AARC2 EISCAT_3D pilot
Authentication and Authorisation for Research and Collaboration

Ingemar Häggström
EISCAT Scientific Association
+ Arnout, Niels, Mario, Matteo, Jouke, Ioannis, Carl-Fredrik

13th FIM4R Workshop
11 February 2019, Vienna
EISCAT/EISCAT_3D

- Large radar facilities in Tromsø (NO), Longyearbyen (SJ), Kiruna (SE), Sodankylä (FI)
  - 1981-
  - Space Physics
  - Plasma Physics (with HF heater)
  - Campaign/event based

- EISCAT_3D
  - 85% of Stage1 budget, 56M€
    - Implementation started 1 Sep 2017
  - ESFRI landmark 2018
  - Geospace Environment
  - Radar to run 24/7
User categories

• Services for Users
  – Data + Processing
    • Users
    • Associate (RC, country), >1000
      – Affiliate (institute), >100
      – 3P (individual), >1
      – Staff, ~10
    – Other, >10000
    • Some data have embargo times
      – 1yr, 4yrs according to membership
    • (non military/commercial use)
  – Operation
    • Request (member..), ~100
    • Expert (selected users), ~10
    • Wizards, ~3
    • Machine (predefined APIs), ~10
Current EISCAT portal, python cgi

- **Portal**
  - Metadata, public
  - No login

- **Schedule (Operation)**
  - Request (cgi)
    - Manually scheduled

- **Data selection**
  - Check IP
    - Basically whois → country
    - Lists for affiliates, staff, individuals
  - Link to data (separate) server
    - Makes same IP check
  - Processing at EISCAT
    - cgi making task lists
EISCAT_3D pilot data server

- Keycloak proxy
  - + qq idp
- Portal
  - SAML
  - AuthZ layer
  - Create JWT token
- Data server
  - Token in url
  - Time/Usage limited
- Logging
EISCAT_3D pilot data server

- Exchanged and Tracked information
  - The system will track relevant information to uniquely identify a user and a transaction, together with providing hooks for logging / accounting/

- Tracked (logged) on the Master Portal
  - Consumed Data by the Master Portal
  - Produced Data on the Master Portal
  - Received Data by the Master Portal
  - Sent Data from the Master Portal to the Data Server
    - TransactionID
      - Hashed (userID+timestamp)
    - Download URL

- Received by the Data Server
  - Token including the transactionID

- Tracked on the Data Server
Implementations

- Describe agreed architecture
- Set up common GIT repo
- Reproduce current EISCAT environment in Docker
- Identify relevant code bits to be modified on the Master Portal
- Set up SP to protect Master Portal and allow for SAML based AuthN/Z
- Set up the IDP in the test env
- Implement script from the Data Server side to handle tokens generated on the portal
- Implement token generation based on user idp-released attributes
- Keycloak setup and config
- Test of consistency and basic testing between the token server-client sides (Portal to Data Server)
- Final test of pilot set up
- Report on testing
Sustainability

- EISCAT_3D to run for >30 years
  - EISCAT staff to maintain services
  - Associates to continue DataBase

- EISCAT_3D
  - First 5 years
    - EOSC portal
      - EISCAT services
      - (eInfra data/processing services)
    - Cost issue
  - With extra funding (updates)
    - Much more data
    - May move services to eInfras
Thank you
Any Questions?

Ingemar.Haggstrom@eiscat.se

https://aarc-project.eu