Building a Data Transfer Federation

NFDI4Ing Conference – Mozhdeh Farhadi*, Serge Sushkov*, Andreas Petzold*

* SCC / KIT

www.kit.edu

Motivation

- The expanding cross-site collaboration among research centers fuels the demand for access to storage systems of various organizations.

- Research centers collaboration results in the need for large data transfers between different storage systems.

- They require:

  - User-friendly way to access data → **WebDAV**

  - Authentication for accessing their data in any storage system → **Federated AAI**

  - Possibility to transfer huge amount of data between systems, e.g: data archiving, transfer to compute site → **FTS3 (File Transfer Service)**

- Context: NFDI4Ing and bwHPC-S5

Large Scale Data Facility: Online Storage (LSDF OS)

- Storage system for hot/warm research data

- 12 PiB in use, 22 PiB capacity

- Available to KIT members and collaborators

- File system Software: GPFS (IBM Spectrum Scale)

- Multi-Protocol Access: SSH/SFTP, NFS, SMB, **WebDAV**

- Also mounted on HPC systems at KIT

WebDAV Protocol

- Web Distributed Authoring and Versioning is a HTTP-based *data access protocol.*

- Enables users to share, copy, move and edit files through a web server.

- Suitable also as a *data transfer protocol* → copy data into/from/between storage systems

- Apache HTTPD as the battle-tested basis for our endpoint server
  - Enhanced with community and self-developed "modules" for specific functionality

- Currently deployed endpoints
  - Production: LSDF OS (os-webdav.lsdf.kit.edu) and (os-webdav-oauth2.lsdf.kit.edu)
  - Testing: HPC at SCC, SDS@HD

HTTPD WebDAV Software

- Components: Apache HTTPD Server + Custom Modules

- Published alongside "reference configuration"

- Available for Docker and RHEL

- https://codebase.helmholtz.cloud/kit-scc-sdm/onlinestorage/httpd-webdav

Request Authentication via Basic Auth

- User prompted for username & password on access through Basic Auth
  - Universal support in clients
  - E.g. Browser, mounting clients in Windows/MacOS/Linux

- Validation via LDAP
  - Delegated to local infrastructure proxy (RegApp's LDAP Facade)
  - Users for some institutions have "password forwarding" to their home organization.
  - Others set a service password

Request Authentication via OAuth2

- Beyond username & password: Authentication via OAuth2 tokens
  - Short-lived tokens are issued by trusted provider
    - Provider is local infrastructure proxy (RegApp)
  - Token represents Authn & Authz for user and a set of actions (e.g. WebDAV access)
    - Responsibility for Authn & Authz logic moved to provider
  - Suitable for delegation to tools and services

- JWT tokens: self-contained, JSON payload
  - Validated locally via signature in token and provider's public key
  - May contain arbitrary claims about user
  - Must negotiate content of token, how to check it with provider admins

28.09.2023   Mozhdeh Farhadi – Building a Data Transfer Federation   Steinbuch Centre for Computing

File Transfer Service: FTS3

- FTS3 is a low-level data management service, responsible for scheduling reliable bulk transfer of files from one site to another.

- It distributes the majority of the Large Hadron Collider data at CERN across the Worldwide LHC Computing Grid (WLCG) infrastructure.

- Why FTS3:

  · Simplicity for the end users.

  · Reliability by ensuring data integrity with checksum comparison and the retrial of failed transfers.

Projects Using FTS

- ## 8 WLCG Instances
  - BNL, CERN (4), FNAL, RAL, MIT

- ## 16 non-WLCG Instances
  - CERN (DAQ, Public), RAL, KEK(2), Imperial (also used by CMS), PIC, MWT2, CESNET (WebFTS + RCAuth), JINR, CNAF, SARA, SLAC, IHEP, Fermilab (containers), FENIX Research Infrastructure (Human Brain Project)

FTS Features

- Cross-protocol

  · GridFTP, XRootD, SRM and HTTP (WebDAV, S3)

- Third Party Copy (TPC): Passing data directly between source and destination, bypassing the client

- OAuth2 and X.509 support

- User's tools:

 · Command line interface

  · REST API

Third Party Copy (TPC)

- Instead of streaming data through the FTS, storage systems directly transfer files between themselves.

- Expected to be more performant compared to streaming.

- Enabled by GFAL2 libraries.

-FTS only communicates with the active storage (A).
-FTS provides URL for Storage B and authz. token.

FTS3

Request: Send file 1 to URL on storage B.

Storage A

GET/ PUT

Storage B
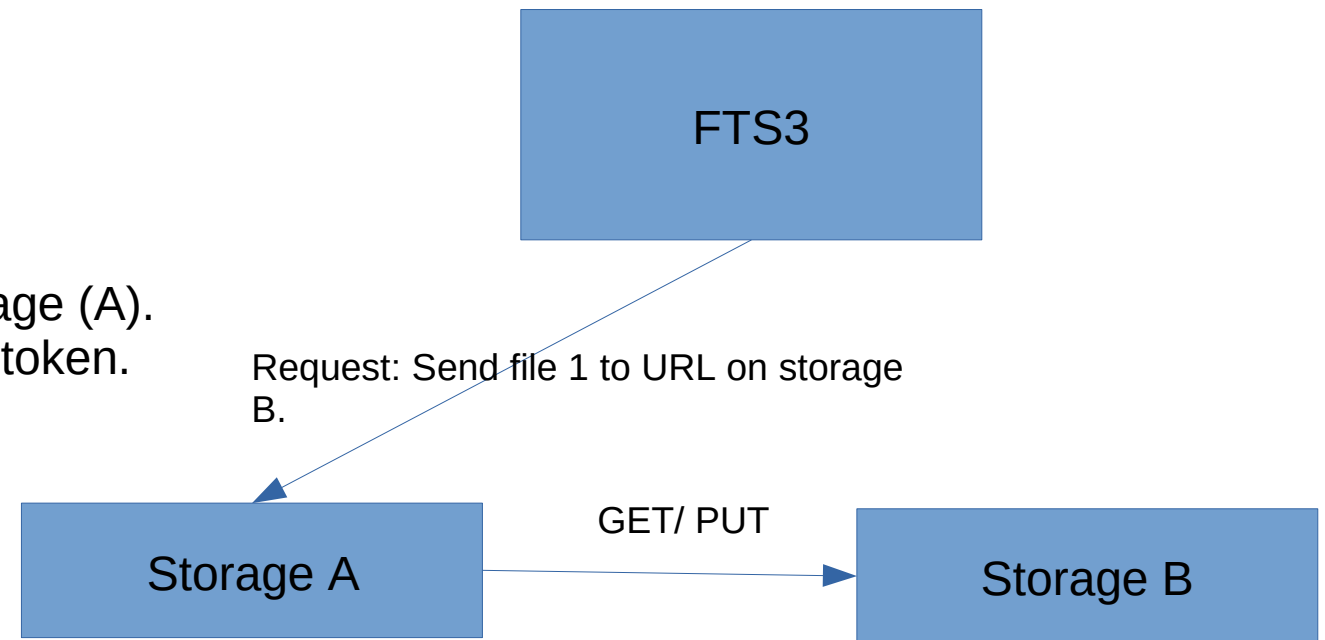
Data Transfer Federation
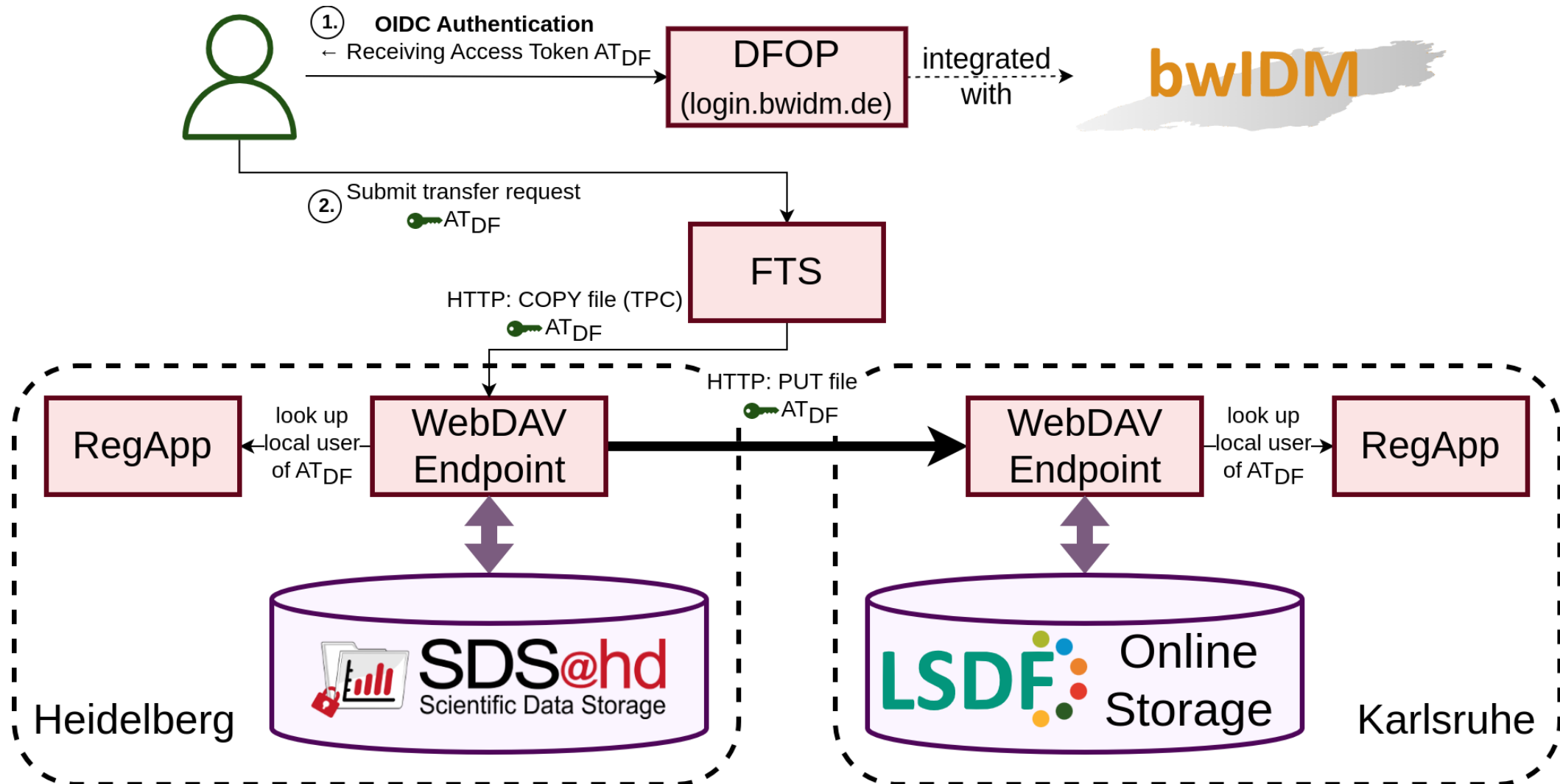
Conclusion

- At SCC we are building a data transfer federation by employing different technologies and services.

- At SCC we are able to transfer files between different WebDAV endpoints using OAuth2 tokens.

- Testing prototypical implementation of file transfer between KIT and external sites.

Thank you
Questions?