Karlsruher Institut für Technologie

Building a Data Transfer Federation

NHR Data Management Workshop 14.06.23 – Mozhdeh Farhadi, Paul Skopnik

Motivation

- The expanding cross-site collaboration among research centers fuels the demand for access to storage systems from 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 → **FTS**
- Context: bwHPC-S5 and NFDI4Ing

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
- Software: GPFS (IBM Spectrum Scale)
- Multi-Protocol Access: SSH/SFTP, NFS, SMB, **WebDAV**
  - Also mounted on HPC systems at KIT

HPC systems at KIT: HoreKa and bwUniCluster

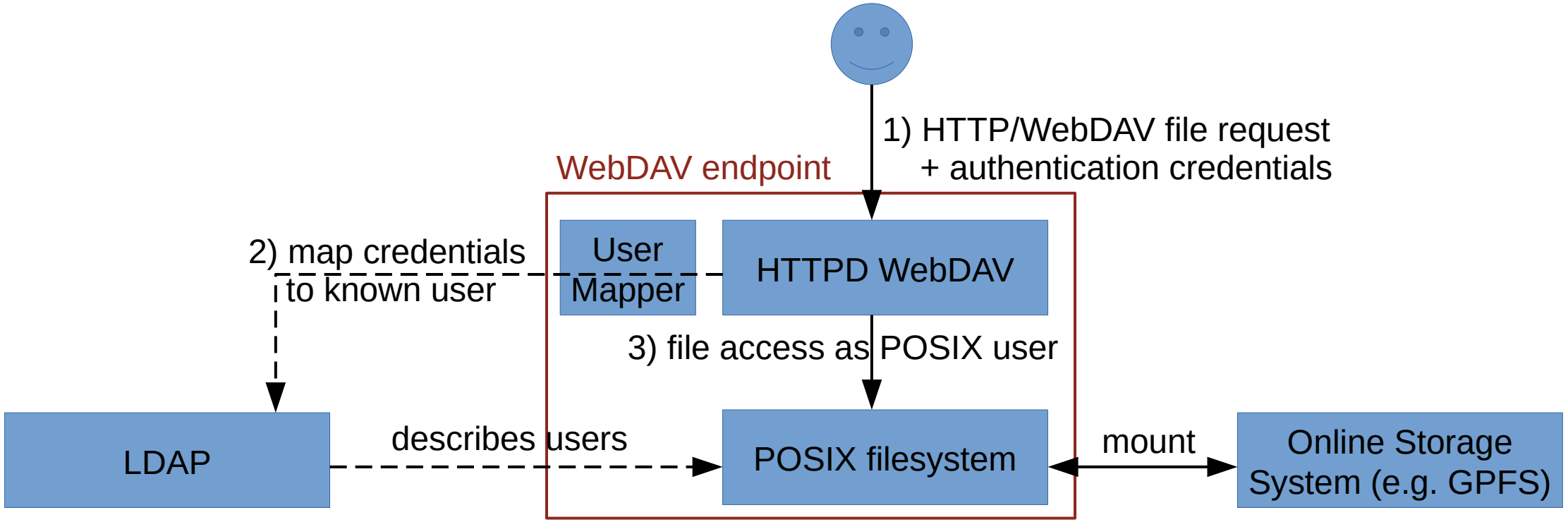
- Horeka
  - Two parallel Spectrum Scale file systems with a total capacity of more than 15 petabytes are used for data storage.
  - HoreKa is also connected to the SCC's LSDF with a data rate of up to 45 GB/s.
  - The system is available to scientists from all over Germany.
- BwUniCluster
  - Total memory expansion of approx. 5 petabytes.
  - Serves the universities of the state of Baden-Württemberg

WebDAV Protocol

- WebDAV as an HTTP-based *data access protocol*
- 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
  - Augmented with community and self-developed “modules” for specific functionality
- Currently deployed endpoints
  - Production: LSDF OS (os-webdav.lsdf.kit.edu)
  - Testing: HPC at SCC, SDS@HD

HTTPD WebDAV on Existing Filesystems

- HTTPD WebDAV software is deployed on top of POSIX filesystems
- Authentication via Basic Auth (LDAP) or OAuth2 token



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 org
  - 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

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

File Transfer Service (FTS)

- FTS 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 (LHC) data across the Worldwide LHC Computing Grid (WLCG) infrastructure.

- Why FTS:
  - Simplicity for the end users.
  - Reliability by ensuring data integrity with checksum comparison and the retrial of failed transfers.

Projects Using FTS

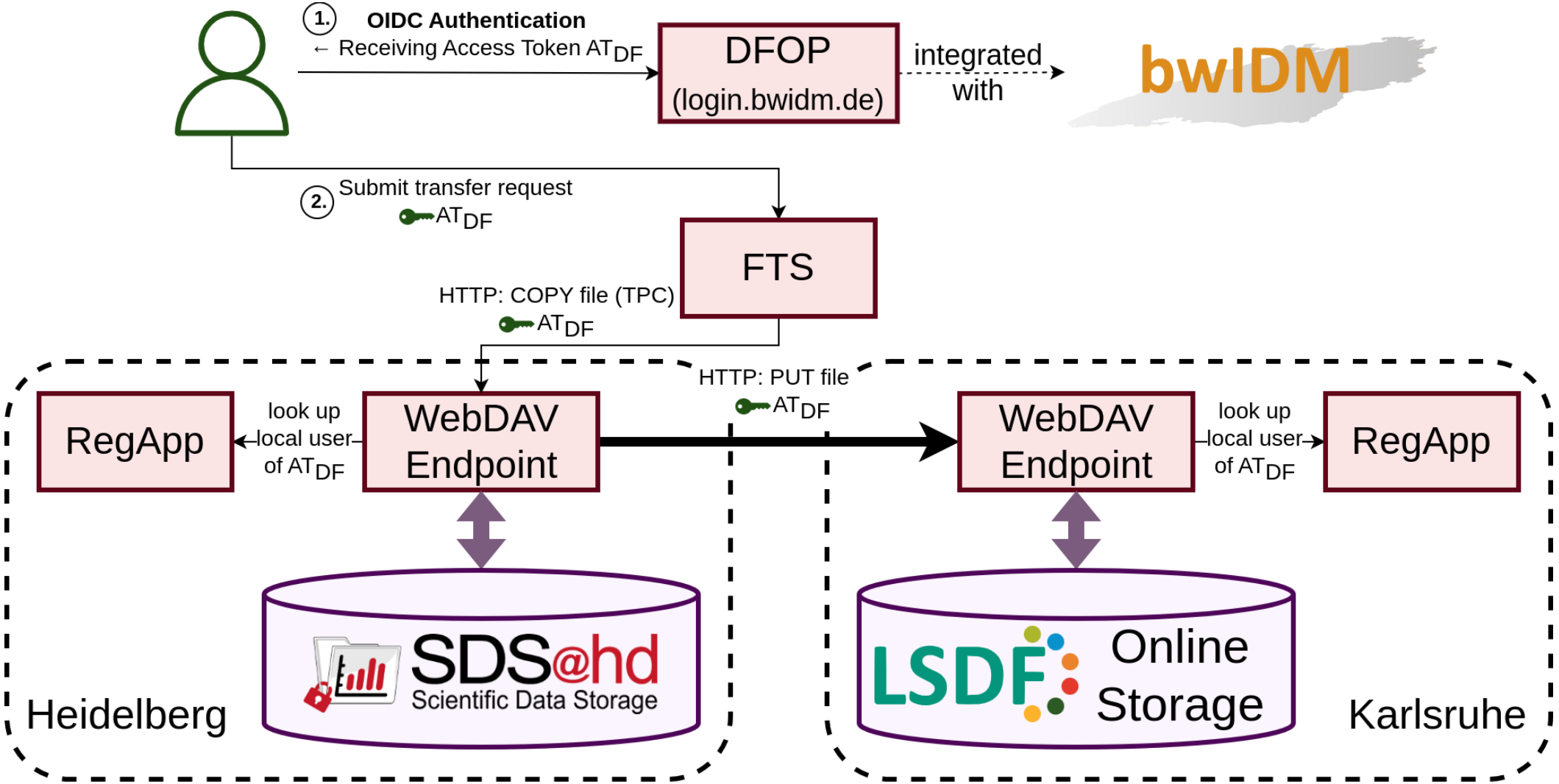
- 8 WLCG Instances
  - BNL, CERN (4), FNAL, RAL, MIT

- 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

Data Transfer Federation



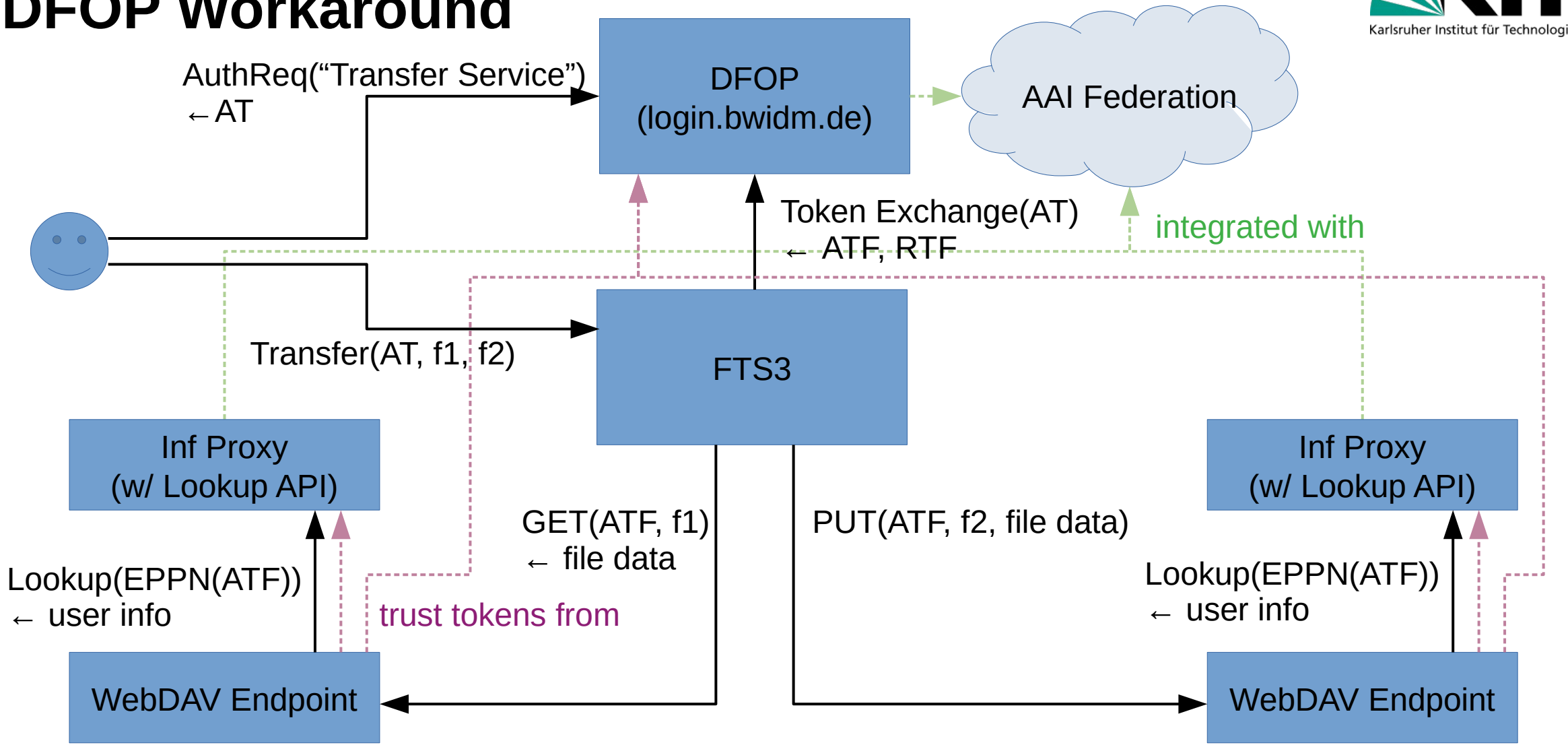
Conclusion

- 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.
- Successful prototypical implementation of file transfer between KIT and external sites.
- Future work:
  - Integration of further storage services within the federation.
  - Representation of the “Data Transfer Federation” to the users.

Thank you
Questions?

Backup Slides

Schema: Data Transfer Federation with DFOP Workaround



BPA: Flow of User Identity Information