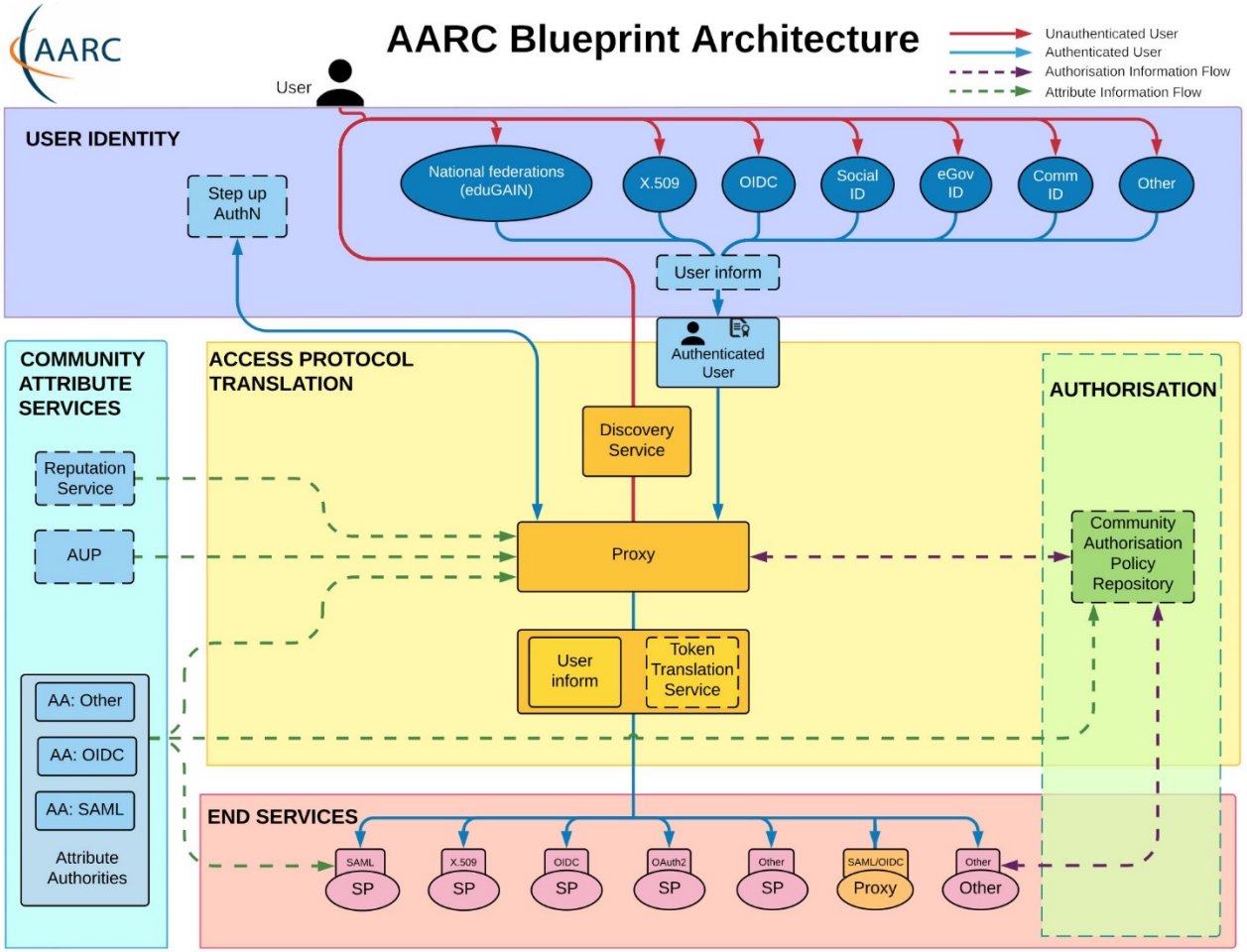
# SKAO AAI Report

19.07.2022

https://jira.skatelescope.org/browse/SPO-1893

# Architecture




Distilled by the AARC projects from >> 1 projects' FIM architectures

Like hub-and-spoke rather than full mesh – proxy *translates* protocols and *harmonises* attributes

aarc-community.org

# Principles

- Users are authenticated individually
  - No shared accounts
- Federated identity management
  - Users bring their own identities
  - Usually from the home organisation
- Understand the LoA
  - Sometimes low assurance identities are OK
- Authentication ≠ Authorisation
  - Authorisation normally linked to groups and roles (RBAC, ABAC)
  - Not to individual identities

# Principles

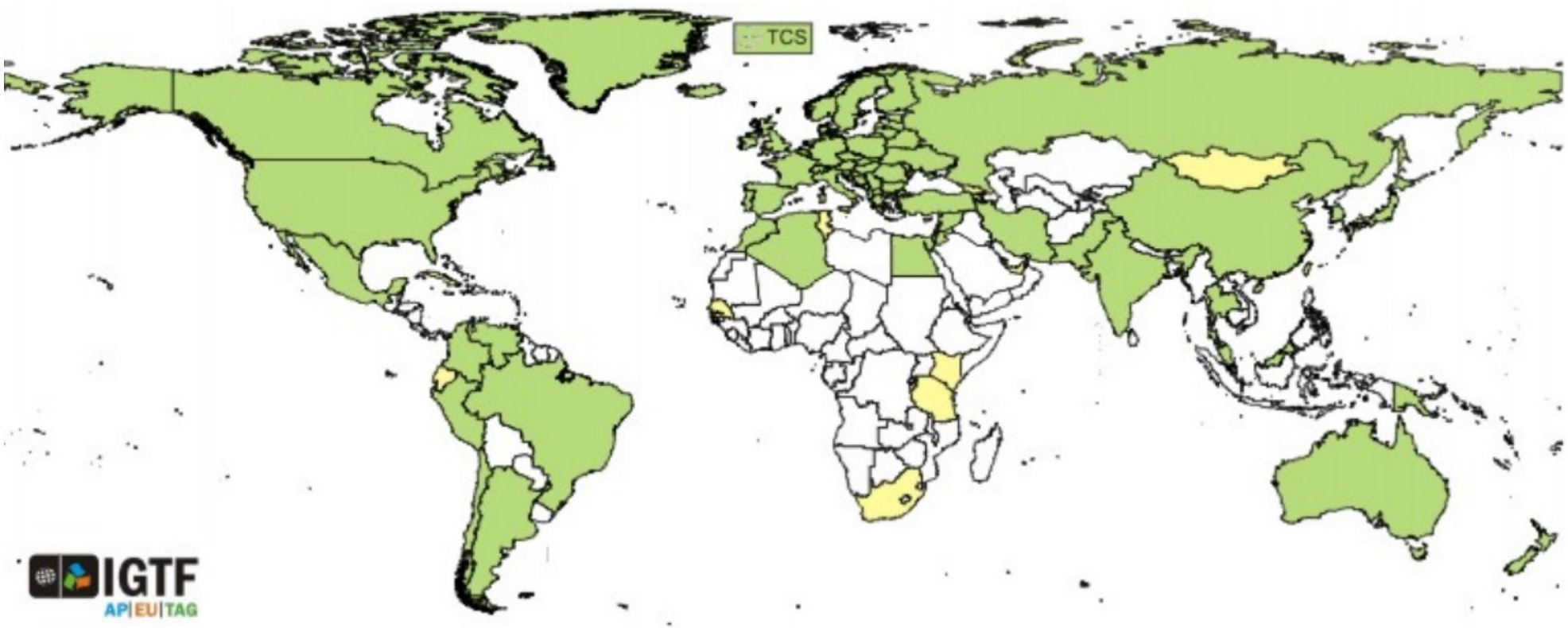
- Data protection and minimisation
  - IdPs publish a list of “necessary” attributes
  - SPs process only those that they need (for the purposes they need them)
  - Sometimes SPs can ask for more (“step up”)
  - SP guidance to proxy on selecting best IdP
- Usability
  - The classic Security ⇔ Usability question
  - Operational support
- Interoperation
  - Use of standards promote interoperation

# Principles

- Policy – building on Policy Development Kit
  - https://aarc-community.org/policies/policy-development-kit/
- WISE interoperation guidelines
- Policy documents are intentionally quite short and simple
- Technical interoperation “guidelines”
  - https://aarc-community.org/guidelines/
  - Ongoing development through “appint”
  - Approval through AEGIS

# Technology

- Trusted Infrastructure = security
  - Best practice is IGTF certificates (www.igtf.net)
    - IGTF covers all participating countries *except ZA which is not yet full member*
    - Not browser friendly for all countries – but free, and available in bulk, and high LoA



# Technology

- “We want token based authentication”
  - OAuth2 (RFC 6749) is an *authorisation* protocol
  - OIDC does not do federations very well
    - Though we are working on it (RandE and FastFed)
- The need for “delegated credentials”
  - Some things need to work without the user being present
  - Automated data transfers (beware credential timeout)
  - Credentials with workflows
  - Traditionally done with bearer tokens (RFC 6750) or GSI certs (RFC 3820)
- UKSRC IAM proxy prototype will be open to all (thru eduGAIN)

# The Landscape Report

Written by UKSRC but with contributions globally

- Overview
- Technology
- User stories
- International and National AAI
  - International includes eduGAIN and eduTeams (GEANT)
  - Every SKA country has IdPs in eduGAIN
  - National AAI = national identity federations run by NRENs
- Open for comments/contributions
- https://confluence.skatelescope.org/display/SRCSC/Purple+Team%3A+Landscape+Report+Working+Page