HEXAA@eduID
(nagytotál → kistotál)

Bajnok Kristóf - NIIFI
Héder Mihály - SzTAKI
Magyar Zsuzsanna - SzTAKI
Tétényi István - SzTAKI

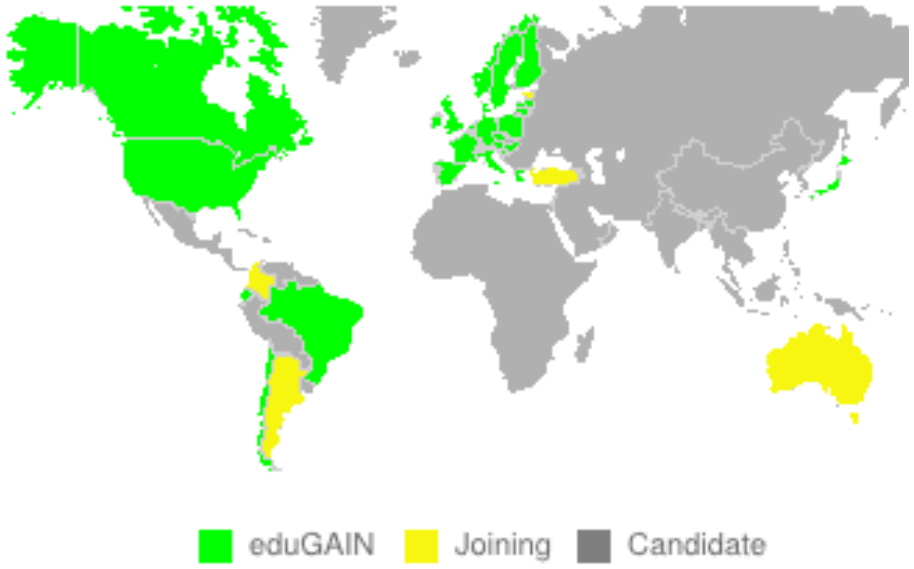
2014.11.19

Tartalomjegyzék

- Bevezetés
  - “Térkép-e táj”
  - Az AuthN + AuthZ probléma
  - Szereplők egy föderációban
  - Közvetlen előzmények
- HEXAA
  - Célkitűzések
  - Tanulságok
  - Eredmények
- Továbblépési lehetőségek

Föderációk a világban

eduGAIN



eduroam

Amit szeretünk: szolgáltatások határok nélkül

Amit keresünk: csoportok határok nélkül

Az AuthN + AuthZ probléma

AuthN = authenticatioN
(azonosítás, megadott felhasználó névhez tartozó jelszó ellenőrzése)
AuthZ = authoriZation
(jogosultság kezelés, egy adott azonosított felhasználó jogosultságainak a kezelése)

Mi az általános probléma?
Hogyan lehet biztosítani az azonosítást és jogosultság kezelést egységesen, de minél nagyobb kör számára?

Tradicionális megoldás: X.509 certificate + VOMS (grid specifikus VO) vs. web specifikus

Amit bemutattunk az egy szabványos, együttműködésre képes Sztaki+NIIFI fejlesztésű szoftver, amely SAML2 szabványt használ.

SAML = Security Assertion Markup Language

Szereplők egy föderációban

Trivialitások: Mastercard/Visa bankkártya föderáció; mobil szolgáltatók föderációi

A szereplők összefognak és megállapodnak közös célok elérése érdekében az alkalmazott műszaki, pénzügyi, adminisztratív elvekben.

Pl: Eduroam is egy föderáció (radius hierarchia és 802.1X)

felhasználó
azonosítás szolgáltató (IdP)
alkalmazás szolgáltató (SP)
föderáció eduID operátor (NIIF)

} eduID föderáció (SAML2) - nemzeti föderáció

+

eduGAIN operátor (az ötödik szereplő) - konföderáció (föderációk halmaza)

+

attribute authority - pl. HEXAA (a fenti környezetben, a hatodik szereplő)

Történeti előzmények

- Gyakorlati probléma, a valós környezet igényei
- IFAR@SzTAKI → illetve az IFAR korlátai → virtuális szervezet kezelés
- VO bevezetése a SzTAKI-ban, SzTAKI cloud VO
- eduID föderáció kiterjedése
- YAVOM a TNC 2013 konferencián
- Hazai előadások: Bajnok Kristóf, Szabó Gyula, Magyar Zsuzsanna
- GN3plus OpenCall - External Attribute Authority (attribútum szolgáltató)
- SzTAKI kezdeményezésére közös pályázat az NIIFI-vel 2013 májusában

  HEXAA - Higher Education eXternal Attribute Authorithy

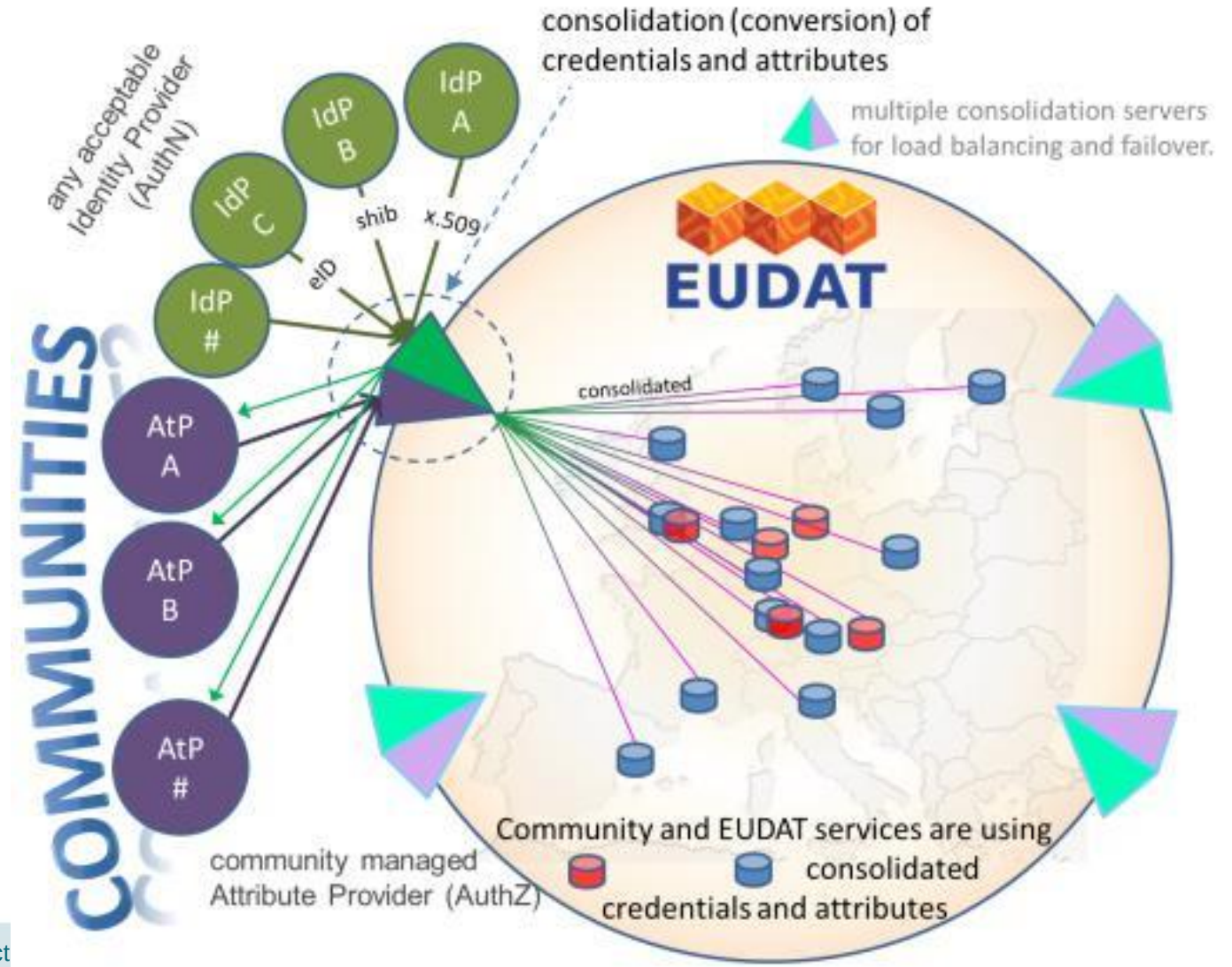
HEXAA célkitűzések

- AuthN és AuthZ megtervezett szétválasztása
  - AuthZ legyen “közösségi” kezelésben (VO)
- Legyen mód profil attribútumok kezelésére
  - Pl: ORCID, X.509 cert, e-mail, etc.
- Legyen könnyű telepíteni, üzemeltetni és használni
  - ~ SimpleSaml PHP és mások
- Bővítse ki azokat szolgáltatási lehetőségeket, amelyek hozzáférhetőek
- Nemzetközi beágyazódás
- Open source projekt, Apache licensz

HEXAA projekt eddigi tanulságai
Mi a “pálya” ?

- Környezet:
  - a hálózati igények kielégítése ütemesen és az igényeknek megfelelően halad
  - kutatási célú adatfeldolgozási környezet grid, cloud alapon
  - felhő alapú piaci szolgáltatások tömeges megjelenése
- viszont, jelentős hiány a kutatást támogató kollaborációs middleware területen
  - mindenki maga oldja meg a problémát, ebben a grid/HPC közösség a legsikeresebb, de a megoldás X.509 alapú (VOMS) - nincs web/SSO, stb.
  - a SAML2 és eduGAIN támogatottság jelen van, de az ettől eltérő műszaki megoldások is erősek

HEXAA projekt tanulságok
Heterogén felhasználói igények



HEXAA projekt tanulságok
Jogi keretek

- viszony az EU-n belüli jogi szabályozáshoz
- a TERENA Code of Conduct túl laza
- AA jogi követelmény rendszer egységesítésére lenne szükség
- AA üzemeltetési követelményrendszer pontos meghatározása szükséges
- ami az EU-n kívül van, az még ennél is áttekinthetetlenebb
- vö.: mindezt a mobil roaming-gal

HEXAA alkalmazási lehetőségek

Szervezeti hierarchia	Célközönség
helyi	egyetem/kutatóintézet/közgyűjtemény
kutatói hálózat	eduID illetve mások
konföderáció	eduGAIN
tudományos közösségek	EGI ún. science gateways
+	
Alkalmazási környezet	**Alkalmazási területek**
tartalom szolgáltató rendszerek	Liferay, MediaWiki, Drupal
felhő	OpenNebula, *OpenStack*
egyéb	Pydio/Ajaxplorer, racktables, edujabber, Icinga, owncloud

Eredmények a HEXAA projektben

- Működő HEXAA program
- eduID integráció
- simpleSAMLphp modulok
- Működő integrációs környezetek
  - Liferay (WS-Pgrade/gUSE Portal/EGI FedCloud)
  - pydio, mediawiki, OpenNebula, Drupal
  - eduJabber, Racktables, owncloud
  - NREN HPC portal; API alapú
- Kényelmes migrációs út a VO környezetből

Eredmények a HEXAA projektben

nemzetközi együttműködés:

- Cesnet (PERUN), Pioneer (Unity), Surfnet (Surfconext) - AA együttműködés területén
- EGI - cloud integráció területén
- WS-Pgrade - science gateways + fed. azonosítás

közzétett új software komponensek:

- Drupal, Liferay, SimpleSamlPHP, OpenNebula

Továbblépési lehetőségek

- további alkalmazások támogatása
- kutatói föderációk támogatása (Umbrela, stb.)
- HEXAA → OpenStack
- HEXAA → eduGAIN
- HEXAA → PERUN AA kollaboráció
- HEXAA → AA cluster > 2
- non-web környezetek támogatása
- HEXAA → OpenConext
- oauth2, openID, SCIM, VOOT, community ID
- HEXAA as a Service

Kérdések?

Web oldal: www.hexaa.eu

Connect | Communicate | Collaborate

www.geant.net

www.twitter.com/GEANTnews | www.facebook.com/GEANTnetwork | www.youtube.com/GEANTtv

Háttér anyagok

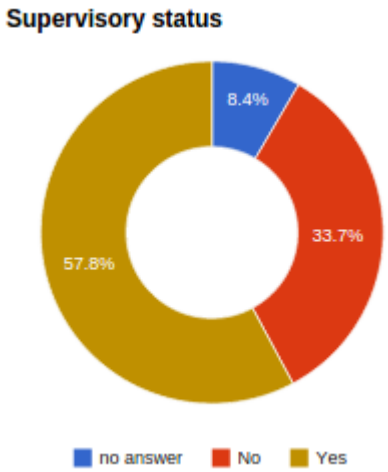
1. eduGAIN videó
2. e-Science gateways with external attribute authorithy (EGI community forum, May 2014)
3. Extending eduGAIN with HEXAA (EGI-GEANT symposium, September, 2014)
4. HEXAA at GEANT

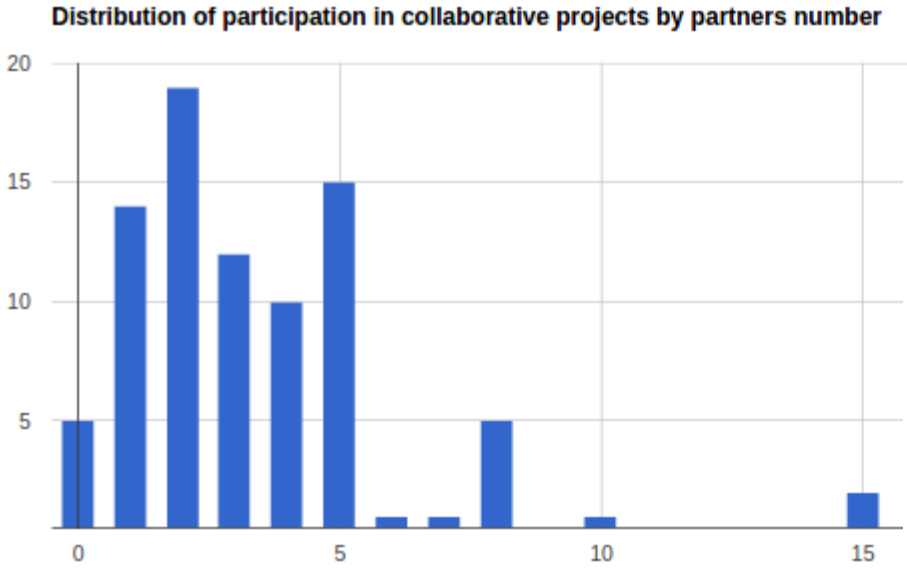
Háttér anyagok

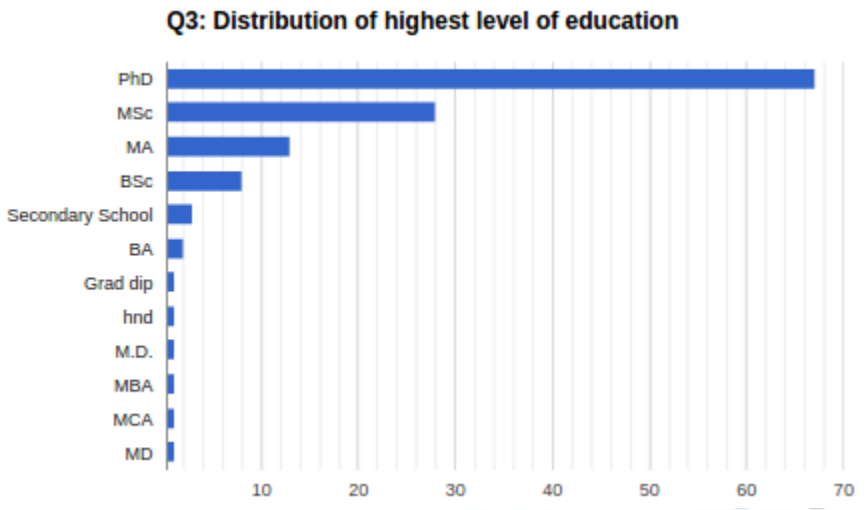
1. eduGAIN videó
2. e-Science gateways with external attribute authorithy (EGI community forum, May 2014)
3. Extending eduGAIN with HEXAA (EGI-GEANT symposium, September, 2014)
4. HEXAA at GEANT

HEXAA survey

- 186 responses from 23 countries
- **Collaboration** is absolutely common
- **AAI awareness** is varying
  - Most well known logo: **Shibboleth**







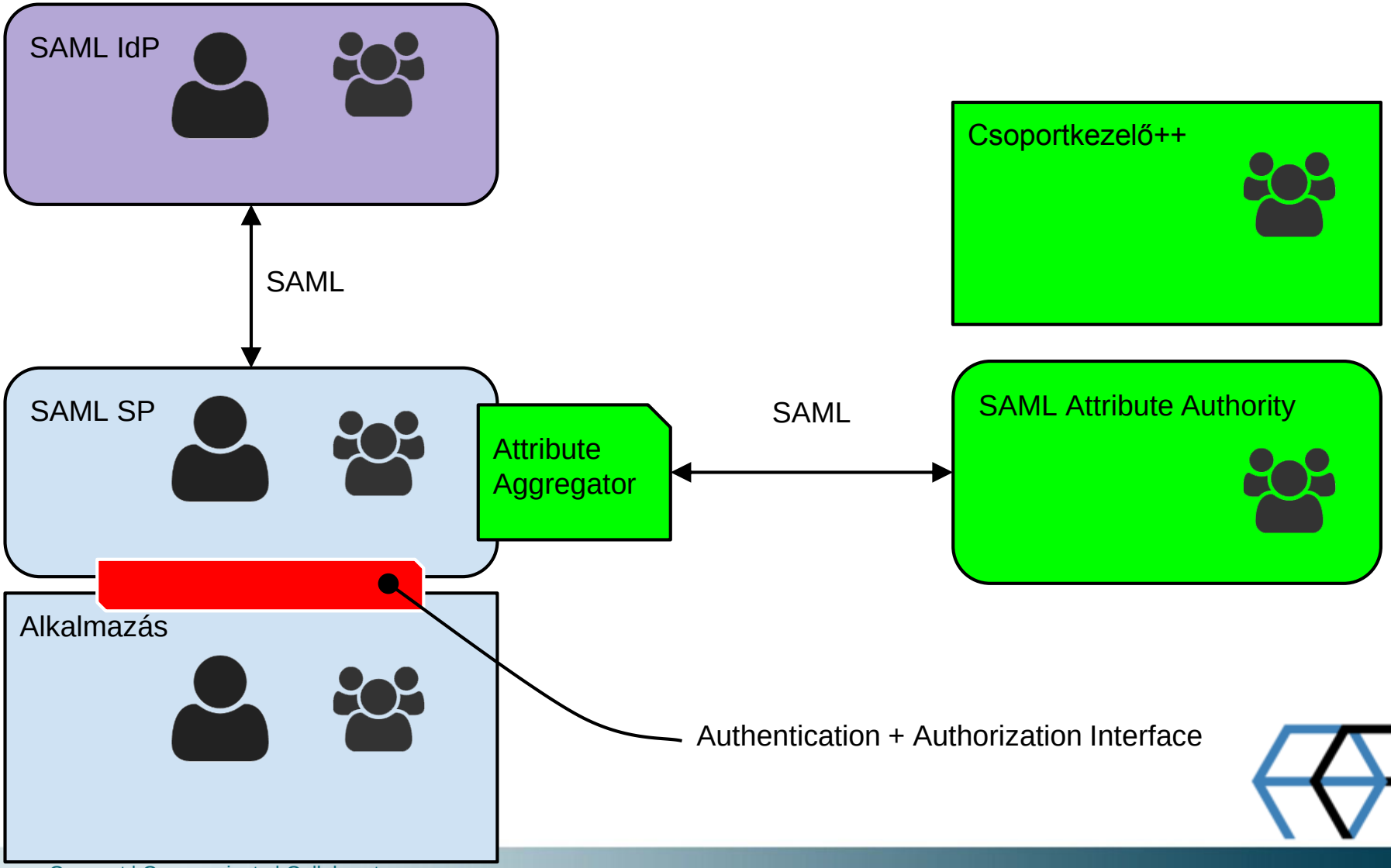
A HEXAA projekt

- WP1 projekt management
- WP2 műszaki lehetőségek és igények felmérése, műszaki specifikációk elkészítése
- WP3 jogi környezet elemzése és ajánlások készítése az AA kialakítása és az AA üzemeltetése vonatkozásában
- WP4 szoftver fejlesztés
- WP5 projekt információk terjesztése

Motivációk I.

- Jól ismert alaphelyzet: külső felhasználók, közös projektek, web alapú alkalmazások - mihez férhetnek hozzá,
- Megoldás I:
  - LDAP alapú intézményi backend - minden authorizálást visszavezetünk LDAP kérdésekre
  - Problémák:
    - Hogyan alakítunk ki csoport attribútumokat LDAP-ban?
    - Hogyan kerülnek be külső felhasználók az intézményi LDAP-ba?
    - Hogyan oldjuk meg a jogosítási igények leképzését?
    - Hogyan tudjuk az alkalmazásoknak szabványosan megválaszolni a felhasználó azonosítási és jogosítási kéréseket?
    - Hogyan illeszkedik mindez egy nagy szervezet belső szabályozásába?
    - Mi a helyzet az adatvédelmi/adatkezelési előírásokkal?
    - Single Sign-on?
  - megpróbáltuk - csináljuk - nem szeretjük eléggé

AA működési modell



Mit nyújt a HEXAA?

- **Virtual Organization** manager
- **Profile** Attribute manager
- **Data protection** by design (nem részletezzük)
  - Consent
  - Data expiration
  - Regular data re-checks
- **API** call for everything

A HEXAA felépítése