LSDMA

What we want from this meeting

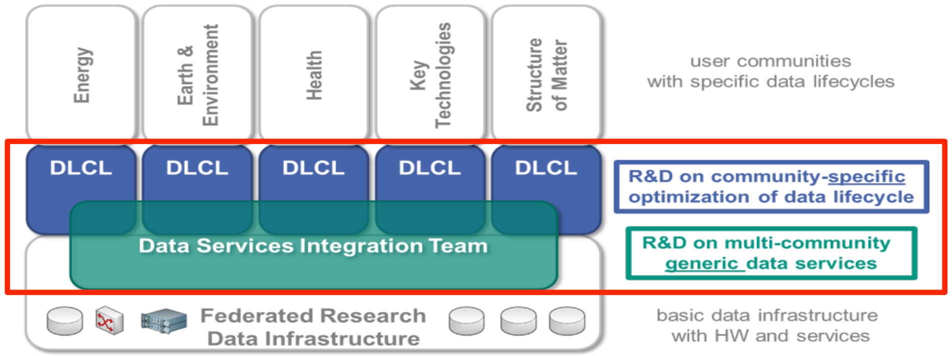
- We (LSDMA (Desy + KIT)) need
  - credential translation to
    - make german scientists more productive
    - maximise the output of german laboratories and scientific communities
- Why DFN?
  - HGF centres don't have the mandate
- Convince you (DFN-CERT) to extend the current SLCS service
  - Add support for non-web access (ECP)
  - Add support for delegated SAML-assertions
- Researchers cannot use distributed computing infrastructres available
  - Huge resources require X.509 vs. lots of scientists only having home-IdP
- We need to agree on how to proceed
  - Arsen & Paul are ready and motivated to develop and collaborate
  - Happy to tighten the communication in the collaboration
- Are you willing to support our requirements to the SLCS service?

LSDMA

- Helmholtz Portfolio Extension
  - HGF Partner: Desy, GSI, FZJ, KIT, DKRZ
  - Uni Partner: TUD, HTWB, UniHH, UniUlm, UniHD, UniDa
- LSDMA is not a project, it’s a programme
  - We are a long term institution

Structure and goals of LSDMA

- Data Life Cycle Labs
  - **Common R&D together with communties**
    - Optimisation of Data Life Cycle
    - Specific Analysis tools and services
- Data Services Integration Team
  - **Generic, Cross Community R&D**
    - Interface between federated infrastructures and DLCLs
    - Integration of services into the scientific workflows



Energy

Earth & Environment

Health

Key Technologies

Structure of Matter

user communities with specific data lifecycles

DLCL DLCL DLCL DLCL DLCL

R&D on community-specific optimization of data lifecycle

Data Services Integration Team

R&D on multi-community generic data services

Federated Research Data Infrastructure

basic data infrastructure with HW and services

DLCLs+DSIT:
Content and unique feature of LSDMA

Datalabs in LSDMA

- Key Technologies (Uni-HD + KIT)
  - Image analysis e.g. for ANKA Beamlines
- Energy (KIT)
  - Big data tools for predicting power outages
- Earth and Environment, Climate (KIT)
  - Geospatial queries on satellite data
- HumanBrain (FZJ)
  - Brain Connectome from microscoped brain slices
  - Unicore Workflows
- Structure of Matter (Desy)
  - HEP
  - XFEL

Using distributed computing infrastructures

- X.509 Access required for Storage and Compute
  - Majority of HTC storage and computing resources only accessible via X.509
- No problem for
  - WLCG
  - Climate pleople
- Problem for the long tail science
  - EGI
    - FedCloud
    - Science Gateway
  - ANKA / Synchrotron community
  - bwArchiv project
  - CFEL
  - XFEL

AAI work in LSDMA

- Expose only SAML to the users
  - Migrate away from X.509 where possible
  - Provide token translation services where reasonable
  - e.g. saml-grid-proxy-init
- Extend SAML support to non-web and non-SAML services
- Provide web portal for global group management

Sharing experience of our initial ECP service

- ECP configuration became simpler in shibboleth after 2.5
- Complex only on client side
  - https requests, PAOS, xml parsing, ...
  - Clients available for bash, perl, python
- SP configuration only requires this addition in shibboleth.xml

```
<SSO
+++ type=“SAML2” Location=“/ECP” ECP=“true”
--- EntityID=“https://idp.example.org”
></SSO>
```

- Example implemented for
  - https://saml-delegation.data.kit.edu
    - Web-SSO endpoint
    - ECP endpoint
  - Returns a SAML assertion to the user
  - Publishes encrypted SAML assertion and returns the URL

Arsen’s experience with GridShibCA and Shibboleth SP

- Software:
  - GridShib CA version 2
  - Shibboleth SP version 2.5
  - IdPs used: KIT production IdP, KIT test IdP
  - ECP client: ecp.pl from CILogon

- ECP configuration for SP works correctly
  - SAML assertion issued, authN works, access to gridshibca cert-req script granted
  - gridshibca cert-req script does not work
    - can’t find the shibboleth authN session file, asks for re-authentication

Conclusion

- LSDMA represents a large number of scientists
- To access resources they need SLCS to support
  - ECP (non-web)
  - Portals
- We are ready to collaborate
- Are you willing to support these extensions to the SLCS service?

EMI Security Token Service (STS)

- From: Henri Mikkonen henri.mikkonen@nimbleidm.com
- STS currently supports one profile of the **CMP** protocol (interoperability tested with software called **EJBCA**). There's also a **PoC** implementation for using SOAP-interface to an online CA running at CERN.
- Just FYI, I made the SOAP interface implementation for the CERN CA in less than one week.