Exploring an Alternative Model for Tokens

Dimitrios Christidis

Introduction

- There remain concerns as to what level of service the token issuers can provide
  - Both in terms of instantaneous token rate and overall uptime
  - Specifically for IAM at CERN: no SLAs
- Many parties agree that file-specific tokens offer the best security
  - But come at an unacceptable cost, hence the need for compromise
- An alternative model has been proposed
  - This will be an *exploration*; there are no set expectations at this time
  - The in-progress implementation will be completed and remain supported

The model in short

- The Rucio instance mints its own tokens, effectively becoming a token issuer itself
  - But won’t implement any of the Oauth flows
- Advantages:
  - No compromises on security
    - Including finer control over token lifetimes
  - No concerns over future scalability
  - No additional service becoming a single point of failure
- A token issuer remains necessary for other operations (e.g. user authentication, compute)

The model in practice

The storages must be configured to accept the Rucio instance as an issuer

```
[Issuer atlas-rucio]

issuer = https://atlas-rucio.cern.ch

base_path = /eos/atlas/

…
```

The Rucio instance must provide interfaces for storages to verify its tokens
(JSON Web Key Sets)

```
{

    "iss": "https://atlas-rucio.cern.ch/",

    …

}
```

https://atlas-rucio.cern.ch/.well-known/…

Questions?