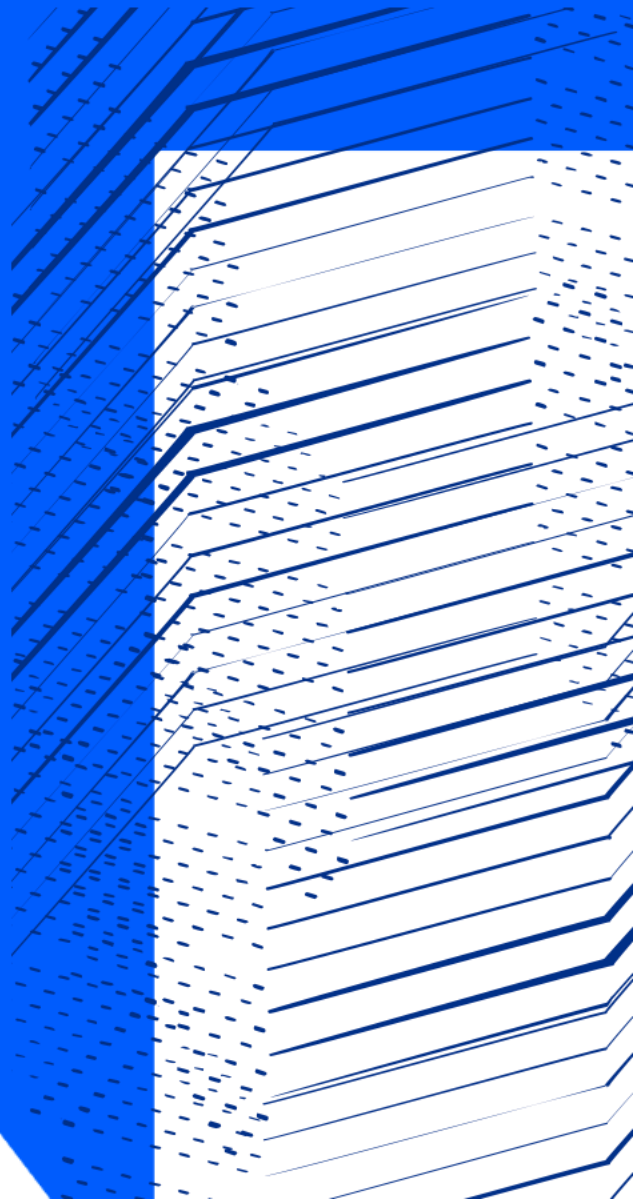
Image © STFC Alan Ford

Report on the INDIGO IAM Users Workshop

GDB 10/03/21

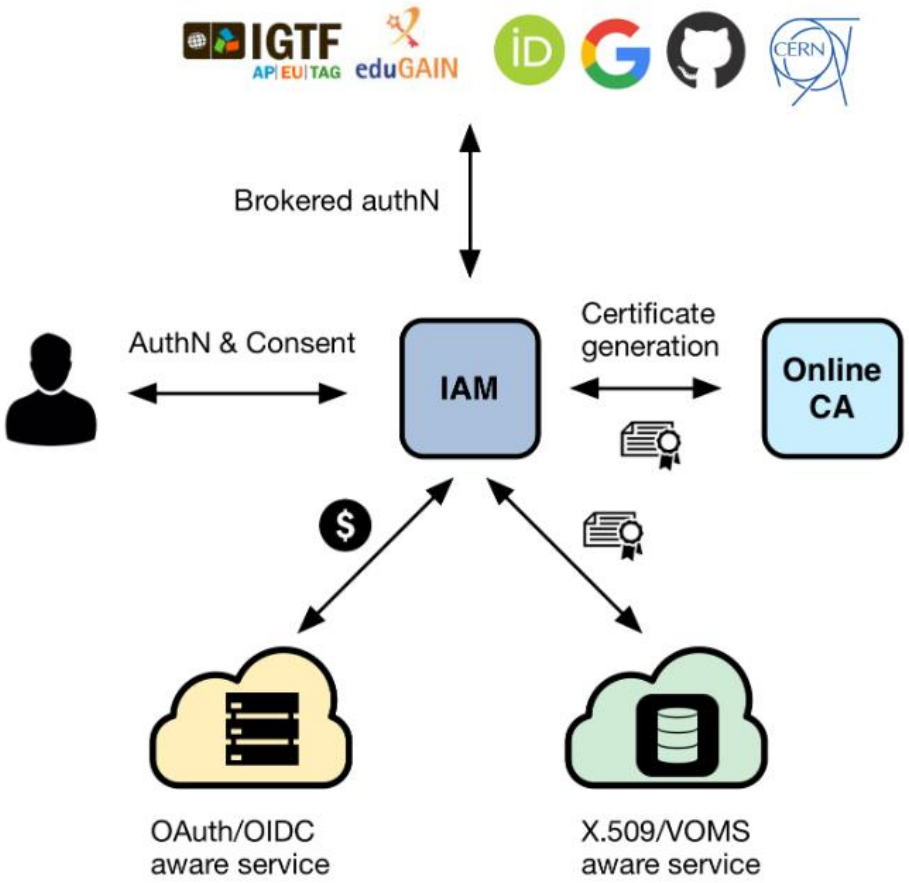
Tom Dack



INDIGO Identity and Access Management Service

A **VO-scoped** authentication and authorization service that

- supports **multiple authentication mechanisms**
- provides users with a **persistent, VO-scoped** identifier
- exposes **identity information**, **attributes** and **capabilities** to services via **JWT** tokens and standard **OAuth & OpenID Connect** protocols
- can integrate existing **VOMS**-aware services
- supports **Web** and **non-Web access**, **delegation** and **token renewal**



Science and Technology Facilities Council

Why INDIGO IAM is Important for WLCG

- IAM acts as the token issuer in the ongoing move to tokens for WLCG
- Adoption within other communities ensures support and development
- Lessons may be learnt from integration done by other deployments

INDIGO IAM Users Workshop

- Workshop took place on 27-28th Jan 2021
- Hosted talks from a range of institutions/organisations
  - INDIGO IAM administrators
  - IAM client services
- Dedicated timeslots to facilitate discussion

- All slides are available at:
  - https://indico.cern.ch/event/970568/

Science and Technology Facilities Council

- 78 Registered Attendees
- Attendees from a range of institutions:
  - CERN
  - CNAF/INFN
  - Czech Technical University
  - DESY
  - DiRAC
  - Durham University
  - European Gravitational Observatory
  - Fermilab
  - IJCLAB- CNRS -Université Paris-Saclay
  - IRIS
  - ISIS - STFC
  - Nikhef
  - PIC
  - STFC
  - Square Kilometre Array
  - … and more

Overview of Talks

And Key Discussion Takeaways

Deployment Focused: Day 1

- INDIGO IAM: Development Update and overview

  Andrea Ceccanti

  - Overview of IAM deployment strategies
  - Information on v1.7.0 release, including:
    - Attribute API & Dashboard
    - Group Membership Expirations
    - Scope Policy API
  - Overview of IAM NG and Keycloak

  Discussion:

  - Extended group management capabilities
  - Greater control for admins to monitor and suspend users or clients based on a central source of information
  - Usage of custom user attributes

Deployment Focused: Day 1

- Managing multiple IAM deployments on Kubernetes @ INFN-CNAF
  Andrea Ceccanti & Cristina Duma
  - ~20 instances ran by INFN all on Kubernetes
  - Overview of deployment and configuration

- The INFN Cloud AAI: how IAM supports INFN Cloud use cases
  Marica Antonacci
  - IAM is used to provide access to resources and services
  - IAM integrated with OpenStack, Apache Mesos, Kubernetes, HashiCorp Vault

- IAM Adoption at WLCG
  Hannah Short
  - Overview of move to tokens, AAI design and claims schema
  - Integration with CERN DB and Certificates

Deployment Focused: Day 1

- IRIS IAM: An Overview
  Tom Dack
  - Introduction to IRIS and why the IAM is needed
  - IRIS architecture compared to the AARC Blueprint

- Accessing SSH Resources using IRIS IAM
  Will Furnell
  - https://github.com/stfc/pam_oauth2_device
  - PAM module implementing OIDC device flow
  - Can check authorization via IAM groups

- IRIS Trust Framework and Operational Security
  David Crooks
  - Establish the necessary policies to allow interoperation between resource providers, services and user groups - Utilising AARC Policy Development Kit
  - A number of these policies are directly influenced by IAM capabilities
  - Explanation of Operational Security Work

Client Focused: Day 2

- GOCDB integration with IAM

  Greg Corbett & Sarah Byrne
  - GOCDB IAM Integration allows user account and API access via IAM
  - Authorization via IAM Groups, Token info populates new GOCDB accounts

- The IRIS Accounting Dashboard and IAM

  Adrian Coveney
  - Move from a single shared user account to accounts created on login via IAM
  - Integration with Grafana, future work to allow more granular AuthZ

- GlideinWMS and IAM

  Marco Mambelli
  - Utilise IAM for pilot submission to resources
  - Tokens requested from WLCG IAM via OIDC Agent

Client Focused: Day 2

- A platform for heterogeneous data processing: how IAM supports the PLANET project (**P**ollution **L**ake **AN**alysis for **E**ffective **T**herapy)
  Diego Ciangottini
  - Multidisciplinary project focussing on the comprehension of the effective role of pollution in Covid-19 Pandemic.
  - IAM provides users with a single entry point, including data and compute infrastructure
  - Plan to expand to allow batch systems to manage tokens on a users behalf to access data

- IRIS DynaFed: IAM-integrated Echo Storage
  Sam Glendenning
  - S3 data storage integrated with IAM using DynaFed – bucket access depends on groups
  - Easy to import and remove Echo buckets and assign access to groups you belong to
  - General users do not need knowledge of bucket keys

Client Focused: Day 2

- IAM @ INFN-T1
  Lucia Morganti
  - Utilises both a “Catch-all” instance with users controlled via groups and dedicated instances for larger experiments or specific requirements
  - Storage integration via StoRM WebDAV – both browser and command line

- IAM and the INFN Cultural Heritage Network (CHNet) use cases
  F. Giacomini, L. dell’Agnello
  - IAM provides access to data repository and services to non-INFN users
  - Planned implementation of fine access control, and tokens passed upstream

- JupyterHub & IAM Integration
  Rohini Joshi
  - Access to SKA IRIS/ESCAPE JupyterHub controlled via relevant IAM instances
  - Currently used for authentication more than authorization
  - Plans to check IAM groups to correspond to varying levels of access

Thoughts on the Workshop

- Extremely well attended,
  - Excellent representation, with key communities and contributors present

- Received positive feedback from attendees, speakers, and IAM development team
  - Request for a central location for documentation, use-cases, examples
  - Comment that a fourum/mailing list would be useful
  - Helped identify use-cases development team weren't aware of

- Has had positive outputs, eg:
  - Discussion of centralised suspension at WLCG AuthZ WG
  - New communities taking up using DynaFed & IAM

Next Steps

- Google Group has been made to facilitate ongoing discussions:
  - https://groups.google.com/g/indigo-iam-users
  - Potential for moving to Discourse in the future, if required

- Plan for another workshop ~6 months after first
  - Shorter format
  - Potentially hosted alongside a relevant meeting
    - Any Synergy between this and WLCG plans?

Science and Technology Facilities Council

Questions?

https://groups.google.com/g/indigo-iam-users

UKRI Science and Technology Facilities Council

Thank you

Science and Technology Facilities Council @STFC_matters Science and Technology Facilities Council