

Rucio Token workflows

[Martin Barisits](#)

on behalf of the Rucio team



Background

- [OIDC Tokens](#) added to Rucio in 2019 via XDC project funding
- Functional, and continuously tested in DOMA testbed
- However, functionality is quite coarse
 - Largely replaces usage of X509 proxies with fat-tokens
- Ongoing discussion in [WLCG AuthZ workgroup](#)
- Lots of interest from non-HEP Rucio communities
 - Especially Astronomy sector, since fine-grained tokens could solve their data-embargo issues
 - X509 is a big barrier-of-entry for new (non-HEP) communities
- Rucio token workflows currently being refined
 - For security reasons (Fine-grained vs. fat tokens)
 - But also for functional reasons (Data embargos, ...)

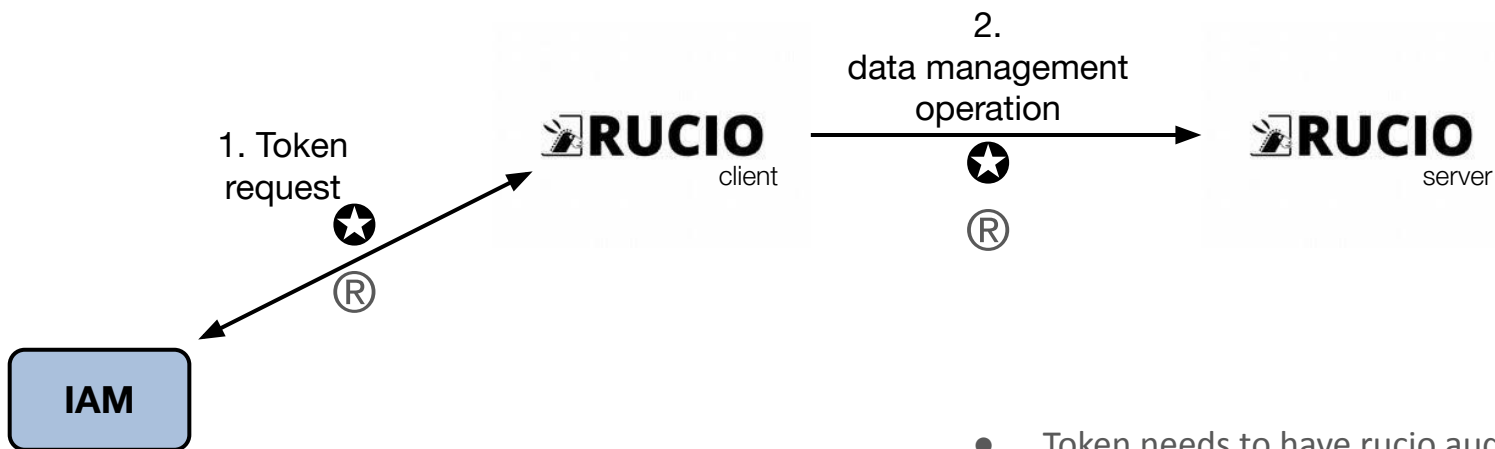


Workflows involving tokens

- Largely four different workflows involving tokens in Rucio
 - Authenticating to Rucio itself to submit rucio commands/requests
 - Listing replicas
 - Listing Datasets
 - ...
 - Rucio-initiated third-party-copy requests via FTS
 - Rucio-initiated deletion requests to storage
 - Downloading/Uploading data to storage (+registering it to Rucio)



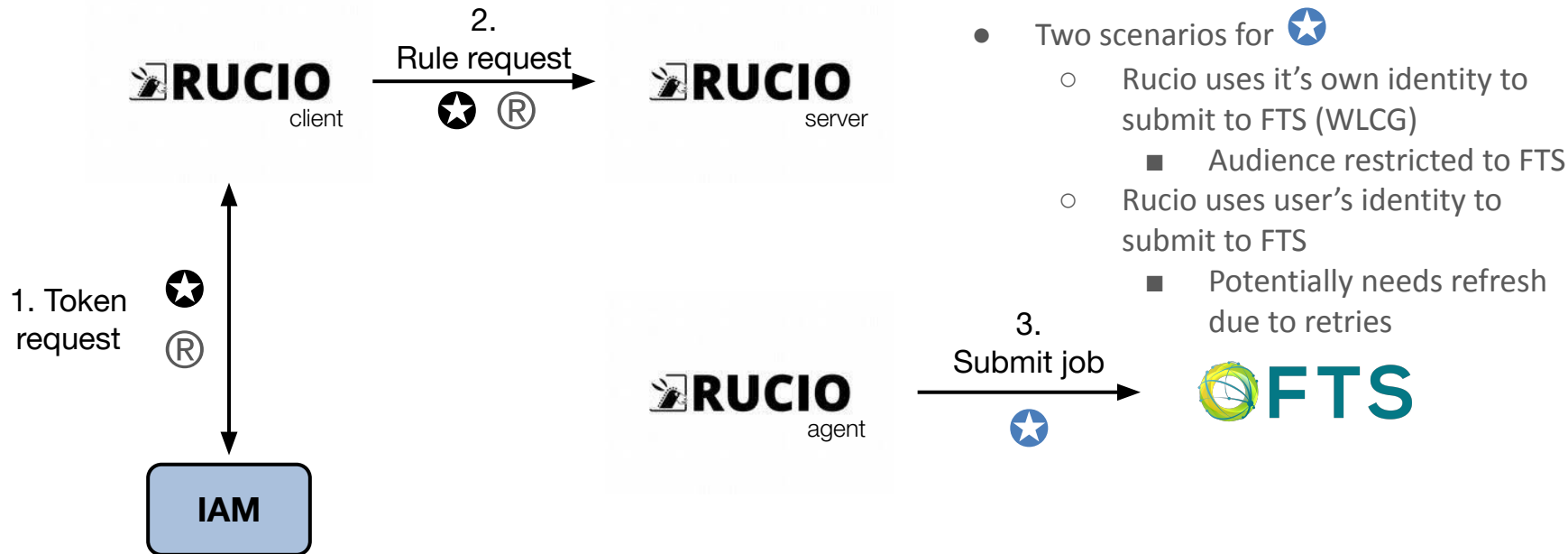
Authenticating to Rucio



- Token needs to have rucio audience
- Refresh token is optional but might be needed in certain setups (see later)

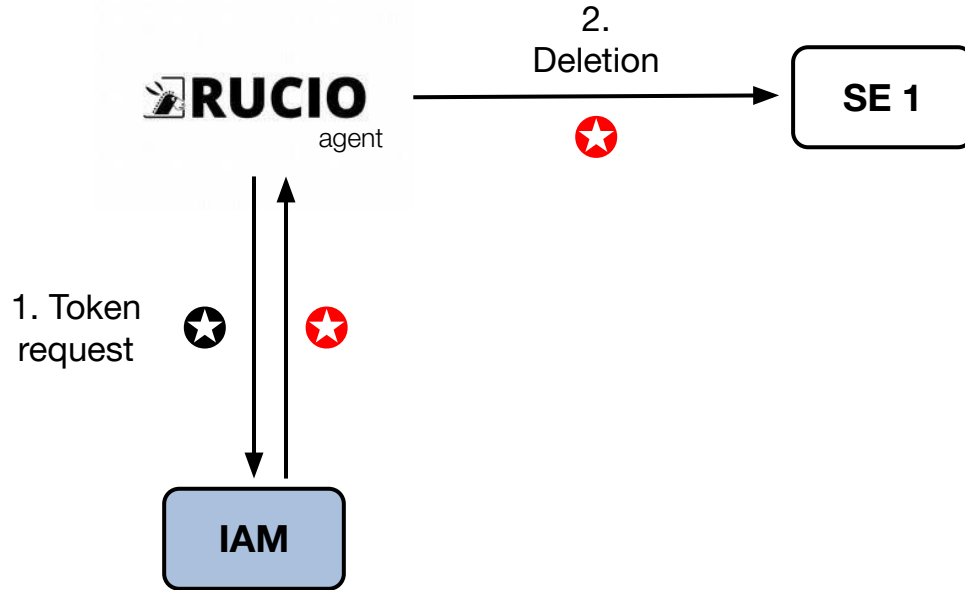


Third-party-copy request





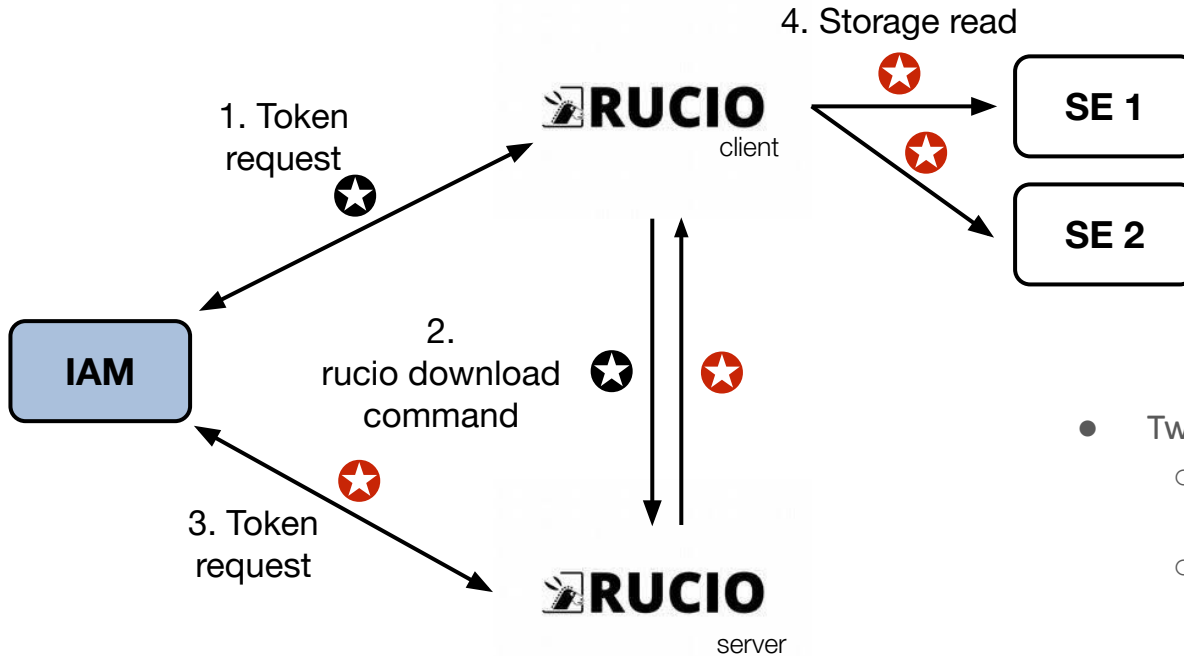
Rucio initiated deletion request




- Rucio requests a new token for its own identity which is properly scoped and audience restricted



Rucio download



- Two options for 
 - Rucio identity, properly scoped and audience restricted
 - User identity, properly scoped and audience restricted



Remarks

- Properly scoped and audience limited tokens
 - Plan is to return these as part of the `list_replicas` query to the Rucio server
 - Will probably also need alternative REST endpoint to request SE-tokens for users who do not use Rucio clients to download data
- Rucio as the central token-issuing component
 - Tokens can be very specifically scoped/audience restricted
 - Gives us unique opportunity to limit data access (very interesting for non-HEP sciences)
 - Data embargos based on projects/scopes/datasets/metadata
 - Risk needs to be properly assessed
 - Not only Rucio, but entire token-driven software stack
 - Security audits



More information

Website



<http://rucio.cern.ch>

Documentation



<https://rucio.cern.ch/documentation>

Repository



<https://github.com/rucio/>

Images



<https://hub.docker.com/r/rucio/>

Online support



<https://rucio.slack.com/messages/#support/>

Developer contact



rucio-dev@cern.ch

Publications



<https://rucio.cern.ch/publications.html>

Twitter



<https://twitter.com/RucioData>