An OAuth2-based GMS implementation

Sonia Zorba & IA2 team - INAF-OATs

INAF ISTITUTO NAZIONALE DI ASTROFISICA

Virtual Interoperability Meeting 2020

Identity is retrieved from token

A token is obtained from an OAuth2 authorization server (RAP) and sent in the request header:

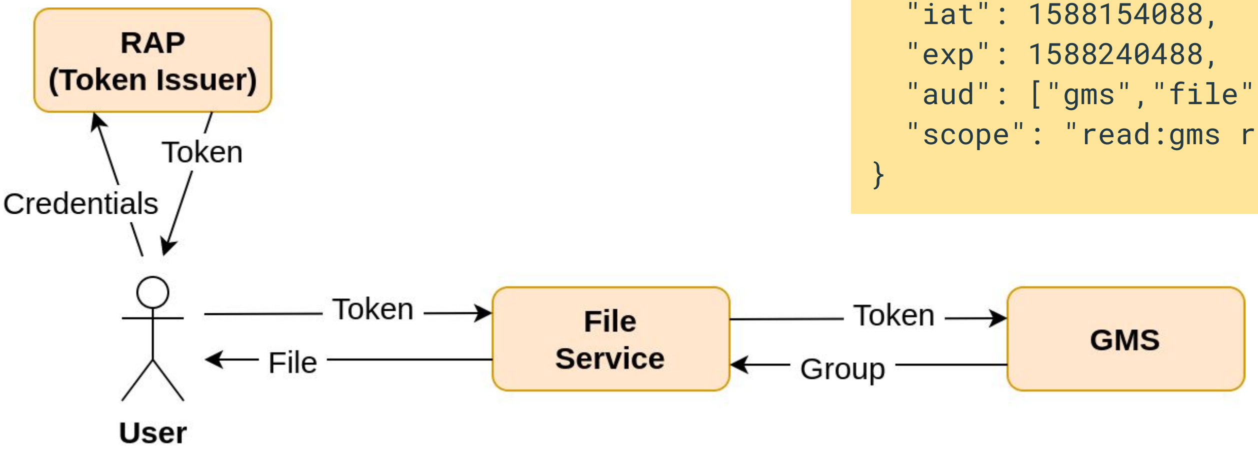
```
GET /search
Authorization: Bearer <TOKEN>
```

For working together with other services it is necessary to define Credentials Delegation with tokens.

Current delegation implementation

JWT token relay with multiple audience (allowed by RFC 7519)

```
{
  "iss": "sso.ia2.inaf.it",
  "sub": "RAP:2386",
  "iat": 1588154088,
  "exp": 1588240488,
  "aud": ["gms","file"],
  "scope": "read:gms read:file"
}
```



Alternative: OAuth2 Token Exchange (RFC 8693)

Groups of Groups

Nested groups response:

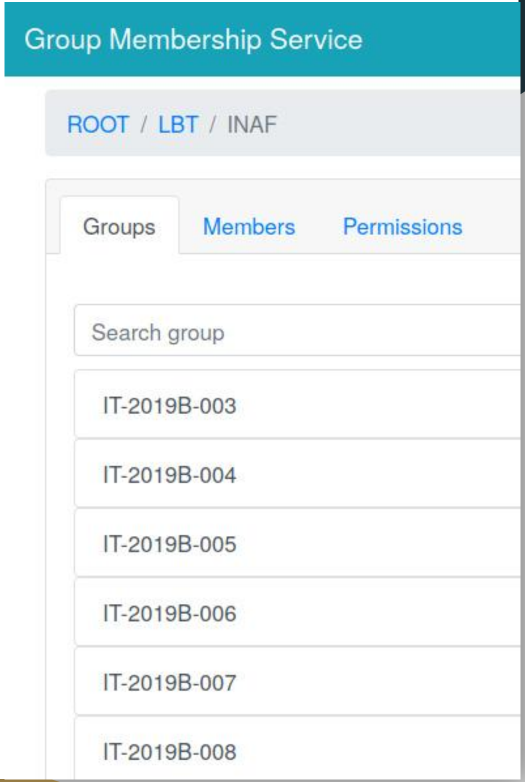
```
LBT.INAF.IT-2019B-008
LBT.AZ.AZ-2019B-004
LBT.OSU
```

Dot is used as separator between parent groups and children.

Standardize separator?

What if a group name contains dot symbol?

Current implementation uses ltree PostgreSQL extension



IT-2019B-003
IT-2019B-004
IT-2019B-005
IT-2019B-006
IT-2019B-007
IT-2019B-008