EGI and HEXAA

/Higher Education eXternal Attribute Authority/

Istvan Tetenyi - tetenyi@sztaki.hu
HEXAA - project manager

Introduction

- HEXAA is a GEANT3plus Open Call project
- Participants:
  - SZTAKI (Computer and Automation Institute)
  - NIIFI (Hungarian Academic and Research Network Organization)

- SZTAKI and NIIF/Hungarnet have a long successful history of cooperation
- This included:
  - identity management
  - federated identity service (eduID)
  - day-to-day working relationship

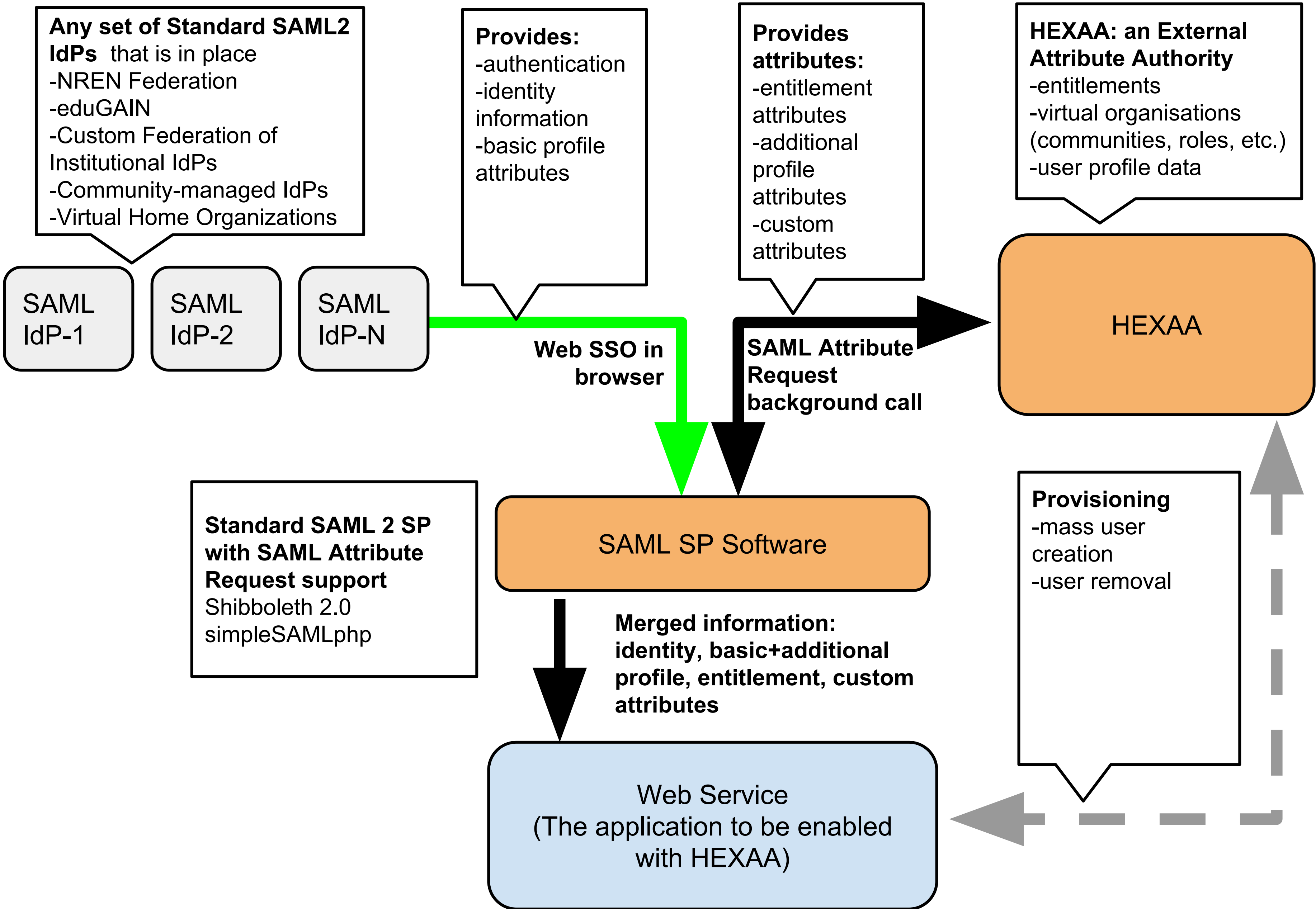
HEXAA project

- 18 months, started in October 2013, part of GEANT3plus Open Calls
- Four work packages
  - Use case discovery and analyses (M1-M8)
  - Policy and regulatory issues (M1-M8)
  - Software development (M9-M17)
  - Dissemination (M9-M17)
- Our key questions are:
  - How to identify use cases for HEXAA?
  - How to find communities that need HEXAA?
  - How to extend HEXAA functionality?
- Deliverables:
  - proof of concept and working HEXAA software
  - presentation at TNC 2014, journal paper submission

HEXAA motivation

- HEXAA is the outcome of a successful integration of OpenNebula and federated identity management
- HEXAA answered two critical questions:
  - where could we store information that does not suit well with institutional identity management procedures?
  - how could we provide (external data) in a standard way to web applications?
- Our answers:
  - External Attribute Authority
  - SAML 2 (attribute request)

HEXAA general architecture



Any set of Standard SAML2 IdPs that is in place
-NREN Federation
-eduGAIN
-Custom Federation of Institutional IdPs
-Community-managed IdPs
-Virtual Home Organizations

Provides:
-authentication
-identity information
-basic profile attributes

Provides attributes:
-entitlement attributes
-additional profile attributes
-custom attributes

HEXAA: an External Attribute Authority
-entitlements
-virtual organisations (communities, roles, etc.)
-user profile data

SAML IdP-1

SAML IdP-2

SAML IdP-N

Web SSO in browser

SAML Attribute Request background call

HEXAA

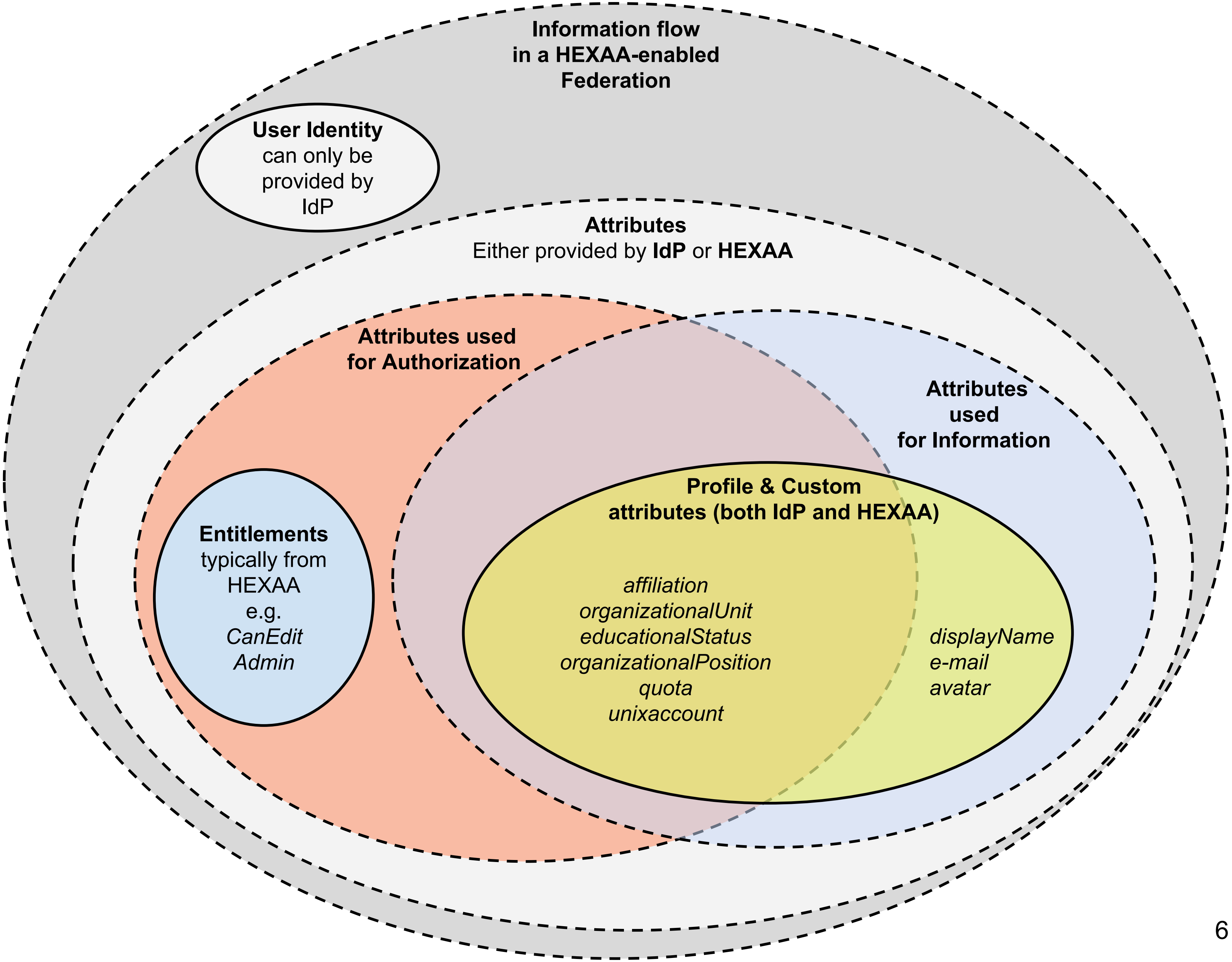
Standard SAML 2 SP with SAML Attribute Request support
Shibboleth 2.0
simpleSAMLphp

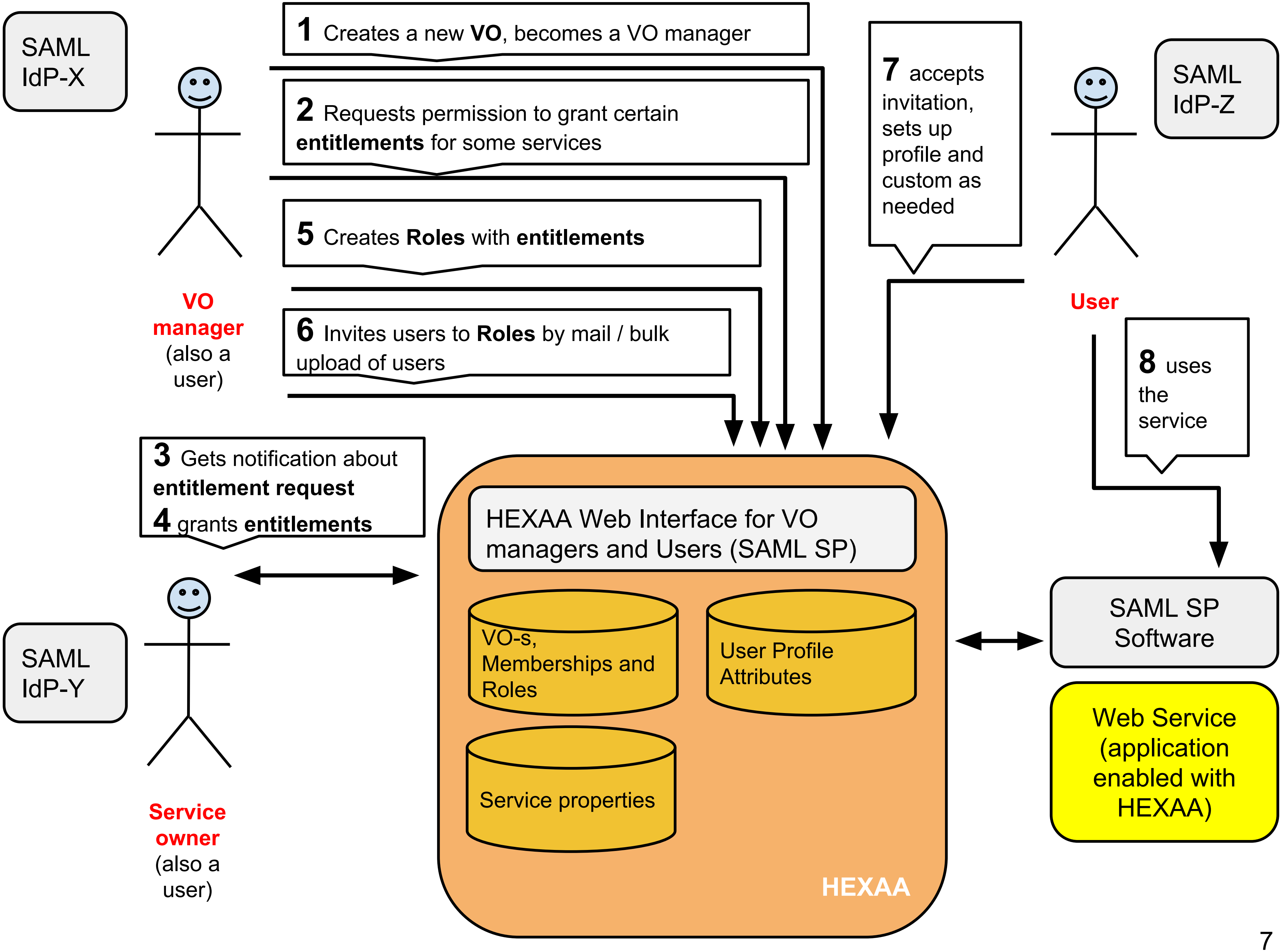
SAML SP Software

Merged information: identity, basic+additional profile, entitlement, custom attributes

Provisioning
-mass user creation
-user removal

Web Service
(The application to be enabled with HEXAA)


Information flow in a HEXAA-enabled Federation
User Identity can only be provided by IdP
Attributes Either provided by **IdP** or **HEXAA**
Attributes used for Authorization
Attributes used for Information
Entitlements typically from HEXAA e.g. *CanEdit* *Admin*
Profile & Custom attributes (both IdP and HEXAA)
affiliation
organizationalUnit
educationalStatus
organizationalPosition
quota
unixaccount
displayName
e-mail
avatar



SAML IdP-X

VO manager (also a user)

SAML IdP-Y

Service owner (also a user)

SAML IdP-Z

User

1 Creates a new **VO**, becomes a VO manager

2 Requests permission to grant certain **entitlements** for some services

3 Gets notification about **entitlement request**

4 grants **entitlements**

5 Creates **Roles** with **entitlements**

6 Invites users to **Roles** by mail / bulk upload of users

7 accepts invitation, sets up profile and custom as needed

8 uses the service

HEXAA Web Interface for VO managers and Users (SAML SP)

VO-s, Memberships and Roles

User Profile Attributes

Service properties

HEXAA

SAML SP Software

Web Service (application enabled with HEXAA)

HEXAA support for VO workflow

Typical workflow:

1. *Service owner* defines the entitlements that are to be used for authorization of different actions in the service
2. *VO manager* requests the service owner for granting permissions for entitlements
3. Service owner gives granting permission to VO manager
4. VO manager defines VO specific roles and assigns entitlements to them
5. VO manager invites the user(s) to roles (a user can have multiple roles)
6. User accepts invitations
7. Service becomes available for the user with proper entitlements

Key:

- Entitlements = attribute name/value + service-specific interpretations
- Attribute value can be provided by: IdP or VO manager or user

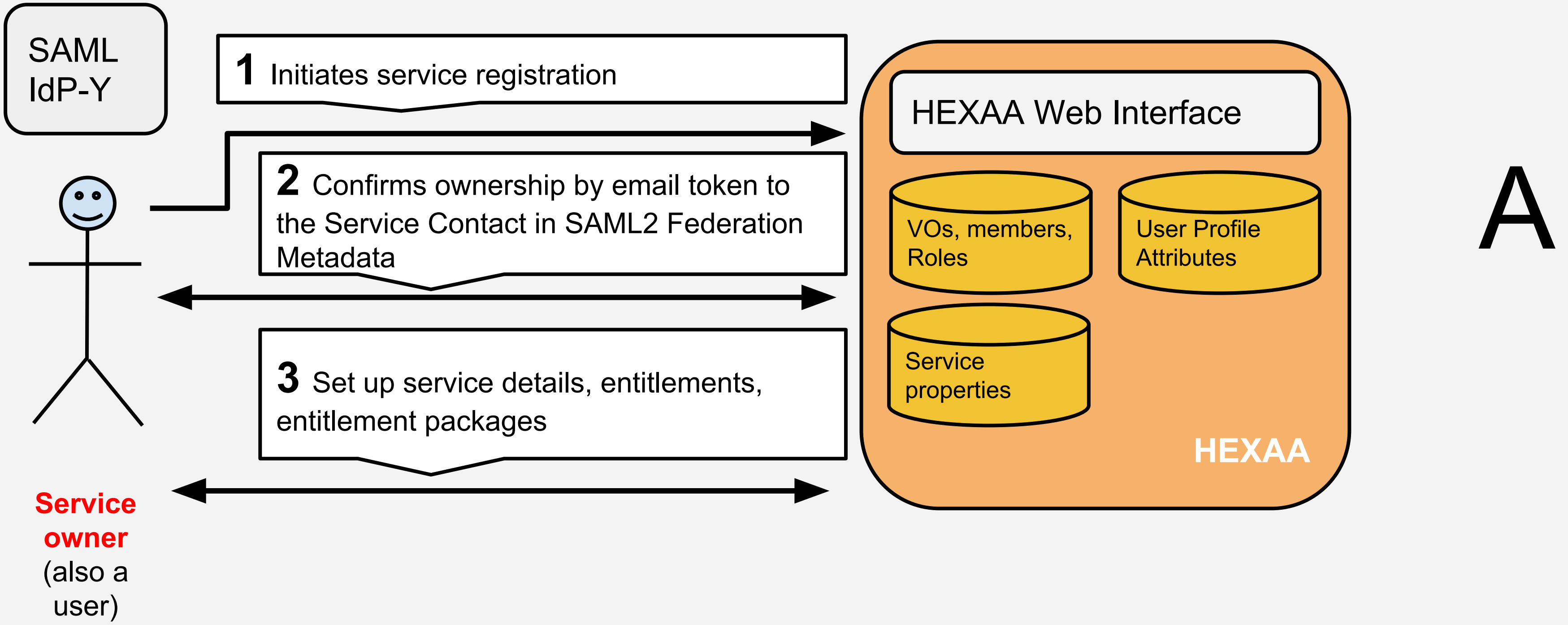
HEXAA status

- videoconferences with interested parties
  - EGI /four groups/
  - UMBRELLA
  - PERUN
- Integration with: Open Nebula, Icinga (Nagios), MediaWiki, Drupal, AjaxPlorer
- Planned for near future:
  - Liferay, OpenStack
  - outcome of the case study requirements
- Next steps:
  - consolidate use case requirements
  - identify test cases
  - software development / system integration
- Known open questions
  - handling of Level of Assurance
  - scoped attributes / responses - e.g. affiliation
  - attribute release policy issues and user consent handling

HEXAA future directions

- the solution is based on SAML 2 Attribute Query (standard)
- many similar initiatives (platforms, protocols, re-tailoring, etc.)
- application areas
  - huge research communities with specific needs
  - NRENs
  - universities
  - projects with cross border activities
- open source (Apache)

Questions?



SAML IdP-Y

1 Initiates service registration

2 Confirms ownership by email token to the Service Contact in SAML2 Federation Metadata

3 Set up service details, entitlements, entitlement packages

HEXAA Web Interface

VOs, members, Roles

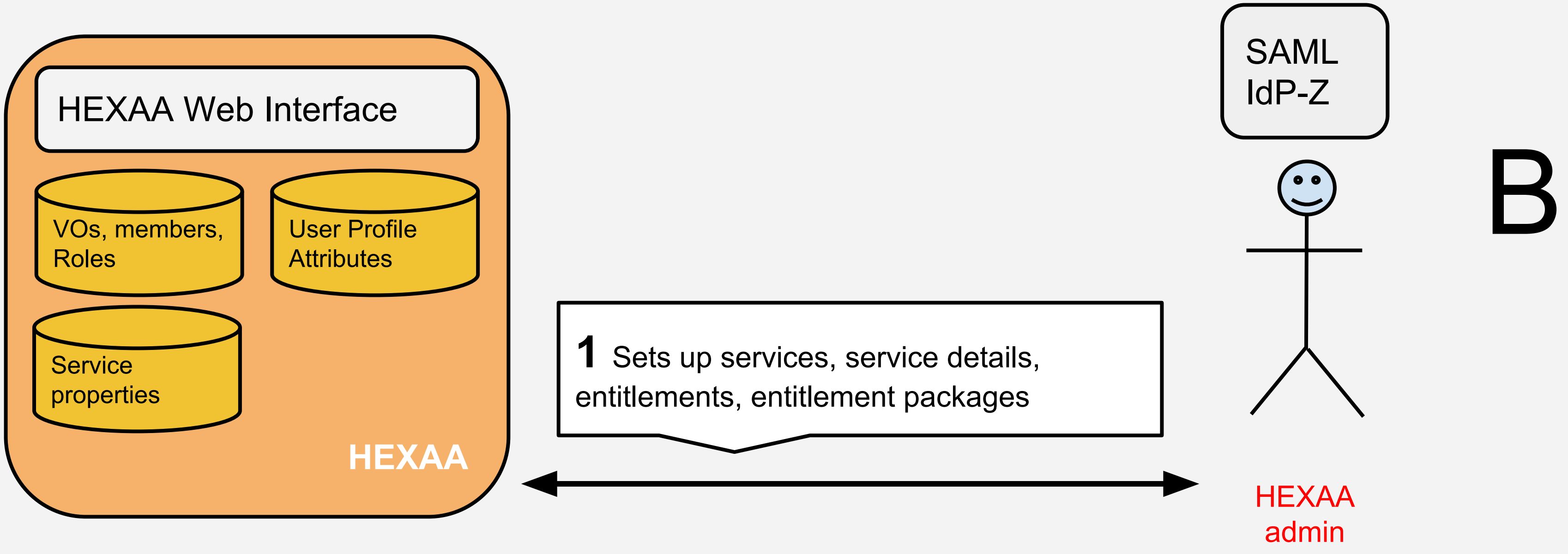
User Profile Attributes

Service properties

HEXAA

A

Service owner (also a user)



HEXAA Web Interface

VOs, members, Roles

User Profile Attributes

Service properties

HEXAA

1 Sets up services, service details, entitlements, entitlement packages

SAML IdP-Z

B

HEXAA admin