Trust Framework Meeting Notes

Location:

- Online
- Monday 25th March 2024
- 16.00-18.00 CET
- Zoom Link

Straw-dog Doc:

https://docs.google.com/document/d/1EzR7Ao9Gpbc7StQw-5QkhP6TcQRrKUCzkWXzdc8UeM4

Agenda:

1. Explain the focus of the workshop
    a. Identify main topics
    b. Consolidate document to a roadmap draft
2. (Depending on the number of attendees a round table)
3. OSCARS
4. Review of the straw-dog proposal/roadmap
5. AARC Project https://aarc-project.eu/about/
6. Identification of topics
7. Identification of contact persons and potential leads
8. Summary
    a. AA and next steps

Note: As the meeting is 2 hours we propose a ~10 min break at the 1 hour maker.

Notes:

1. (outline agenda)
2. too many of us :-) Gareth Hughes (CTAO), Rosie Bolton (SKAO), Xavi Espinal (CERN), David Crooks (STFC UK), Enrique Garcia (CERN), Jutta Schnabel (km3net), Cristiano Bozza (KM3NeT), Sara Bertocco (INAF), Francesco Giacomini (INFN), Federica Agostini (INFN), Marjolein Verkouter (JIVE), Matthias Fuessling (CTAO), Jens Jensen (SKAO)
3. OSCARS:

ID potential items for Cascading grant
Limited in time and money 100-200 keuro 1-2 years
Prototype for future calls
Portfolio cards span into the grants

4: Document review, notes in document

Common Understanding:

- Cristiano Bozza: ID should come from RIs. e.g. User will have multiple identities.
- Rosie Bolton: We should have a **common understanding of architecture**. Framework and model should be the aim.
- Francesco Giacomini: Distinction between identity and authorization
- David Crooks: Establish morals for how we work together. How this relates to AARC or complimentary to. Cyber Security should take a risk based approach. How do you secure things?
- **Not aiming to *build* a common service, but to develop a model and tools to enable alignment.**

What ESFRIs are doing:

- **CTAO**/ Gareth: Ramping up AAI, but a little behind. Experience of Indigo IAM from ESCAPE. Need to consider data protection and access control. Sites across several countries. A zoo of functionality.
- Cristiano/ **KM3NeT**: Also need to consider having people move institutes. Need to keep a central database of identities, but the sense is that moving to an institute is hard.
- Sara Bertocco: Yes, also if the same person is part of multiple ESFRIs (?)
- David Crooks: Consider where we hold information about people and why
- Rosie Bolton: **SKA** RC prototype IAM service, next step deploy Attribute Authority.
    - Who issues the token? The **IAM.**

User Information:

- Gareth: PI access, proprietary period, overlapping groups. Limitations of IAM - some info that wouldn't want to store on IAM but instead on AA (so ESFRI has complete control)

Indigo-IAM:

- Rosie Bolton: Does IAM have limit on the # of grps?
- Francesco Giacomini: Potentially HW limitations. But what are the limitations of the model?
- Rosie Bolton: Limitation on number of groups when requesting a token? Character limit?
- Federica Agostini: v1.8.2 there was an issue this has now been fixed.
- Francesco Giacomini: 1 MB http header limit on information. There are ways around - not IAM specific.

Levels of Assurance:

- Cristiano Bozza: in another experiment (not KM3NeT), had to register some people just using their name, so possibility of name clashing. Need proper identification, understanding of certification chain for users.

- Francesco: can keep and **propagate level of assurance within tokens**. New account needs validation with VO admins
- Jutta Schnabel: Flat auth procedure in/out. Important in the future to have a lightweight account. Another layer that would promote a user to a higher level.
- David Crooks: Level of assurance ….

Higher-level Use Cases:

- Rosie Bolton: SKAO will have control over its AAI and resources - multi wavelength / multi ESFRI support comes later. Multi ESFRI data analysis?
- Gareth Hughes: UCs for MW/MM
- Matthias Füßling: MM MWL agree. Sharing UCs and finding common solutions.
- Agree need to identify use cases in a consistent way

IAM Wishlist:

- Rosie Bolton: IAM question, is there a wish list. Common ESFRI topics. Big topics?
- Federica Agostini: List of requests of issues and questions. e.g. Level of assurance is in the roadmap. A list of topics would be useful.
- Examples / best practice / set up support from IAM community to help ESFRIs make good use of IAM
- Jens Jensen: SKAO use cases could be made available.
- Rosie Bolton: **IAM-ESCAPE interface manager**? Someone to support deployment of IAM at ESCAPE ESFRIs?
-

Access Control:

- Matthias Füßling: Access control, where does this happen?
- Rosie Bolton: Well defined API to link things together. use of services / data via permissions API

Advert:

- Enrique Garcia: Could someone come to the meeting tomorrow.
    - (https://indico.cern.ch/event/1393398/ between 1300 and 1500 CET)

Cross-Cluster Auth:

- Marjolein Verkouter: Scaling of authorization from ESFRI level to Cluster level.
- Rosie Bolton: Cross Cluster authorization?
- Jens Jensen: Complexity should be hidden from the user. Issue of multiple authorities.
- David: 2 aspects. 1st AAI model level of assurance e.g MFA. 2nd How do we approach CS in the model of across the Cluster. What should be done and by whom? Would be worth looking at what else is out there.

Data Protection:

- Gareth Hughes: Data Protection / GDPR: common approaches for best practice to support appropriate sharing (and protection) of data.

Action Items:

- Use Case collection and sharing, including use case selection method.
- Friday 25th March: Attendees fill out the portfolio cards. 5 days.
- Friday 29th March: Make notes “public” to ESFRIs/RIs to comment, sign-up to contribute or lead and rank projects. ~1 week.
- April 8th consolidate projects and follow-up.

Project Cards

Summary	[AAI]:IAM-Cluster Interface Management Lead(s): Interest: Gareth
Benefit Hypothesis	Indigo-IAM has been identified as a key component for many ERI’s AAI systems. ERIs have overlapping use cases and needs. Working with CNAF/Indigo-IAM through a single interface will increase efficiency and target key priorities.
Description and target outcomes	A person(s) who would act as a coordinator between the ESCAPE collaboration and Indigo-IAM. Collecting user stories, use cases and ERI AAI infrastructure, identifying missing technology. Working with and coordinating groups within the RIs and CNAF to implement the most important of these technologies.
Priority value	[weighted sum of priority from ESCAPE ESFRIs]
Sizing estimate	[how many person months]
Skills needed	[what competencies does someone need to have to undertake this work]

Summary	[AAI]:Propagation of Levels of Trust Lead(s): Interest: Volodymyr
Benefit	Advanced/Future Use Cases imagine ERIs users being able to conduct an

Hypothesis	analysis with data from multiple experiments. If users are on boarded via their ERIs this level of trust will have to be propagated to all members of the cluster.
Description and target outcomes	Identify the methods by which users are on-boarded into specific ERIs. Validation methods may vary depending on the experiment or type of user. This level of assurance needs to be present to other experiments. Identify and implement a token based method to transmit this information.
Priority value	[weighted sum of priority from ESCAPE ESFRIs]
Sizing estimate	[how many person months]
Skills needed	[what competencies does someone need to have to undertake this work]

Summary	[AAI]: Common ESCAPE/ERI User Model Lead(s): Interest: Gareth, Cristiano
Benefit Hypothesis	In order for ERIs to work together a Common User Model could/should be adopted by all ERIs. This would reduce development work both for the ERIs internally but also for any interface work.
Description and target outcomes	Collect user model information and requirements from ERIs. Develop a model that incorporates this information. Promote its adoption as a standard across the cluster.
Priority value	[weighted sum of priority from ESCAPE ESFRIs]
Sizing estimate	[how many person months]
Skills needed	[what competencies does someone need to have to undertake this work]

Summary	[AAI]: Multiwavelength / Multimessenger Use Cases Lead(s): Interest: Volodymyr
Benefit Hypothesis	Ability to work on Multiwavelength and/or Multimessenger projects by being able to access data seamlessly across ERIs.
Description and target	[additional context for this and what we want to enable - focussing on what needs to be enabled rather than on how to enable it]

outcomes	
Priority value	[weighted sum of priority from ESCAPE ESFRIs]
Sizing estimate	[how many person months]
Skills needed	[what competencies does someone need to have to undertake this work]

Summary	[AAI]: IAM-dCache Interface Lead(s): Interest: Gareth, Volodymyr
Benefit Hypothesis	The ability of ERIs to easily interface dCache storage with Indigo-IAM. Storage could then be made available via Science Platforms or Data Lake technologies to users of ERIs via their AAI systems. Would also allow for fine-grained authorization.
Description and target outcomes	Ability to access data stored on a dCache instance using a token from an IAM instance. The ability to embargo or limit data access based on user/token information.
Priority value	[weighted sum of priority from ESCAPE ESFRIs]
Sizing estimate	[how many person months]
Skills needed	[what competencies does someone need to have to undertake this work]

Summary	[AAI]: User Management Tools Lead(s): Interest: Gareth, Cristiano, Volodymyr
Benefit Hypothesis	Standardize user management across ERIs. Allows for easy adoption and development.
Description and target outcomes	Develop a set of tools that allow ERIs to manage their users, groups and clients. Interface with Indigo-IAM APIs.
Priority value	[weighted sum of priority from ESCAPE ESFRIs]
Sizing estimate	[how many person months]

Skills needed	[what competencies does someone need to have to undertake this work]

Template for Portfolio cards:

Summary	[workpackage]:[name of this card] Lead(s):
Benefit Hypothesis	[why do we need to solve this?, who benefits - which ESFRIs can confirm they would benefit]
Description and target outcomes	[additional context for this and what we want to enable - focussing on what needs to be enabled rather than on how to enable it]
Priority value	[weighted sum of priority from ESCAPE ESFRIs]
Sizing estimate	[how many person months]
Skills needed	[what competencies does someone need to have to undertake this work]