



## *FTS and Tokens*

*FTS@OSG Token Transition Workshop 2021*

Mihai Patrascoiu  
on behalf of the FTS team

# Open Source software for reliable and large-scale data transfers within WLCG



## Features:

- x509 and OIDC tokens
- Staging + Archiving
- Multihop transfers
- Transfer Optimizer
- Cloud support
- Python bindings + CLI clients



**Intuitive**



**Robust**



**Flexible**



**Adaptive**

**8 WLCG instances**

**16 non-WLCG instances**

**~36 Virtual Organizations**

**5 Token Identity Providers**

Transferred in total in 2019: 1.29 EBs and 1.10B files

Transferred in total in 2020: 1.01 EBs and 976M files

Transferred in total in 2021: 0.78 EBs and 880M files (so far)

| ~65% by CERN FTS instances

During October 2021:

~75% transfers issued by Rucio

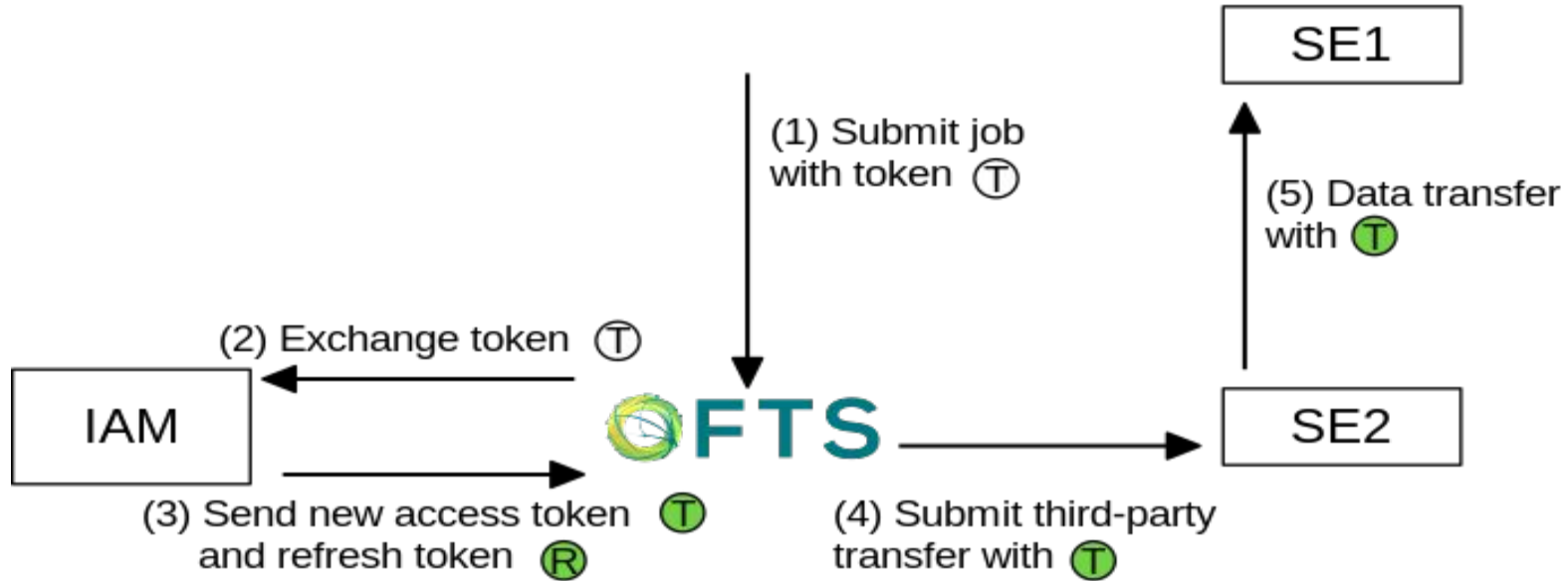


# FTS and Bearer tokens

## Support for two kinds of tokens in FTS

- User-provided tokens: OIDC
  - User provides an Access Token at transfer submission
  - FTS obtains a Refresh Token from the Token Provider
  - At time of transfer, FTS ensures having a valid Access Token
- FTS-obtained tokens: SE-issued tokens
  - User submits a proxy certificate at transfer submission
  - At time of transfer: FTS (/Gfal2) obtains a bearer token from each SE
  - *The proxy is to never be used again after this point*

# OIDC Token Flow

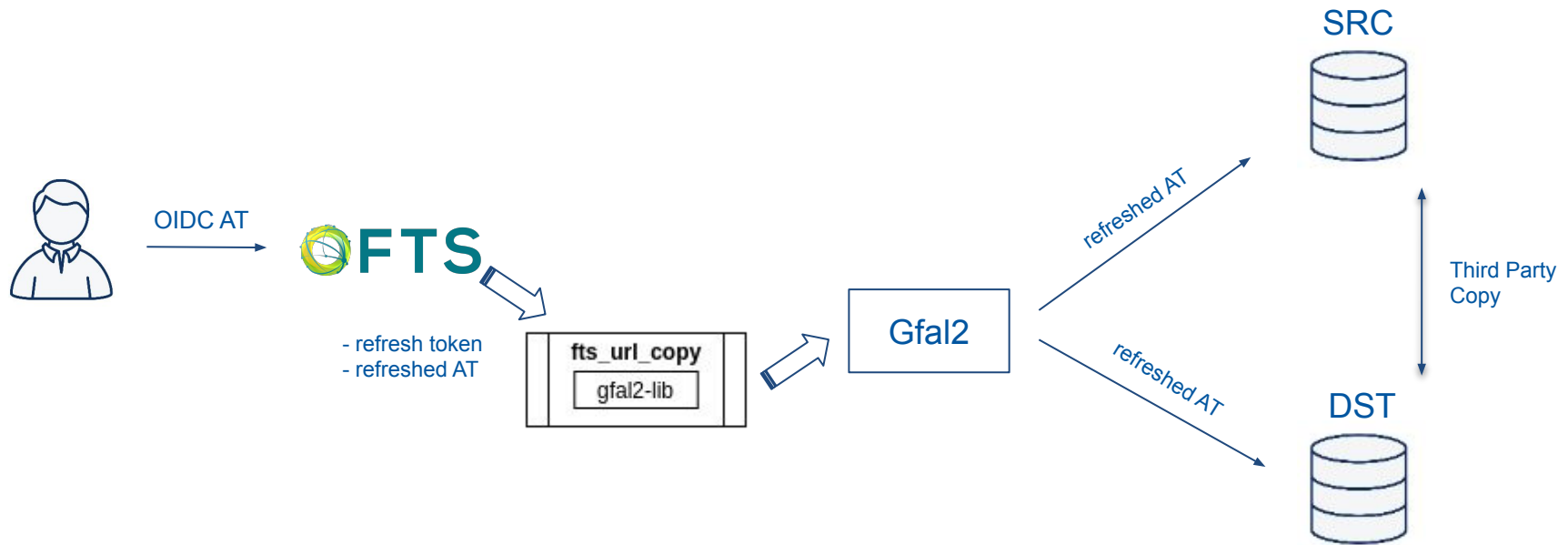


# OIDC Tokens - details

- Token validation done offline or via introspection (based on PyOIC)
- Allows for Audience and Scope claims validation
- Refresh token + access token stored in database (to be used during transfer)
- Enabled by sending `<access_token>` to FTS-REST server

```
fts-rest-transfer-submit --access-token=<access_token>  
-s https://fts3-devel.cern.ch:8446/ <src> <dst>
```

# FTS Transfer with OIDC tokens



# Storage-Element issued tokens

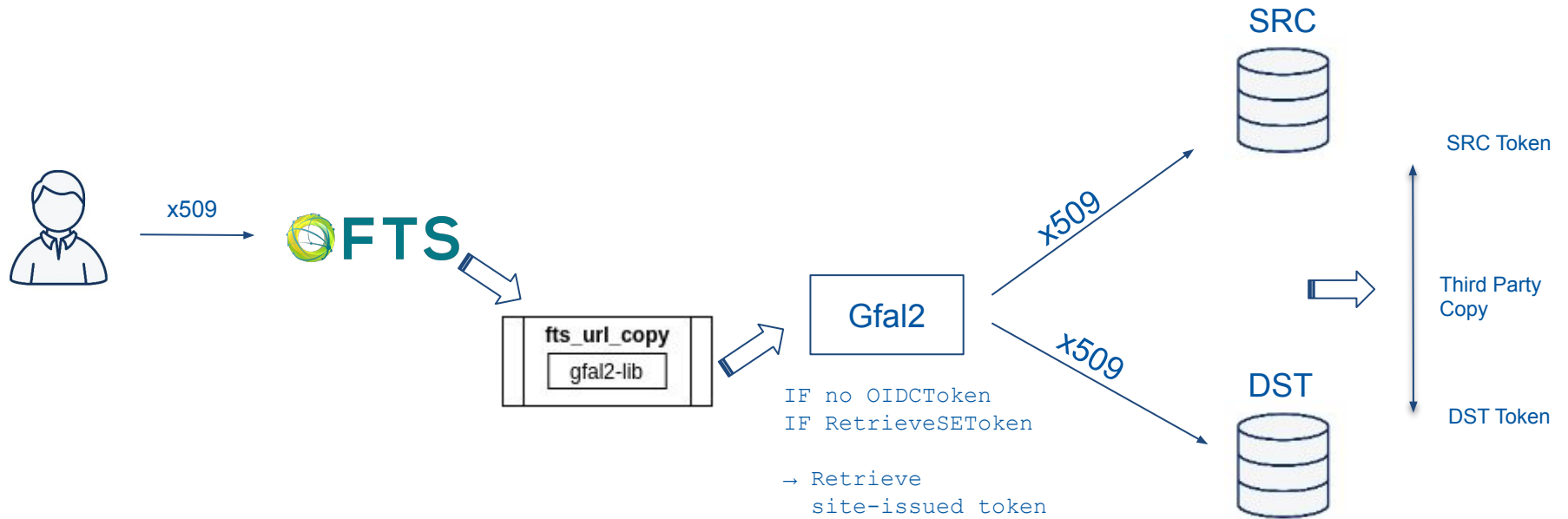
Storage-Element issued token = exchange of a x509 proxy certificate  
for a bearer token issued by the SE,  
for a given path and a given set of capabilities

- SE-issued token retrieval now part of core Gfal2 functionality (no longer FTS)
- Functionality exported via Gfal2 Python bindings and CLI tools
- Available in FTS v3.11.0 + Gfal2 v2.20.0

```
gfal-token [--issuer <host>] [--validity <minutes>] [--write]  
          <host/path> [activities list]
```



# FTS Transfer with site-issued tokens



# Conclusion

- FTS service already accommodates two *separate* token workflows
- SE-issued tokens still require x509, but are a good way forward
- OIDC Tokens use the same token for both the source and the destination
- OIDC Tokens: scopes and audiences are waiting to be refined

# Thank you!

 [cern.ch/fts](https://cern.ch/fts)

 [fts-devel@cern.ch](mailto:fts-devel@cern.ch)

 [cern.ch/fts3-docs](https://cern.ch/fts3-docs)

 <https://gitlab.cern.ch/fts/fts3>

 [cern.ch/dmc-docs](https://cern.ch/dmc-docs)

 <https://gitlab.cern.ch/dmc/gfal2>