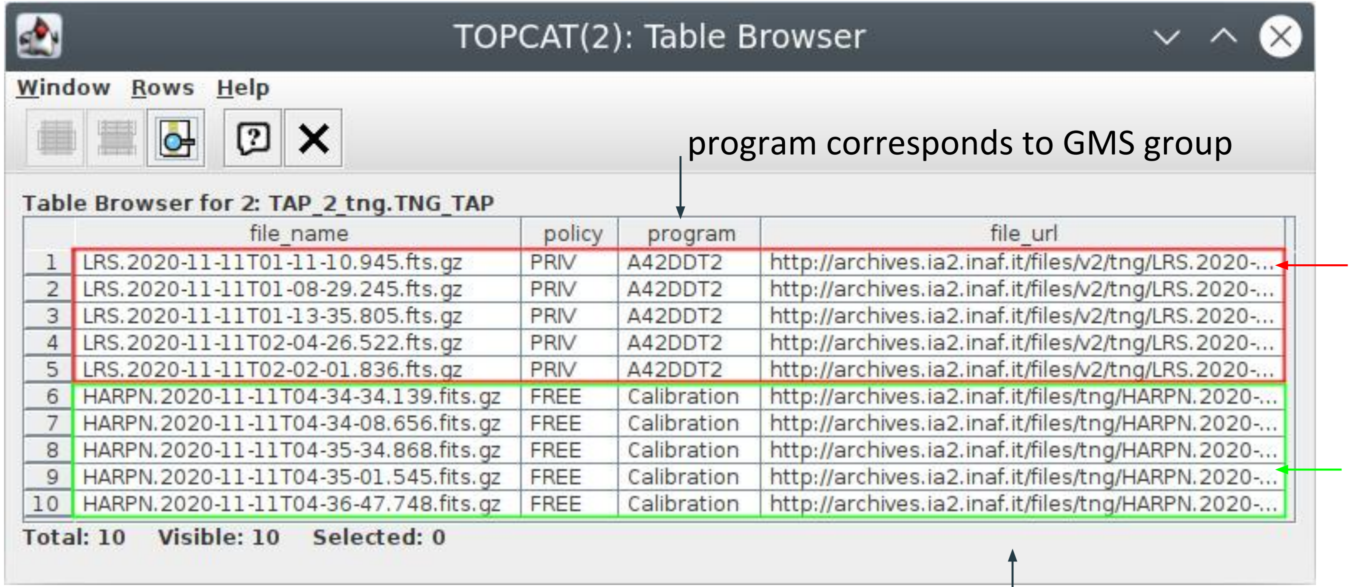
An OAuth2-based GMS implementation - update

Sonia Zorba & IA2 team - INAF-OATs

Virtual Interoperability Meeting - November 2020

Current IA2 use case



program corresponds to GMS group

Table Browser for 2: TAP_2_tng.TNG_TAP

	file_name	policy	program	file_url
1	LRS.2020-11-11T01-11-10.945.fts.gz	PRIV	A42DDT2	http://archives.ia2.inaf.it/files/v2/tng/LRS.2020-...
2	LRS.2020-11-11T01-08-29.245.fts.gz	PRIV	A42DDT2	http://archives.ia2.inaf.it/files/v2/tng/LRS.2020-...
3	LRS.2020-11-11T01-13-35.805.fts.gz	PRIV	A42DDT2	http://archives.ia2.inaf.it/files/v2/tng/LRS.2020-...
4	LRS.2020-11-11T02-04-26.522.fts.gz	PRIV	A42DDT2	http://archives.ia2.inaf.it/files/v2/tng/LRS.2020-...
5	LRS.2020-11-11T02-02-01.836.fts.gz	PRIV	A42DDT2	http://archives.ia2.inaf.it/files/v2/tng/LRS.2020-...
6	HARPN.2020-11-11T04-34-34.139.fits.gz	FREE	Calibration	http://archives.ia2.inaf.it/files/tng/HARPN.2020-...
7	HARPN.2020-11-11T04-34-08.656.fits.gz	FREE	Calibration	http://archives.ia2.inaf.it/files/tng/HARPN.2020-...
8	HARPN.2020-11-11T04-35-34.868.fits.gz	FREE	Calibration	http://archives.ia2.inaf.it/files/tng/HARPN.2020-...
9	HARPN.2020-11-11T04-35-01.545.fits.gz	FREE	Calibration	http://archives.ia2.inaf.it/files/tng/HARPN.2020-...
10	HARPN.2020-11-11T04-36-47.748.fits.gz	FREE	Calibration	http://archives.ia2.inaf.it/files/tng/HARPN.2020-...

Total: 10 Visible: 10 Selected: 0

private file URLs accepting OAuth2 tokens (JWT)

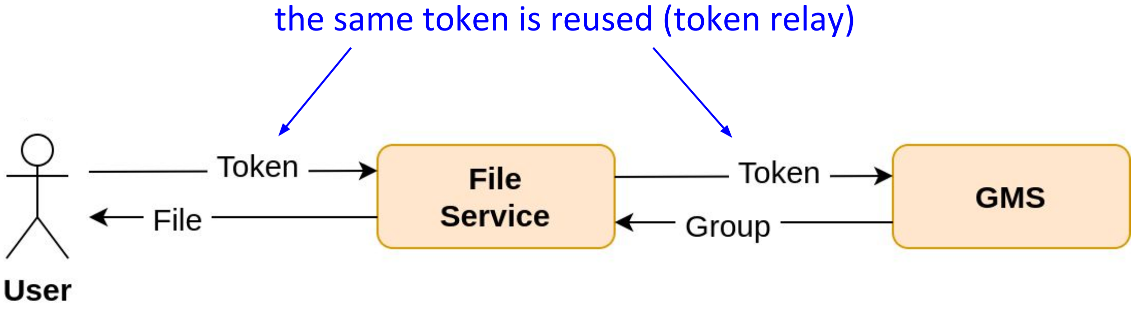
public file URLs

Currently all metadata is public and part of the data (access URLs) is private. Nice to have: authenticated TAP calls, in order to handle also private metadata.

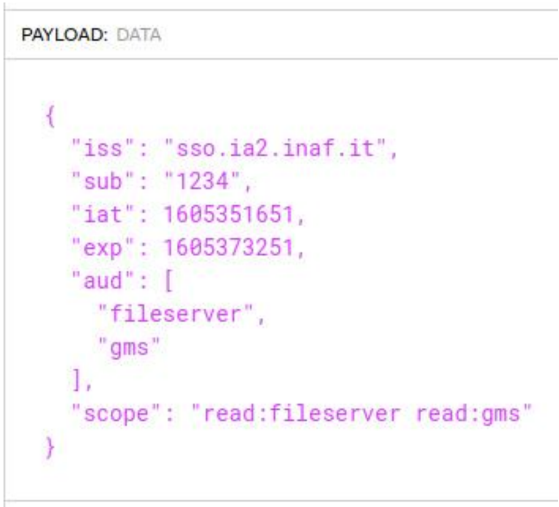
Currently the access URL is exposed directly into the TAP table. In the future: DataLink

Downloading private files

```
wget --header="Authorization: Bearer $(cat token.txt)" -i files-list.txt
```



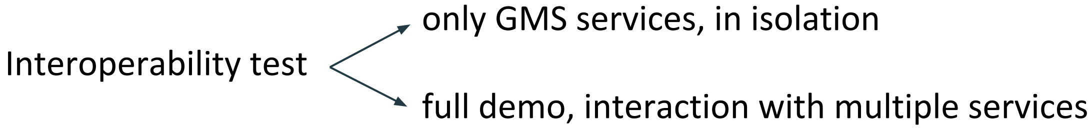
JWT with multiple audience
is allowed by RFC 7519


PAYLOAD: DATA

```
{
  "iss": "sso.ia2.inaf.it",
  "sub": "1234",
  "iat": 1605351651,
  "exp": 1605373251,
  "aud": [
    "fileserver",
    "gms"
  ],
  "scope": "read:fileserver read:gms"
}
```

GMS implementations

- CADC: X.509, Cookies, OAuth2
- IA2: OAuth2



Interoperability test

only GMS services, in isolation

full demo, interaction with multiple services

IA2 implementation is currently in production and used also for LBT (Large Binocular Telescope) and TNG (Telescopio Nazionale Galileo) archives.

It follows OAuth2 standard but at the moment is tightly coupled with IA2 authorization server (RAP). It could be adapted to other authorization servers but the code needs to be rearranged.

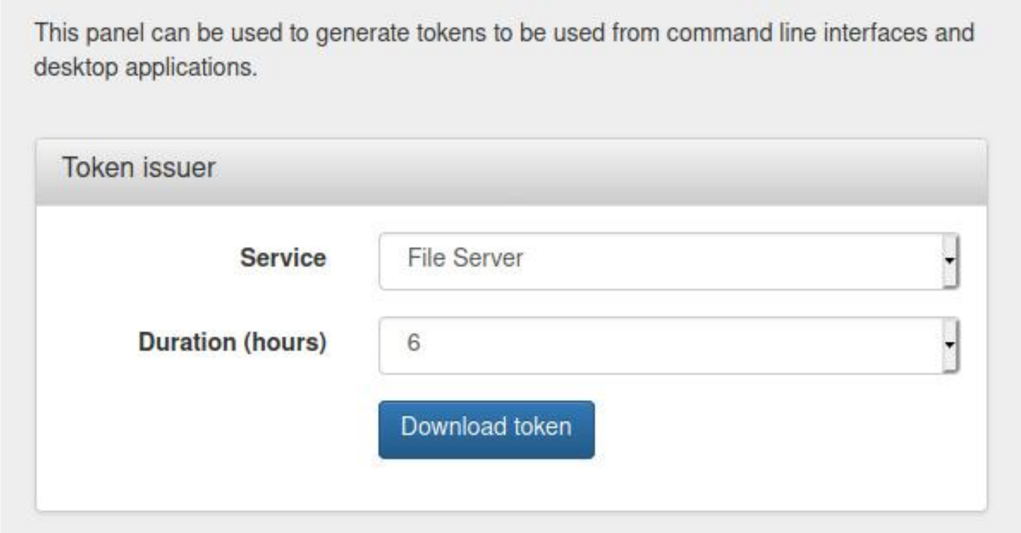
Implementation is straightforward:

```
GET /search
Authorization: Bearer <TOKEN>
```

the difficult part is how to get the token...

How to obtain the token?

Authentication methods supported by RAP: eduGAIN G f in + local accounts



This panel can be used to generate tokens to be used from command line interfaces and desktop applications.

Token issuer

Service: File Server

Duration (hours): 6

The user logs in into a “token issuer” web page and downloads the token.

Alternative: the client implements OAuth 2.0 for Native Apps (RFC 8252)

Problem: token lifespan should be short, so these methods require manual user action every few hours.

How to obtain the token?

Alternative: using **OAuth2 client credentials** flow.

- Special OAuth2 flow used mostly when the client is not a user but a service (machine-to-machine).
- Credentials need to be sent by the client → suitable only for a subset of our users (not feasible for eduGAIN and social network accounts)
- We support account linking, so users needing this feature could create a special account for that specific purpose.

Request:

```
POST /token
Authorization: Basic <user:password>
grant_type=client_credentials
```

Basic authentication: credentials must be handled internally

Response:

```
{"access_token":"eyJ0eXAiOiJKV...
```

Thanks for your attention

Questions?

Contact:
sonia.zorba@inaf.it