FIM Meetings Summary

Presented by David Crooks (STFC-RAL)

Slides by Hannah Short (CERN)

Fall HEPiX 2019, Amsterdam

Recent Meetings

- September 10th: pre-GDB
  - WLCG Authorization Working Group F-2-F
  - Workshop with Fermilab, DUNE and WLCG with AAI exercises
- September 12th: mini-FIM4R
  - Fermilab, Argonne, Brookhaven, DUNE, WLCG, IRIS + CiLogon, Indigo IAM, Internet2

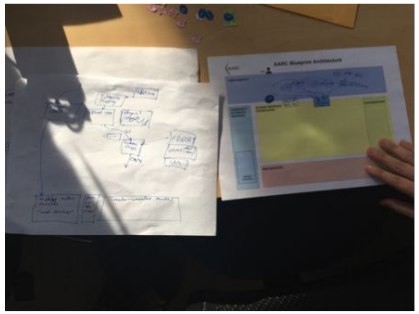
Both held at Fermilab (thank you!). Colocated with the GDB, which attracted a highly relevant list of participants.

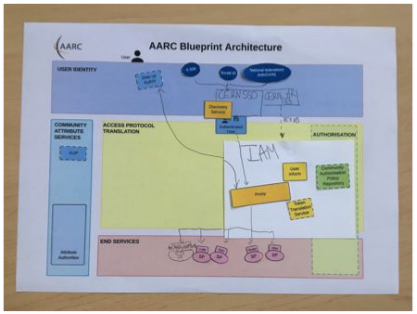
pre-GDB

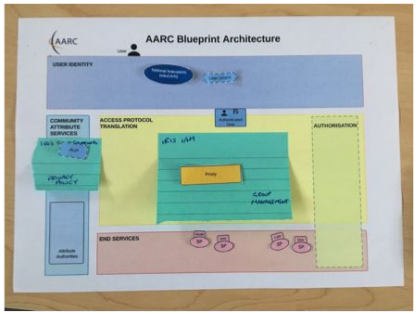
- WLCG Authorization WG F-2-F
  - WLCG Token Schema v1.0 published
  - Discussed Token Issuer to be set up at INFN to facilitate Token integration in middleware

pre-GDB

- Presentations on Indigo IAM (WLCG's chosen AAI*) and SciTokens and IAM interoperability
- Exercise to map out Identity Federation plans following the AARC Blueprint Architecture







*Authentication and Authorization Infrastructure

mini-FIM4R

- mini-FIM4R* held at Fermilab, September 12th
  - Focus on physics communities and grid users
  - Much discussion on backwards compatibility with x.509
  - Internet2/Incommon (US Identity Federation) participation provided helpful input for US laboratories/projects

Research Communities

- WLCG
- DUNE
- Iris (UK)

Labs

- CERN
- Fermilab
- Argonne Labs
- Brookhaven National Lab

Technology

- CiLogon
- Indigo IAM

* FIM4R workshops usually include a much wider set of Research Fields

Key Outcomes

- Improved understanding of chosen technologies (OAuth, SciTokens, IAM…)
- Resolution of several ongoing challenges regarding IOTA X.509 certificate trust
  - Fermilab/DUNE
- Excellent opportunity to build connections between FIM representatives from different labs/experiments

Topics for Continuation

- Combined assurance
- Trust fabric of OIDC/OAuth
- Guidance on Token Flows
- OAuth Challenges
- Additional attribute collection

Combined Assurance

- Although combining low assurance certificates with high assurance VOs works technically, policy level is more complicated
- Assessment of identity proofing being addressed by **IGTF** and **JSPG**
- Aim to keep VO effort to a minimum

Trust Fabric of OIDC/OAuth

- Now possible to separate transport/encryption from token signing
- What level of assurance required for each component?
- How to distribute trust anchors?
- Discussed in **EUGridPMA**
- Call of **WLCG AuthZ WG** yesterday

Trust Fabric of OIDC/OAuth

- OIDC Federation
- Role of IGTF
- OIDC Certificates and Keys

OIDC Certificates and Keys

- Transport cert
  - Must be publicly trusted
  - Opportunity to make life easier for integrators (e.g. LetsEncrypt)
- Signing certs
  - Discovery and distribution well described by standards
  - Lifetimes defined by WLCG Token Schema v1.0
- VOs will need to maintain lists of valid token issuers
- Global list may be useful for opportunistic resources

Guidance on Token Flows

- DOMA WG will continue to run tests and prototypes in conjunction with the AuthZ WG
- **WLCG AuthZ WG** to produce guidelines based on workable models

OAuth Challenges

Challenge 1: Acquire a token from IAM via OAuth2 and use it to upload files to dCache and XRootD.

Challenge 2: Acquire a token from IAM via OAuth2 and use it to submit a pilot job.

Challenge 3: Have the HTCondor "credmon" acting as an OAuth2 client acquire a token from IAM, send the token along with a job, and have the job stage out to dCache.

Challenge 4: Author a whitepaper describing how our community plans to use tokens for data management – including Rucio, FTS, IAM, XRootD, dCache, and others.

Plus...

- Traceability challenge
- Multi-tenancy token issuer model

Additional Attribute Collection

- Implementing federated identity means separating Authentication from Authorisation
- Care must be taken on which attributes are collected and shared
- VOs may have to play a larger role in collection of Authorisation data
- In discussion in **JSPG**

Next Steps

- Discussions to continue in IGTF, EUGridPMA, WLCG AuthZ WG, JSPG

- Meeting concluded early due to Tornado warning :)

Side step:
SLATE Security WG

SLATE Security WG

- Additional pre-GDB on SLATE Security WG
- SLATE: **S**ervices **L**ayer **A**t **T**he **E**dge
  - Federated containerised service deployment
  - See Shawn's talk on Friday
- Opportunity to address security aspects and requirements with key stakeholders

Key outcomes

- Agreement of charter and co-chairs
  - Rob Gardner and Romain Wartel
- Plan to continue discussions during NSF Cybersecurity Summit in San Diego this week
- This is a new trust ecosystem
  - Policies and best practices will need updating (work for the WLCG WG)

Appendix

Additional slides with group background and links

HEPiX AAI List

- Established in October 2018
  https://listserv.in2p3.fr/cgi-bin/wa?SUBED1=hepix-aai
- Kickoff call in November 2018
- Invitation to join mini-FIM4R meeting in September 2019

WLCG Authorization WG

- Objective: Understand & meet the requirements of a future-looking AuthZ service for WLCG experiments
  - JWT Token Schema for WLCG OAuth2/OIDC usage
  - Identified Indigo IAM as future Membership Management Tool and Token Issuer
- Join e-group project-lcg-authz@cern.ch
- https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG

FIM4R

- Federated Identity Management for Research
- Long-standing community, several hundred people, ~ 2 F-2-F meetings per year
- Next meeting December 8th in New Orleans (Internet2's TechEx)
- https://fim4r.org
- Join e-group fim4r-members@cern.ch or email contact@fim4r.org to be added