

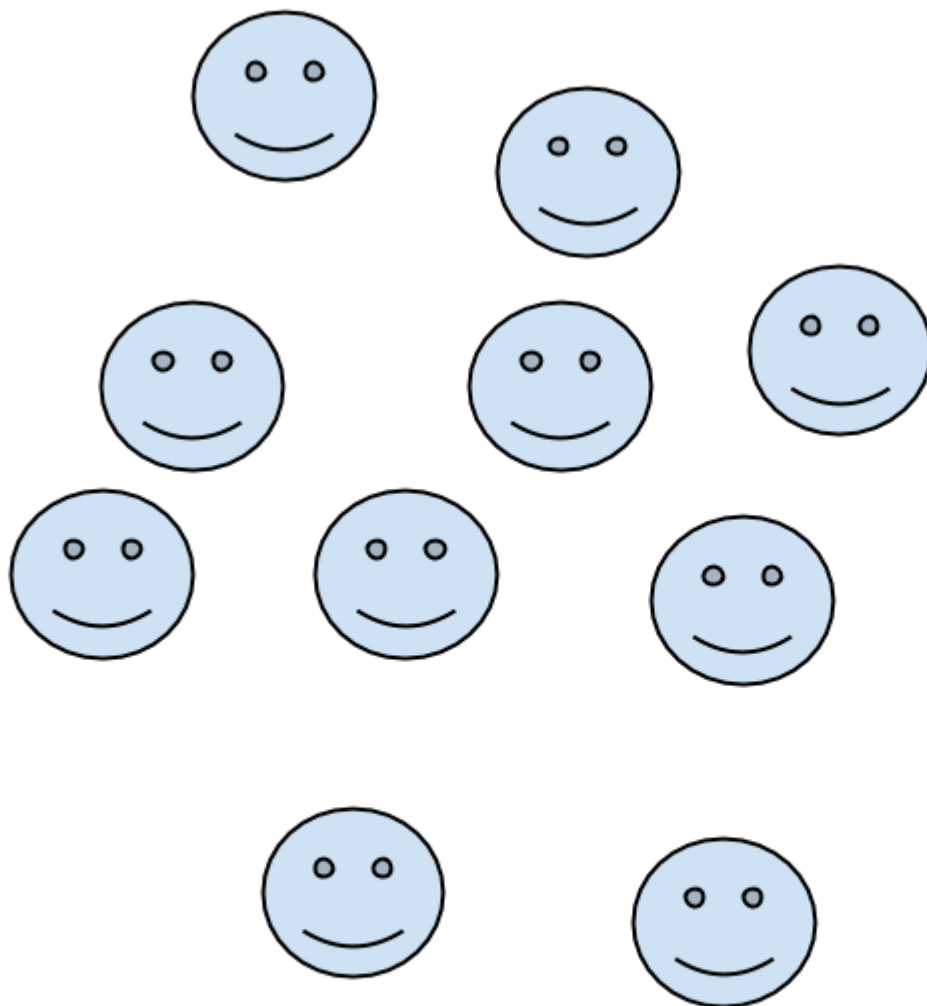
Higher Education eXternal Attribute Authority



Mihály Héder
István Tétényi
(MTA SZTAKI)
19-May-2015



Problems in Collaboration



Collaboration tool 1
(e.g. mailing list)

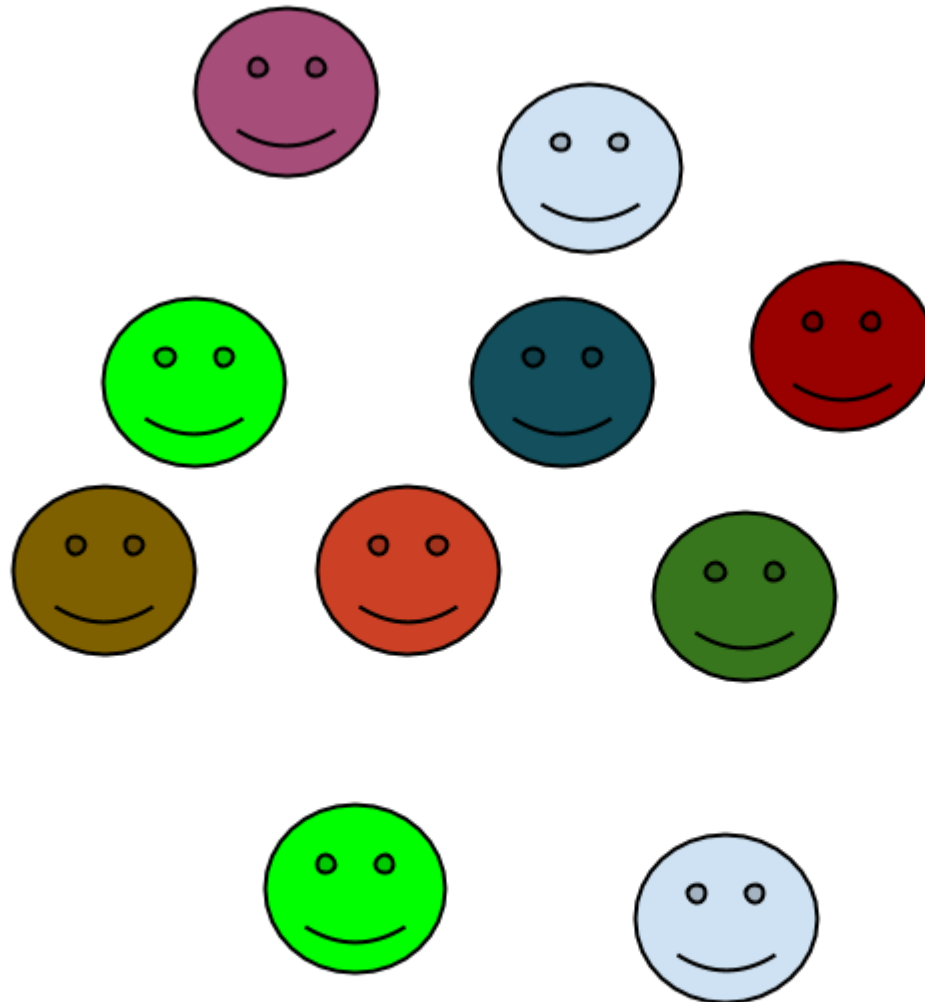
Collaboration tool 2
(e.g. Wiki)

Collaboration tool 3
(e.g. XMPP chat)

Collaboration tool 4
(e.g. WebRTC tool)



Problems in Collaboration



Collaboration tool 1
(e.g. mailing list)

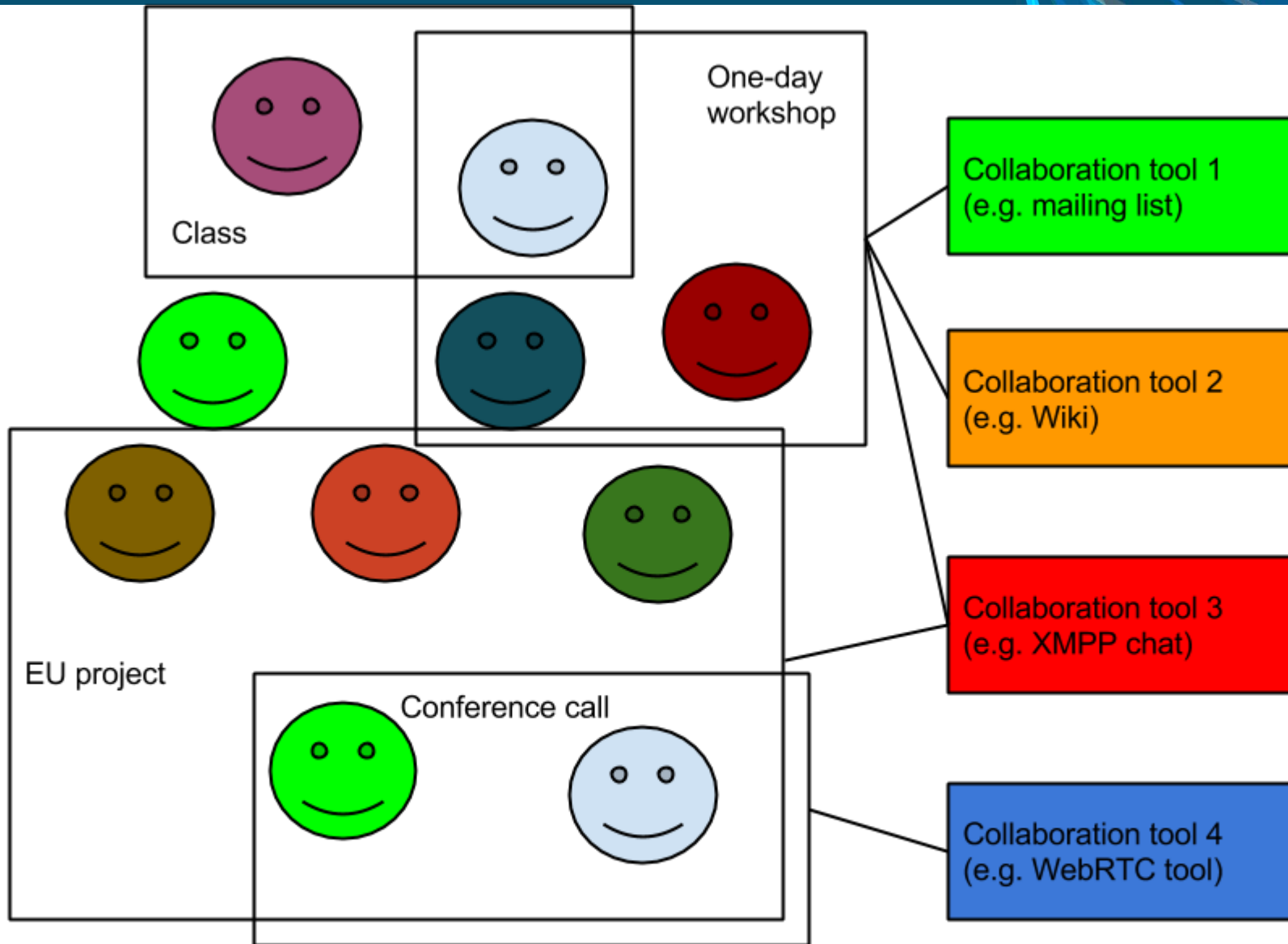
Collaboration tool 2
(e.g. Wiki)

Collaboration tool 3
(e.g. XMPP chat)

Collaboration tool 4
(e.g. WebRTC tool)



Problems in Collaboration



Why we need Attribute Authorities? Motivations for HEXAA



- SP's attribute requirements grow but the IdPs capabilities are constrained and differ in terms of
 - Procedures
 - Bureaucracy
 - Scope
 - Flexibility
 - Authority



Why we need Attribute Authorities? Motivations for HEXAA

- It is possible to outsource some of the administrative burden of the IdPs in federation → External Attribute Provider (EAP)/ Attribute Authority (AA)
 - Separation of AuthN and AuthZ
 - Delegating AuthZ in the hands of the community
 - Providing additional profile attributes
 - e.g. ORCID, X.509 cert, e-mail, etc.
 - Manage attributes where it is least cumbersome and fits best
 - At virtual organizations by VO managers
 - By the users themselves who knows „always” best



Why we need Attribute Authorities? Motivations for HEXAA



- AA is a focal point for provisioning services in a federation by keeping attributes
 - Consistent
 - Coherent
 - Consolidated and centralized in an independent place



- Use case discovery
 - User survey
 - User community requirement assessment
- Legal research/study
 - Common guidelines for AA software developers
- HEXAA software development
- HEXAA dissemination



HEXAA results

Research on the Legal Framework



Generic guidelines:

- EAP shall manage Level of Assurance/Level of Confidence (LOA/LOC).
- EAP shall manage Consents.
- Users should be able to: prohibit release, revoke attributes, self-delete.
- Users should be able to see their attribute release history.
- The requirements analyses and the development were carried out hand-in-hand.

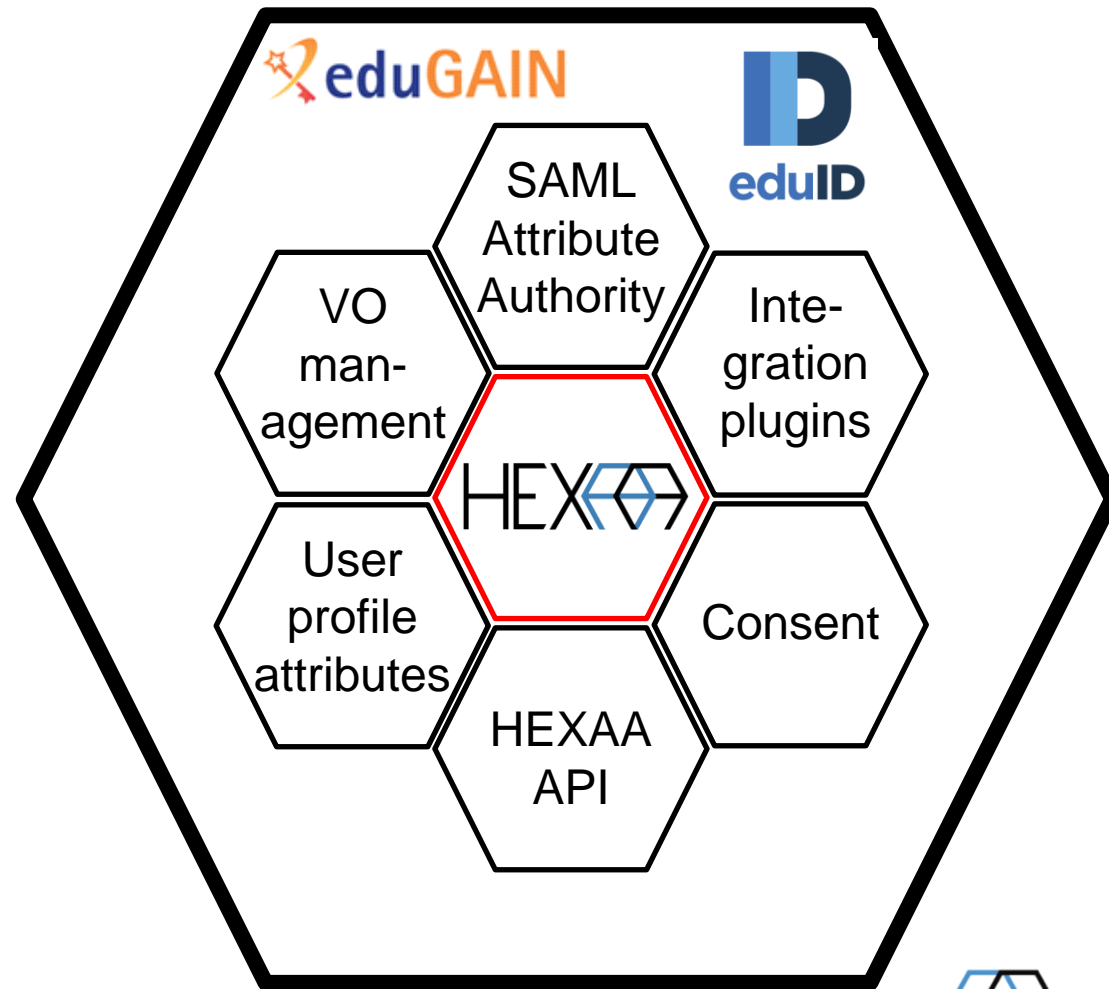


HEXAA results

Software development – core functionality

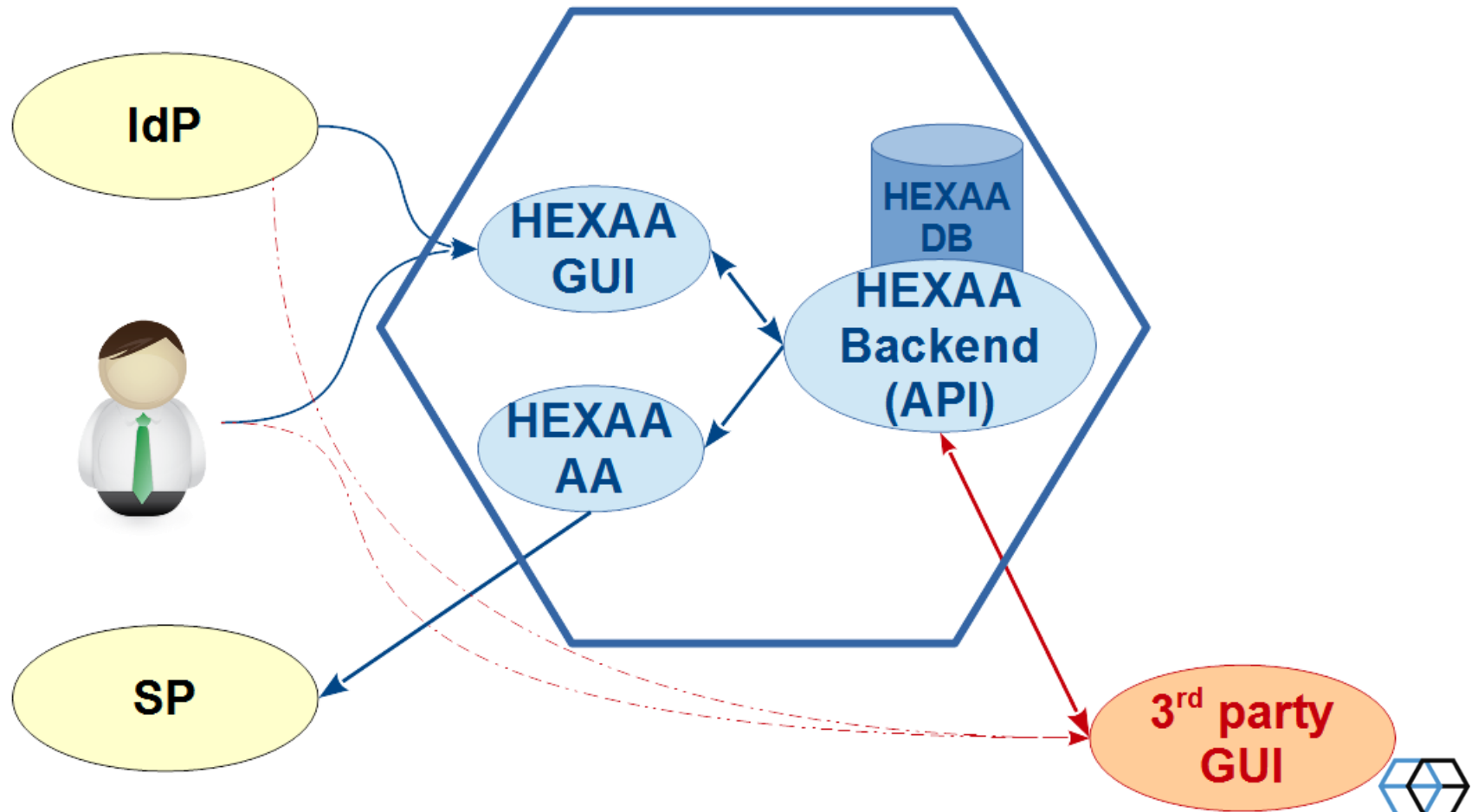
HEXAA core functionality in a nutshell:

- Virtual Organization manager
- Profile Attribute manager
- Data protection by design
 - *Consent*
 - *Data expiration*
 - *Regular data re-checks*
- API call
 - *separated SAML frontend and back-end*
 - *3rd party GUI is an option*



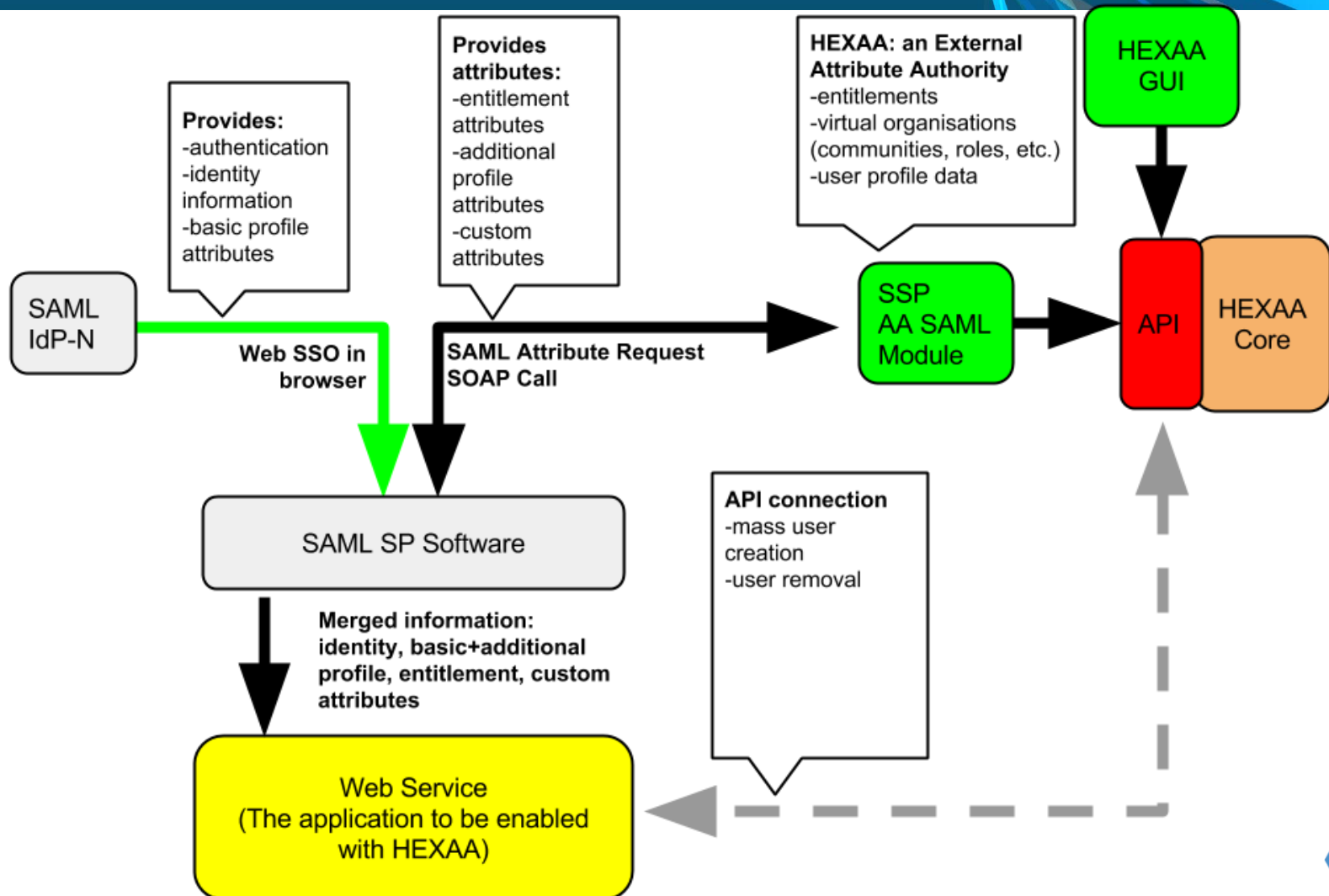
HEXAA results

Software development - HEXAA architecture



HEXAA results

Software development - HEXAA architecture



HEXAA results

Software development - integration

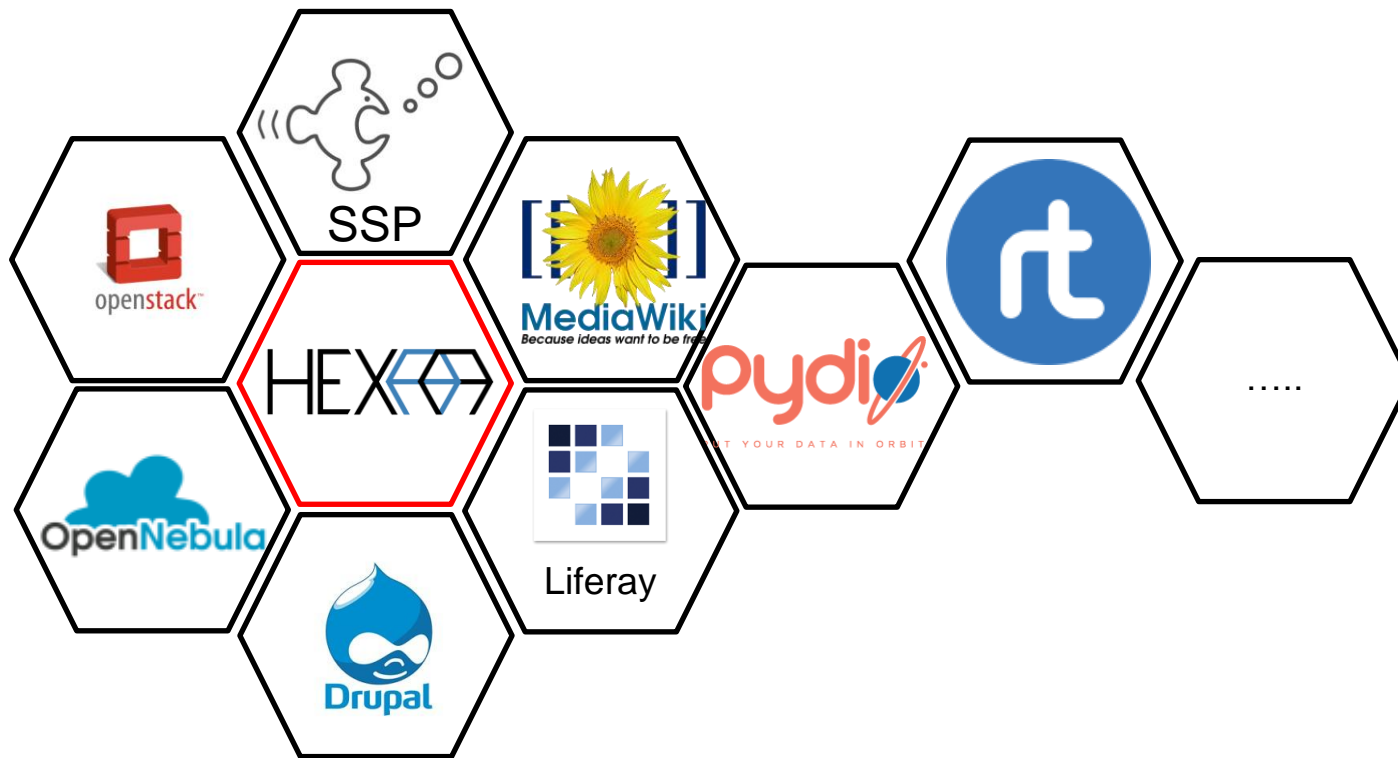


- SimpleSamlPHP modules
 - AA provider and consumer
- Specific integration plugins
 - Liferay (WS-Pgrade/gUSE Portal), Drupal (e-Science gateways)
 - OpenNebula (3.8-4.10.1), OpenStack (juno) (clouds)
 - eduJabber, Racktables, MediaWiki
- Hungarian NREN (NIIFI) HPC portal, custom apps through API
- Software development results available from GitHub with Apache licence



HEXAA results

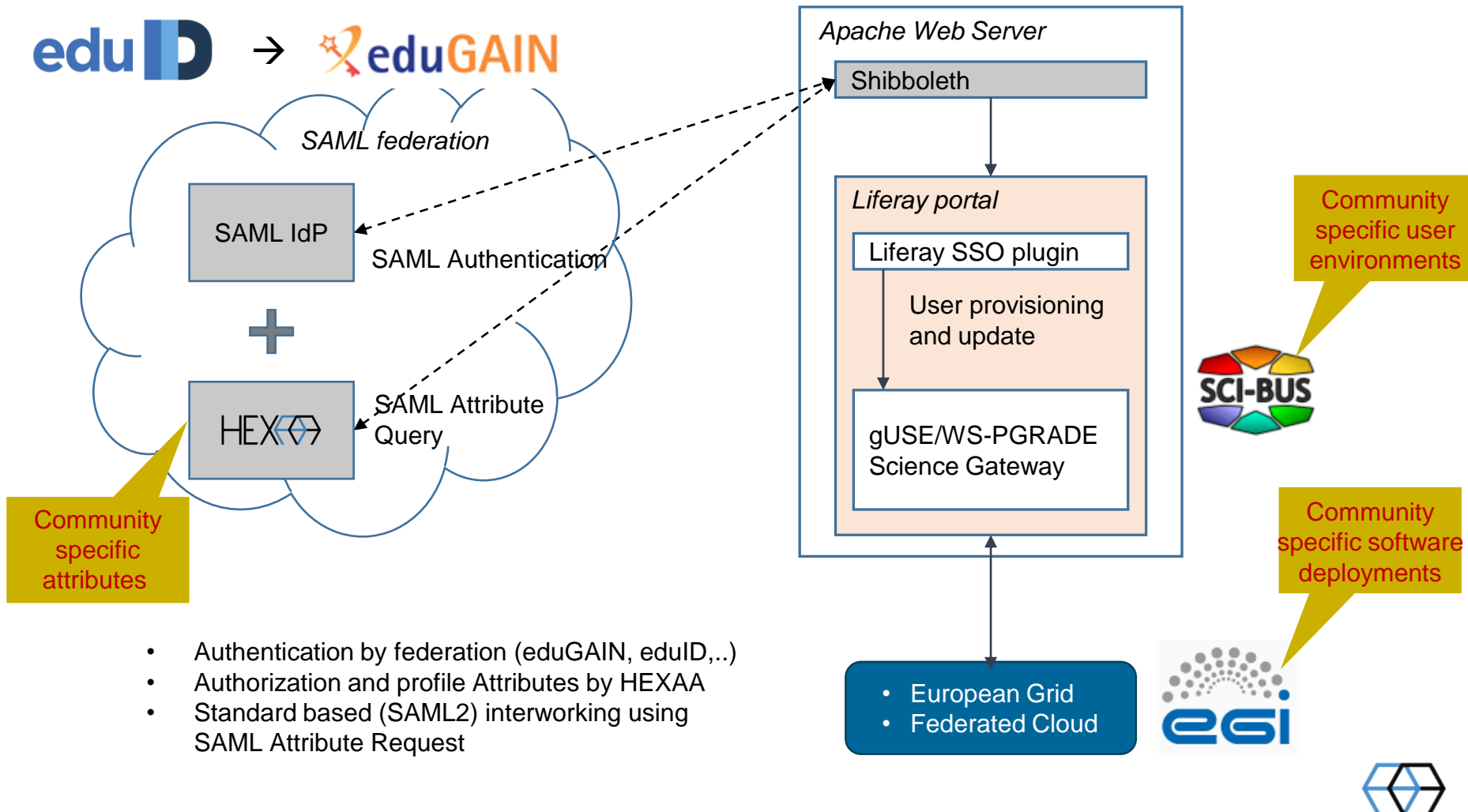
Software development - integration



HEXAA results

HEXAA and e-Science environments

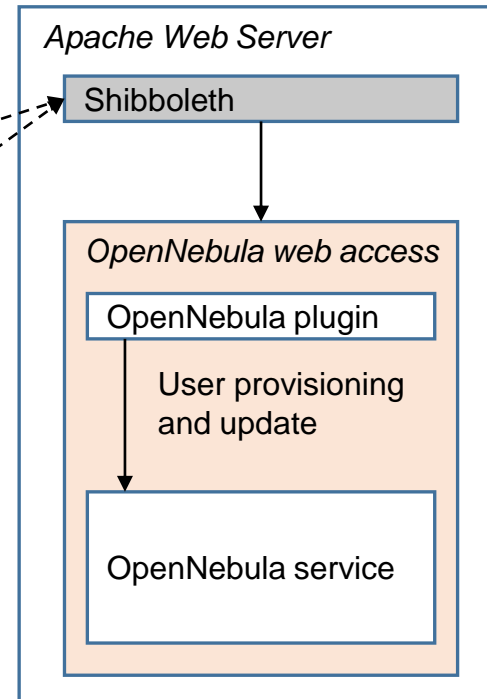
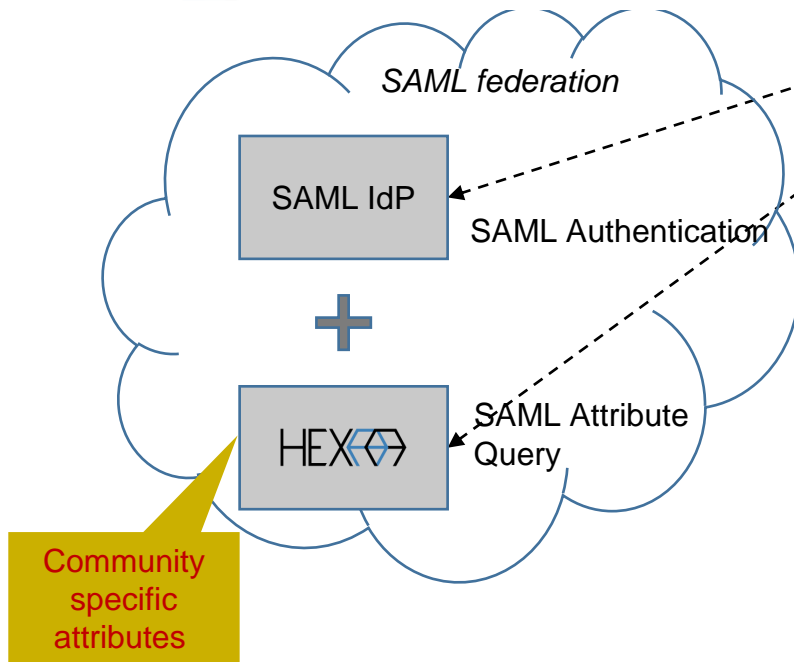
eduID → eduGAIN



HEXAA results

HEXAA and Cloud services

eduID → eduGAIN



- Authentication by federation (eduGAIN, eduID,...)
- Authorization and profile Attributes by HEXAA
- Standard based (SAML2) interworking using SAML Attribute Request

Openstack uses the same operational model



HEXAA and Openstack

[Organizations](#)[Services](#)[Admin](#)

58:55

tetenyi@sztaki.hu ▾

[HELP](#)[News](#)[Me](#)[Attributes](#)[Consents](#)

Organizations

- [HBIT] Kötők klubja
- [HBIT] Ipeter
- [HBIT] Openstack
- [HBIT] Ormos Pál
- [HBIT] Prunk-Éger Edgár
- [HBIT] Rigó Ernő
- [HBIT] Rigó Ernő

[Manage](#)[My Services](#) ▾

Profile

Display Name	Tétényi István
Federal Id	tetenyi@sztaki.hu
E-mail	tetenyi@sztaki.hu

[Manage](#)

HEXAA and Openstack



[Organizations](#)

[Services](#)

[Admin](#)

57:07

[tetenyi@sztaki.hu](#) ▼

[News](#)

[Me](#)

[Attributes](#)

[Consents](#)

[surName](#)

[givenName](#)

[sshPublicKey](#)

[eduPersonNickName](#)

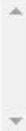
[ORCID](#)

[EduPersonOrcid](#)

[mail](#)

type a name

tetenyi@sztaki.hu



New
attribute

Backend-Version: 0.19.3


Copyright 2014


Frontend-Version: 0.20.0 #2015.01.13 10:34:13





HEXAA and Openstack





ubuntu  OpenStack Dashboard

tenant1 

tetenyi@sztaki.hu  Sign Out

Project 

Admin 

System 

Overview

Hypervisors

Host Aggregates

Instances

Volumes

Flavours

Images

Networks

Routers

Overview

Usage Summary

Select a period of time to query its usage:

From:

To:

Submit

The date should be in YYYY-mm-dd format.

Active Instances: 1 Active RAM: 4GB This Period's VCPU-Hours: 60.30 This Period's GB-Hours: 1272.50

Usage

Download CSV Summary

Project Name	VCPUs	Disk	RAM	VCPU Hours	Disk GB Hours
tenant2	0	0Bytes	0Bytes	1.20	1.20
tenant1	2	40GB	4GB	59.10	1271.30

Displaying 2 items

HEXAA and Openstack



Browser address bar: <https://openstack.hbit.sztaki.hu/horizon/identity/users/>

Browser tabs: Alkalmazások, ITAK Ügyeletési Lap, Gmail - Beérkező lev..., Inbox - tetenyi@sztaki..., Drive@Sztaki, Film, NFSEN hálózati túlh..., hangoskönyv, FileNerd.com - Ever..., Hangoskönyv @ CA...

OpenStack Dashboard | tenant1 | tetenyi@sztaki.hu | Sign Out

Users

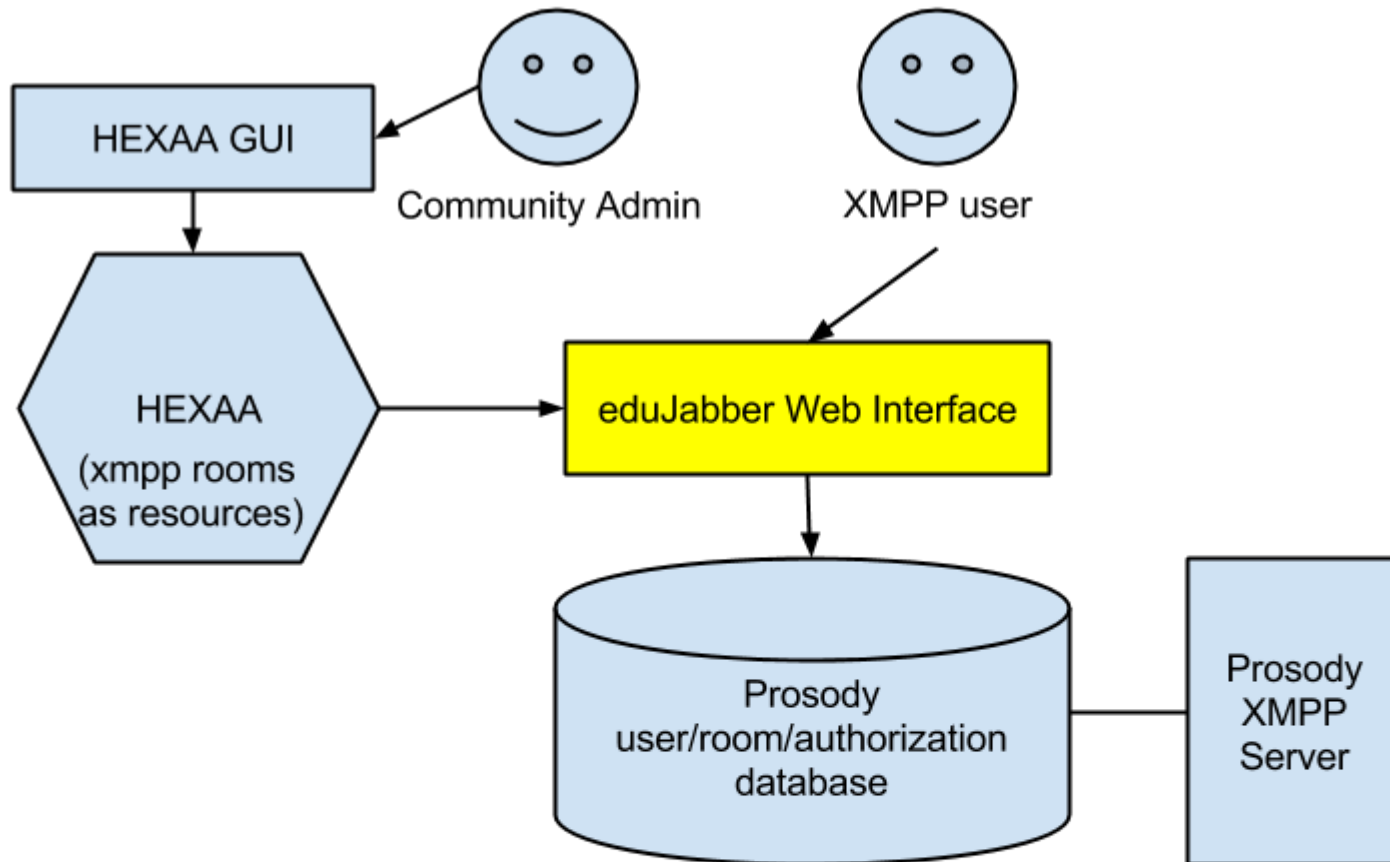
Filter [] [] [Filter] [Create User] [Delete Users]

<input type="checkbox"/>	User Name	Email	User ID	Enabled	Actions
<input type="checkbox"/>	magyarzs@sztaki.hu	magyarzs@sztaki.hu	9b18935910a943e691d70eb7d24947f9	True	Edit
<input type="checkbox"/>	merlin@sztaki.hu	mihaly.heder@sztaki.mta.hu	0d61e0cc5302406b8f56baa1dd41d0e3	True	Edit
<input type="checkbox"/>	burgosz@sztaki.hu	tenczer.szabolcs@sztaki.mta.hu	7cf54e03964d44849144ed57ab464111	True	Edit
<input type="checkbox"/>	tetenyi@sztaki.hu	tetenyi@sztaki.hu	a16e3e7f61cd41678b9566a217b1cca5	True	Edit
<input type="checkbox"/>	admin		00133caa133e4b8e86bc2cc125ecfa85	True	Edit
<input type="checkbox"/>	ormos@sztaki.hu		1d9768a7f7624e58a4c6ac28b4f70208	True	Edit

The plugin is available on GitHub!



eduJabber example



News

Properties

Users

Managers

Management

Invitation
management

Connected Services

Roles

Attribute
specifications

Service catalog

Delete

[SZTAKI] HBIT > Roles



Filter

Page size:

25

+ New

DBpedia



Properties

Name	DBpedia
Description	DBpedia live projekt résztvevők és partnerek

Members

Pablo Mendes <pablomendes@gmail.com>
Joachim Daiber <daiber.joachim@gmail.com>
bana@sztaki.hu <bana.tibor@sztaki.mta.hu>

Permissions

Sztaki felhő::felho: DBpedia

default



Properties

Name	default
Description	Default role

Members

Soltész Balázs <soltesz.balazs@sztaki.mta.hu>
István Tétényi <tetenyi@sztaki.hu>
Héder Mihály <mihaly.heder@sztaki.mta.hu>
Magyar Zsuzsánna <magyarzs@sztaki.hu>
Ormos Pál <ormos@sztaki.hu>
nemecsek@asdf.hu@partners.sztaki.hu
<nemecsek@asdf.hu>
Bálint Marci <balint.marton@sztaki.mta.hu>

Permissions

eduJabber::hbit-room

eduJabber example



Lorem ipsum
dolor sit amet

YOUR EDUJABBER ACCOUNT

EDUJABBER.....

MY PROFILE

CHAT ROOMS

VCARD

CONTACT

MY PROFILE

[Logout](#)

Your basic data:

Name: Mihály Héder

email: mihaly.heder@sztaki.mta.hu

ENTITLEMENTS

Your entitlements

Your jabber id:

merlin_sztaki_hu@edujabber.hexaa.eu

A kukac utáni részt csak akkor változtasd meg ha egy másik domainen regisztrált Jabber ID-t akarsz használni!

Konferencia szerver: conference.edujabber.hexaa.eu

Your password:



Your are entitled to use the following rooms: hbit
hexaa

Plans – Sustainability- Collaboration



Plans:

- Several ideas to extend features (VOOT, SCIM, etc.)
- Interworking with other AA-s Perun, Unity, OpenConext
- Collaborating in large scale projects AARC, MAGIC, EGI

Sustainability:

- eduGAIN integration
 - Any eduGAIN member is able to use it
- Euid.hu – NIIFI/Hungarnet operationally secures HEXAA final version
- Community support



HEXAA overall status



- HEXAA is fully functional, demonstrated at November 2014
 - Demos are available at: <http://hexaa.eduid.hu>
- hexaa.eduid.hu is fully **integrated** into Hungarian identity federation and since May-2015 also in **eduGAIN**
- e-Science gateway /gUSE-WS-PGRADE/ **operational**
- Institutional OpenNebula cloud operational
- OpenStack Juno plugin **operational** Kilo **underway**
- NIIFI NREN HPC portal is **operational**
- eduGAIN integration **DONE**
- HEXAA software modules and plugins are available at **GitHub**



The HEXAA team greets you!



Thank you and
any questions?

Hello!
You can add
your own text
here

