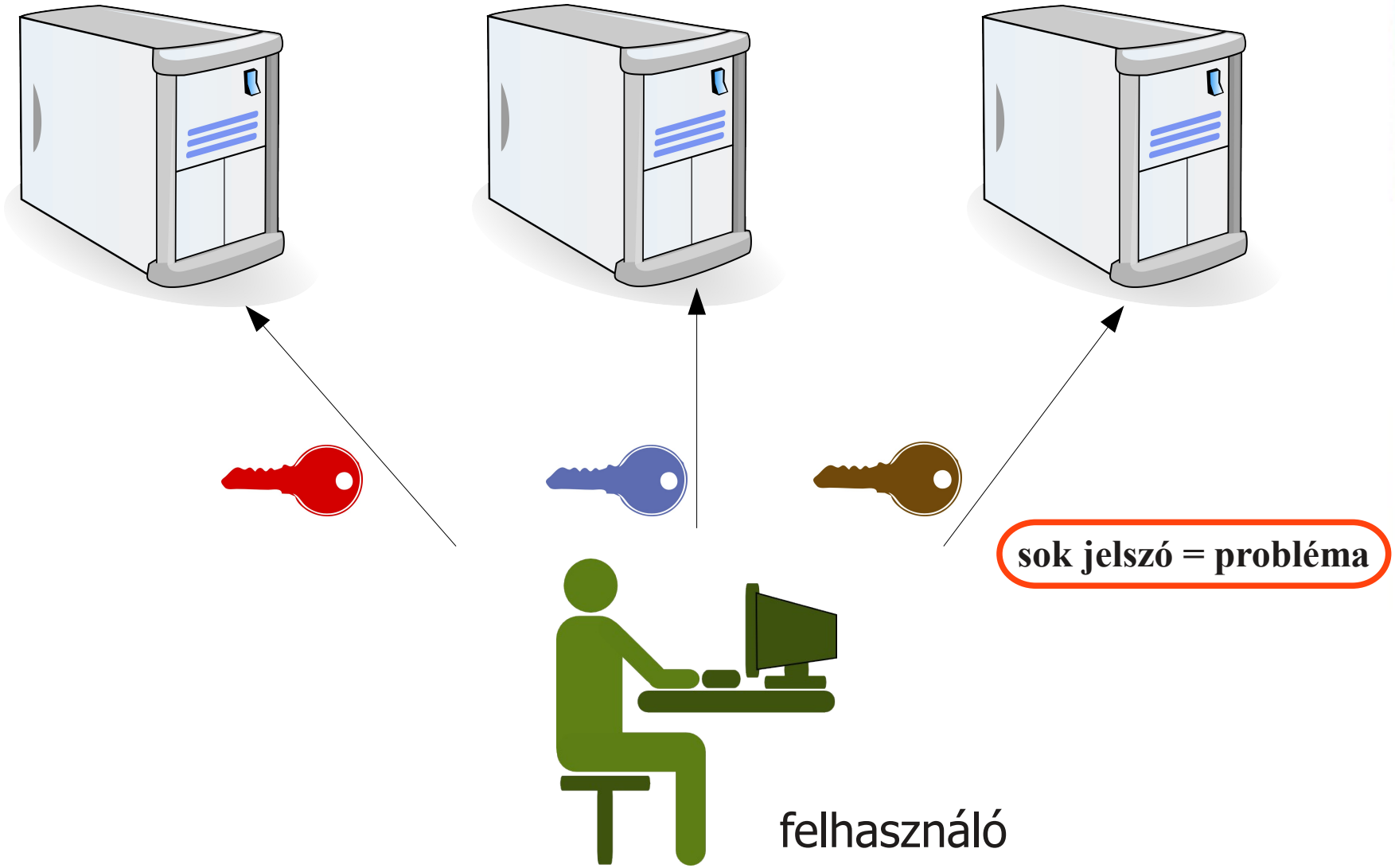
Shibboleth alapú felhasználó-azonosítás a Moodle rendszerben

Dr. Tornóci László, Dr. Kokovay Ágnes

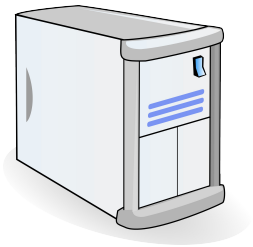
Semmelweis Egyetem
E-learning és Digitális Tartalomfejlesztő Központ

Klasszikus felhasználóazonosítás



A klasszikus rendszer problémái

Az információszolgáltatók oldaláról:

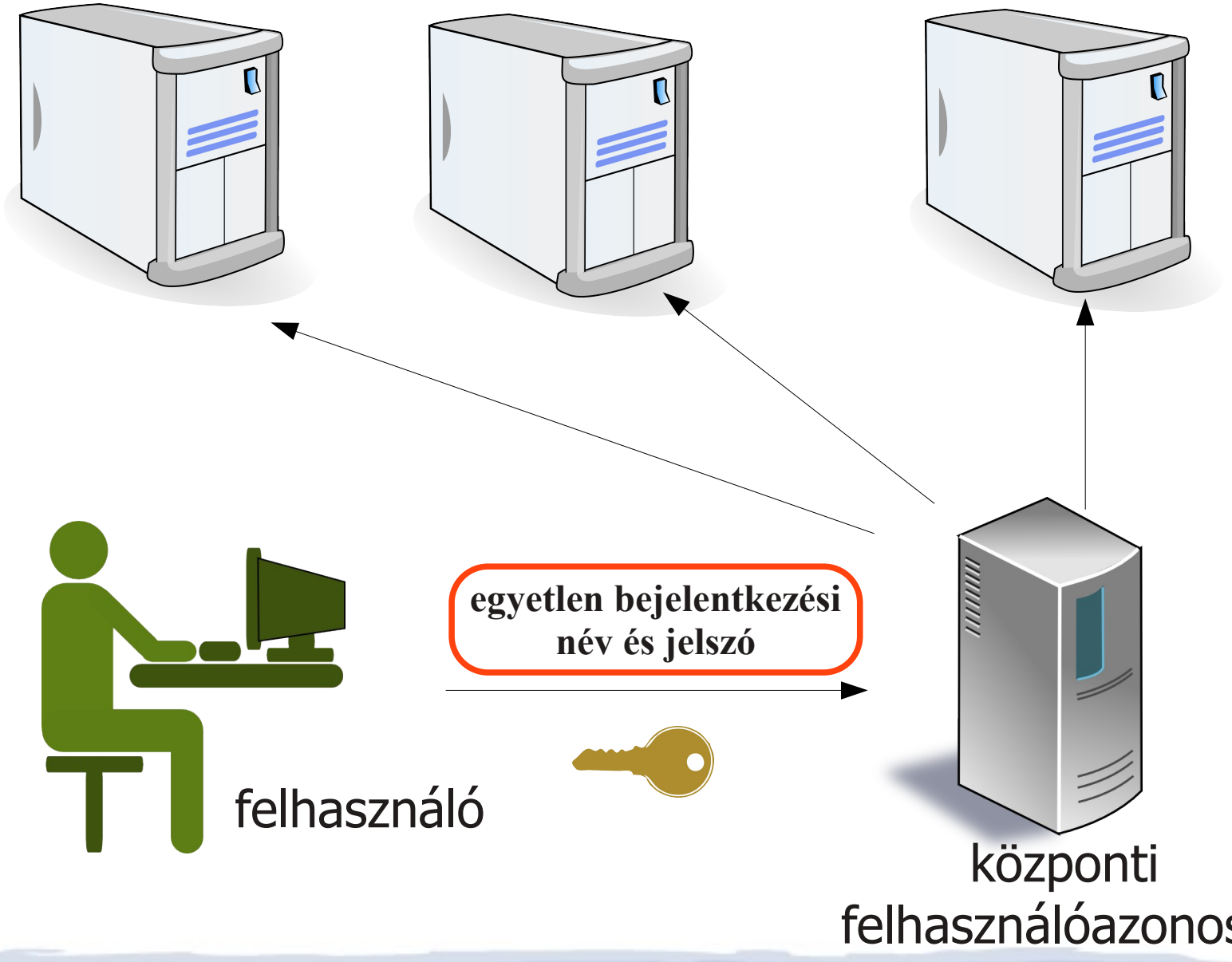


- a jelszó eljuttatása a felhasználókhoz
- a jogosultság ellenőrzése
- a jogosultság visszavonása

A felhasználó oldaláról:

- összekeveri őket
- túl egyszerű jelszavakat választ
- igyekszik ugyanazt használni
- mindez biztonsági probléma

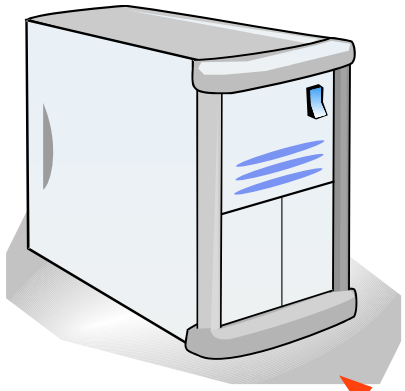
Központi felhasználóazonosítás

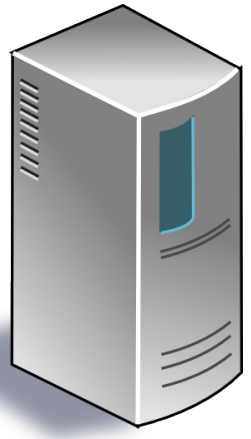


Hogy működik?

információt szolgáltató
kiszolgáló (SP)

központi
felhasználóazonosító (IdP)





1. a felhasználó pl. beírja
   egy védett weboldal címét

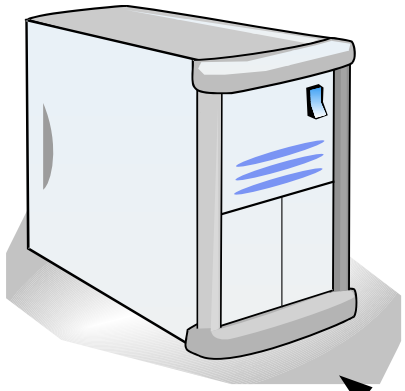
   `https://valami.hu/secure`

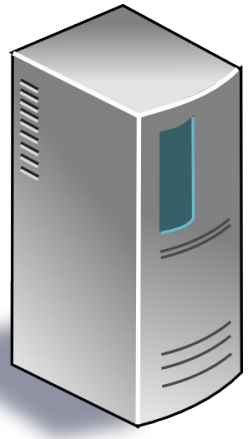
felhasználó

Hogy működik?

információt szolgáltató kiszolgáló (SP)

központi felhasználóazonosító (IdP)





2. átirányítás az IdP-hez

1. a felhasználó pl. beírja egy védett weboldal címét

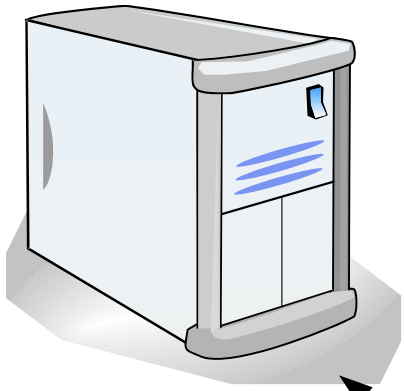
`https://valami.hu/secure`

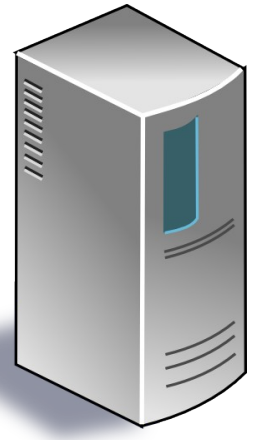
felhasználó

Hogy működik?

információt szolgáltató kiszolgáló (SP)

központi felhasználóazonosító (IdP)





2. átirányítás az IdP-hez

1. a felhasználó pl. beírja egy védett weboldal címét

`https://valami.hu/secure`

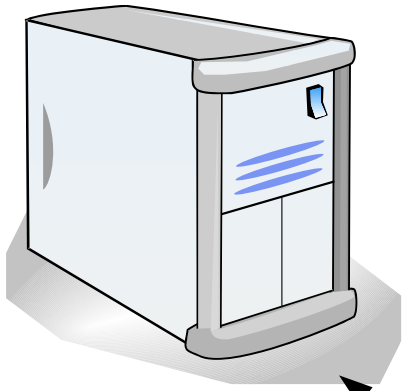
3. kérem a bejelentkezési neved és a jelszavad!

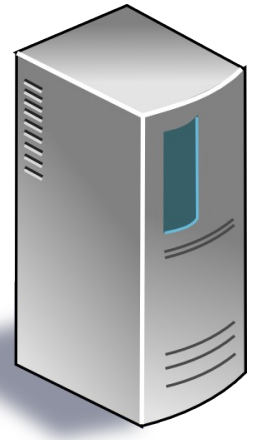
felhasználó

Hogy működik?

információt szolgáltató kiszolgáló (SP)

központi felhasználóazonosító (IdP)





2. átirányítás az IdP-hez

1. a felhasználó pl. beírja egy védett weboldal címét

`https://valami.hu/secure`

3. kérem a bejelentkezési neved és a jelszavad!

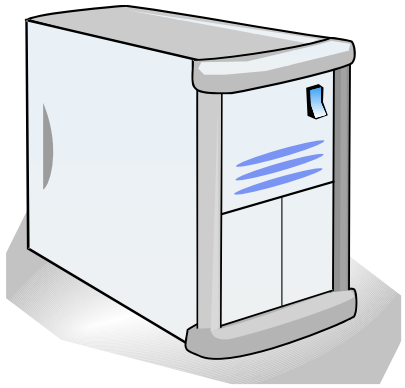
4. bejelentkezés

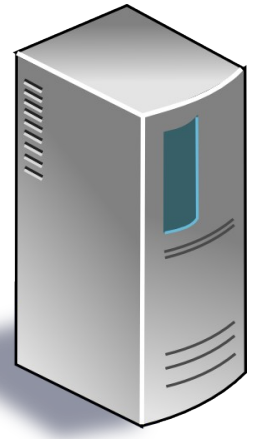
felhasználó

Hogy működik?

információt szolgáltató
kiszolgáló (SP)

központi
felhasználóazonosító (IdP)





5. visszairányítás az SP-hez
+ digitálisan aláírt XML állomány

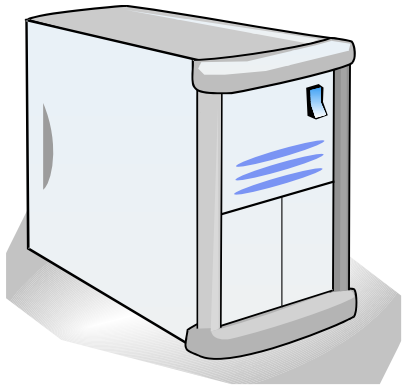
pl. X kar hallgatója,
A, B, C tárgyakat hallgatja

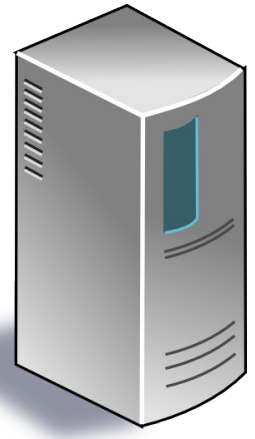
felhasználó

Hogy működik?

információt szolgáltató kiszolgáló (SP)

központi felhasználóazonosító (IdP)





5. visszairányítás az SP-hez
+ digitálisan aláírt XML állomány

pl. X kar hallgatója,
A, B, C tárgyakat hallgatja

6. a kért oldal megjelenik

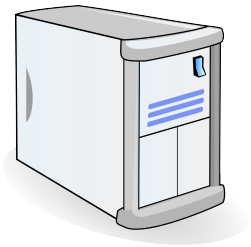
felhasználó

A kiszolgáló nem ismeri a felhasználó jelszavát, de tudja, hogy jogosult!

Mindez a felhasználó számára teljesen transzparens!

A rendszer előnyei 1.

Az információszolgáltatók oldaláról: *egyszerű és biztonságos*



- egyáltalán nem foglalkozik konkrét emberekkel
- egységes jogosultságkezelés (pl. az anatómia oktatói jogosultak megnézni)
- a jogosultság ellenőrzése naprakész

A felhasználó oldaláról: *kényelmes*

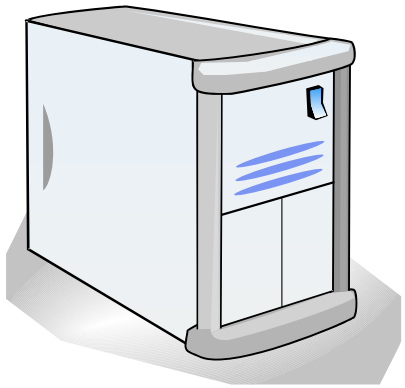
- egy jelszó nagyon sok szolgáltatáshoz jó
- SSO=single sign on: egy munkamenetben elég egyszer bejelentkezni

A rendszer előnyei 2.

- a kommunikáció standard, nyílt protokollon (SAML2: Security Assertion Markup Language) keresztül történik
- nyílt forráskódú implementációk léteznek (pl. Shibboleth, SimpleSAMLphp)
- a rendszert használó intézmények szövetségbe tömörülve föderatív azonosítást használhatnak (pl. EduID)

A Shibboleth program

információt szolgáltató kiszolgáló (SP)



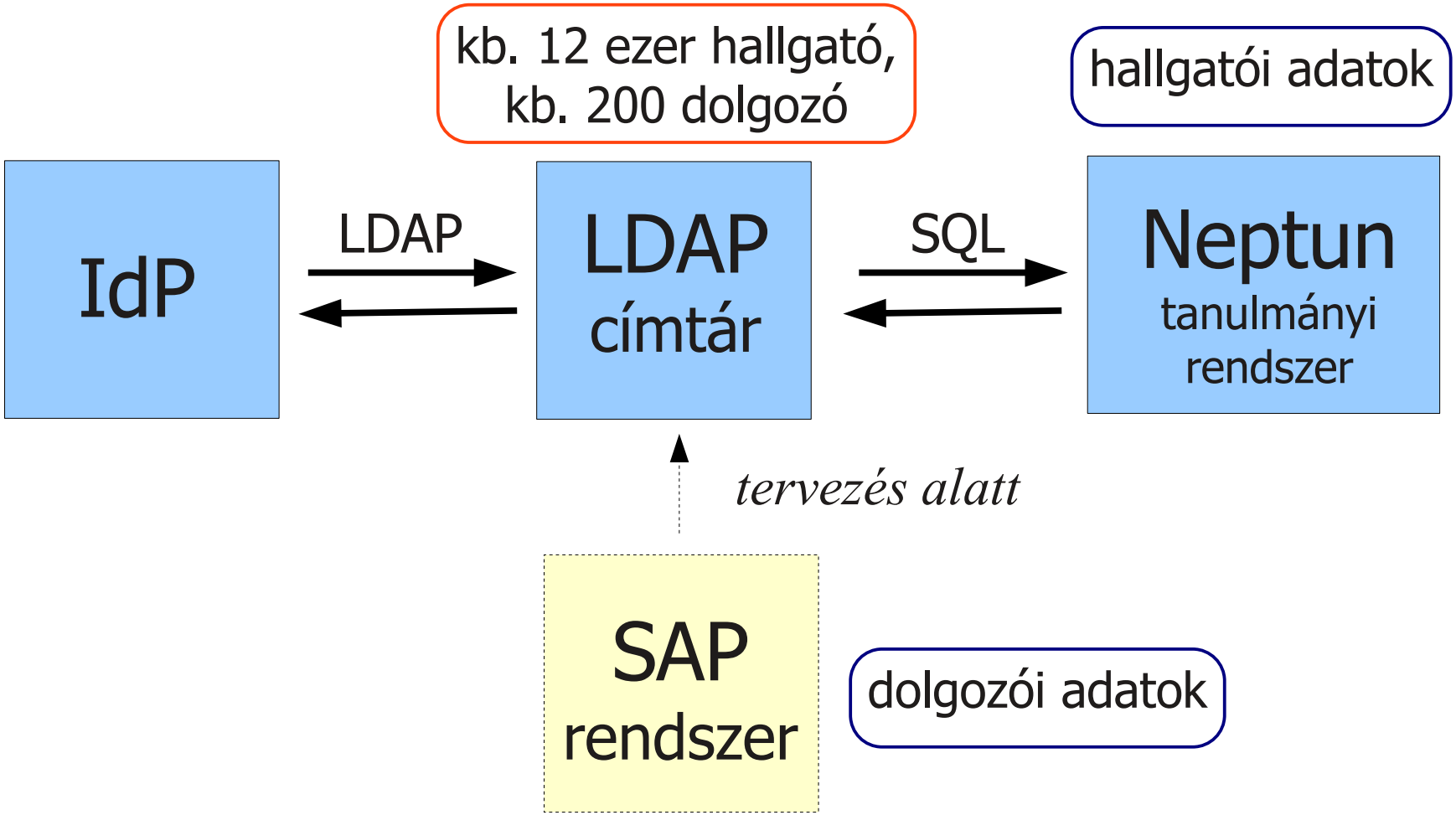
Apache modul + daemon (C-ben van írva)

központi felhasználóazonosító (IdP)

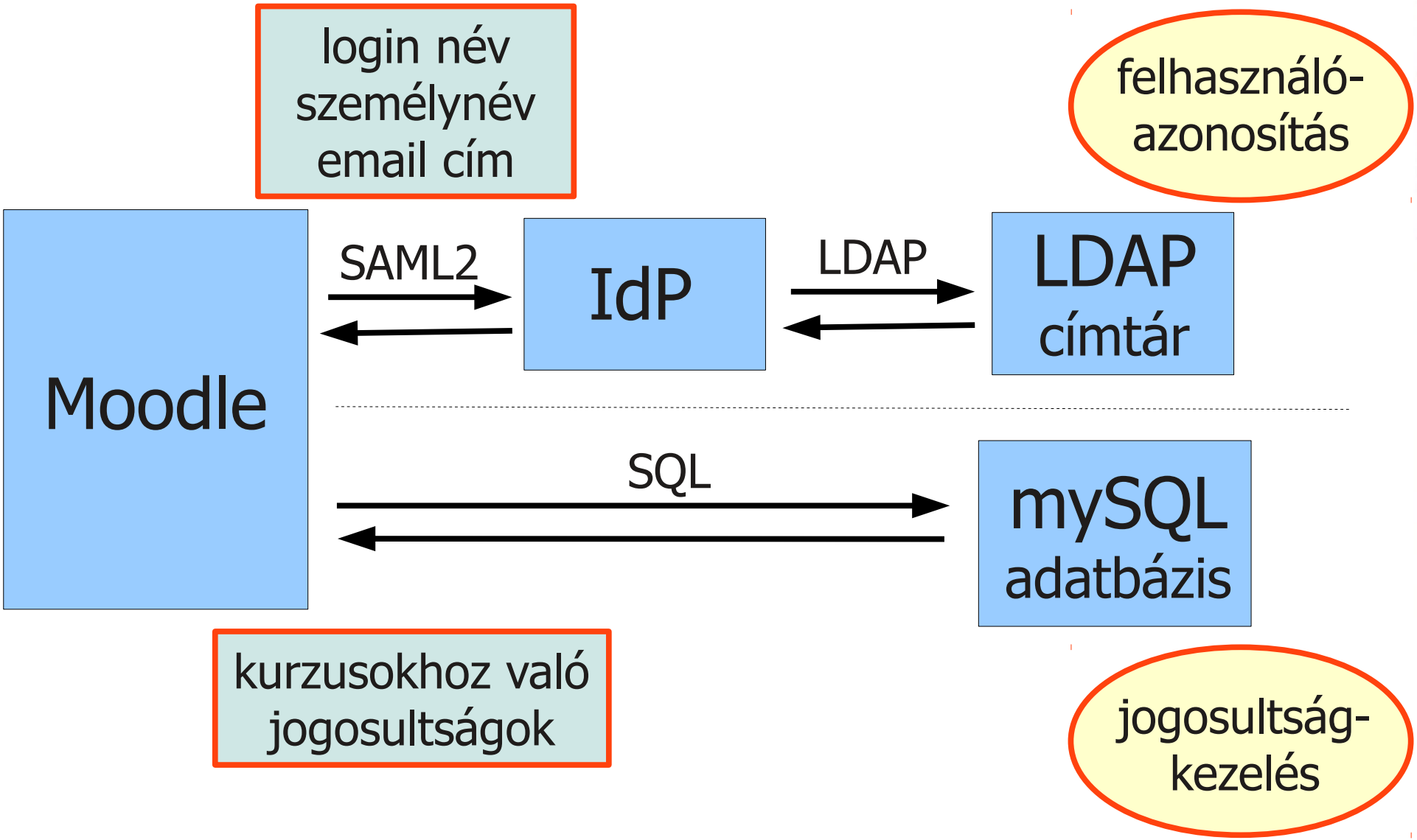
Apache Tomcat + Java alkalmazás

A „shibboleth” héber szó, az angolban azt jelenti, ha valaki a kiejtésével, nyelvhasználatával elárulja hogy valamely embercsoporthoz tartozik-e vagy sem. Egy bibliai történet szerint a gileádiak úgy azonosították az ellenséges efráimiakat, hogy kimondatták velük a „shibboleth” szót, azok ugyanis nem tudták az „s” hangot kiejteni. (Bírák könyve: 12. rész 4-6)

IdP a Semmelweis Egyetemen



A Moodle és az IdP kapcsolata



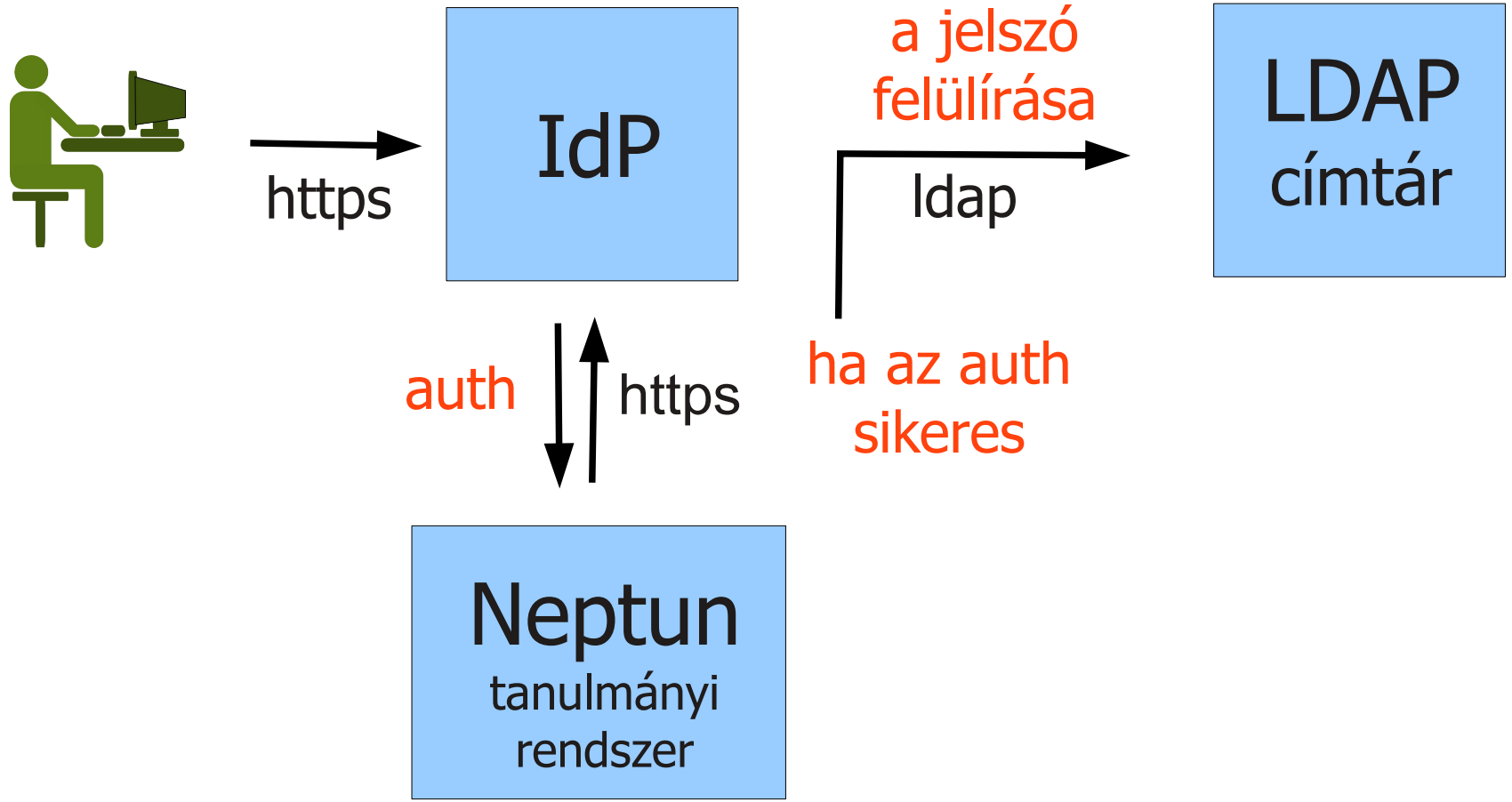
Moodle-Shibboleth előnyök

- Nincs gond a login nevek és jelszók kiosztásával (több ezer hallgatónál ez már nem mindegy)
- A felhasználóknak kényelmes:
  - ha egy jelszóval több szolgáltatást érhetnek el
  - a single-sign-on
- Ha idegen szerverre kell átjelentkeztetnem a felhasználóimat valamelyik kurzusból az authentikáció megőrzésével, akkor egyszerűen fölveszem egy másik SP-nek. Az SSO miatt a felhasználónak nem kell bejelentkeznie, az adatai mégis rendelkezésre állnak az idegen szerveren is.
- Hivatkozhatom a Moodle-ból külső, védett tartalmakra (pl. cikk)

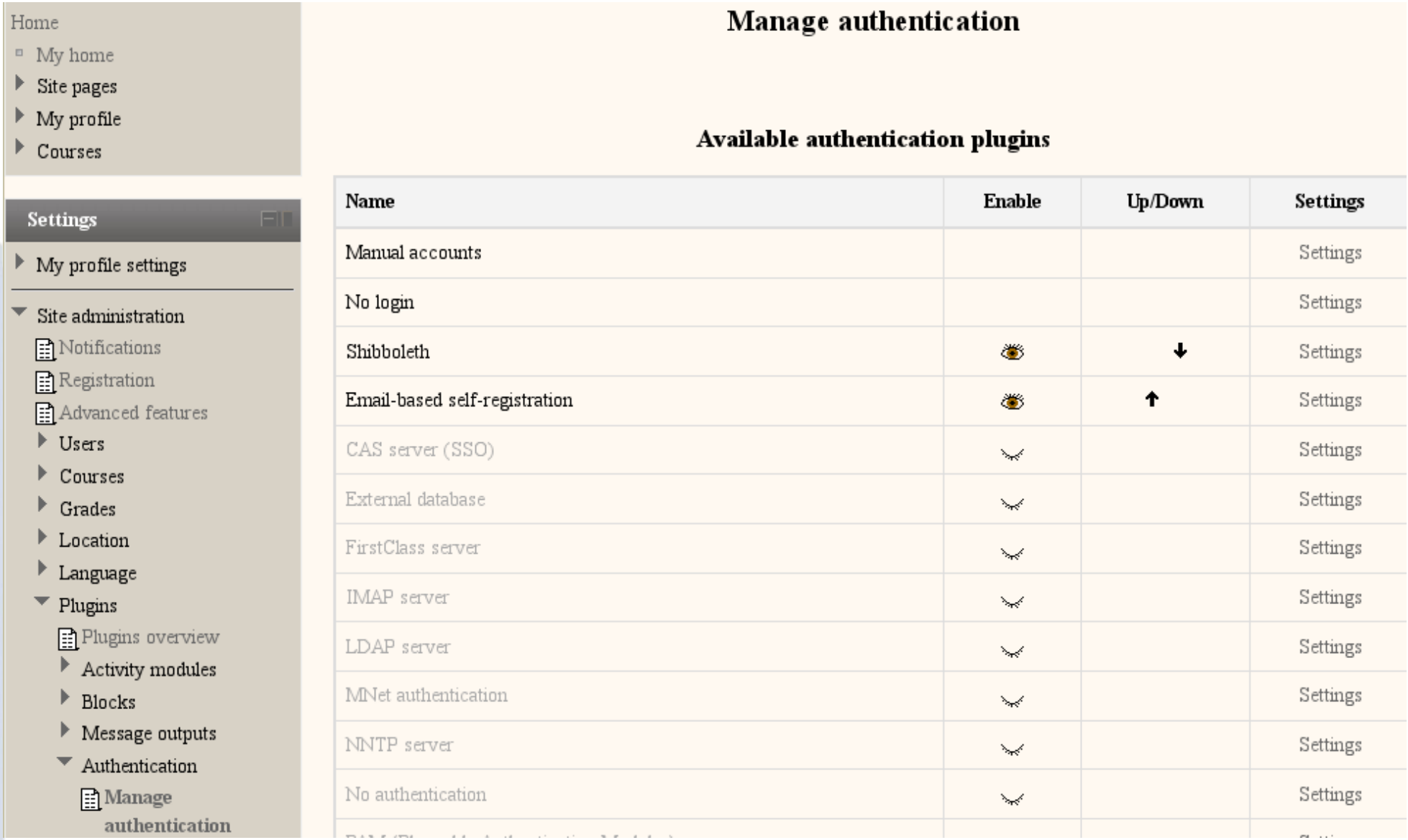
Moodle-Shibboleth hátrányok

- A kurzusok elérési jogosultságára nem terjed ki a megoldás, ezt külön kell megcsinálni (ez nem is biztos, hogy baj)
- A felhasználók csak az első bejelentkezéskor jönnek létre a moodle-ban, addig nem látjuk őket (bár ez LDAP-ból vélhetően megoldható)

Miért nem gond a jelszó kiosztása?



Beállítás 1.


Home
My home
Site pages
My profile
Courses
Settings
My profile settings
Site administration
Notifications
Registration
Advanced features
Users
Courses
Grades
Location
Language
Plugins
Plugins overview
Activity modules
Blocks
Message outputs
Authentication
Manage authentication
Manage authentication
Available authentication plugins
Name
Enable
Up/Down
Settings
Manual accounts
Settings
No login
Settings
Shibboleth
Settings
Email-based self-registration
Settings
CAS server (SSO)
Settings
External database
Settings
FirstClass server
Settings
IMAP server
Settings
LDAP server
Settings
MNet authentication
Settings
NNTP server
Settings
No authentication
Settings

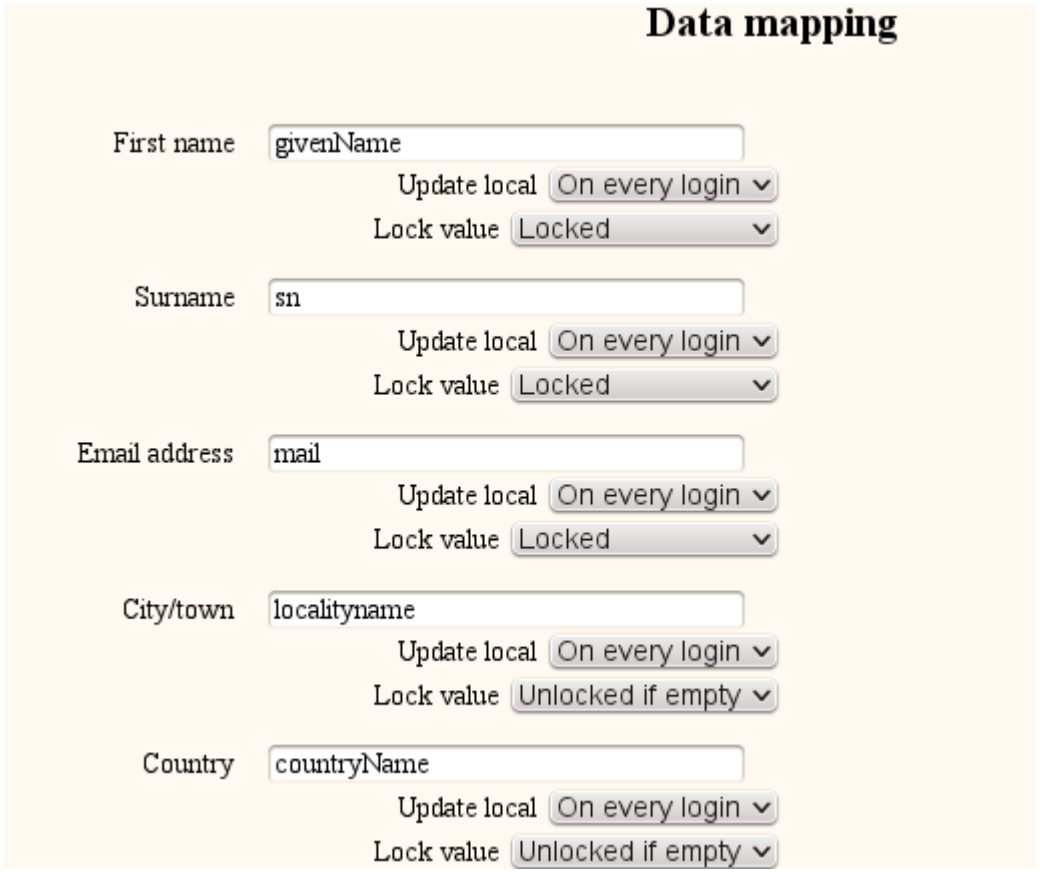
Beállítás 2.

Shibboleth

Using this method users are created and authenticated using Shibboleth.
Be sure to read the README for Shibboleth on how to set up your Moodle with Shibboleth

Username:	uid	Name of the webserver Shibboleth environment variable that shall be used as Moodle username
Data modification API:		You can use this API to further modify the data provided by Shibboleth. Read the README for further instructions.
Moodle WAYF service:	☐	If you check this, Moodle will use its own WAYF service instead of the one configured for Shibboleth. Moodle will display a drop-down list on this alternative login page where the user has to select his Identity Provider.
Identity providers:	https://seka.semmelweis-univ.hu /idp/shibboleth, SeKA	Provide a list of Identity Provider entityIDs to let the user choose from on the login page. On each line there must be a comma-separated tuple for entityID of the IdP (see the Shibboleth metadata file) and Name of IdP as it shall be displayed in the drop-down list. As an optional third parameter you can add the location of a Shibboleth session initiator that shall be used in case your Moodle installation is part of a multi federation setup.
Shibboleth Service Provider logout handler URL:		Provide the URL to the Shibboleth Service Provider logout handler. This typically is `/Shibboleth.sso /Logout`

Beállítás 3.


Data mapping
First name
givenName
Update local
On every login
Lock value
Locked
Surname
sn
Update local
On every login
Lock value
Locked
Email address
mail
Update local
On every login
Lock value
Locked
City/town
localityname
Update local
On every login
Lock value
Unlocked if empty
Country
countryName
Update local
On every login
Lock value
Unlocked if empty

Apró nyűgök

- Ha nincs a Neptunban beállítva egy hallgató emailcíme, akkor a profiloldalra kerül, amit nem tud elhagyni
- Előfordul, hogy a hallgató nem is tud arról, hogy belépési jogosultsága van
- Vannak külső felhasználóink is, akik a klasszikus módon közvetlenül a Moodle-ba jelentkeznek be (login/jelszó). A legtöbb gond onnan van, hogy néha a belső felhasználók elfelejtik, hogy nekik nem a Moodle-nak kell a login nevüket/jelszavukat megadni, hanem a központi azonosításnak.

Tapasztalatok

- Shibboleth IdP (Tomcat+java)
- Shibboleth SP (Apache modul)

A fenti programokat 2 félév óta használjuk éles környezetben, több ezer felhasználóval. Igen megbízhatónak bizonyultak. (Csak linuxos tapasztalataink vannak.)

Jelenleg teszteljük:

- SimpleSAMLphp SP része (nginx alatt)

Nézzük meg!

http://itc.semmelweis-univ.hu

http://filesender.niif.hu