HELMHOLTZ

RESEARCH FOR
GRAND CHALLENGES

HIFIS | HELMHOLTZ FEDERATED IT SERVICES

Cloud Platform Access Layer Plus AAI intro from Backbone

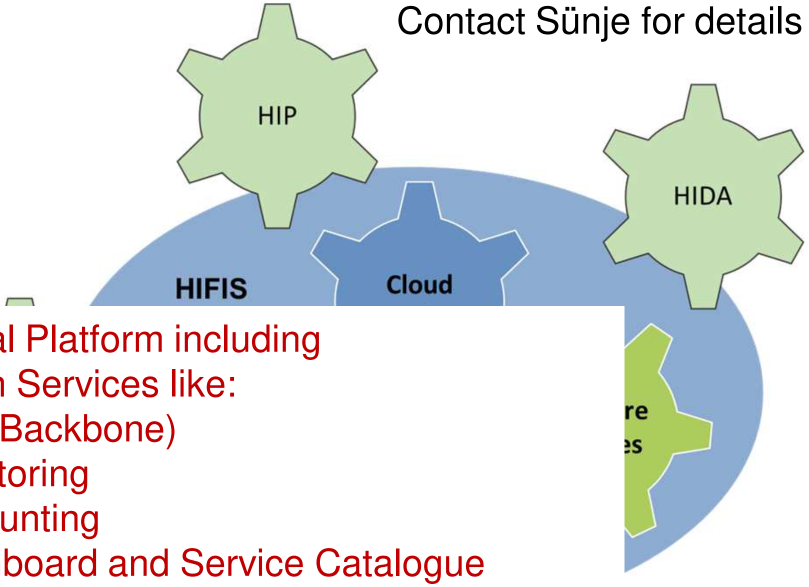
Patrick Fuhrmann, DESY
with contributions by Gergerly from EGI and Marcus from KIT

www.helmholtz.de

Reminder : The grant picture and my piece of it.

- **Cloud Services**
  Federated Platform, offering established first class Cloud-Services
- **Backbone Services**
  High performance secure Network Infrastructure with harmonized Core Services (e.g. Authentication)
- **Software Services**
  Platform, Training and Support for high quality and sustainable Software Development.

Contact Sünje for details



Technical Platform including Common Services like:

- AAI (Backbone)
- Monitoring
- Accounting
- Dashboard and Service Catalogue
- Services (Tender) vetting and registration
- And more ....

We are definitely not the first, building such a system ...

EGI,

EOSC,

GEANT,

SWITCH.CH

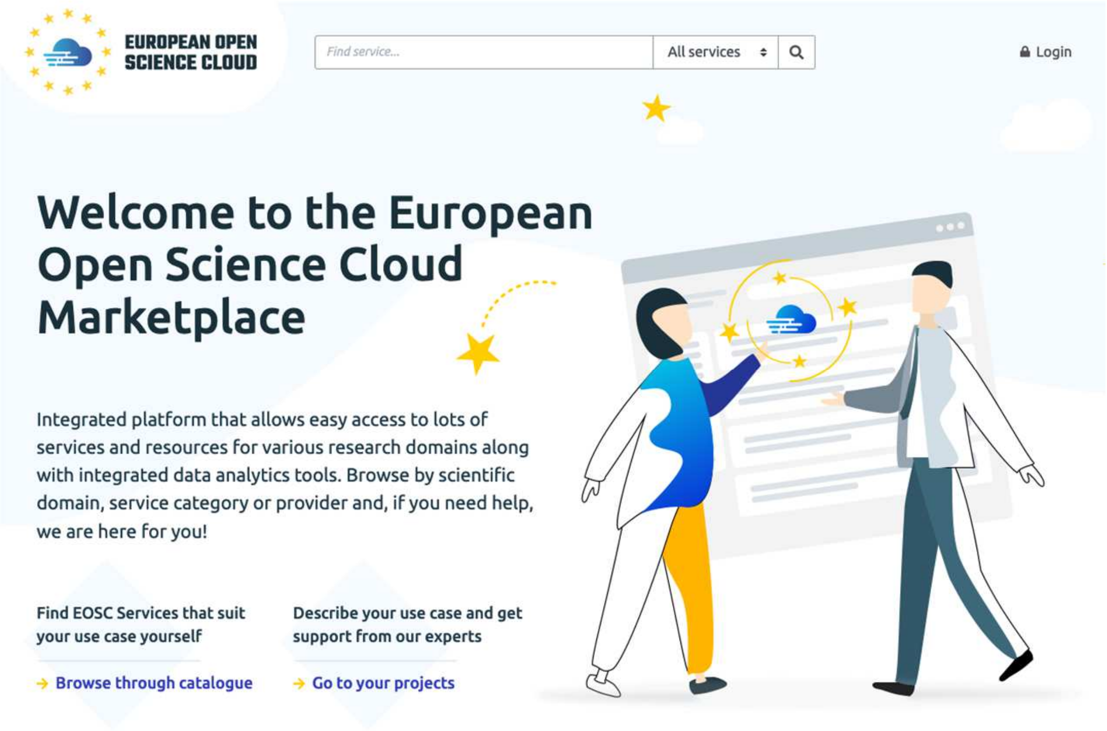
Portugal,

Fraunhofer,

....

Available role models for Marketplaces

Picking the EOSC marketplace as an example



EUROPEAN OPEN SCIENCE CLOUD

Find service...

All services

Login

Welcome to the European Open Science Cloud Marketplace

Integrated platform that allows easy access to lots of services and resources for various research domains along with integrated data analytics tools. Browse by scientific domain, service category or provider and, if you need help, we are here for you!

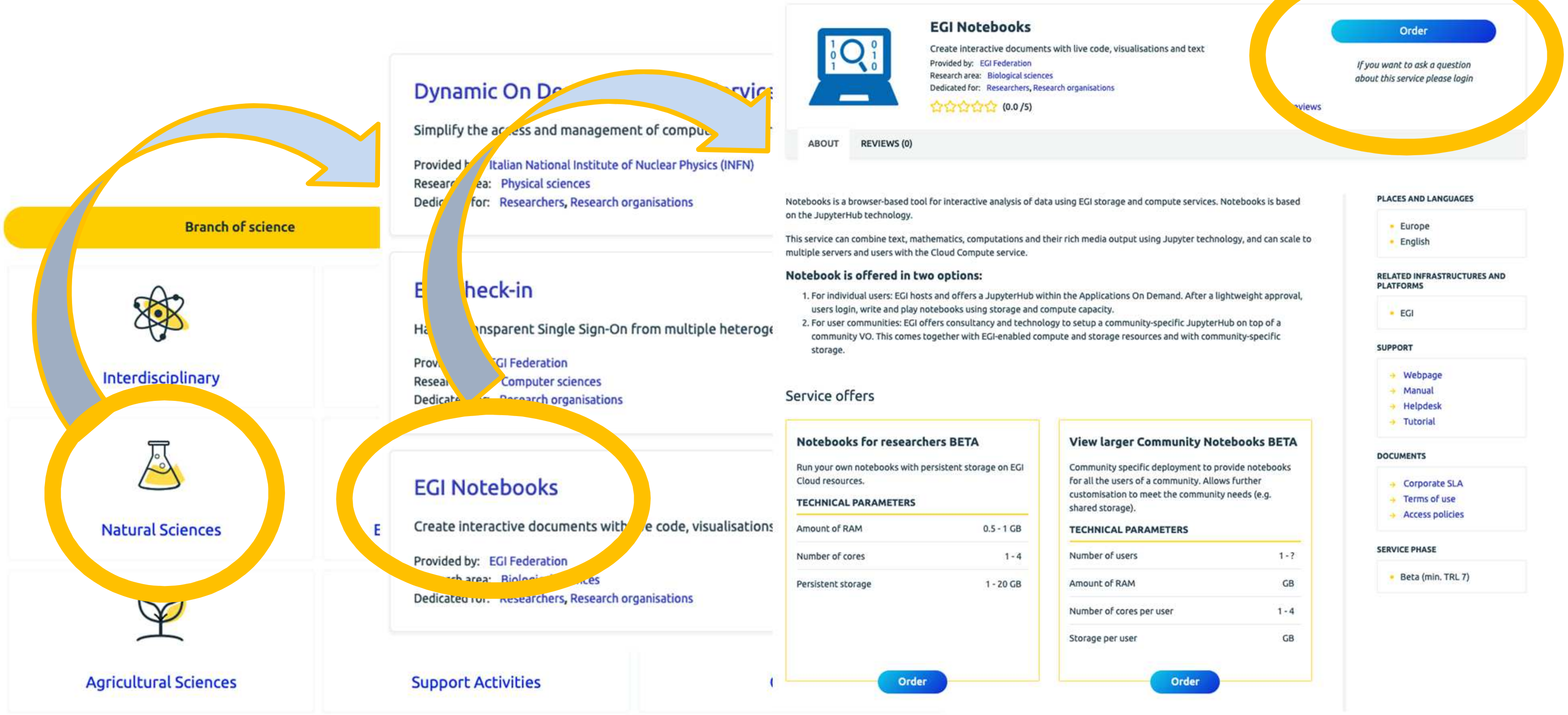
Find EOSC Services that suit your use case yourself

→ Browse through catalogue

Describe your use case and get support from our experts

→ Go to your projects

Available role models for Marketplaces



Dynamic On De… …rvic…

Simplify the ac…ess and management of compu…

Provided b… Italian National Institute of Nuclear Physics (INFN)
Resear… …ea: Physical sciences
Dedic… …for: Researchers, Research organisations

E… …heck-in

Ha… …nsparent Single Sign-On from multiple heteroge…

Prov… …GI Federation
Resea… Computer sciences
Dedicate… …esearch organisations

EGI Notebooks

Create interactive documents with… …e code, visualisations

Provided by: EGI Federation
…ch area: Biologi… …ces
Dedicated for: Researchers, Research organisations

EGI Notebooks

Create interactive documents with live code, visualisations and text

Provided by: EGI Federation
Research area: Biological sciences
Dedicated for: Researchers, Research organisations

☆☆☆☆☆ (0.0 /5)

If you want to ask a question about this service please login

Notebooks is a browser-based tool for interactive analysis of data using EGI storage and compute services. Notebooks is based on the JupyterHub technology.

This service can combine text, mathematics, computations and their rich media output using Jupyter technology, and can scale to multiple servers and users with the Cloud Compute service.

Notebook is offered in two options:

1. For individual users: EGI hosts and offers a JupyterHub within the Applications On Demand. After a lightweight approval, users login, write and play notebooks using storage and compute capacity.
2. For user communities: EGI offers consultancy and technology to setup a community-specific JupyterHub on top of a community VO. This comes together with EGI-enabled compute and storage resources and with community-specific storage.

Service offers

Notebooks for researchers BETA

Run your own notebooks with persistent storage on EGI Cloud resources.

TECHNICAL PARAMETERS	
Amount of RAM	0.5 - 1 GB
Number of cores	1 - 4
Persistent storage	1 - 20 GB

View larger Community Notebooks BETA

Community specific deployment to provide notebooks for all the users of a community. Allows further customisation to meet the community needs (e.g. shared storage).

TECHNICAL PARAMETERS	
Number of users	1 - ?
Amount of RAM	GB
Number of cores per user	1 - 4
Storage per user	GB

PLACES AND LANGUAGES
- Europe
- English

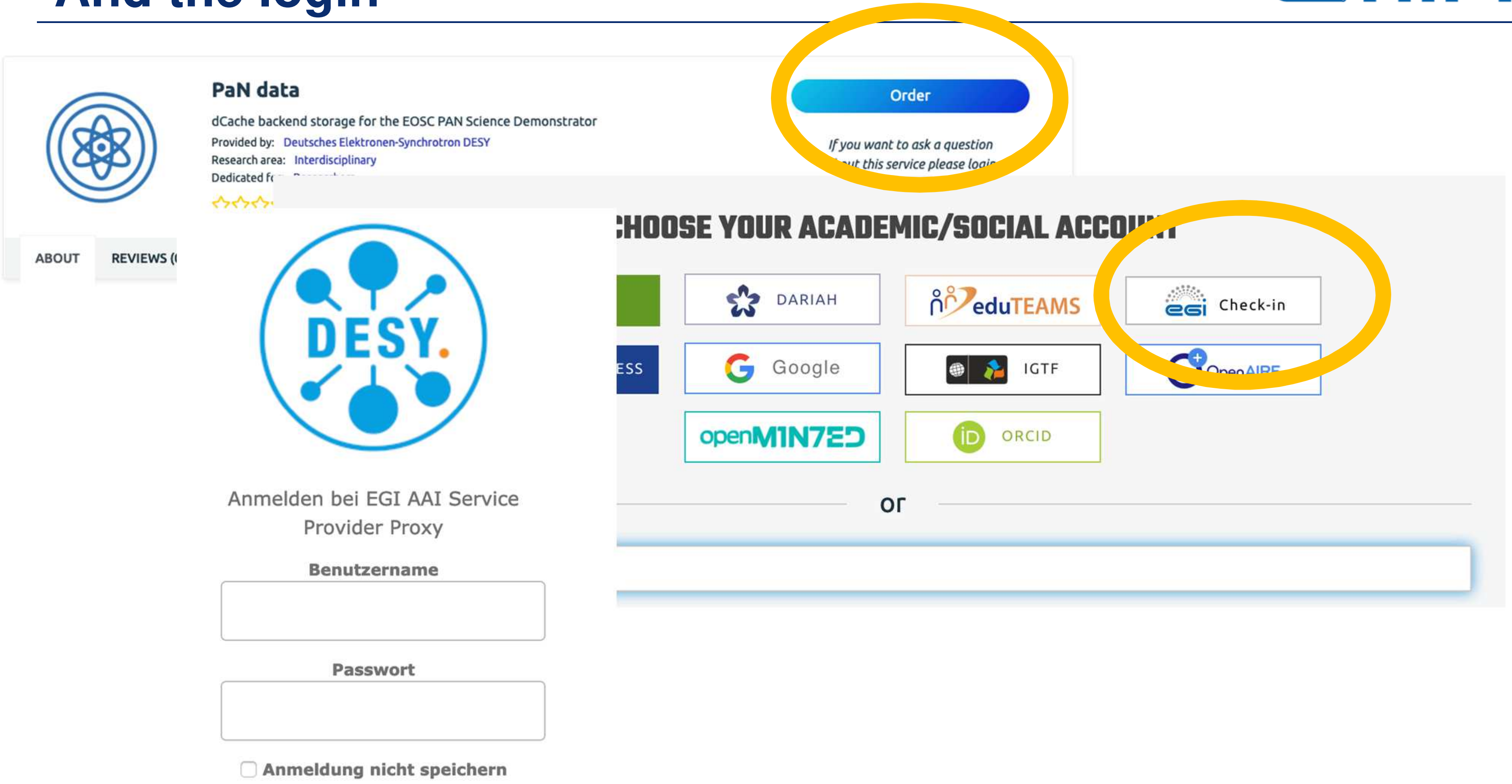
RELATED INFRASTRUCTURES AND PLATFORMS
- EGI

SUPPORT
- Webpage
- Manual
- Helpdesk
- Tutorial

DOCUMENTS
- Corporate SLA
- Terms of use
- Access policies

SERVICE PHASE
- Beta (min. TRL 7)

And the login



PaN data

dCache backend storage for the EOSC PAN Science Demonstrator

Provided by: Deutsches Elektronen-Synchrotron DESY

Research area: Interdisciplinary

Dedicated fo

If you want to ask a question
ut this service please logi

HOOSE YOUR ACADEMIC/SOCIAL ACCOU

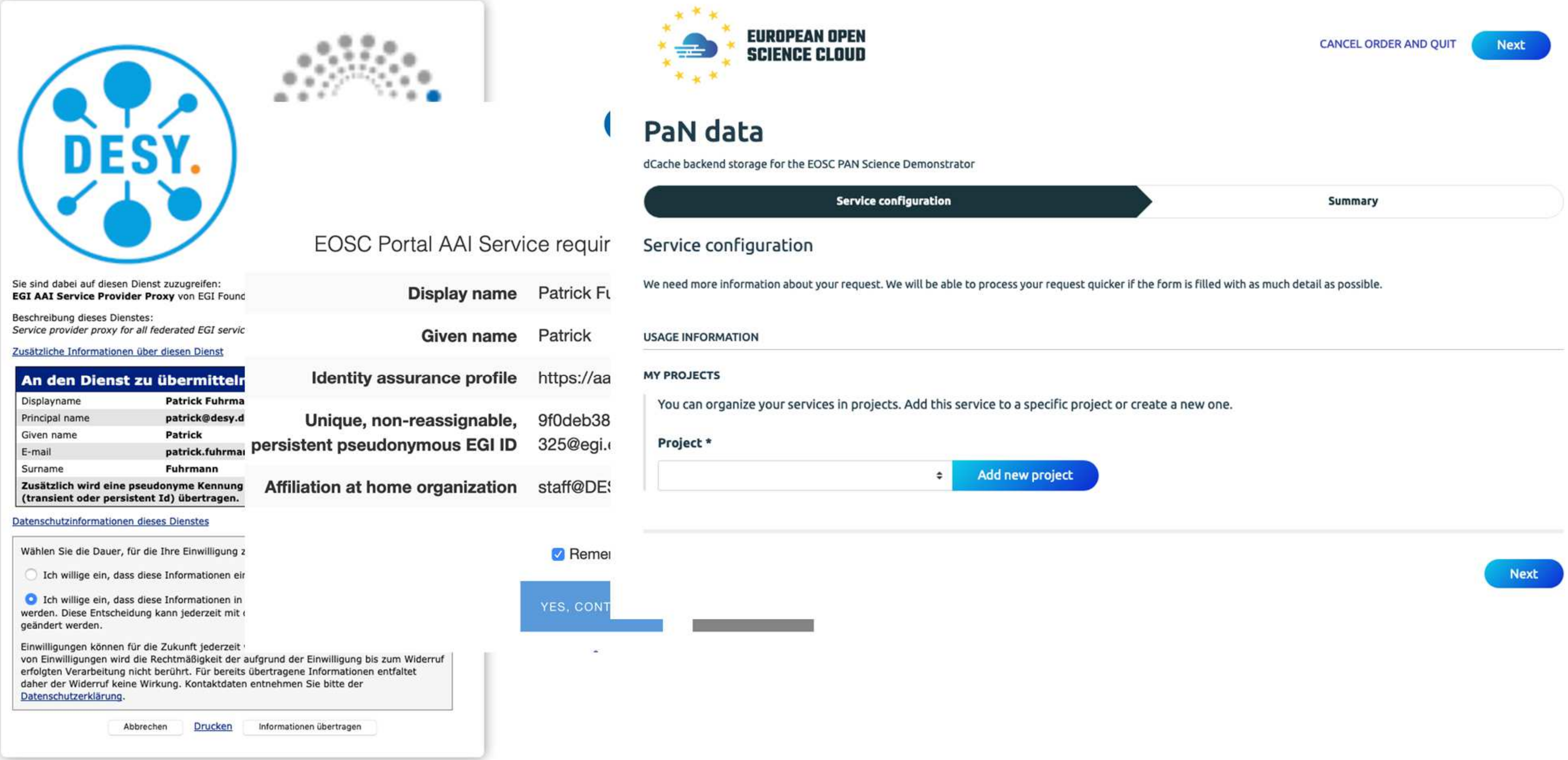
Anmelden bei EGI AAI Service Provider Proxy

Benutzername

Passwort

□ **Anmeldung nicht speichern**

And getting closer



Sie sind dabei auf diesen Dienst zuzugreifen:
EGI AAI Service Provider Proxy von EGI Found

Beschreibung dieses Dienstes:
Service provider proxy for all federated EGI servic

Zusätzliche Informationen über diesen Dienst

An den Dienst zu übermitteln	
Displayname	**Patrick Fuhrma**
Principal name	**patrick@desy.d**
Given name	**Patrick**
E-mail	**patrick.fuhrmai**
Surname	**Fuhrmann**
Zusätzlich wird eine pseudonyme Kennung (transient oder persistent Id) übertragen.	

Datenschutzinformationen dieses Dienstes

Wählen Sie die Dauer, für die Ihre Einwilligung z

○ Ich willige ein, dass diese Informationen eir

● Ich willige ein, dass diese Informationen in werden. Diese Entscheidung kann jederzeit mit geändert werden.

Einwilligungen können für die Zukunft jederzeit von Einwilligungen wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Für bereits übertragene Informationen entfaltet daher der Widerruf keine Wirkung. Kontaktdaten entnehmen Sie bitte der Datenschutzerklärung.

EOSC Portal AAI Service requir

Display name	Patrick Fu
Given name	Patrick
Identity assurance profile	https://aa
Unique, non-reassignable, persistent pseudonymous EGI ID	9f0deb38 325@egi.(
Affiliation at home organization	staff@DE!

☑ Remei

PaN data

dCache backend storage for the EOSC PAN Science Demonstrator

Service configuration

We need more information about your request. We will be able to process your request quicker if the form is filled with as much detail as possible.

USAGE INFORMATION

MY PROJECTS

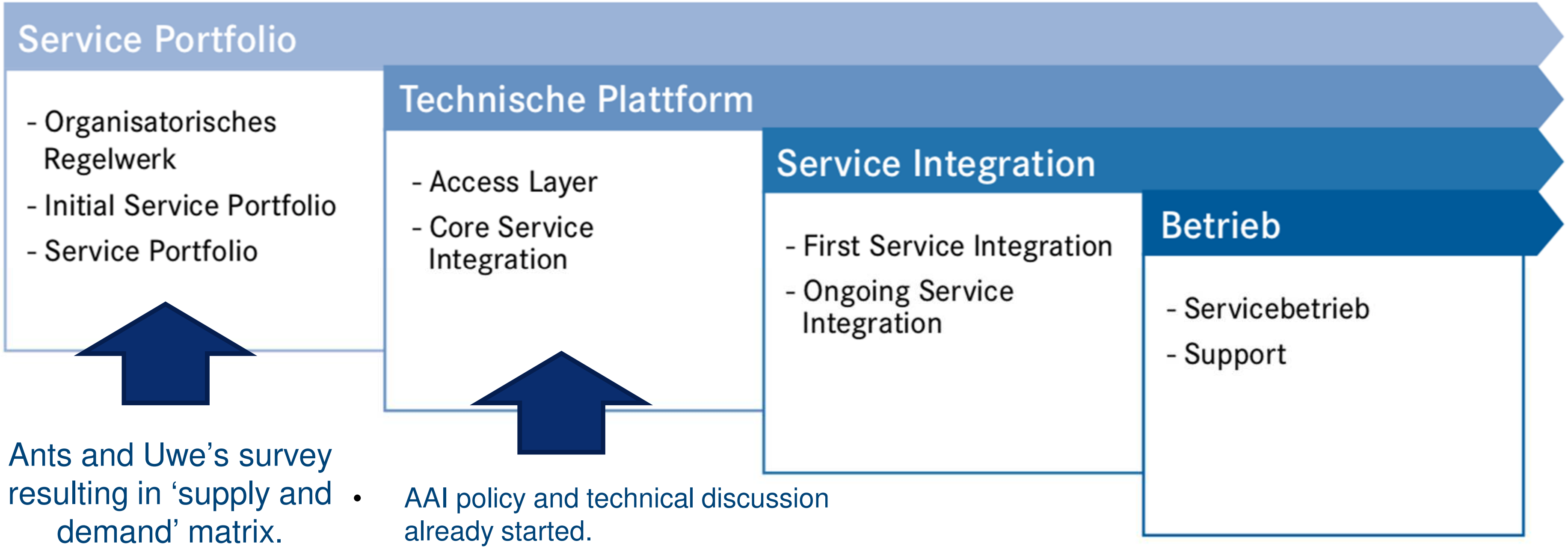
You can organize your services in projects. Add this service to a specific project or create a new one.

Project *

Now moving to the implementation ...

Logical Timeline

Portfolio, Platform, Integration and Operation



Service Portfolio

- Organisatorisches Regelwerk
- Initial Service Portfolio
- Service Portfolio

Technische Plattform

- Access Layer
- Core Service Integration

Service Integration

- First Service Integration
- Ongoing Service Integration

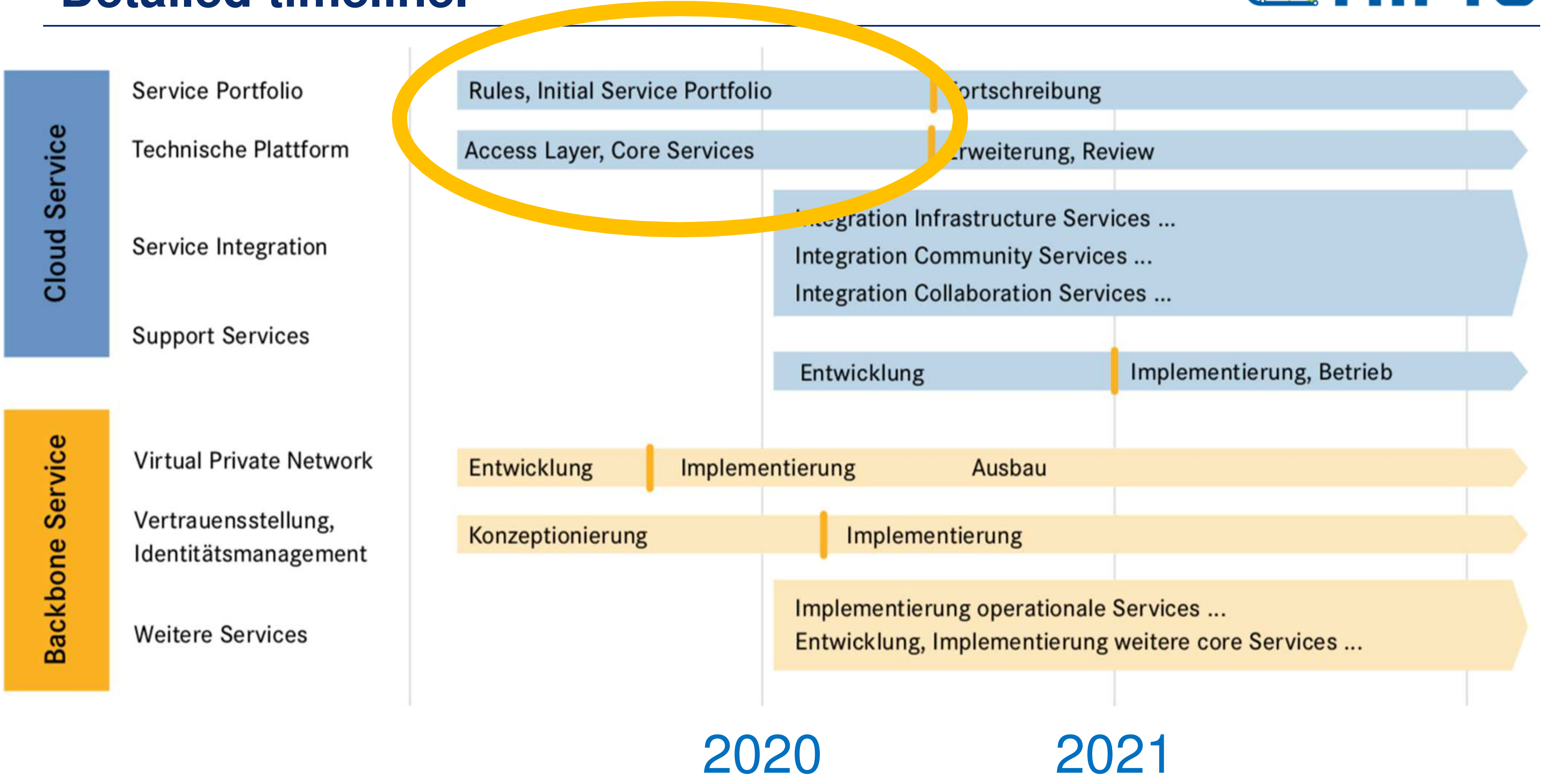
Betrieb

- Servicebetrieb
- Support

Ants and Uwe's survey resulting in 'supply and demand' matrix.

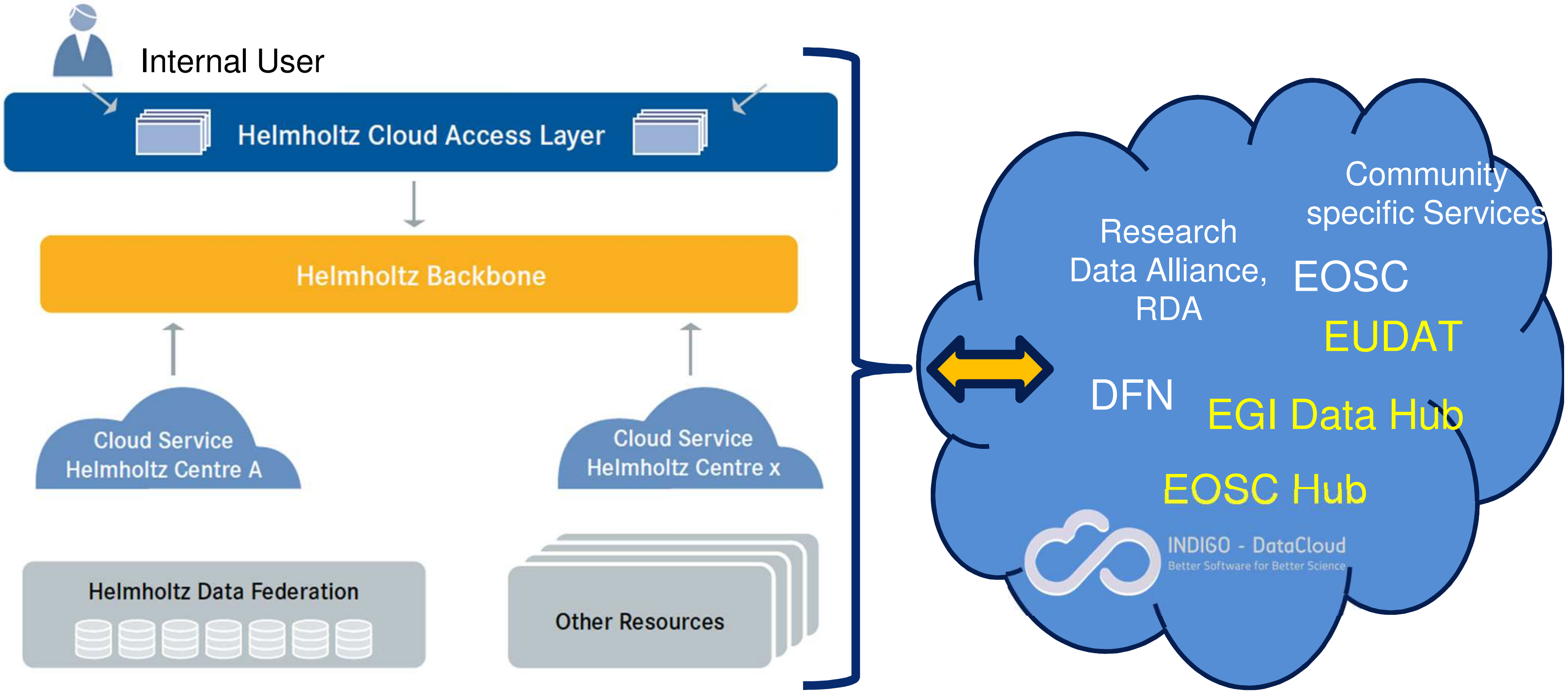
- AAI policy and technical discussion already started.
- Meeting with EGI on EOSC and EGI marketplace as a role model.
- Lead hired for Feb 1, 2019

Detailed timeline.



Cloud Service
Service Portfolio
Technische Plattform
Service Integration
Support Services
Backbone Service
Virtual Private Network
Vertrauensstellung, Identitätsmanagement
Weitere Services
Rules, Initial Service Portfolio
ortschreibung
Access Layer, Core Services
rweiterung, Review
...egration Infrastructure Services ...
Integration Community Services ...
Integration Collaboration Services ...
Entwicklung
Implementierung, Betrieb
Entwicklung
Implementierung
Ausbau
Konzeptionierung
Implementierung
Implementierung operationale Services ...
Entwicklung, Implementierung weitere core Services ...
2020
2021

Architecture, taken from the proposal.



Internal User

Helmholtz Cloud Access Layer

Helmholtz Backbone

Cloud Service Helmholtz Centre A

Cloud Service Helmholtz Centre x

Helmholtz Data Federation

Other Resources

Community specific Services

Research Data Alliance, RDA

EOSC

EUDAT

DFN

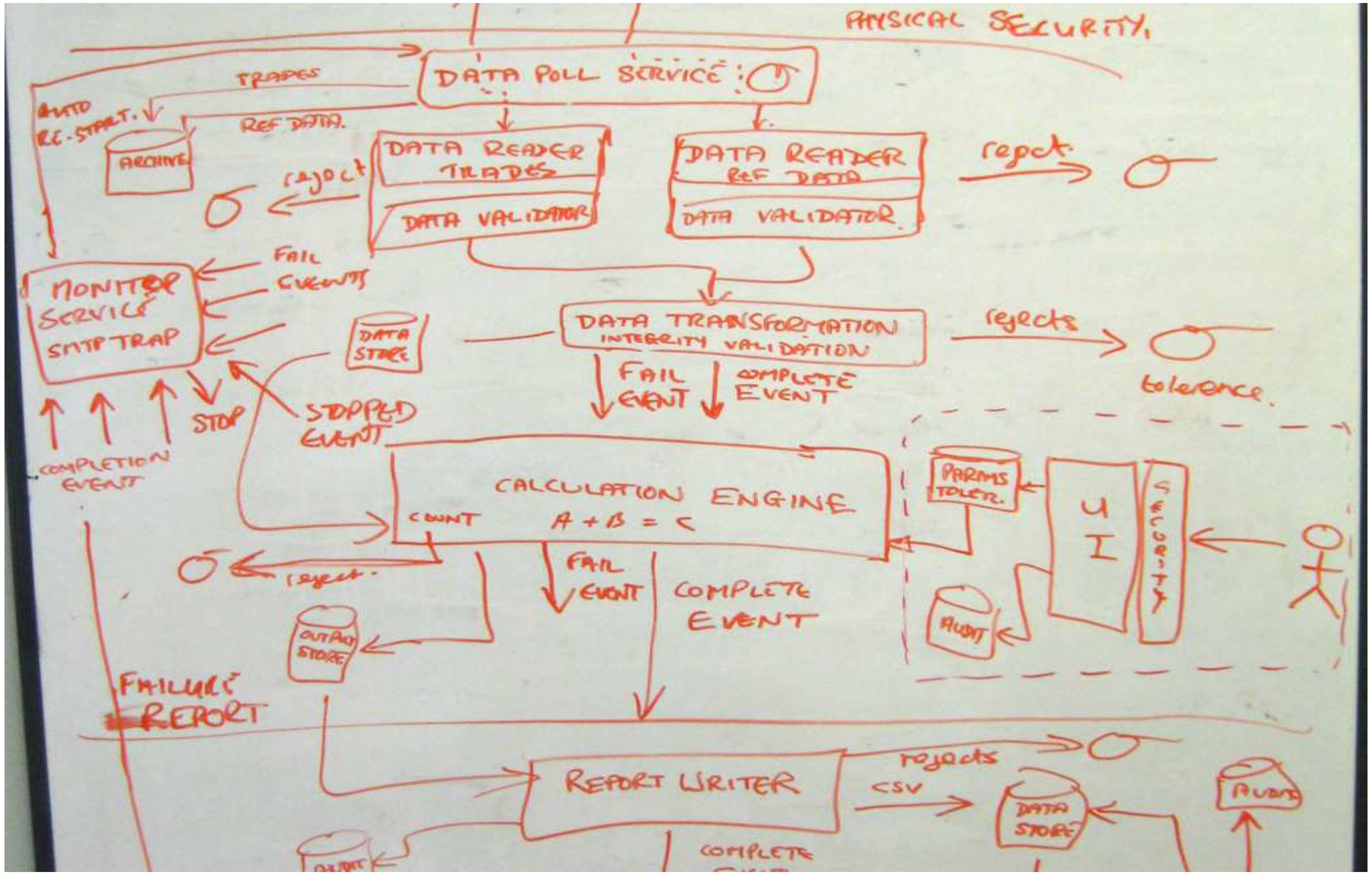
EGI Data Hub

EOSC Hub

INDIGO - DataCloud

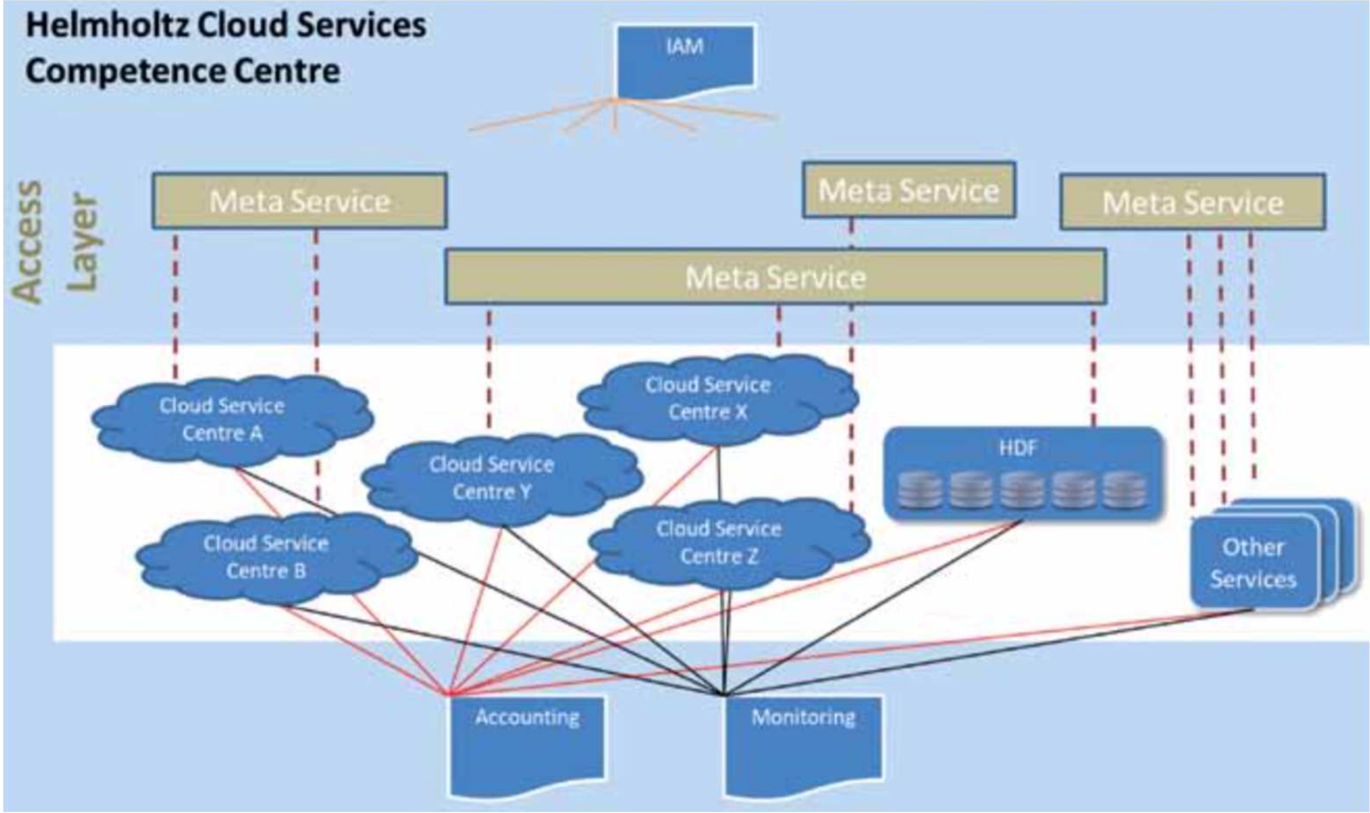
Better Software for Better Science

And now the first attempt of an architecture



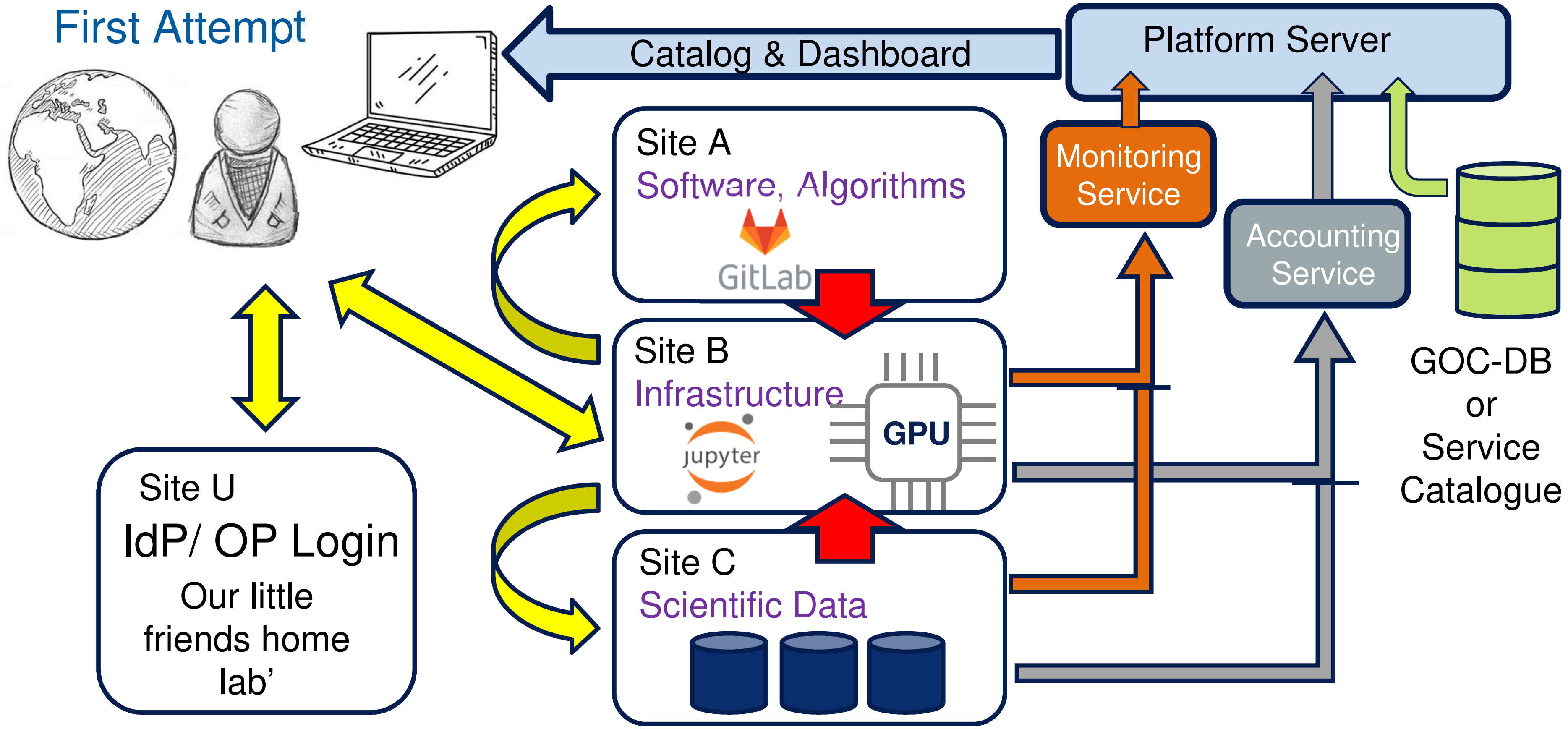
Composed Service Offerings

From Proposal Document



Simple Architecture Proposal

First Attempt



Catalog & Dashboard

Platform Server

Site A
Software, Algorithms

Site B
Infrastructure

Site C
Scientific Data

Monitoring Service

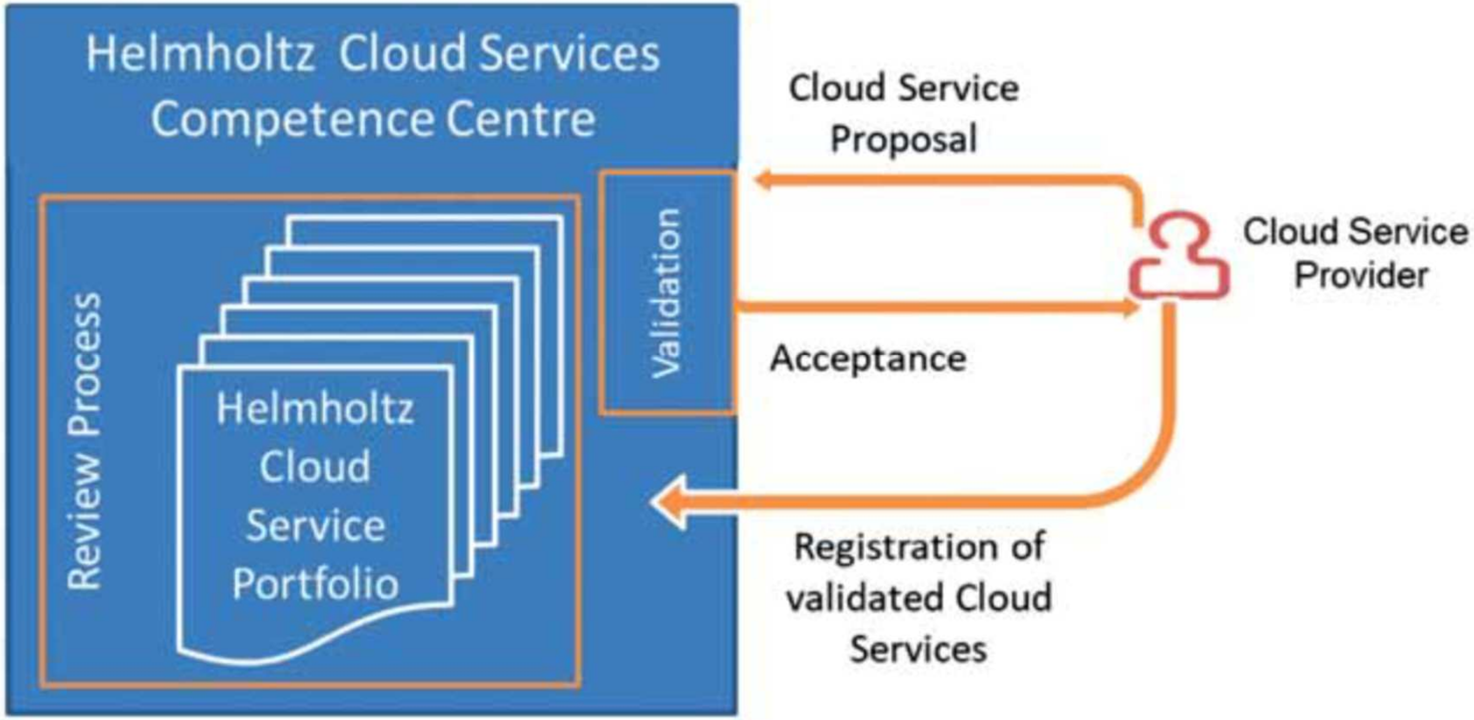
Accounting Service

GOC-DB or Service Catalogue

Site U
IdP/ OP Login
Our little friends home lab'

Validation and registration process

Validation and registration process


Helmholtz Cloud Services Competence Centre
Review Process
Helmholtz Cloud Service Portfolio
Validation
Cloud Service Proposal
Cloud Service Provider
Acceptance
Registration of validated Cloud Services

Validation and registration process

Multi Step Process

- Initially this will be handled manually
- However, in a second step we envision an automated two step process (similarly to EGI)
  - A, Simple online registration card, briefly describing the service and the target user.
  - B, The request will be evaluated by the appropriate (Cloud Service Competence Center)
  - C, On approval a detailed registration form will have to be filled in, including
    - Service Level Agreement
    - Legal restriction on the target audience
    - Level of integration (predefined levels)
  - D, This information, will be added to the service catalogue.
- Compensation will be handled at a different level.

Now for something completely different ...

AAI, which is actually part of Backbone.

Please refer to the
talks by our
Colleagues from
KIT

Requirements for the common AAI service

Thanks to Dr. Millar for helping out with this.

- Must work and must be simple
- Should work with professional (industry standard) software.
- Must work with my UNI and Lab identity provider system.
- Support of common authentication mechanisms
  - Open ID Connect
  - SAML (as UNIs and Labs)
  - Legacy X509/Proxies for user authentication and services.
    - Mostly from WLCG / HEP world
- Transparent translation service, including delegation.
- Group management services independently from Authentication service
- Authorization based on individual and group membership
  - Banning of users (on the global and site level)
- Waterproofed (legally approved) and realistic policy infrastructure
  - Including NON HGF services and identities.

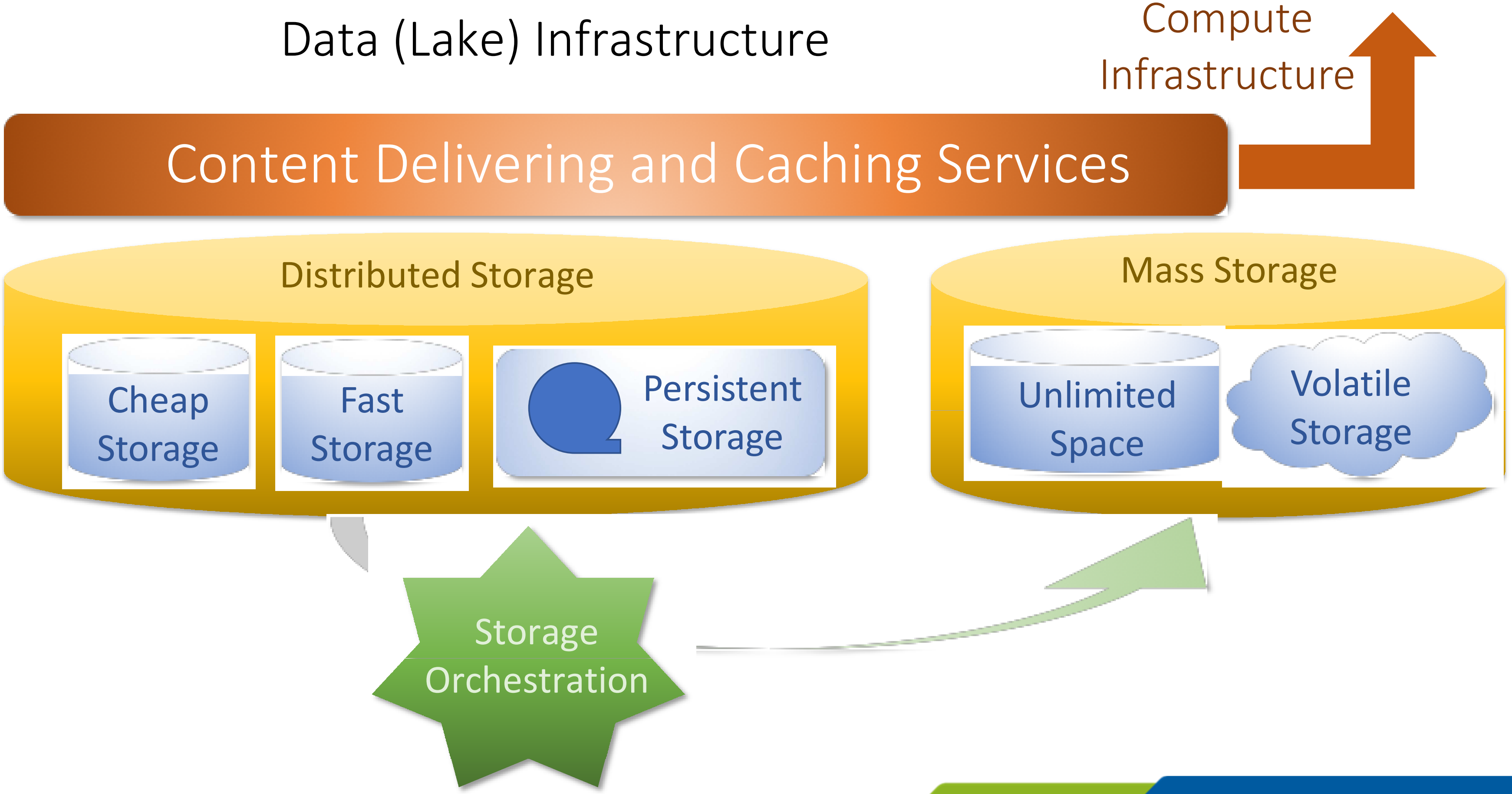
What do we need AAI Policies for ?

- Site B: How can I be sure that User X is really ....
  - ... who Site A claims he is
  - can I point the policy to Site A to reveal his ID?
  - ... authenticated with secure mechanism (proper password, 2FA, ...)
  - ... identified with a unique identifier (i.e. the same ID when he comes back)
  - ... identifier is not reassigned
  - ... not able to authenticate after his account at Site A expired?
  - What happens if that users credentials were stolen?
  - Whom do I contact in case of fire?
  - What to do with personal data?
  - What relation do I have with PI?
- Site A: How can I possibly ....
  - ... trust Site B with personal data?
  - ... be informed of security breaches that involve personal data of my user?
  - ... are there requirements regarding authentication strength (2FA, see above)
- PI:
  - How can I be sure I authorize the correct user?
  - What do I need to to to manage my group members correctly?

Stolen from Marcus

The END

Data (Lake) Infrastructure


Compute
Infrastructure
Content Delivering and Caching Services
Distributed Storage
Cheap Storage
Fast Storage
Persistent Storage
Mass Storage
Unlimited Space
Volatile Storage
Storage Orchestration