Karlsruhe Institute of Technology

HELMHOLTZ
RESEARCH FOR GRAND CHALLENGES

Lessons learned HDF-AAI and BW-AAI

Policy Management – Technology – Federation Management

Matthias Bonn, Marcus Hardt, Martin Nußbaumer, Uli Weiß

RESEARCH FIELD KEY TECHNOLOGIES / INFORMATION

Goals

- Observation: Established trust *facilitates* the provision of services
  - Decision support for connecting services with well defined trust models (i.e. federations and virtual organisations)
- Providing authentication and authorisation infrastructure
  - Enable a wide sprectrum of application scenarios (levels of assurance, novel technologies and devices)
  - Support more systems, frameworks and programming languages
- Integration in federations
  - Explore the existing possibilities of OpenID Connect (OIDC)
  - Extend existing federation mechanisms towards novel concepts and technologies, keep compatibility

Skip?

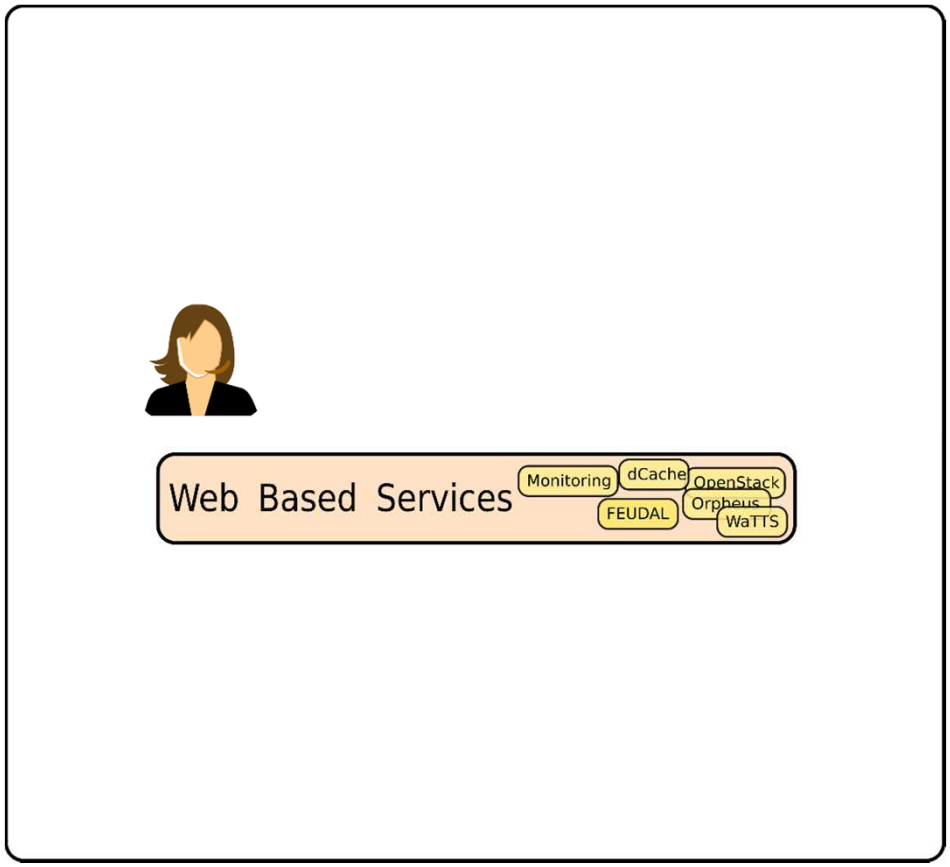
Lessons Learned from HDF AAI

HDF AAI Goal: Evaluation prototype

- Explore features beyond SAML
  - OIDC to support non-web use cases and delegation
- Exploit recent developments in EU Projects (AARC, EOSC)
  - CTA, CORBEL, DARIAH, EGI, ELIXIR, EPOS, EUDAT, GÉANT, Life Sciences, LIGO
- Explore advanced assurance mechanisms
- Evaluate the AARC Policy Development KIT

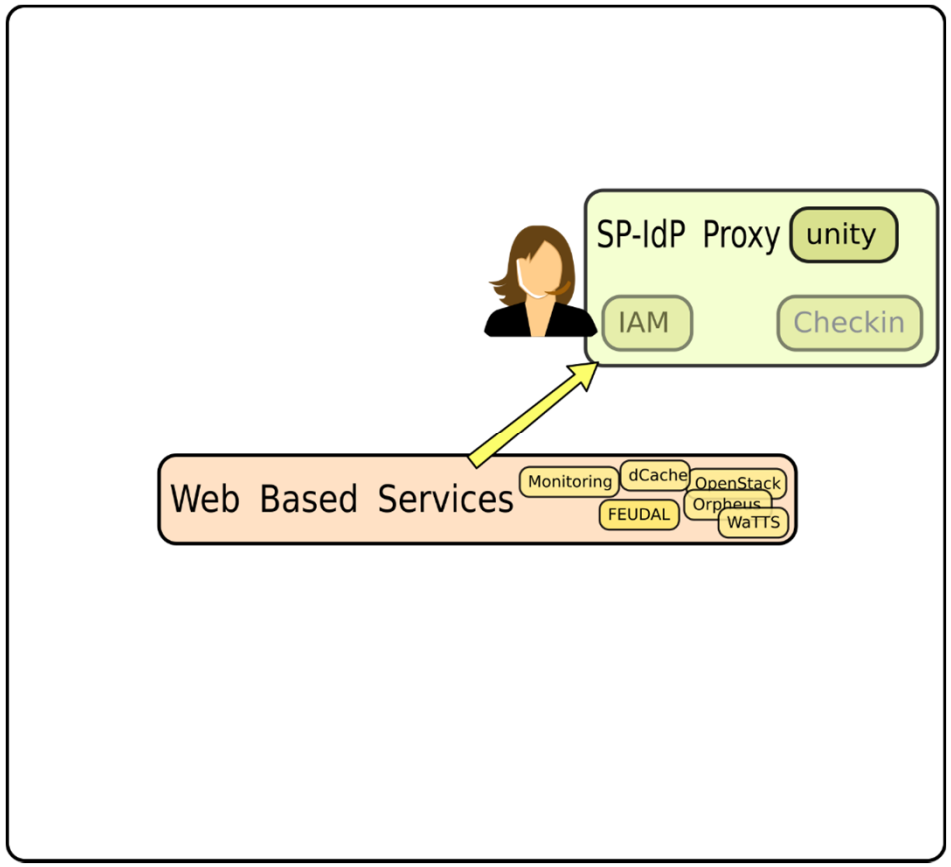
HDF AAI (Works today, Proxy based)

- User visits a (web based) service



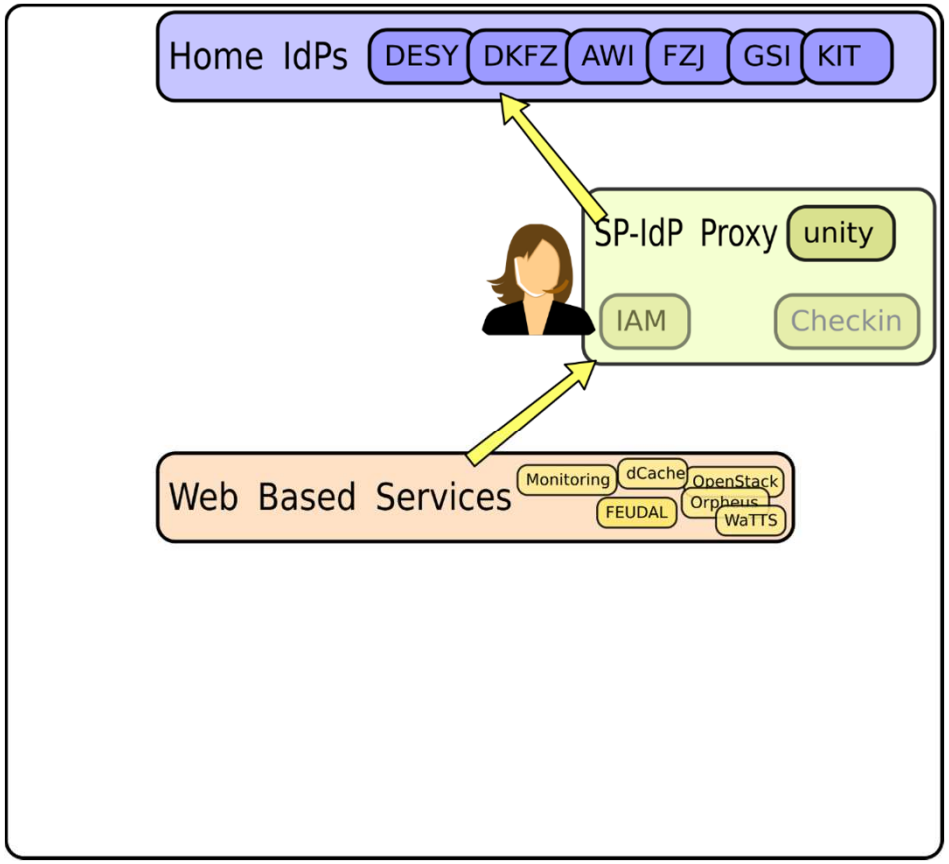
HDF AAI (Works today, Proxy based)

- User visits a (web based) service
- User is redirected to an IdP
  - Which is actually an SP-IdP proxy
  - Many implementations available:
    - Unity, IAM, Checkin, eduTeams, ...



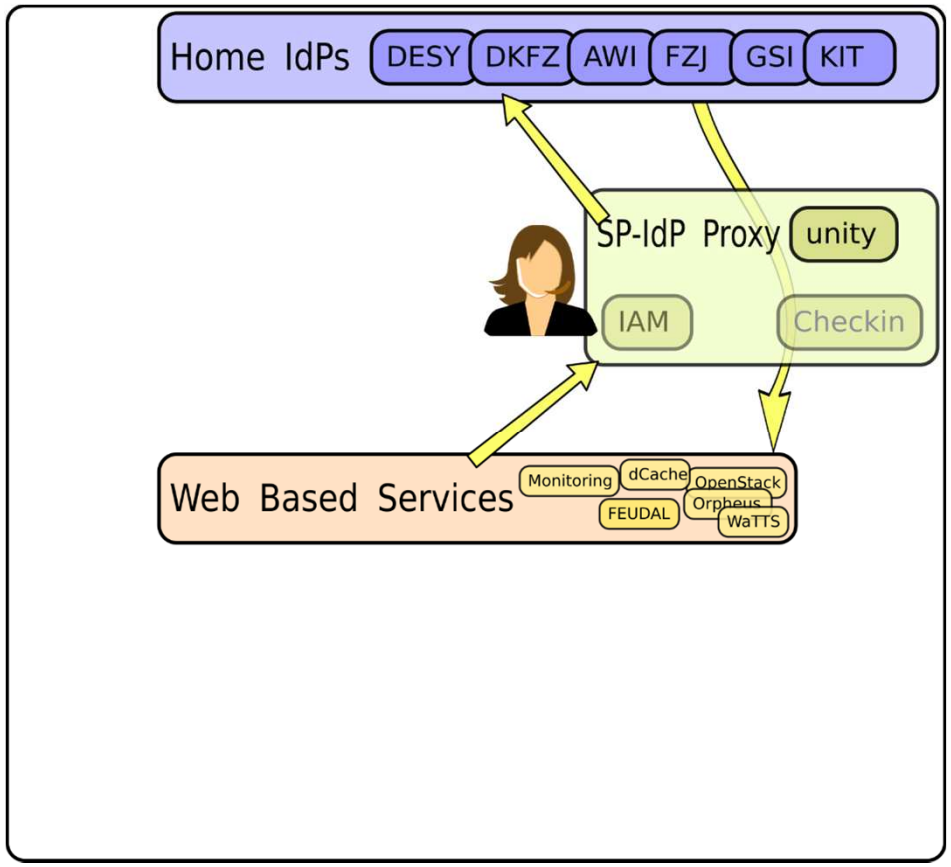
HDF AAI (Works today, Proxy based)

- User visits a (web based) service
- User is redirected to an IdP
- User is redirected **again** to home IdP



HDF AAI (Works today, Proxy based)

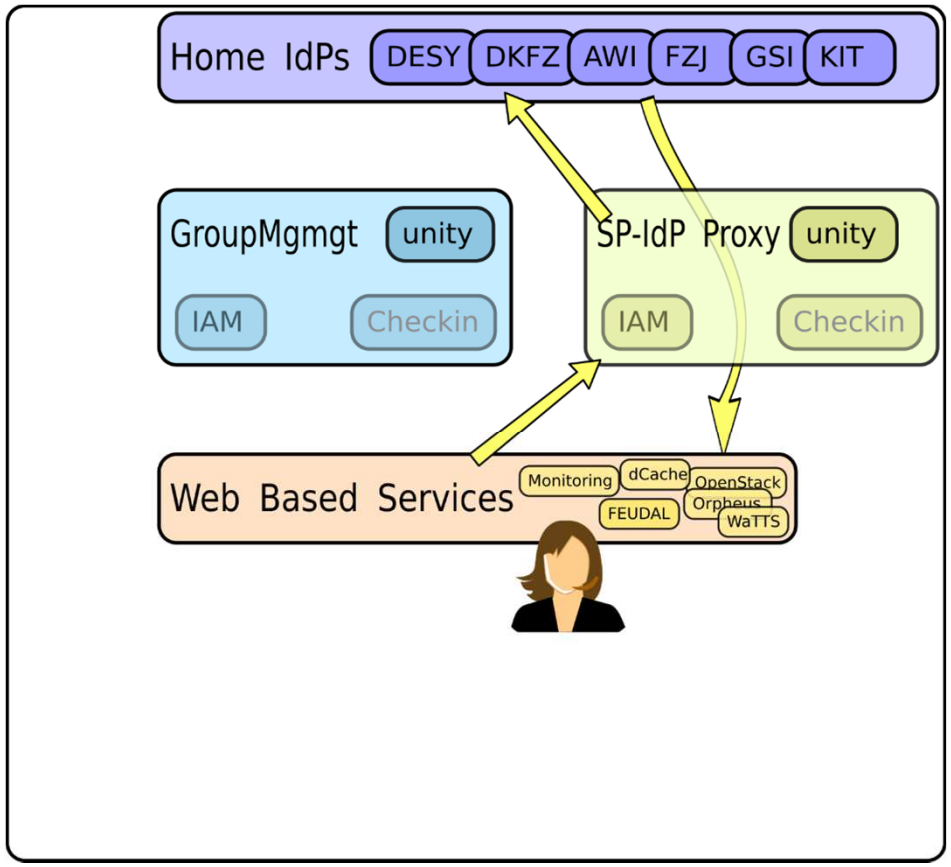
- User visits a (web based) service
- User is redirected to an IdP
- User is redirected **again** to home IdP
- Home IdP releases attributes to proxy
- Proxy releases attributes* to service
- Service makes his authorisation decision
- User reaches the service



Attributes
- Some IdPs don't release attributes
- Some IdPs impose restrictions on the proxy, which attributes to release
- Some communities use groups to organise themselves

HDF AAI (Works today, Proxy based)

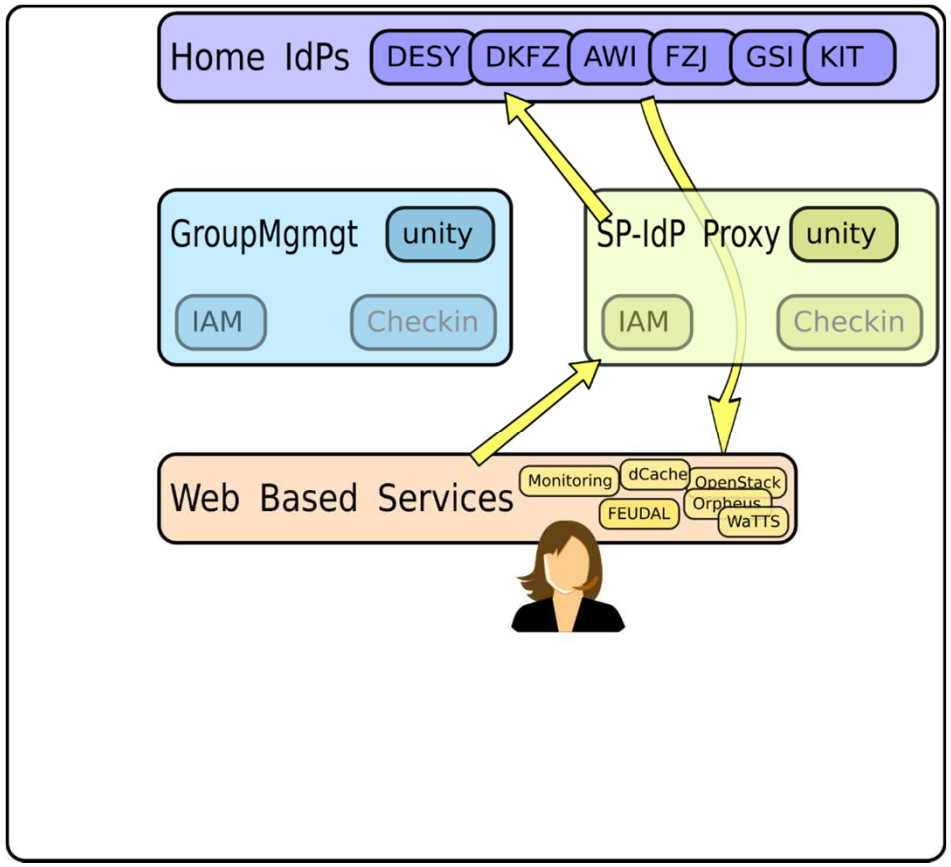
- Group Management
  - Typically delegated to a PI of the community
  - Allow community to request resources at multiple computer centres
  - Group membership decides upon usage
  - Example: WLCG, …



HDF AAI (Works today, Proxy based)

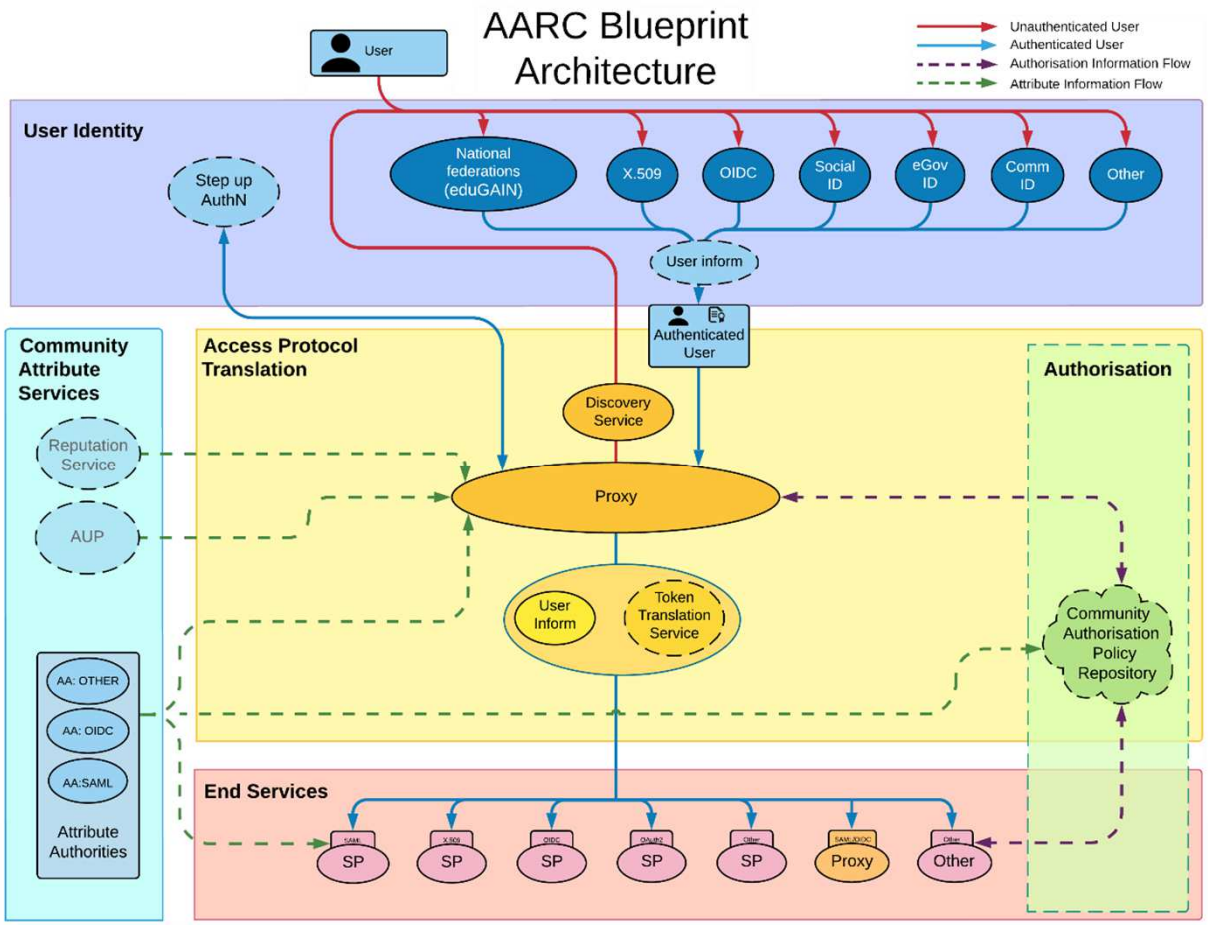
- Group Management
  - Typically delegated to a PI of the community
  - Allow community to request resources at multiple computer centres
  - Group membership decides upon usage
  - Example: WLCG, ...
- Group Management is a separate concept
  - Most SP-IdP-Proxies include that component

  => Groups are only available when authentication went “through” the proxy
  - Concept of Proxy and Groups bundle:
    - “Community AAI”



AARC Blueprint Architecture (BPA)

skip?



Services technically integrated in HDF AAI

skip?

- Via OIDC:
  - HDF Cloud Jülich (OpenStack/Web)
  - Test Cloud KIT (OpenStack/Web)
  - DKFZ + Desy evaluate OpenStack/cmdline
  - dCache Prometheus WebDAV
  - WaTTS
  - Icinga monitoring
- Via FEUDAL
  - SSH via regApp at KIT
  - CVMFS at DESY
- For a demo: https://login.helmholtz-data-federation.de
  - (Click “Services” on the bottom)
- More info: http://cvs.data.kit.edu/hdf-aai

Lessons learned from HDF AAI

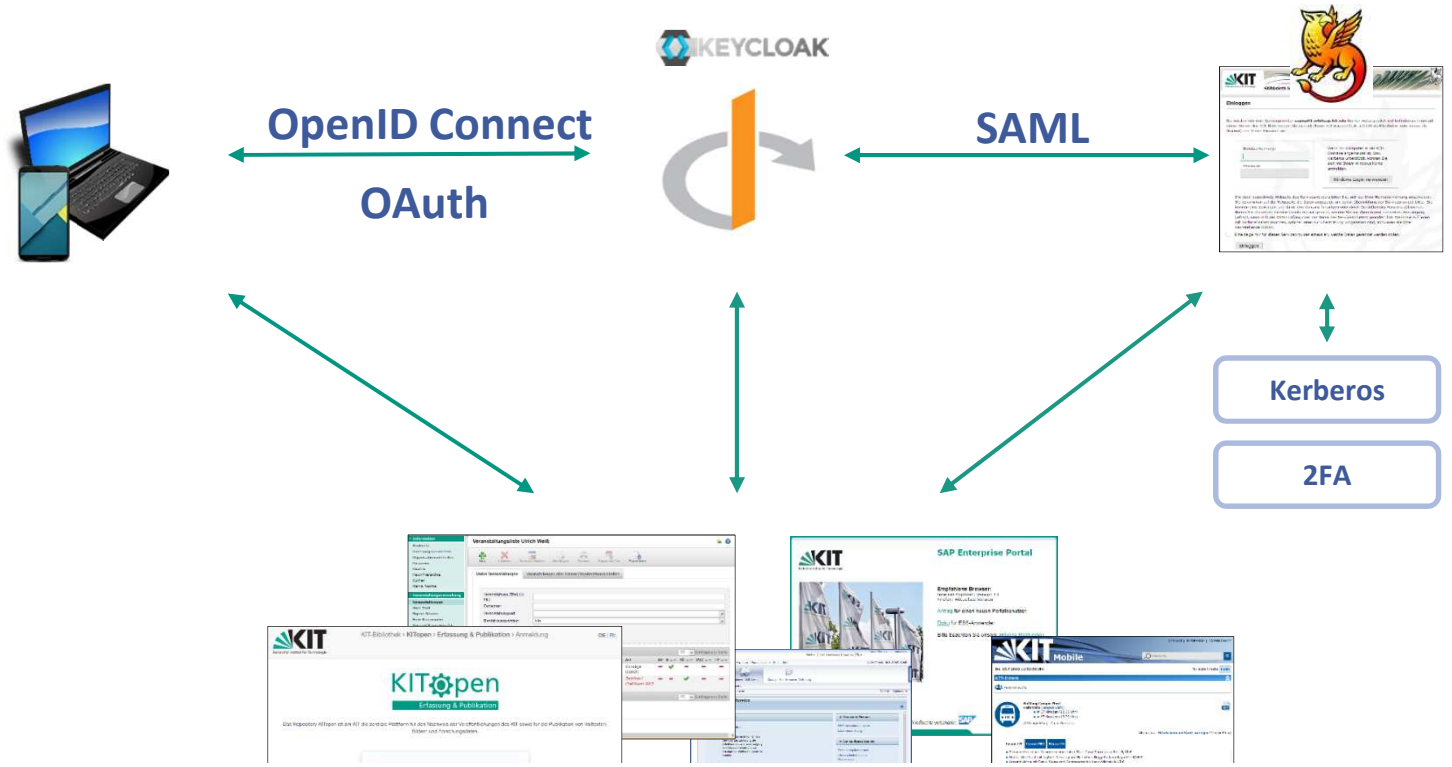
We have cars now…
*… they don't run without roads, gas stations, garages, **fees**, …*

- Technical feasibility of OIDC has been shown
  - Adoptable to standard software
  - Command line services
  - Web interfaces (REST, SOAP, …)
- OIDC is great, but it is technology only
  - Deprovisioning is an issue
  - New tools require policy adjustments: Delegation is a potential privacy issue
  - Non scalable 1:1 trust model hinders cost effective service onboarding
  - → Develop concept for an appropriate federation management

Federation Management Concepts with OpenID Connect

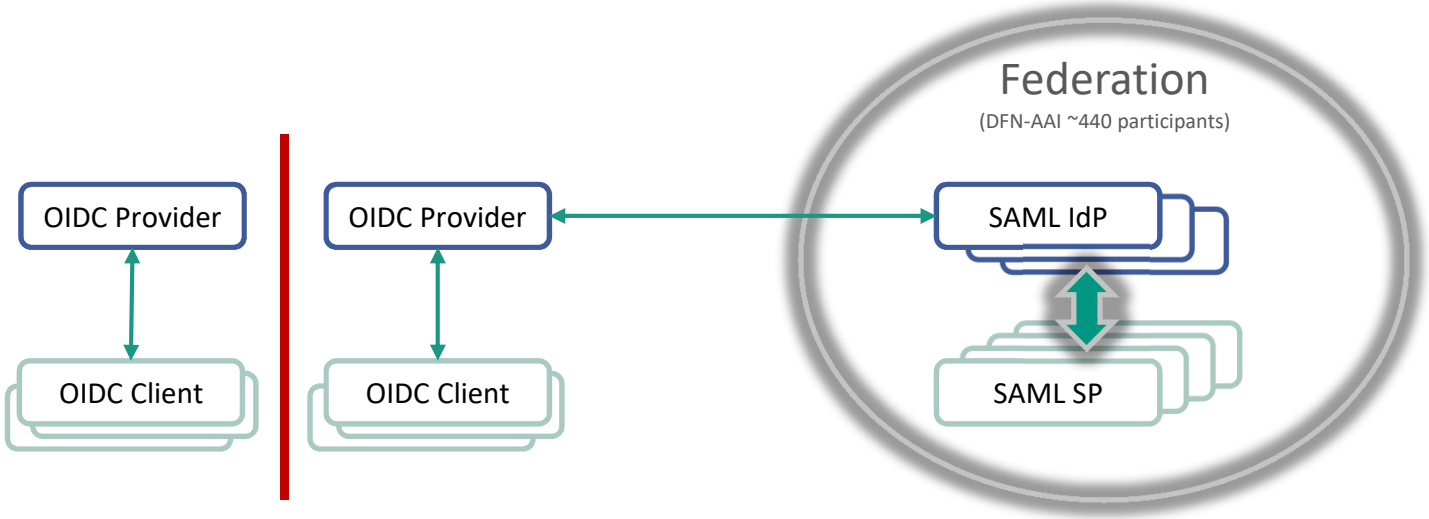
Blueprint for OIDC Integration in SAML

Operational Setup & Experiences at KIT



…, Library, Campus, Ilias, SAP, Mobile, …

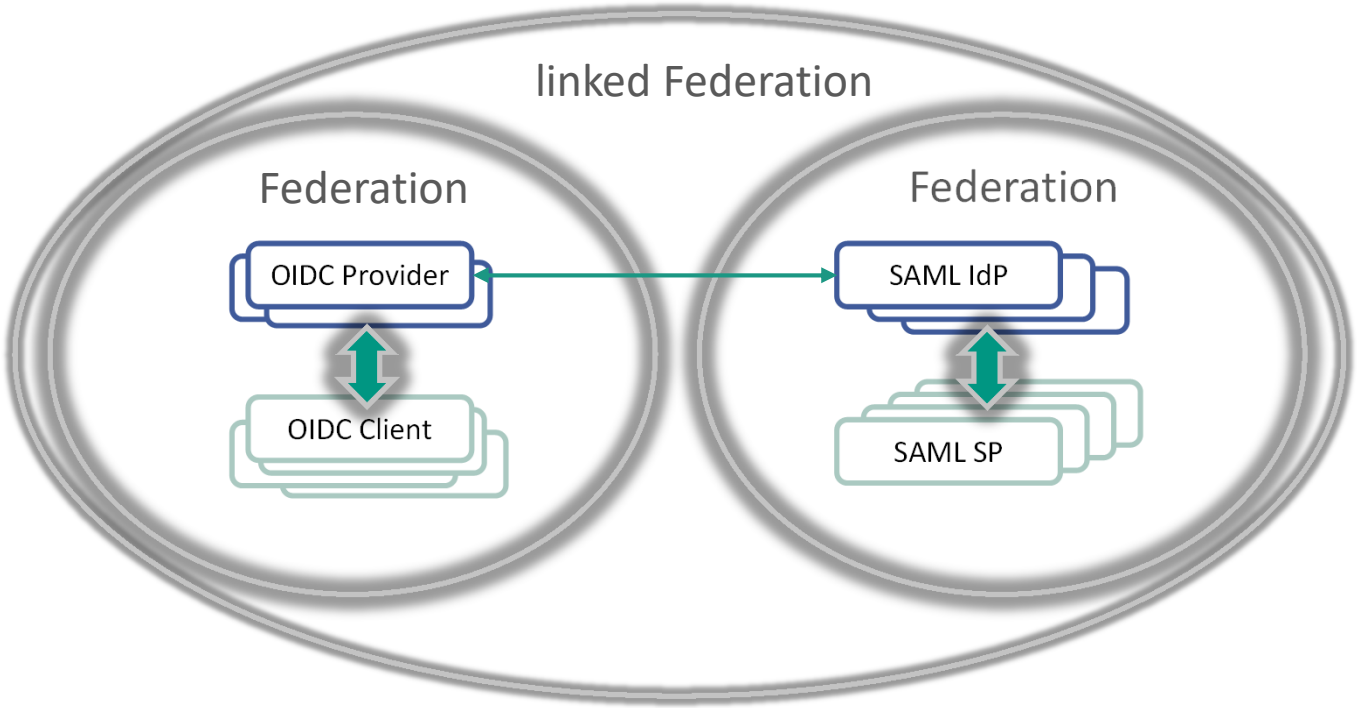
OpenID Connect + SAML: Best of Breed



- No federation, no suitable management
- Heterogenous software landscape, own developments possible
- Functional flexible, many client options und application scenarios, delegation
- Can be implemented and operated securely

- Federation is established, legal conformity
- Stable and flexible IdP standard software, stable SP standard software
- For SPs only standard scenario usage, own developments/extensions are difficult
- Implementation and operation is secure

OpenID Connect and SAML, federated



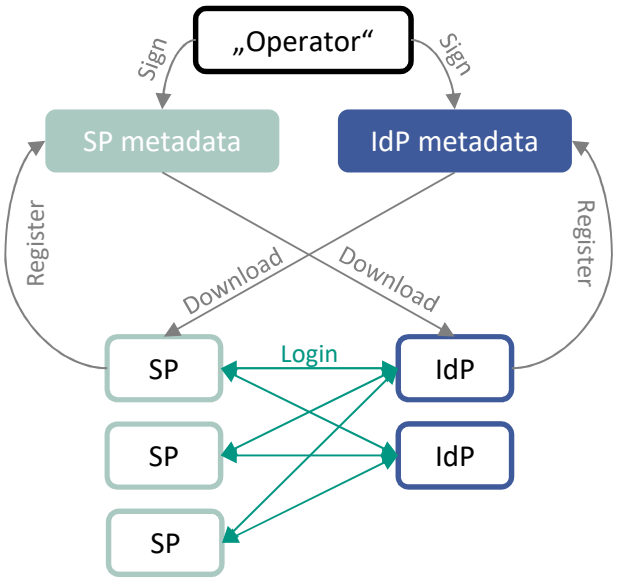
Steps to build a linked SAML-OIDC federation

- SAML Federation: Established, standardized
- OIDC Federation Specification: Work in progress, complex
- OIDC missing federated distribution of metadata
- **Integrate provider metadata using SAML extensions**
- **Provide client metadata via trusted download**
- **Enhance providers and clients to query metadata and reconfigure dynamically**

SAML Federation

Skip?

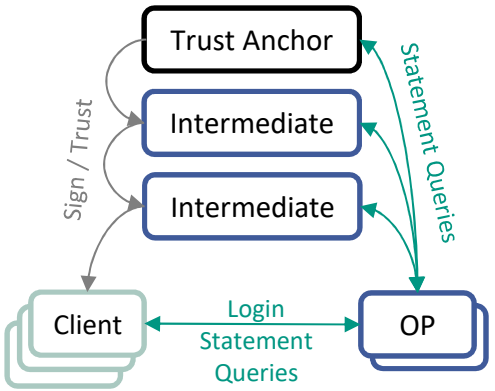
- Established in scientific environments, forming
  „a group of IdPs accepting a dedicated set of rules and polices (the central part) but staying independent in internal affair“
- Core concepts of a federation:
  - **Big centrally managed metadata directory**
  - All metadata is centrally signed
  - Participants know each other, offline
- Standard implementation Shibboleth
  IdP and SP (Apache filter)
- Differing requirements are difficult to realize



OpenID Connect Federation

Skip?

- Work in progress specification
  [https://openid.net/specs/openid-connect-federation-1_0.html]
- Core concepts:
  - **No central big metadata directory**
  - Trust between OIDC provider and client is estabished dynamically at runtime using cryptographically verified trust chains
    - Similar to SSL-certificates: Self-signed trust Anchor/root has to be trusted
    - All federation participants need HTTPS endpoint to allow metadata statement query
    - For standalone applications or Javascript-SPAs this is challenging
- How and when do intermediates sign?
  How do clients get the available OPs?
- Complex, still no production-ready implementations (5 Years)



Bridging Technology

Skip?

- We have metadata URLs of providers/issuers: {issuer}/.well-known/openid-configuration live queryable
  [https://oidc.scc.kit.edu/auth/realms/kit/.well-known/openid-configuration]
- Client metadata is not queryable!
  - Client may not be a web server
  - But can be sent to OP to do a (typically authenticated or access restricted) offline self-registration, prior to usage
    [https://openid.net/specs/openid-connect-registration-1_0.html]
- metadata **formats are specified**, their federated distribution not
- To *establish trust*, both metadata sets have to be stored and signed centrally, for simple download

Integration in existing Federation?

Skip?

Karlsruhe Institute of Technology

- Integrate OIDC provider URLs within Shibboleth IdP metadata
  [https://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd]
  - SAML specifiction allows extension-Tags, for example

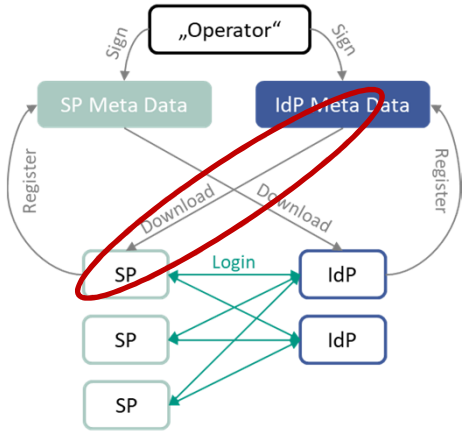
```
<Extensions>
    <oidc:issuer>https://oidc.example.org/</oidc:issuer>
    <oidc:config>https://oidc.example.org/.well-known/openid-configuration</oidc:issuer>
<Extensions>
```

  - Viable only for OIDC providers, whose home organization already participates in federated Shibboleth/SAML
- Client metadata has to be managed separately
  - JSON vs. XML, extension definition would be too complex
  - OIDC clients do not have a corresponding Shibboleth SP
  - Kind of new management interface for registration needed

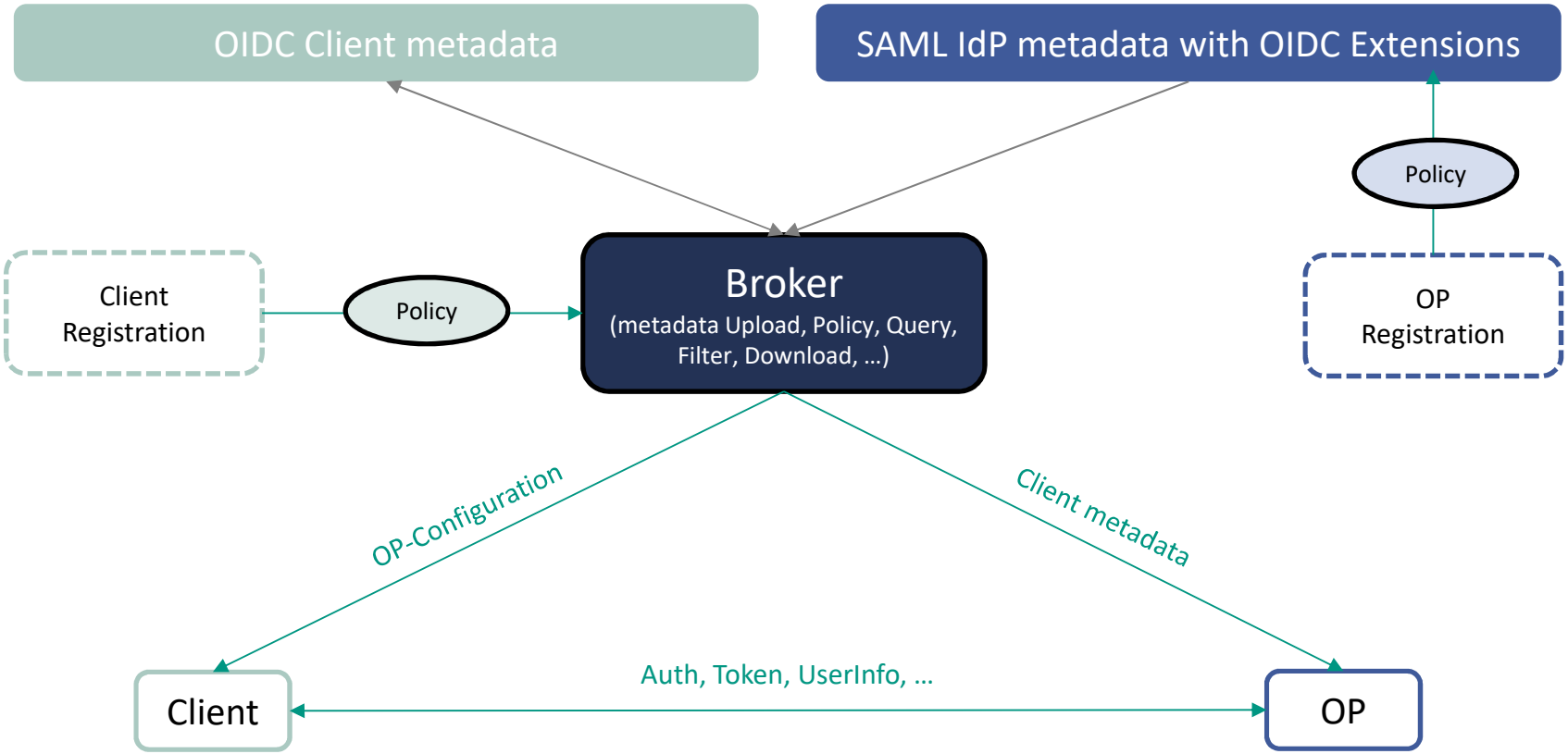
Technical Challenges

Skip?

- OIDC providers have to query client metadata (client federation) periodically and reconfigure themselves
  - No standards, manual effort
    - Register federated clients
    - Deregister clients which leaved the federation
  - Automation can be done for OIDC software Keycloak, for example
- OIDC clients have to query provider metadata periodically, present some kind of OP selection dialog to end users
  - Existing OIDC Client librarys lack of that
  - Could be integrated or put in front, but manual effort
- Same counts for pure OIDC RPs (JWT secured API), they must be able to accept all federated issuers and to verify their tokens



Central Brokering of Metadata



Policy Management

Established trust facilitates the provision of services

AARC Policy Development Kit

		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	

HIFIS Federation Access Policy (FAP)
- Requirements for IdPs to join (operational, responsibility, core attribute set, …)

Privacy Statement (Part of SAP)
- Purpose of data processing
- Whom to contact (data privacy officer, data processor)

HIFIS Service Access Policy (SAP)
- Service Requirement specifications (also in terms of entitlements for using the service)
- Acceptable Use Policy
- Service specific extension

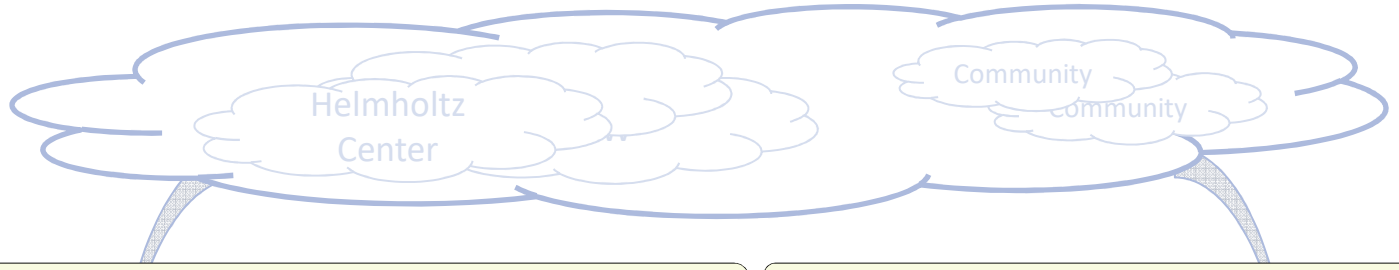
Quality of Identity Assurance (Part of FAP)
- DFN AAI Advanced, REFEDS Assurance Framework

Security Incident Response Procedure
- Security/CERT contact, software updates

Trust Model

How to connect services?

Concepts for Connecting Services



Identity federation driven

Based on existing organisational structure

- Trust based on federation membership
- Authorization by federation entitlements
- General purpose services

- e.g. Helmholtz, BW, NRW, DFN, ...
- Elements: home organisations

Community driven

Based on research topic

- Trust based on community membership
- Mainly individual authorisation
- Targeted group

- e.g. CMS, Plants, ...
- Elements: researchers

Service

- Requirements and responsibilities
- Choice of concept based on *effort driven assessment*

Effort driven model

Home Organisation
Large effort asserting community membership, no effort asserting user´s affiliation

Community
Large effort asserting user´s affiliation, no effort asserting community membership

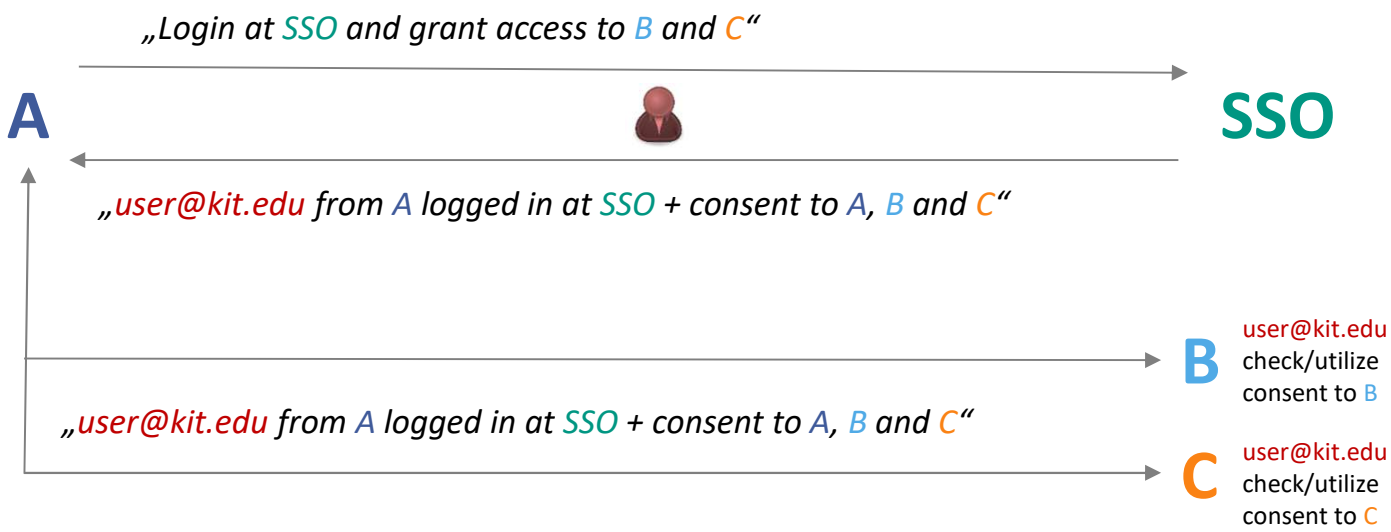
Questions & Discussion

Backup Slides

Application scenario with Delegation

Skip?

- **User** wants to use **Service A**
- **Service A** authenticates **User** at central **SingleSignOn**
- **Service A** also wants to integrate **Service B** and **Service C**



OpenID Connect / OAuth Basics

Skip?

Karlsruhe Institute of Technology

- OAuth
  - **API-Authorization** for desktop, web and mobile applications
  - Specifies basic protocol structures and roles
  - Concept of *Access* and *Refresh Tokens* for (web-)API authentication
- OpenID Connect
  - **Authentication layer** on top of OAuth
  - **SingleSignOn** with browser („Login with Google“) or API
  - Special *ID Token* to describe user identity and profile
  - **Interoperability** and **flexibility**
    - All tokens are specified as **JSON Web Tokens** (JWT)
    - Secure distributed authentication at (Web-)APIs, including service accounts
  - Simplified client development → **standalone** and **mobile clients**

Policies and their justification

- Scenario:
  - Federated identities
  - Federated services
  - Federated authorisation
- User X from Site A wants to access service at Site B
  - Potentially using authorisation information from Attribute Authority AA operated by another site for “PI”
- Site B: How can I be sure that
  - User X who Site A claims he is
    - Can I point the police to Site A to reveal his ID?
  - User X fulfills password policies (proper password, 2FA, ...)
  - User X is identified with a unique identifier (i.e. the same ID when he comes back)
  - What happens if that users credentials were compromised?
  - [...]
- Site A: How can I possibly ....
  - ... trust Site B with personal data?
- PI:
  - How can I be sure I authorise the correct user?
  - What do I need to to to manage my group members correctly?

Two different Answers

- 1: BW Federation Access Policy (FAP)
  - Focus on
    - Feasibility
    - Legality (inclusion of legal and privacy departments of KIT and State)
  - **Concrete policy, focused on deployability**
- 2: HDF Policy **(Prototype)**
  - AARC Policy Development Kit (PDK)
    - Focus on completeness (Complex, international, security)
    - Based on EGI, EUDAT, WLCG, ...
    - Takes into account GDPR
  - HDF Policy: Simplified, concrete implementation of PDK
  - **Complex Prototype, based on a universal approach**
- Both follow the same goals
  - **Comparison of FAP and HDF/PDK as a first Milestone in HIFIS**

Example for Assurance

Should identifiers be unique, personal and traceable?	Should identifiers be unique across the infrastructure?	How fresh do attributes need to be?	What kind of ID Proofing is required?	Is Multi-Factor Authentication required?
Unspecified	Unspecified	Unspecified	Unspecified	Unspecified
Yes	Yes	1 month	Low (self asserted)	Single factor authentication
			Medium (e.g. postal credential delivery)	Multifactor authentication
			High (e.g. face to face)	

AARC Assam
IGTF Dogwood
RAF Cappuccino
IGTF Birch
RAF Espresso

Concepts for Connecting Services

- Federated services have requirements
  - Legal requirements (contracts on usage)
  - Assurance levels (RAF / DFN-AAI-Advanced, e.g. passport checked, identifier quality)
  - Attributes
- Two concepts for connecting services

Identity federation driven
- Trust based on federation membership
- Coarse grained authorization by federation entitlements
- General purpose services

Community driven
- Trust based on bilateral agreement with community
- Mainly individual authorisation
- Targeted group

- Both concepts are necessary
- Both require defined trust model for membership
- Effort driven decision based on authoritative source of information