CILogon Token Test: Rucio + FTS3

Anil Panta

Nov 26, 2024

Rucio + FTS Token

- 3 client is needed for Rucio+FTS3 token infrastructure.

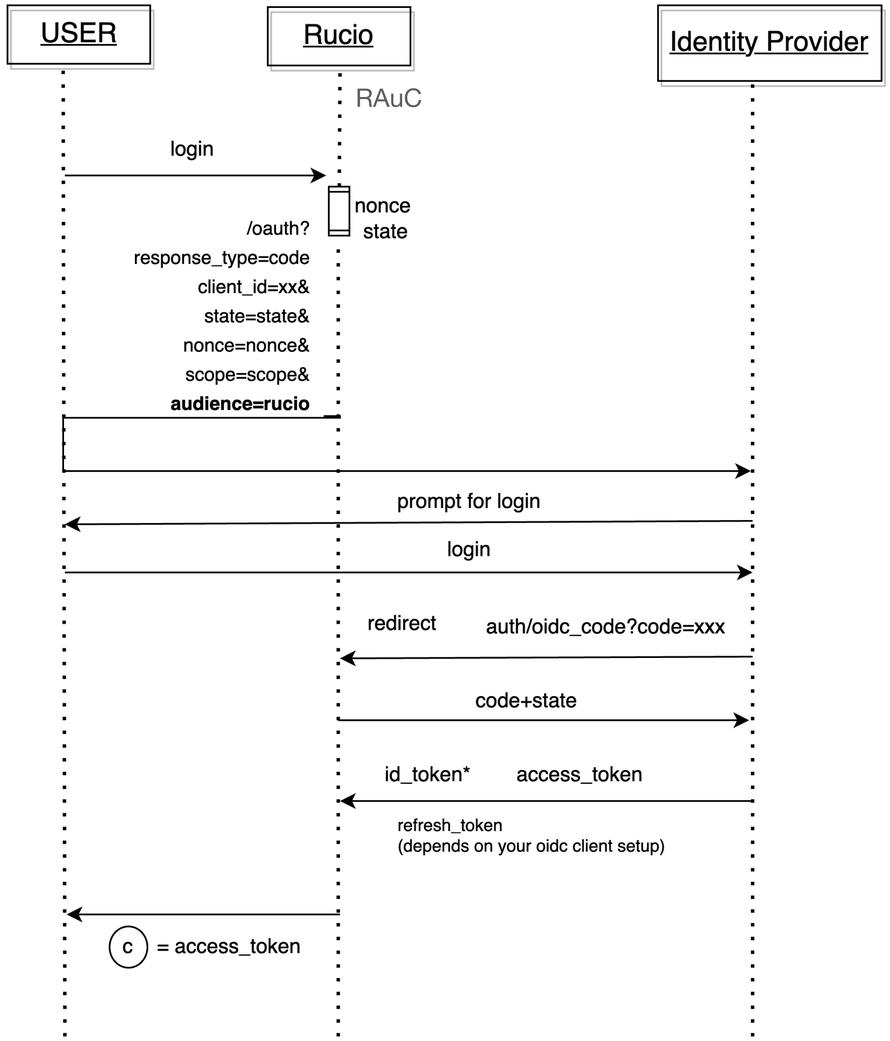
- Rucio Auth Client (RAuC):
  - For User authentication to rucio.
  - Grant type: Authorization code flow
  - Scopes: openID & profile (min) , offline_access (to allow rucio to refresh)

- Rucio Admin Client (RAdC):
  - Use for transfer submitted by Rucio to FTS.
  - Grant type: client_credentials flow
  - Scopes: fts, storage.create, storage.modify, offline_access

- FTS3 Client :
  - Use for token exchange and refresh.
  - Grant type: token_exchange, token_refresh

Explicitly ask cilogon to issue all access and refresh token as JWT.
(as they can also be opaque string)

Rucio : User Auth (OIDC authorization code flow)



Default scope = “openid+profile”

Default audience= “rucio”

RAuC = Rucio Auth Client

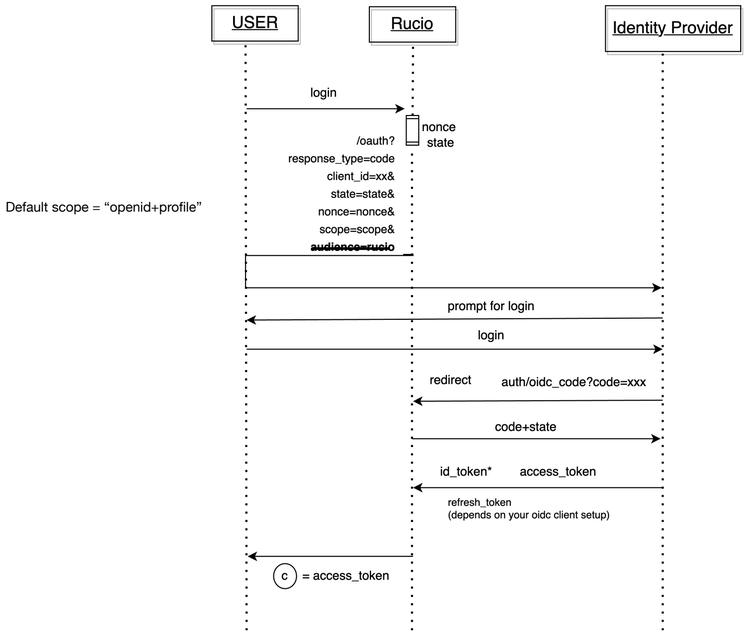
Jefferson Lab

Rucio + CILOGON : User Auth Test

- Created a standalone script (using pyoidc) : standalone_script
- **Removed audience parameter** in request. (In construct_AuthorizationRequest)
- All test passed with pyoidc.

- Refresh token test was done.
  - Can't figure out how to from pyoidc library.
  - But the refresh token standard flow is okay and tested.

```
curl -d grant_type=refresh_token \
    -d client_id=$CILOGON_CLIENT_ID \
    -d client_secret=$CILOGON_CLIENT_SECRET \
    -d refresh_token=$CILOGON_REFRESH_TOKEN \
    -d scope= xxx
```



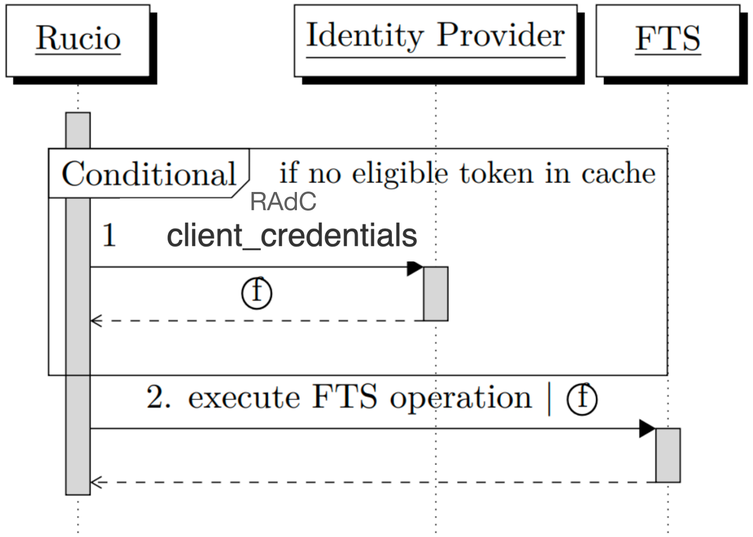
TODO in Rucio:
Audience parameter should be optional

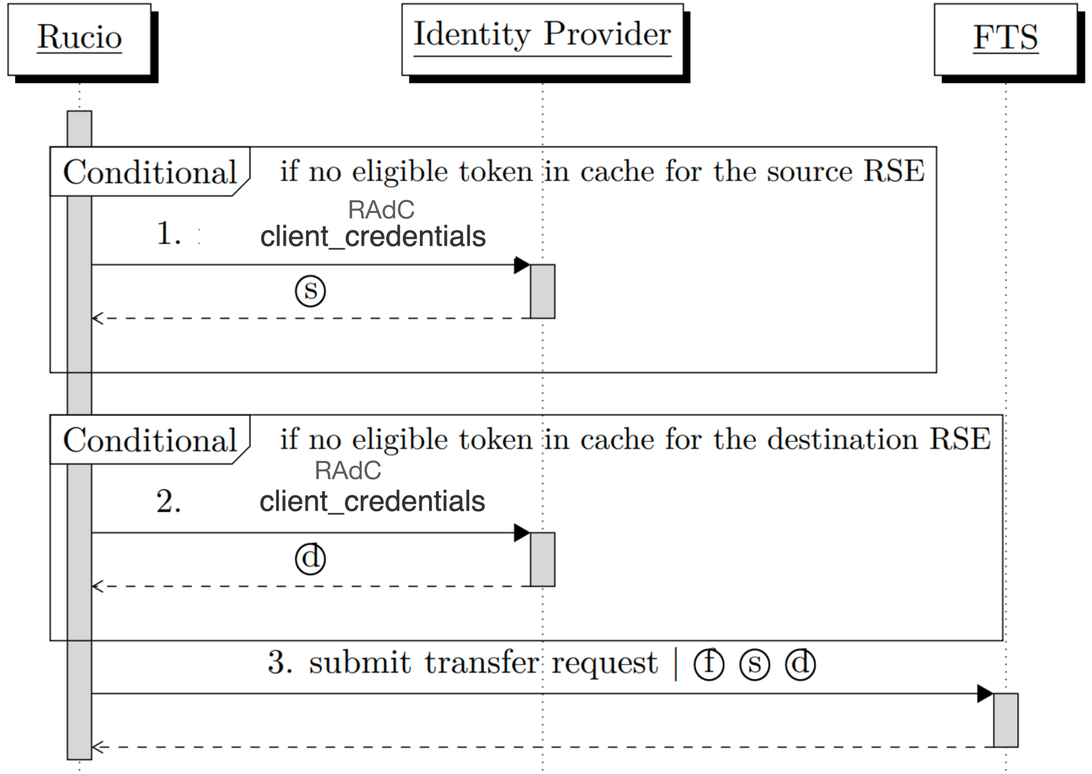
openID specification request doesn't have audience parameter as required.
openid-auth-request

RAuC = Rucio Auth Client

Jefferson Lab

RUCIO: Transfer oauth

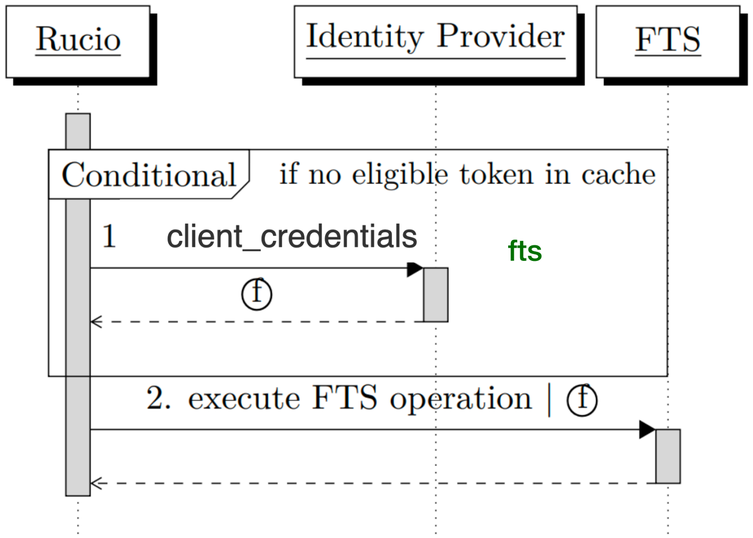


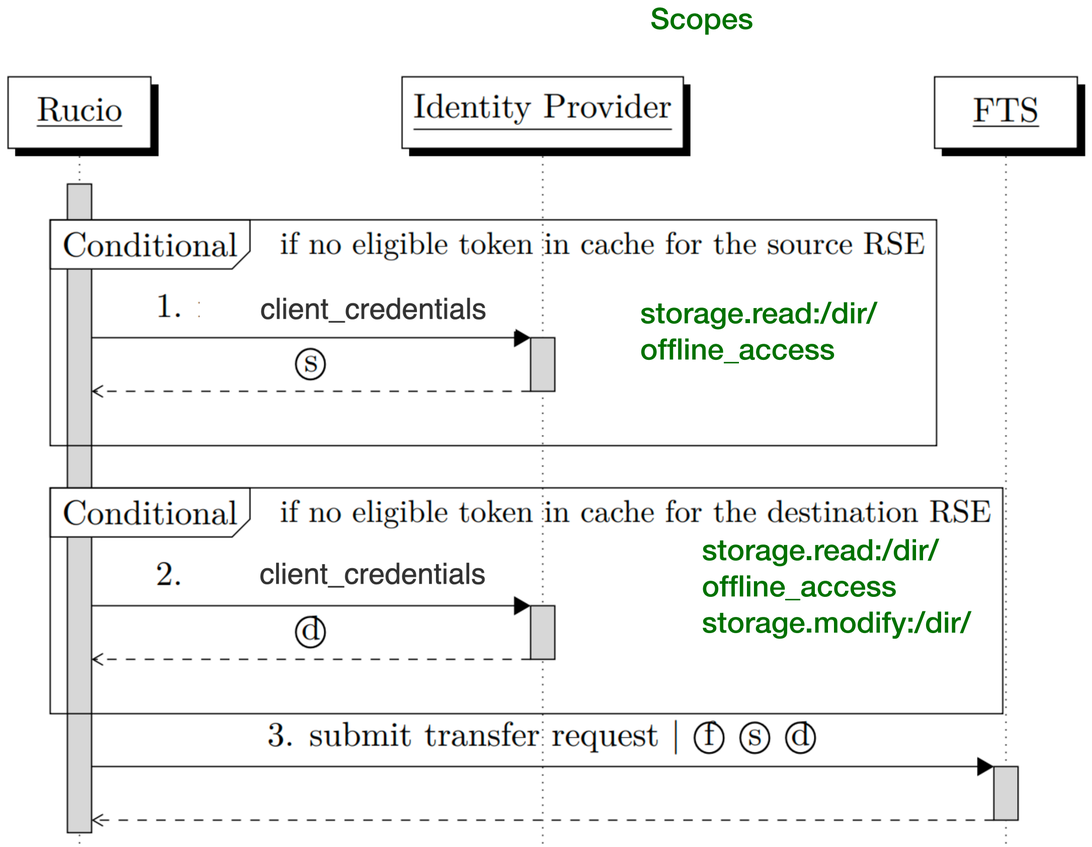


client_credentials of Rucio Admin Client (RAdC)

client_credentials = client_id + client_secret

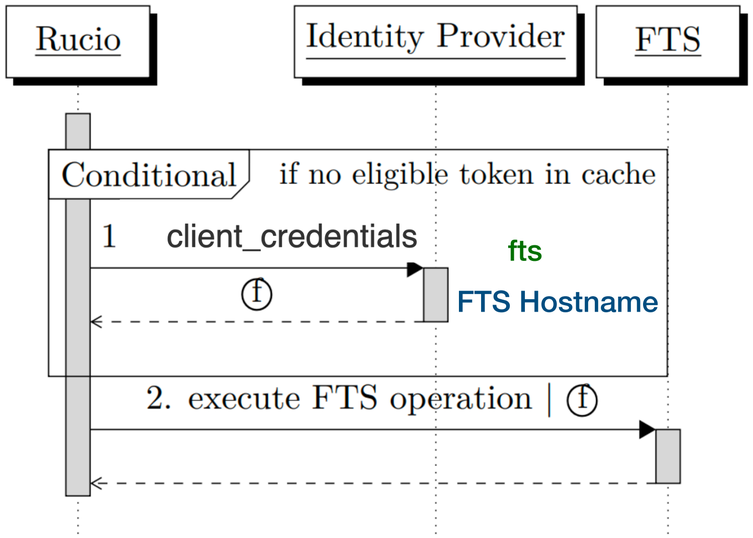
RUCIO: Transfer oauth with scopes



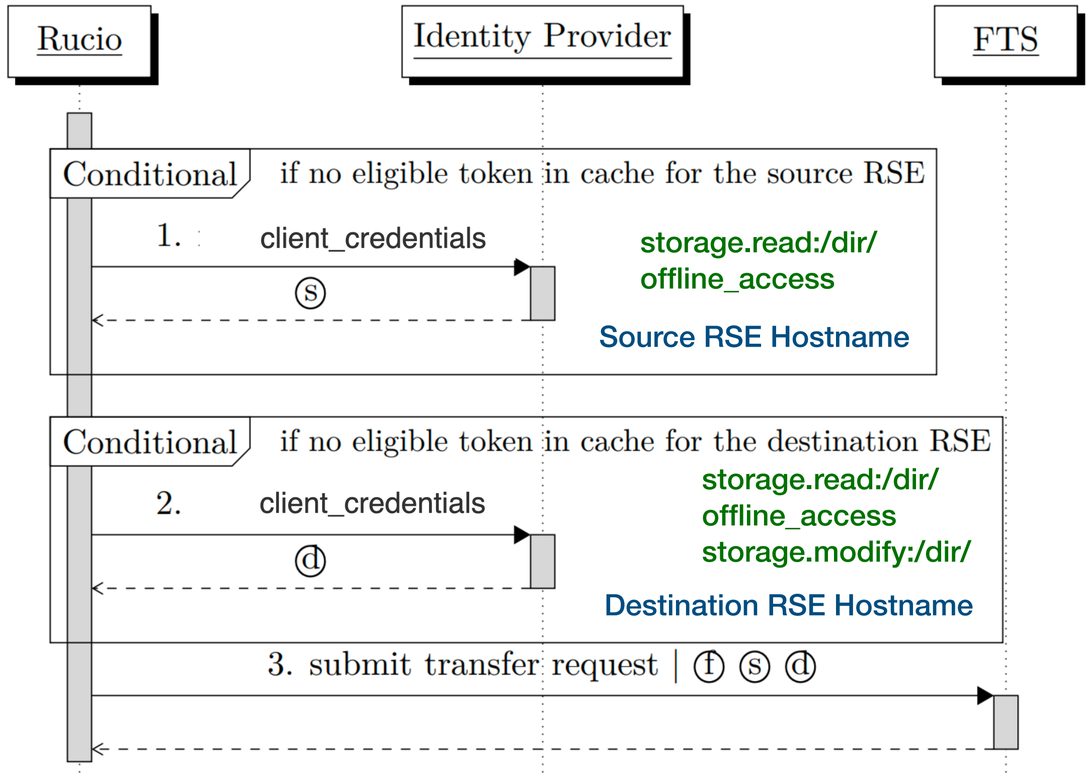


Jefferson Lab

RUCIO: Transfer oauth with scopes and audience



Scopes Audience



Jefferson Lab

RUCIO + CILOGON: Rucio admin test

- Created a standalone script : standalone_script
- cilogon allowed client_credentials grant in test instance.
- **Removed audience parameter** in request.
- Successful to get 3 tokens f, s and d.
- Audience of token is : https://wlcg.cern.ch/jwt/v1/any

```
response = requests.post(
    url=IAM_ENDPOINT,
    auth=(rucio_admin_CLIENT_ID, rucio_admin_CLIENT_SECRET),
    data={
        "grant_type": "client_credentials",
        "scope": des_storage_scope,
    },
    verify=False,
    timeout=60,
)
response.raise_for_status()
payload = response.json()
des_storage_access_token = payload["access_token"]
```

RUCIO + CILOGON: Rucio admin test

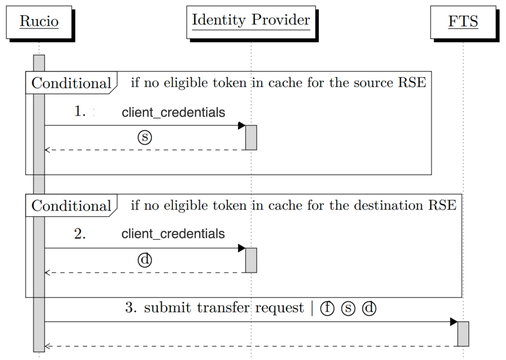
- Created a standalone script : standalone_script
- cilogon allowed client_credentials grant in test instance.
- **Removed audience parameter** in request.
- Successful to get 3 tokens f, s and d.
- Audience of token is : https://wlcg.cern.ch/jwt/v1/any

- TODO: CILogon is working to make it work with audience parameter.
  - i.e. token “aud’’ to be same as asserted/requested audience.

```
response = requests.post(
    url=IAM_ENDPOINT,
    auth=(rucio_admin_CLIENT_ID, rucio_admin_CLIENT_SECRET),
    data={
        "grant_type": "client_credentials",
        "scope": des_storage_scope,
        "audience": des_storage_hostname,
    },
    verify=False,
    timeout=60,
)
response.raise_for_status()
payload = response.json()
des_storage_access_token = payload["access_token"]
```

FTS : Token operations

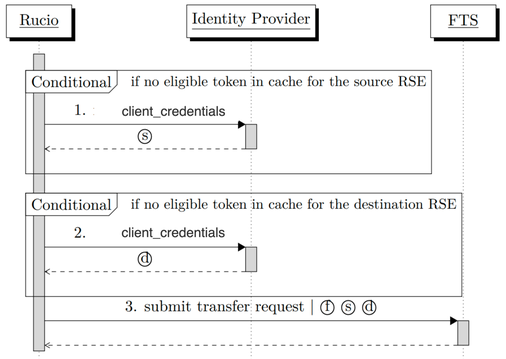
- FTS provides token compliance script: fts-token-compliance.py
- 2 phase:
  - 1st phase: token_exchange to get the refresh token.
  - 2nd Phase: refresh_token to get the new access token.



Jefferson Lab

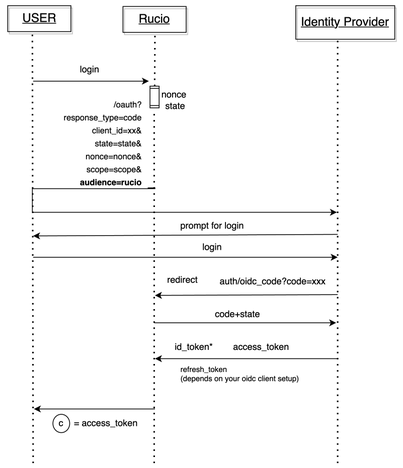
FTS + CILOGON: Test

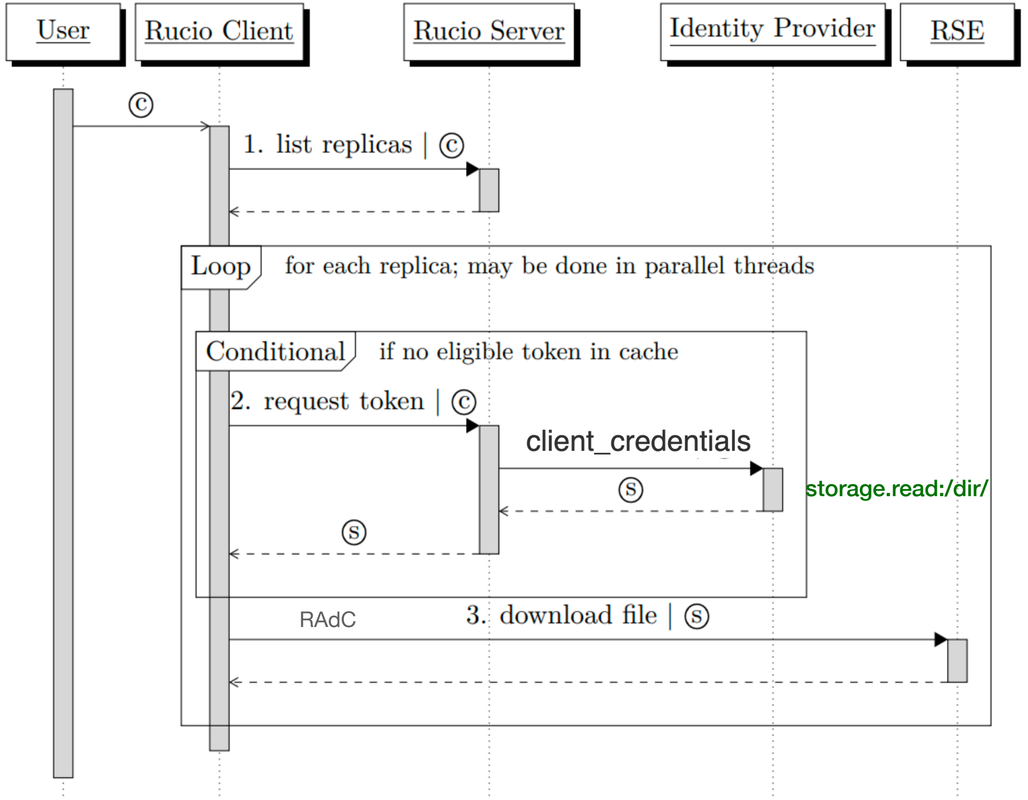
- 1 phase: token_exchange to get the refresh token.
  - Got the access and refresh token
- 2 phase: Failed: “"error_description":"invalid refresh token"
  - cilogon: “token exchange followed by a call to the refresh endpoint is failing”
- cilogon is looking into.



Jefferson Lab

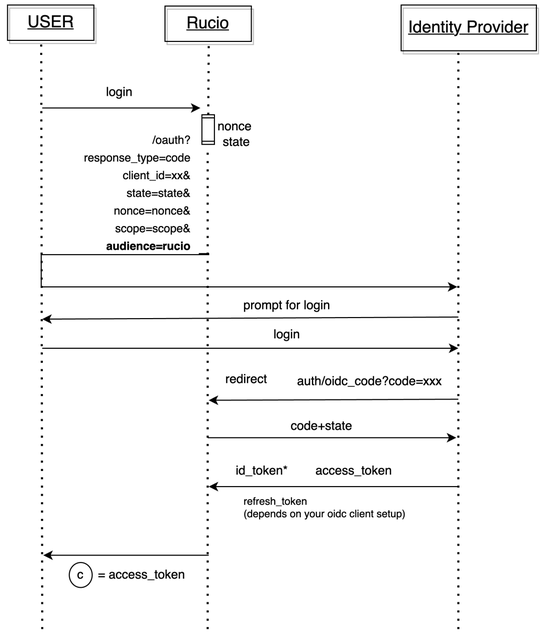
Rucio Download

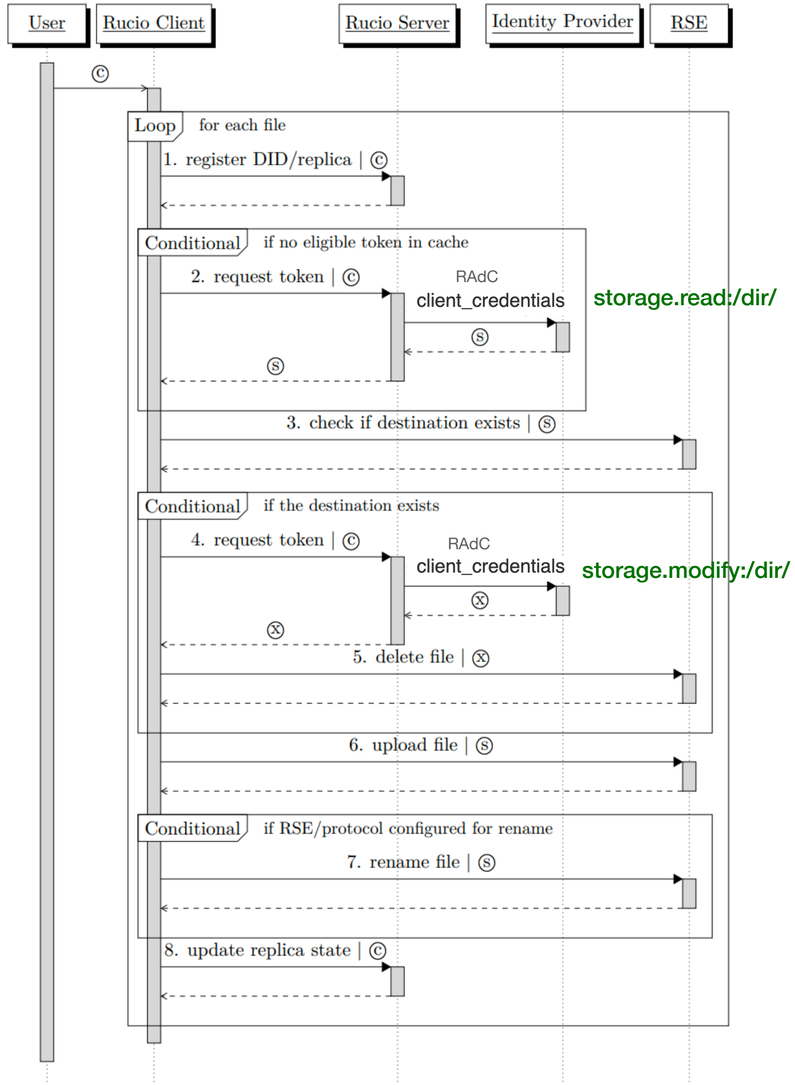




Rucio Upload

Scopes





Jefferson Lab

Storage: Issuer and Audience

xrootd config

```
[Global]
audience = rse_hostname

[Issuer cilogon]
issuer = https://cilogon.org
base_path = /vo/dir
```

dache config

```
gplazma.scitoken.issuer!cilogon = https://cilogon.org /vo/dir
gplazma.scitoken.audience-targets = rse_hostname
```