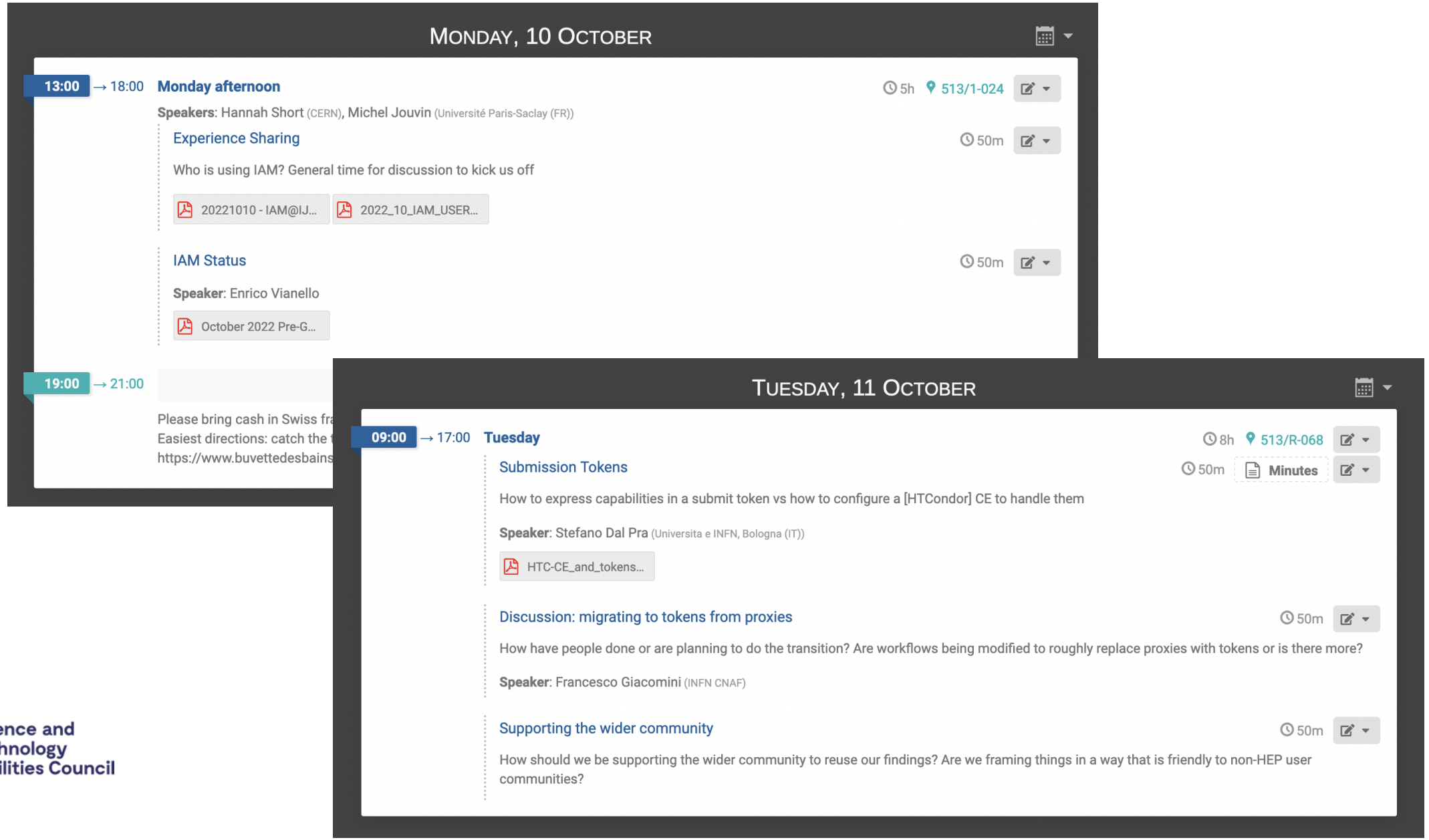
Science and Technology Facilities Council

Pre-GDB Report: AuthZ and IAM Workshop

Tom Dack

Science and Technology Facilities Council

AuthZ & IAM Workshop



Monday, 10 October

13:00 → 18:00 **Monday afternoon** — 5h — 513/1-024

Speakers: Hannah Short (CERN), Michel Jouvin (Université Paris-Saclay (FR))

Experience Sharing — 50m

Who is using IAM? General time for discussion to kick us off

20221010 - IAM@IJ... 2022_10_IAM_USER...

IAM Status — 50m

Speaker: Enrico Vianello

October 2022 Pre-G...

19:00 → 21:00

Please bring cash in Swiss fr
Easiest directions: catch the t
https://www.buvettedesbains

Tuesday, 11 October

09:00 → 17:00 **Tuesday** — 8h — 513/R-068

Submission Tokens — 50m — Minutes

How to express capabilities in a submit token vs how to configure a [HTCondor] CE to handle them

Speaker: Stefano Dal Pra (Universita e INFN, Bologna (IT))

HTC-CE_and_tokens...

Discussion: migrating to tokens from proxies — 50m

How have people done or are planning to do the transition? Are workflows being modified to roughly replace proxies with tokens or is there more?

Speaker: Francesco Giacomini (INFN CNAF)

Supporting the wider community — 50m

How should we be supporting the wider community to reuse our findings? Are we framing things in a way that is friendly to non-HEP user communities?

UKRI Science and Technology Facilities Council

IAM Status

Latest release: IAM v1.8.0 (1/4)

Released on: **2022-09-09**

Highlights:

- Spring Boot upgrade
- Refactored client management & registration
- JWT-based client authentication
- More support for AARC guidelines
- New consent page

other minor **improvements** & **bug fixes**

Planned release: IAM v1.8.1

To-Be-Added:

- Add scope policy management into IAM dashboard #382
- Migrate scope management to IAM dashboard #85
- Improve support for AARC guidelines

To-Be-Fixed:

- IAM VOMS attribute authority should not issue attribute certificates to users with an expired AUP signature #446
- IAM should not allow token refresh for users with an expired AUP signature #447
- Can't add certificate with same subject and different issuer #454
- IAM should not allow token refresh for disabled users #508
- IAM should issue a new RT when making token refresh flow #509

Planned release: IAM v1.9.0

To-Be-Added:

- Support for HA deployments #436
- Support for Multi-factor Authentication #418

and other remaining open issues

Science and Technology Facilities Council

IAM Open Discussion

- Lots of topics covered here!

- Considerations around Admin Tokens (privileges granted independent of scopes) and Service Accounts
- User Suspension flows and VOMs importer
- Refresh token flows
- Automatic import and activation of accounts from CERN HR-DB
- Group Management responsibility delegation
- Progress with MFA integration
- … and more

Experience Sharing Session

- Short presentations from CERN (Hannah Short) , IJCLab (Michel Jouvin) and IRIS/STFC (Tom Dack) to facilitate discussion

- Decided to trial use of INDIGO IAM GitHub discussions page as a community forum, using this as a permanent home for discussion and knowledge sharing: https://github.com/indigo-iam/iam/discussions

Submission Tokens

- Slides by Stefano Dal Pra

- More work to be done to review compute scopes so as to contain required levels of information
  - compute scopes working document: https://docs.google.com/document/d/1J85iNV1gIn4HX3owVrP4DdhTZKH7dzq11nv7Qv0Wj3U/edit?usp=sharing

- Further work within the AuthZ WG to understand and produce guidelines for when it makes sense for authorization logic to live within IAM and when it should be client side

Science and Technology Facilities Council

Latest Version of Token Transition Timeline

- Publish 22/08/22 on Zenodo: https://zenodo.org/record/7014668#.Y0VhWlJBzVE

Timeline

Milestone ID	Date	Description	Dependencies	Teams
M.1	Sep 2022	IAM is also in production for ALICE and LHCb.		CERN IT, IAM devs
M.2	Dec 2022	DIRAC versions supporting job submission tokens deployed for concerned VOs (LHCb, Belle-II, …).		DIRAC, LHCb, Belle-II, …
M.3	Feb 2023	VOMS-Admin is switched off for one or more experiments. Prerequisites: • Significant VO admin functionality issues in IAM have been resolved • User registration, group and role management have been switched to IAM • IAM services are sufficiently HA • CERN IAM team is sufficiently staffed • Remaining VOMS-Admin use cases have been moved or will be dropped		IAM devs, CERN IT, experiments
M.4	Mar 2023	HTCondor installations at EGI sites have been upgraded to supported versions > 9.0.x. Prerequisites: • DIRAC versions supporting job submission tokens have been deployed for the concerned VOs (LHCb, Belle-II, EGI catch-all, …) • HTCondor CE supports (adjusted) EGI Check-in tokens • IAM or equivalent in production for ALICE, LHCb, Belle-II, …	M.1 M.2	HTCondor Dev Team, WLCG ops, EGI ops, sites

• • •

Science and Technology Facilities Council

Token Migration Discussion

- Shutdown of VOMs server – need to ensure that IAM can cope with the request rate
  - In particular, understand how High Availability IAM could affect request rates

- Plans to update test suites for use with different token issuers (for example CILogon) and service types

- Need for a small group to form a plan for migration for services. Francesco G. will lead this, with a subset from the AuthZ WG

Wider Community Support

- We should work out how to discover other communities beyond the “usual suspects” – CERN, INFN, IJCLab, IRIS - who are using IAM

- Implement a feature like Indico, to register instances into a "community platform" that allows to track production instances and the version they run, and include community links in deployment guidance

Future Plans

- 1-week Hackathon, likely CERN based, at the end of the winter
  - Timeframe intended to suit CERN’s ongoing recruitment for IAM team

- This should include a workshop day to engage with user communities as well

Summary

- A productive meeting with *lots* of varied discussions – thank you to all who attended, both in person and remote
- Aim to publish minutes (that aren't my janky notes) next week
- Recordings will be available on the agenda page also
- IAM has a range of established deployments, and building the community aspects here will be important!

Science and Technology Facilities Council

Science and
Technology
Facilities Council

Questions?

UKRI Science and Technology Facilities Council

Thank you

Science and Technology Facilities Council @STFC_Matters Science and Technology Facilities Council