Joint Actions in AAI

Andrea Ceccanti (INFN)

ESCAPE Progress Meeting Bruxelles

February, 26/2/2020

Joint actions on AAI

- A clear definition of the AAI-related requirements from the technical WPs is needed

    - How do we tackle this? Do we need a cross-WP dedicated AAI task force?

    - We can start by focusing on secure data access/management, i.e. on the interface between WP2 and other technical WPs

    - Set up AAI dedicated communications channels?

        - We already have an AAI channel on the ESCAPE Rocket Chat

- Training and knowledge sharing is another key topic

    - Task 2.5 will organize a training event/webinar on OAuth/OpenID Connect/IAM and the Data lake AAI (i.e. the WLCG token-based AA approach)

    - We'll then have a WP5-WP2 hackathon to enable integration between the ESAP and IAM. Objective: enable authenticated access to the data lake from the ESAP

    - It's not clear to me if the CEVO will interact directly with the Data lake, but we could have a similar WP2/WP4 hackathon if needed

    - I see that CEVO has done a lot of work on SSO and X509- based credential delegation: we could have knowledge sharing sessions to discuss approaches and find common ground (e.g., on token-based delegation, which is of key importance also for WLCG)

Understand key AAI requirements

- How are users and agents authenticated?

- What's the authorization model? What's the delegation model? How are authorization privileges and policies managed?

- What are the legacy AuhtN/AuthZ mechanisms that must be supported?

- What are the key software components that needs to be integrated?

- Does the integration require changes in the software or just changes in its configuration?

Identify integration use case

- Objective: demonstrate controlled access to ESCAPE high level services and data

- Covering the "full" ESCAPE stack

  - DIOS, OSSR, ESAP, CEVO (or selected subsets)

- Identify AAI showstoppers, understand authN/Z flows

Thanks for your attention. Questions?