

HDF AAI

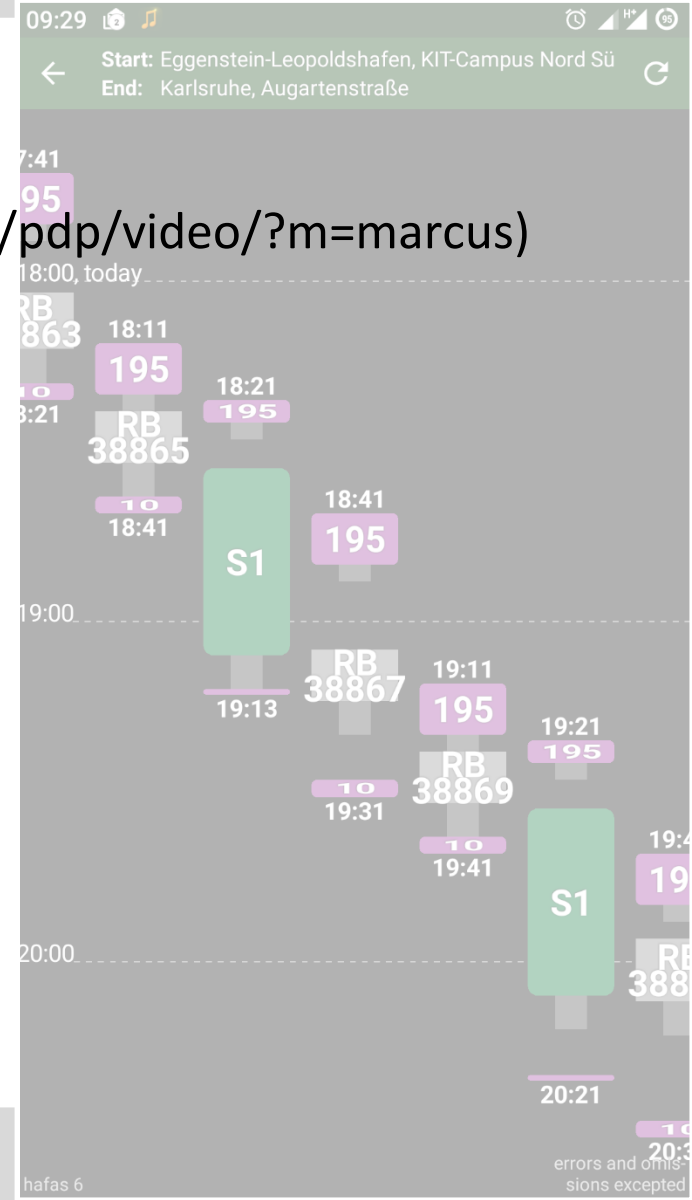
Overview, Status, Issues

Marcus Hardt, KIT



Organisational

- For presenting: Join Vidyo (<https://www.nikhef.nl/pdp/video/?m=marcus>)
- Coffee / Cookies / Fruit
 - **Thanks to Ingrid!!**
- **Two Parts**
 - Today:
 - Technical Talks
 - **Preparation of demos**
 - Friday: HDF Technical Board (via remote)
 - 9:00-10:15: Demos
 - 10:45: Policy Discussion
- Dinner:
 - GridKa Bus: 18:00
 - Last Public Transport: 19:11
 - Schlosslichtspiele 21:00 - 23:30
 - <http://schlosslichtspiele.info>
 - Badisch für Anfänger: "Wo ihsch dehs Schlohss"



■ HDF Proposal:

- 6 Helmholtz Centres (AWI, DESY, DKFZ, FZJ, GSI, KIT), 10 M€/a
- Focus on **hardware**, to “satisfy the additional resource needs of a wide spectrum of scientific domains covering the Helmholtz research fields Energy, Earth and Environment, Health, Key Technologies and Matter”...
- ...**“data centres will be federated”**...
- ...“the federation is open and **extensible for additional data centres from Helmholtz, universities and other research institutions in Germany**”...
- ...“Links to European and international research data and supercomputing **infrastructures like EUDAT, EU-T0, WLCG, PRACE and NDS** will be established”...
- ...**“enable a better cooperation of scientists in Germany with their international colleagues and ESFRIs”**...

Goals

1. Extensible Federated Authentication and Authorisation Infrastructure
2. Compatible with international initiatives
3. Resources mainly in Germany, but international users

■ Derived / technical Goals:

1. Be in line with **European activities** focusing around the European Open Science Cloud **EOSC**
2. Enable the **participating centres to connect services** to federated infrastructure
 - Including non-web services
3. **Enable Principal Investigators / Virtual Organisations**
 - => **allocate resources** on behalf of their group
 - => **manage membership and authorisation** for their groups
4. Enable **global researchers** to use services provided by Centres
(Given they are properly authorized and their identity is adequately understood)
5. Ensure that **federated users are well known**, based on **solid authentication**
 - => **Policies**
6. Proof of Concept Demonstrator:
 - Example services
 - Deployment
7. Policies

General Plan in HDF-AAI

- Unity is the SP-IdP-Proxy
 - <http://unity.helmholtz-data-federation.de>
- Use OIDC to integrate services
- Group based access control
 - Services filter access by group membership
- Delegated Group Management
 - E.g. Communities can self manage their membership
 - Centres can provide services for selected communities
- Delegated Authentication / Identity verification
 - **Services trust other centres to do their thing right**

1. Be in line with European Initiatives

■ Problem

- Current multitude / shift of technologies (X.509, SAML, OAuth, OIDC, ...)
- Grid shifts to token-based, SAML stays around, NRENs moving to OIDC-Fed

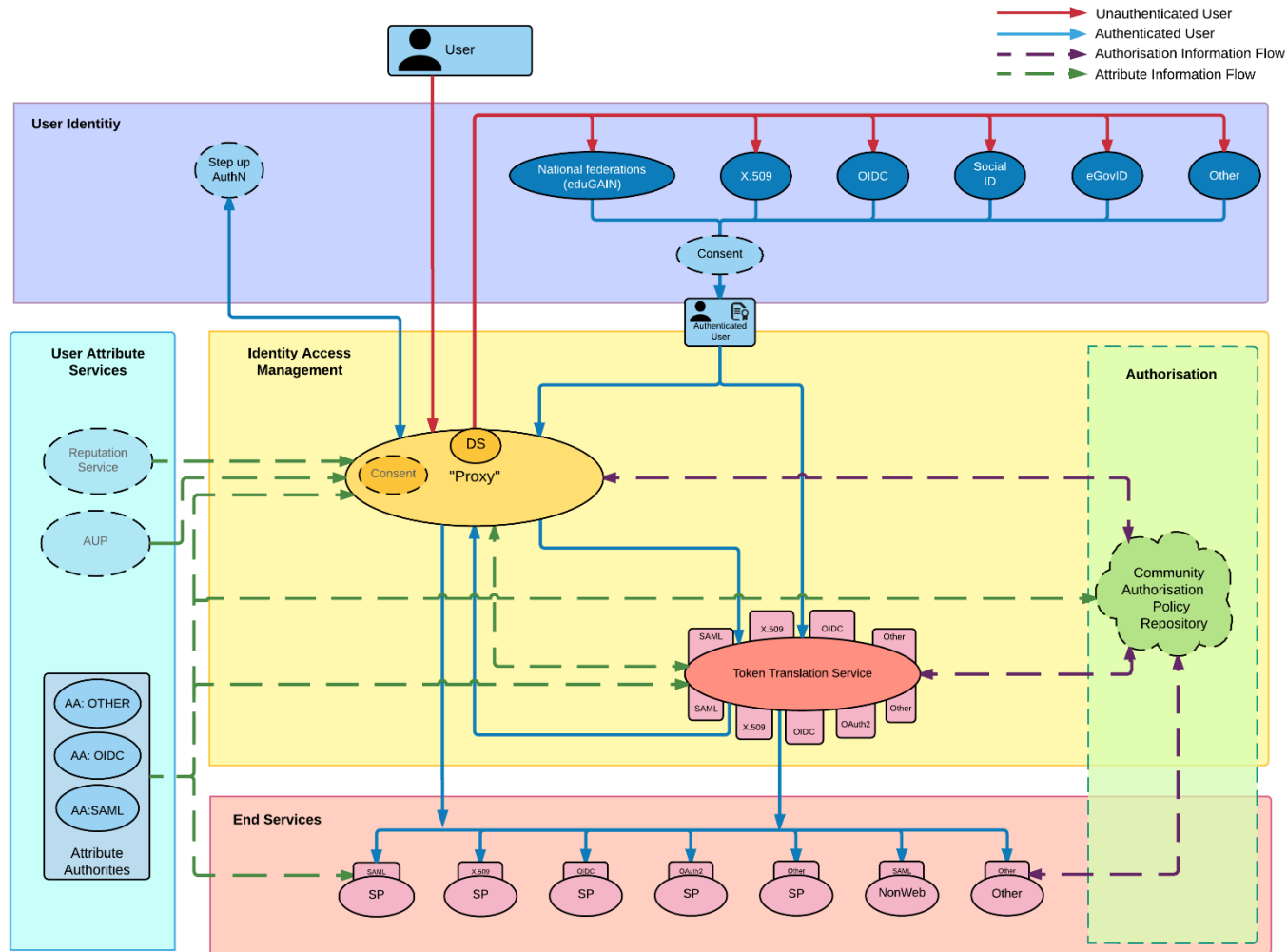
■ Plan for HDF

- Follow the AARC Blueprint Architecture (BPA)
 - SP-IdP Proxy solves issues (Attribute release, service-friendliness, ...)
 - **Central** SP-IdP-Proxy implementations: IAM, EGI-Checkin, EduTEAMS, B2Access/**unity**
 - HDF to provide an initial SP-IdP-Proxy
 - Communities are supposed to self-service themselves in the future
- Users come “in” via SAML (i.e. DFN-AAI)
- Services may use SAML and **OIDC**
- OIDC is preferred
 - API / non-web
 - Delegation
 - Ease of use

■ Status

- Unity instances running, demonstrator services connected
- <https://unity.helmholtz-data-federation.de>

AARC Blueprint Architecture



Why the proxy model?

- All internal Services can have **one statically configured IdP**
- **No need to run an IdP Discovery Service** on each Service
- Connected SPs get **consistent/harmonised user identifiers**
and accompanying attribute sets from one or more AAs
that can be interpreted in a uniform way for authZ
purposes
- External IdPs only deal with a **single SP** proxy



Who is deploying the AARC Blueprint?



2. Enable Centres to provide services / accept users

■ Problem

- OIDC is not used much in scientific context
- Non-Web use cases were not well supported
- Manual / paper based procedures to create accounts for remote users

■ Plan for HDF

- Establish OIDC services at the sites
- Provide integration for non-web services
 - User (De)Provisioning for commandline Services
 - Integration of REST-API services

■ Status

- OIDC Services available at most sites (others have plans)
- Provisioning service (FEUDAL) available as a demonstrator

3. Enable Virtual Organisations

■ Problem

- Access rights management for user is already very cumbersome
- For federated users this requires delegated (3rd party) user management

■ Plan for HDF

- Establish Virtual Organisation (VO) concept
 - => VO Managers can administer members
 - => Services can filter users by VO membership

■ Status

- Unity provides rudimental management capabilities
- Future integration of advanced tools possible (Perun, Grouper, Hexaa, EduTEAMS, ...)

5. Ensure users are well known (and: 4. Include global users)

■ Problem “Assurance”

- Services require some guarantee about the user
- Services might want to filter based on users’ assurance
- IdPs don’t explicitly send assurance information

■ Plan for HDF

- Use DFN-AAI and initial f2f communication to describe IdPs in RAF terms
- Unity to provide this information in OIDC claims

■ Status

- Planning

A few words on assurance

■ REFEDS Assurance Framework (RAF)

■ ID-Uniqueness:

- ID/unique ($\leq$ **unity**)
- ID/no-eppn-reassign ($\leq$ **WLCG**)
- ID/eppn-reassign-1y

■ ID-Proofing:

- IAP/low
- IAP/medium ($\leq$ **WLCG, DFN-AAI**)
- IAP/high
- IAP/local-enterprise

■ Attribute freshness:

- ATP/ePA-1m ($\leq$ **WLCG, DFN-AAI**)
- ATP/ePA-1d

■ Services should trust this information

- This should also work for eduGAIN users (e.g. french scientist that needs to access data at e.g. DESY)

■ In addition (or instead) Services **MAY** run their own whitelists for home IdPs (once external_authn works)

■ Note: Whitelists will require the **n-m** relation in practice. This does not scale.

■ SIRTFI

- Provide Security Contact (and a bit more)
- See Uros presentation for details

Value	Cappuccino	Espresso
\$PREFIX\$	X	X
\$PREFIX\$/ID/unique	X	X
\$PREFIX\$/ID/eppn-unique-no-reassign		
\$PREFIX\$/ID/eppn-unique-reassign-1y		
\$PREFIX\$/IAP/low	X	X
\$PREFIX\$/IAP/medium	X	X
\$PREFIX\$/IAP/high		X
\$PREFIX\$/IAP/local-enterprise		
\$PREFIX\$/ATP/ePA-1m	X (*)	X (*)
\$PREFIX\$/ATP/ePA-1d		

6. Proof of Concept Demonstrator

- FEderated User credential DEployment PortaL (FEUDAL)
 - <https://hdf-portal.data.kit.edu>
- KIT OpenStack Test Service <https://oscloud-1.scc.kit.edu>
- Monitoring <https://hdf-mon.gsi.de>
- Prometheus <https://prometheus.desy.de>
- WaTTS <https://watts.helmholtz-data-federation.de>
- LSDF ssh hdf_<username>@hdf-login.lsd.f.kit.edu

7. Policies

■ Policy Matrix

■ Details on

https://docs.google.com/document/d/1J3L_dcjzjCqfqrKVqygLE_SgX2Jjwsn1_oNqNpgRBc4

■ More in Uros' talk (Fri 11:45)

		Management	Infrastructure Security Contact	User Community Management	Service Management	User
Top Level	Infrastructure Policy	Defines & Abides by	Abides by	Abides by	Abides by	Abides by
Data Protection	Privacy Statement	Defines			Defines	Views
Membership Management	Community Membership Management Policy	Defines		Abides by		
	Acceptable Use Policy	Defines		Defines		Abides by
	Acceptable Authentication Assurance	Defines		Abides by	Abides by	
Operational Security	Incident Response Procedure	Defines	Abides by		Abides by	

Backupslides

Steinbuch Centre for Computing
Dr Marcus Hardt



Protocols and Technologies

■ Upstream IdPs:

- DFN-AAI, eduGAIN, ORCID => SAML2
- google, github, ... => OIDC, OAUTH2

■ Downstream Services

■ SAML2 supported in principle, however:

- No delegation
- No API calls
- Non-web is fishy

■ OIDC

- Basically everybody moves to OIDC, or similar token based (GEANT, DFN, CERN, EOSC,)
- Large commercial pickup (google, microsoft, oracle, paypal, ping-identity)

Issues / Future work

- Not much HDF hardware available via HDF-AAI
- Almost zero feedback on the policies that we sent around
- Technically we are quite fine
 - Everything works as **we** expected it
 - This might not be sufficient!

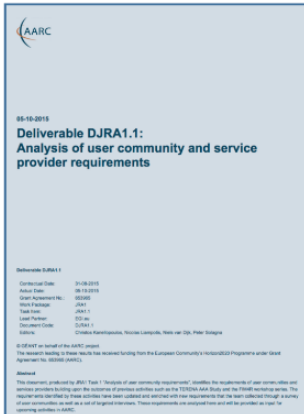
=> We need practical feedback and involvement!
- Organisationally we should move ahead:
 - Precise requirements and use cases needed to move on:
 - From Services: Policy requirements (AUP, User-Identification, Technical interfaces)

The goals



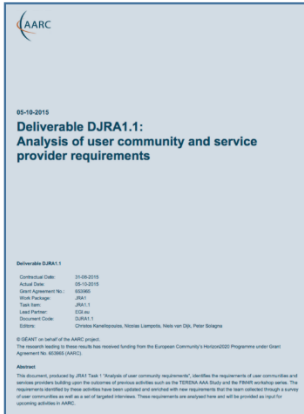
1. Users should be able to access the all services using the **credentials from their Home Organization**
2. Users should have one **persistent non-reassignable non-targeted unique identifier**.
3. Attempt to **retrieve user attributes** from the user's Home Organization. If this is not possible, then an alternate process should exist.
4. Distinguish **(LOA)** between self-asserted attributes and the attributes provided by the Home Organization/VO
5. **Access** to the various services should be granted **based on** the **role(s)** the users have within the collaboration
6. Services should not have to deal with the complexity of multiple IdPs/Federations/Attribute Authorities/technologies.

Attribute Release	Attribute Aggregation	User Friendliness	SP Friendliness
Credential translation	Persistent Unique Id	User Managed Information	Credential Delegation
Levels of Assurance	Guest users	Step-up AuthN	Best Practices
Community based AuthZ	Non-web-browser	Social & e-Gov IDs	Incident Response



The functional Components

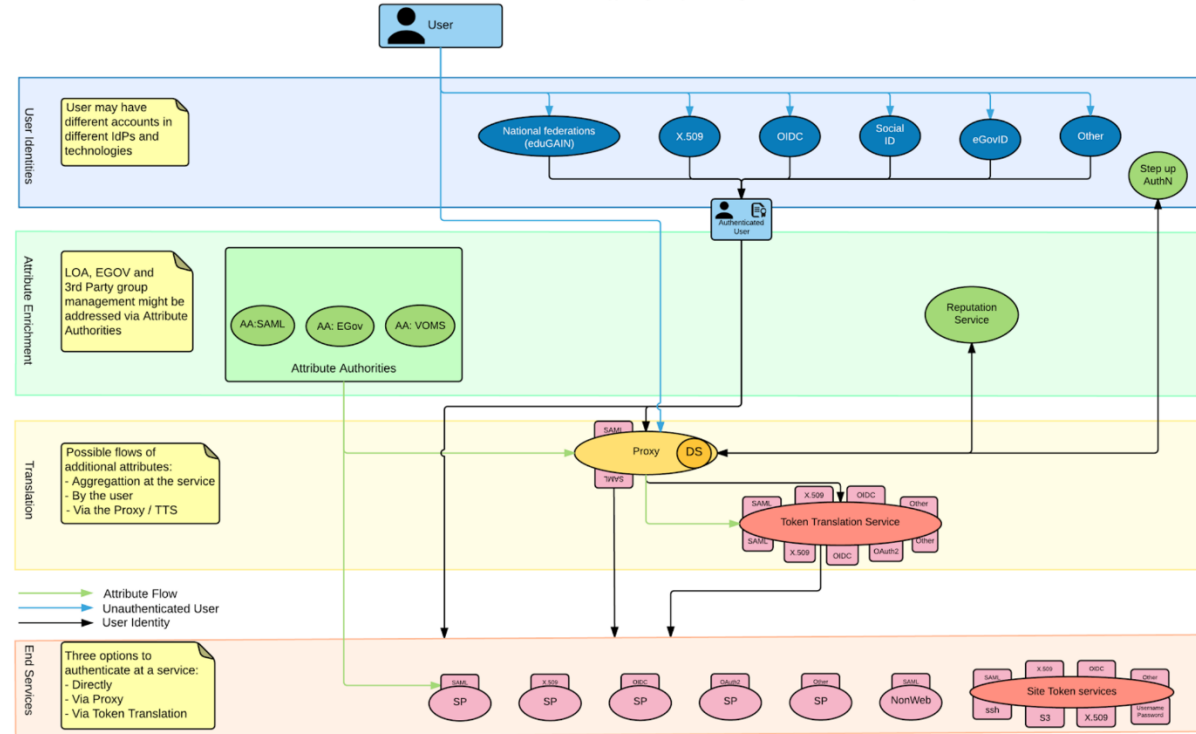
User Community Requirements



<https://goo.gl/kSxENp>

AAI: The e-Infrastructure view

What is happening on top of existing Federation infrastructures today



aarc-project.eu