JÜLICH
FORSCHUNGSZENTRUM

UNICORE and Unity
complex scenarios

7 September 2015 | Krzysztof Benedyczak, Mathilde Romberg, Bernd Schuller

Outline

Complex scenarios

- DFN-AAI for a NGI-DE successor (Jülich, Dresden, Karlsruhe)
- OpenID Connect in the Human Brain Project

Outlook to future Unity releases

DFN-AAI

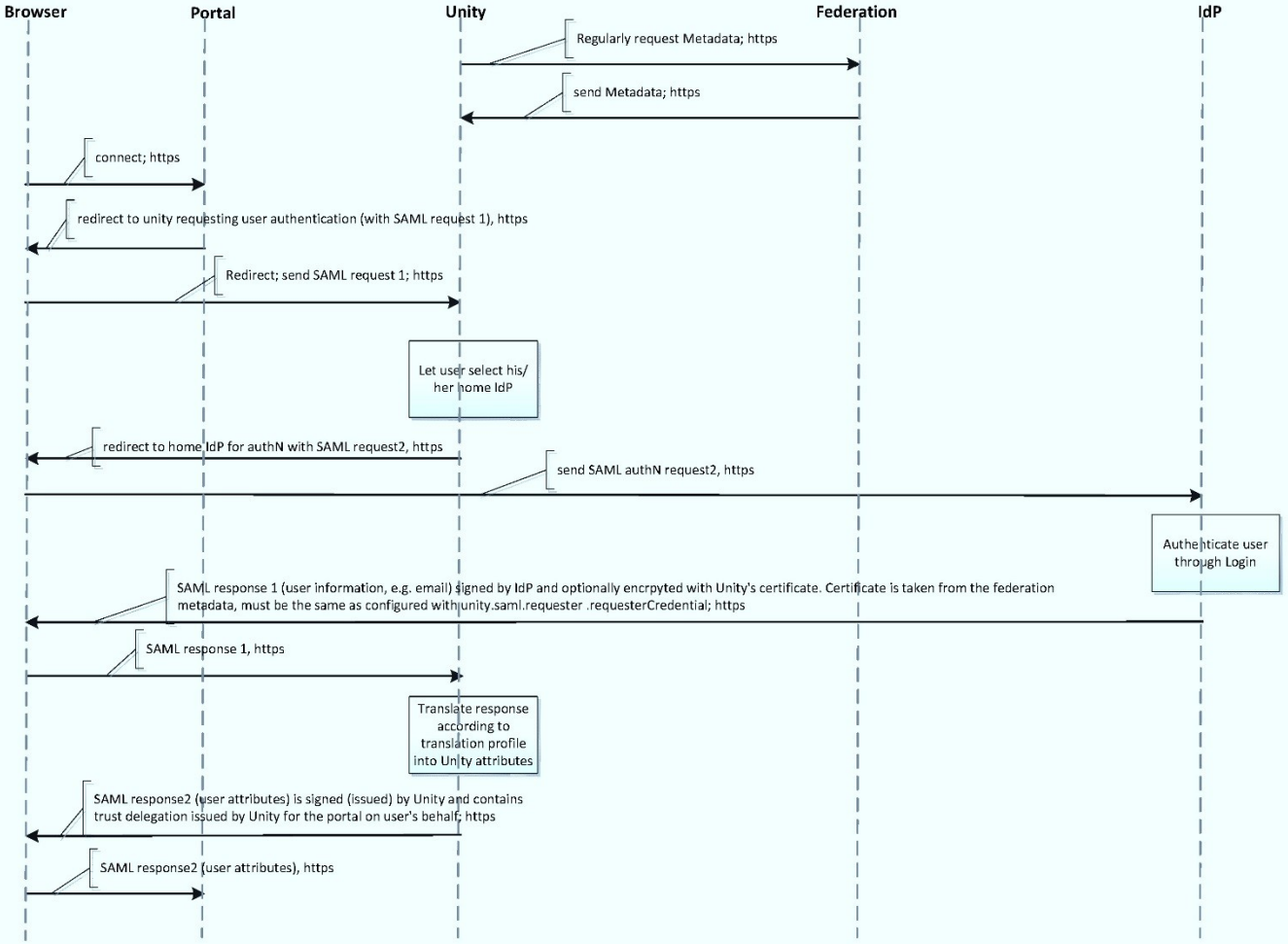
Scenario:

- Users using the UNICORE Portal should be allowed certificate-less access to UNICORE services. They all belong to institutions whose IdP is part of a federation

Prerequisites:

- Unity Grid certificate for SSL-Handshake with UNICORE services
- Credential for accessing the federation
- Metadata of Unity needed to be accepted as SP by the federation

Handshake



Affected endpoints

saml-webidp (web browser only)

- the server's unique URI which is inserted into SAML responses
- credential used to sign assertions
- trusted SAML issuers
- group to be used for providing attributes
- clients acceptance policy
- response consumer address of the Portal (SP)
- X.500 DN of the Portal (trusted SP)

Affected authenticator

samlWeb (remoteSamlAuth.properties)

- unity.saml.requester.requesterEntityId= *URL of unity service's metadata*
- unity.saml.requester.metadataPath= *metadata1*
- unity.saml.requester.requesterCredential= *certificate entry in pki.properties*
- unity.saml.requester.acceptedNameFormats.*n*=…
- unity.saml.requester.displayName= *name, used in portal and in metadata*
- unity.saml.requester.metadataSource.*federation.*url= *URL to federations metadata file*
- unity.saml.requester.metadataSource.*federation*.perMetadataTranslationProfile= *name of translation profile*
- name of the federation's public certificate as defined in pki.properties
- name of the registration form

Translation Profile

The sequence of actions is important:

- first, map identity to create the DN;
- second, map attribute to assign the group;
- third, map attribute to create a cn;
- fourth, map group to map the assigned group to an existing one; ...

BUT …

…if it works for users from your IdP it might not for those from other IdPs within the federation

because

the minimal output from IdP is yes / no
but none of the attibutes identifying the user

For this scenario where users don‘t have to register with Unity but are automatically registered, you need at least the user‘s e-mail address

Still to do

Map automatically created DNs to the corresponding Xlogins → fill the XUUDB

OpenID Connect in the Human Brain Project

Scenario:

- Human Brain Project users should be allowed certificate-less access to UNICORE services.
- UNICORE Portal (=web) and REST API access

- Human Brain Project uses OpenID Connect (OIDC) for single sign-on

Scenario 1: REST API access to the HPC platform

HBP Portal,
other applications

1. authenticate

returns token

OIDC server
user login

3.1 validate

2. access UNICORE
job submission, data movement, ...

3. validate token

OK

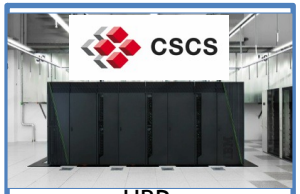
Unity

REST API

UNICORE

HBP Molecular Dynamics Supercomputer

HBP Data Analytics Supercomputer

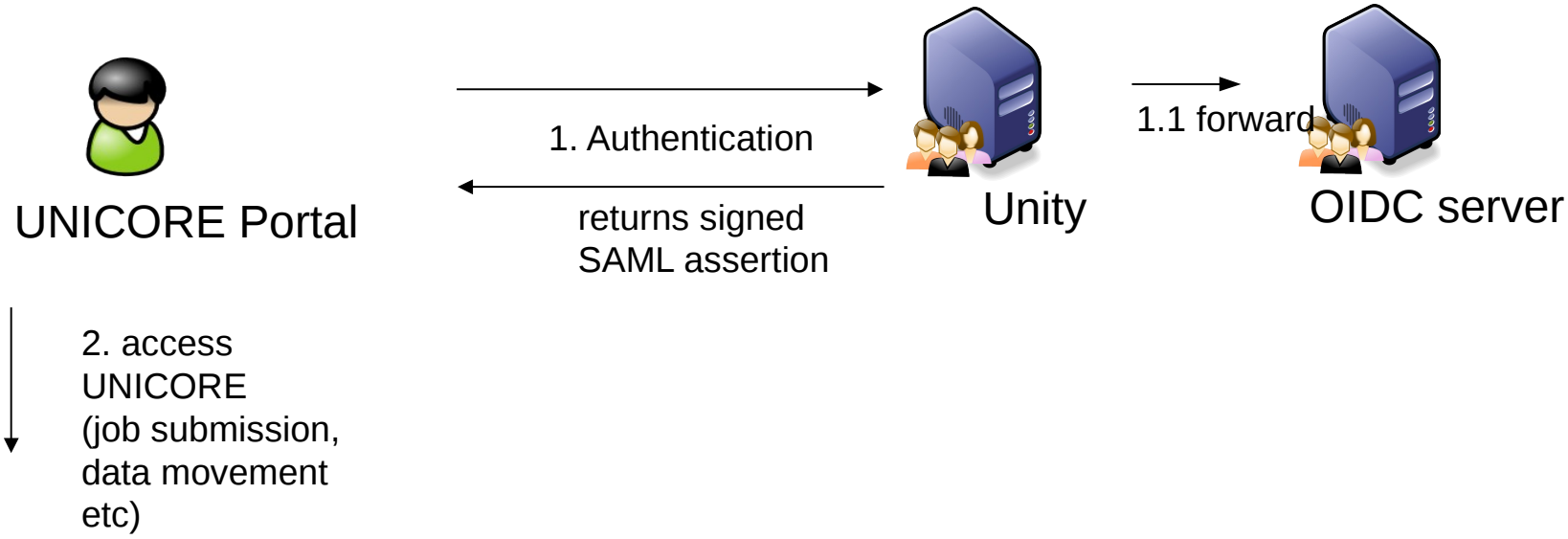


HBP
Development System

HBP
Supercomputer

HBP
Cloud Storage

Scenario 2: login to UNICORE Portal



UNICORE

HBP Molecular Dynamics Supercomputer

HBP Data Analytics Supercomputer

HBP Development System

HBP Supercomputer

HBP Cloud Storage

Need two OIDC enabled endpoints

Validation of bearer token (for REST API access)

unityServer.core.authenticators.5.authenticatorName=oidc
unityServer.core.authenticators.5.authenticatorType=oauth-rp with cxf-oauth-bearer
unityServer.core.authenticators.5.verificatorConfigurationFile=conf/authenticators/remoteOAuth.properties

Forwarding to an external OAuth IdP (for web access)

unityServer.core.authenticators.6.authenticatorName=oauthWeb
unityServer.core.authenticators.6.authenticatorType=oauth2 with web-oauth2
unityServer.core.authenticators.6.verificatorConfigurationFile=conf/authenticators/externalOAuth.properties

Setup

Register Unity as OIDC client with OIDC server:

- Different OIDC profiles for web and token validation
- Each endpoint requires its own „client ID“ and „client secret“

Translation profile:

- Create or map user identity
- Map user DN from common name and unique user ID: 'CN='+attr['name']+' '+attr['sub']+',O=HBP'"
- Map to „/“ group
- Create „cn“ attribute (for UNICORE portal)

UNICORE user authorisation (at Jülich)

JÜLICH FORSCHUNGSZENTRUM

Using traditional XUUDB

- Map user DN to role „user“, assign Unix login and groups

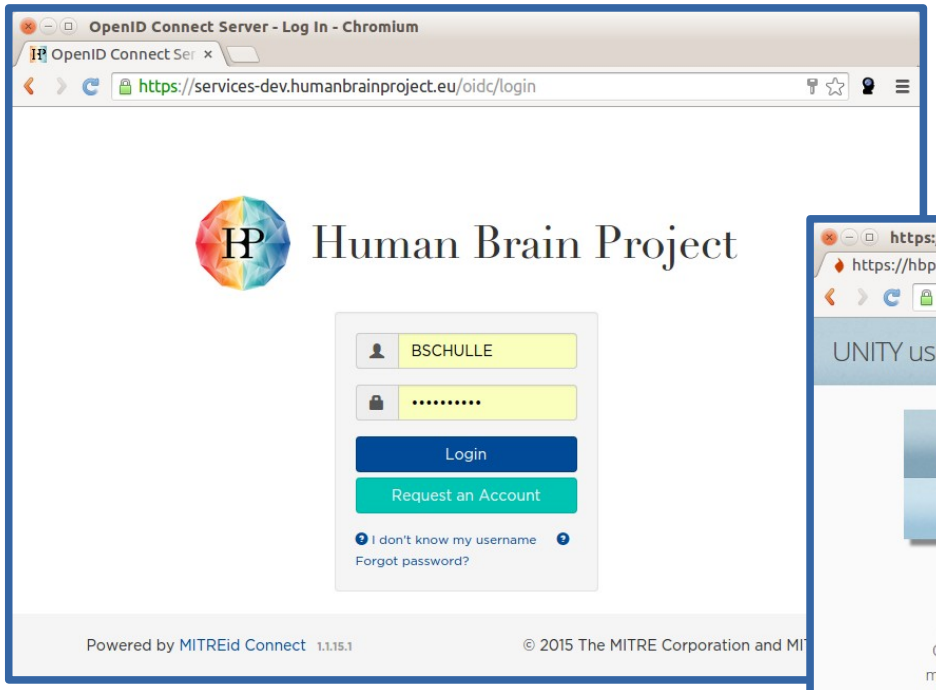
Jülich HPC users are managed in LDAP

- Updated from central HBP LDAP
- Filtered for users with an HPC account
- LDAP info contains CN and unique OIDC user ID: 'sub'

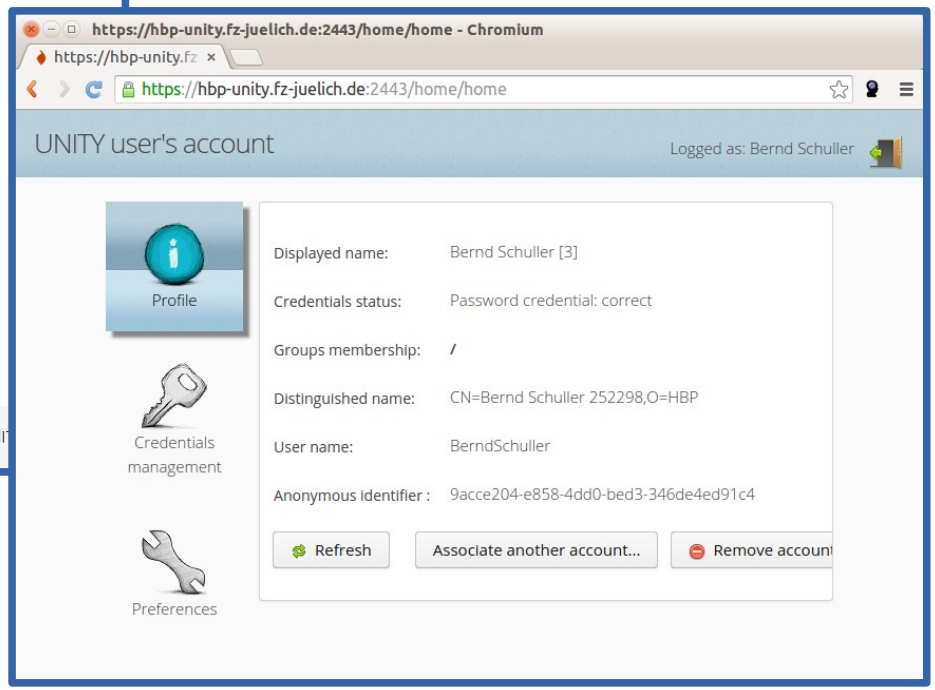
Auto-generate XUUDB content

- Query LDAP (once per day)
- 'CN='+attr['name']+' '+attr['sub']+',O=HBP'"
- Unix login and groups

End result:
Full integration with HBP infrastructure for user authentication and authorisation



OIDC: HBP services login



Unity: Authentication for UNICORE services

Remarks

Reduce number of clicks in web applications?

- Long series of clicks required to reach the „real“ login screen
- Often only a single option exists (e.g. in Portal or on Unity login page)
- Is it possible to automatically forward the user?

Collection of „How-to“s

- Unity documentation is very comprehensive
- Collect complex use cases as a series of setup and configuration steps?

Unity roadmap

Unity - current status

- Deployed in increasing number of infrastructures (not really verified nor exhaustive list):
  - PL-Grid
  - EGI
  - LSDMA
  - EUDAT
  - HBP
  - others
- Six base releases, two additional bugfix releases.
- 1.7.0 soon to come.

Unity - recent developments

- Emails verification
- Translation profile debugger and visual editor
- New, modern theme; possibility to brand the UI
- Constantly enhanced REST interface with read and write ops
- Merging of user accounts (both admin and user driven)

- General trend: provide more user-controlled features.
  - E.g. possibility to remove (or schedule removal) of an account.

Unity - future plans

- Version 1.7.0 will
  - help to provide full synchronization of data with remote IdPs
  - forms for already registered users:
    - additional agreements (pushed by admin),
    - possibility to request additional account features (e.g. apply for another group membership)
- Next version (with small ?)
  - Change of internal authorization
  - user-managed groups
- Further plans:
  - usability
  - better HA support