Science & Technology
Facilities Council

Certificate Stuff

Jens Jensen, STFC

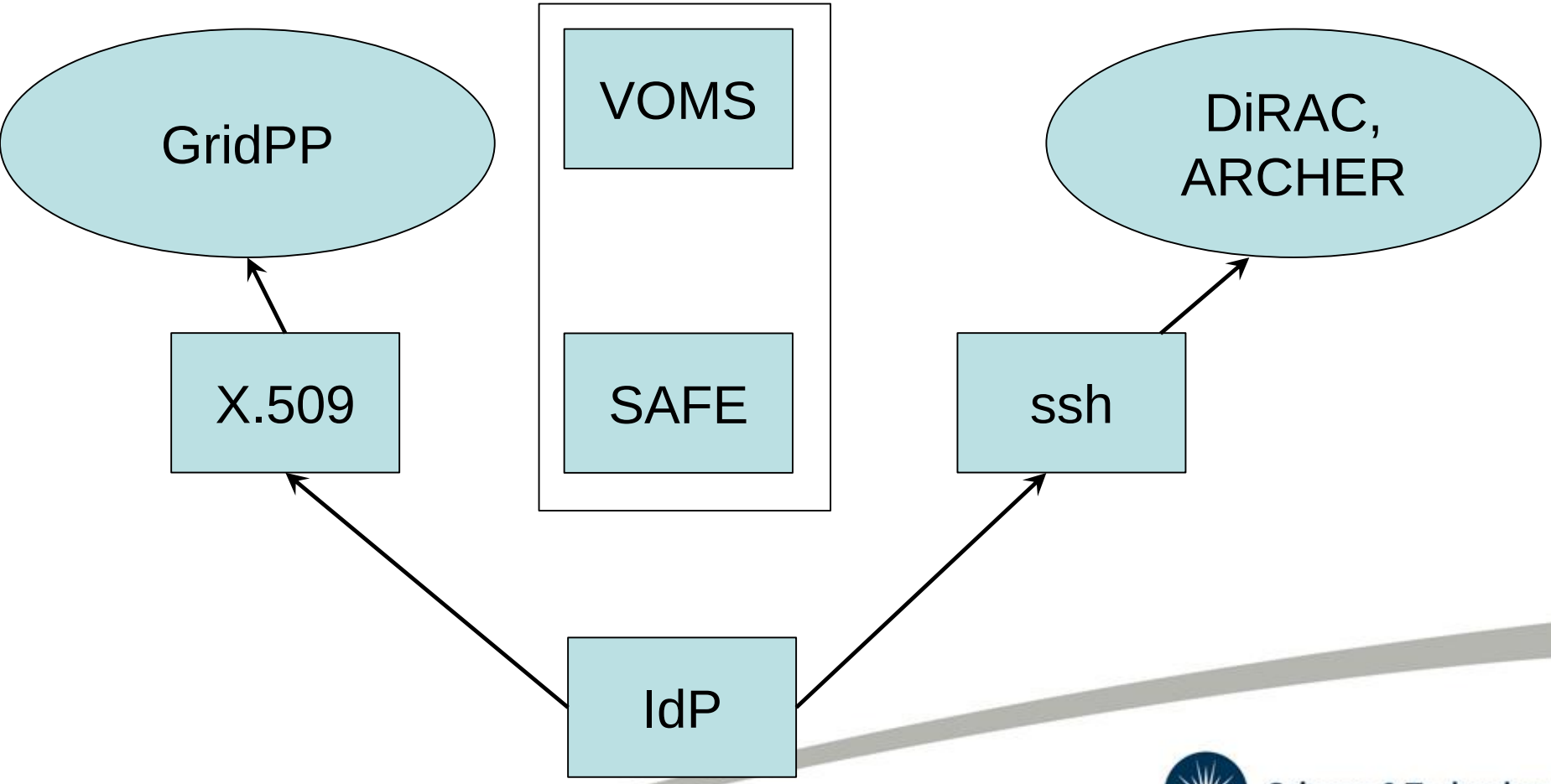
15 Sep. 2017

GridPP39, Lancaster

Contents

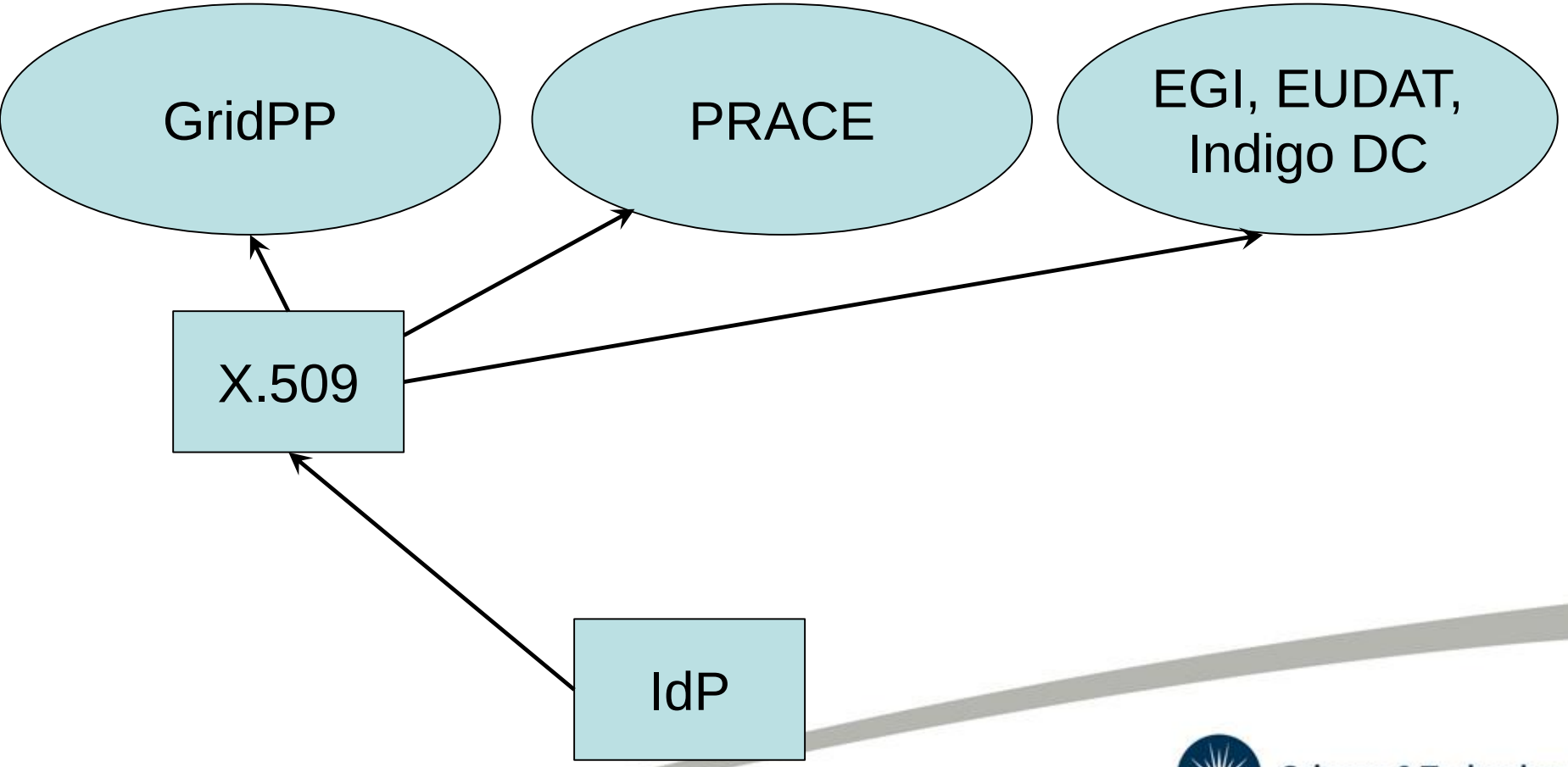
- AAAI Pathfinder
  - More bkg information in presentation to dteam
  - (Also attached to agenda)
- Multiple SANs
  - More information in talk at hepsysman
  - https://indico.cern.ch/event/592622/

AAAI Pathfinder

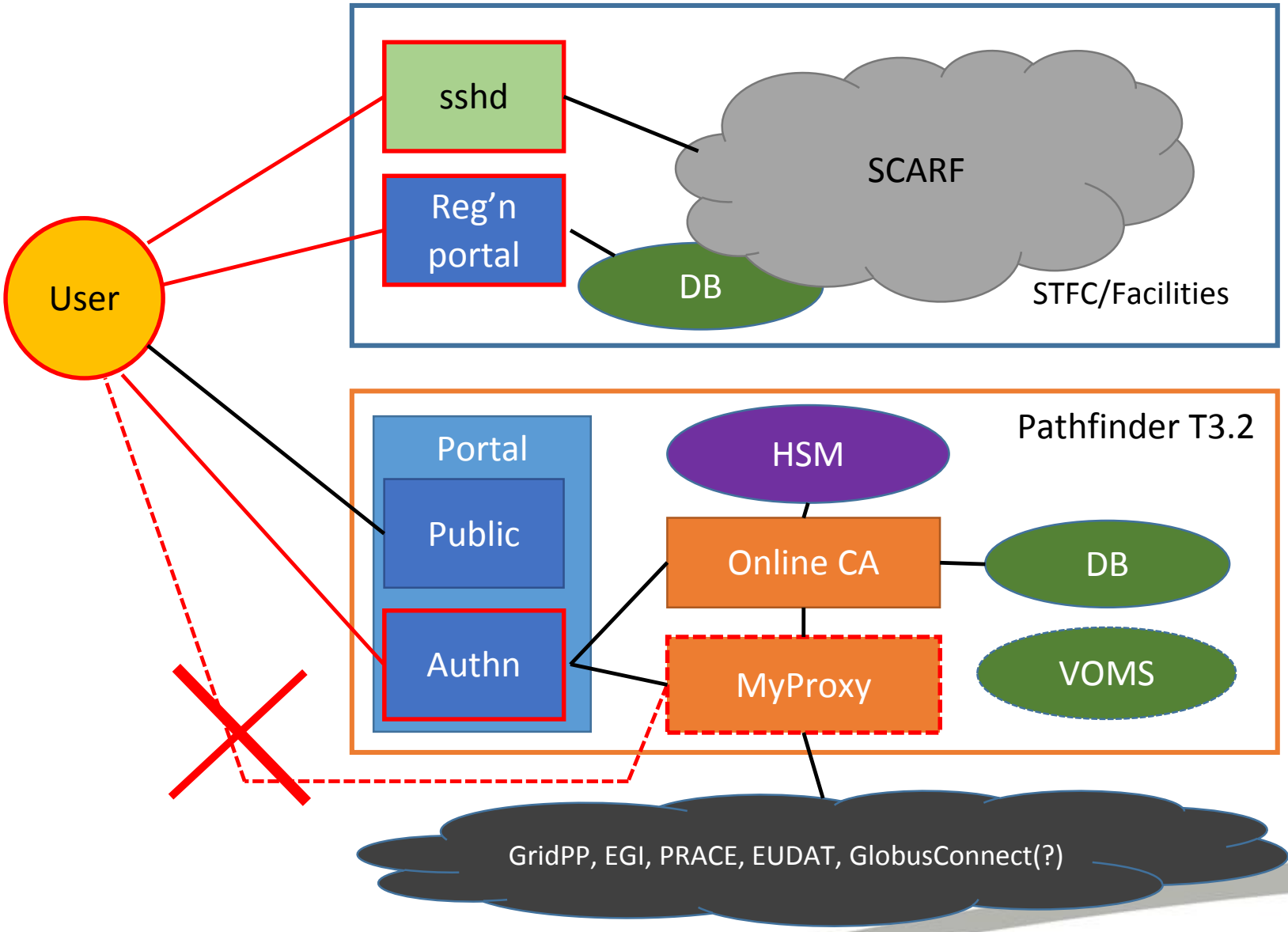


Science & Technology Facilities Council

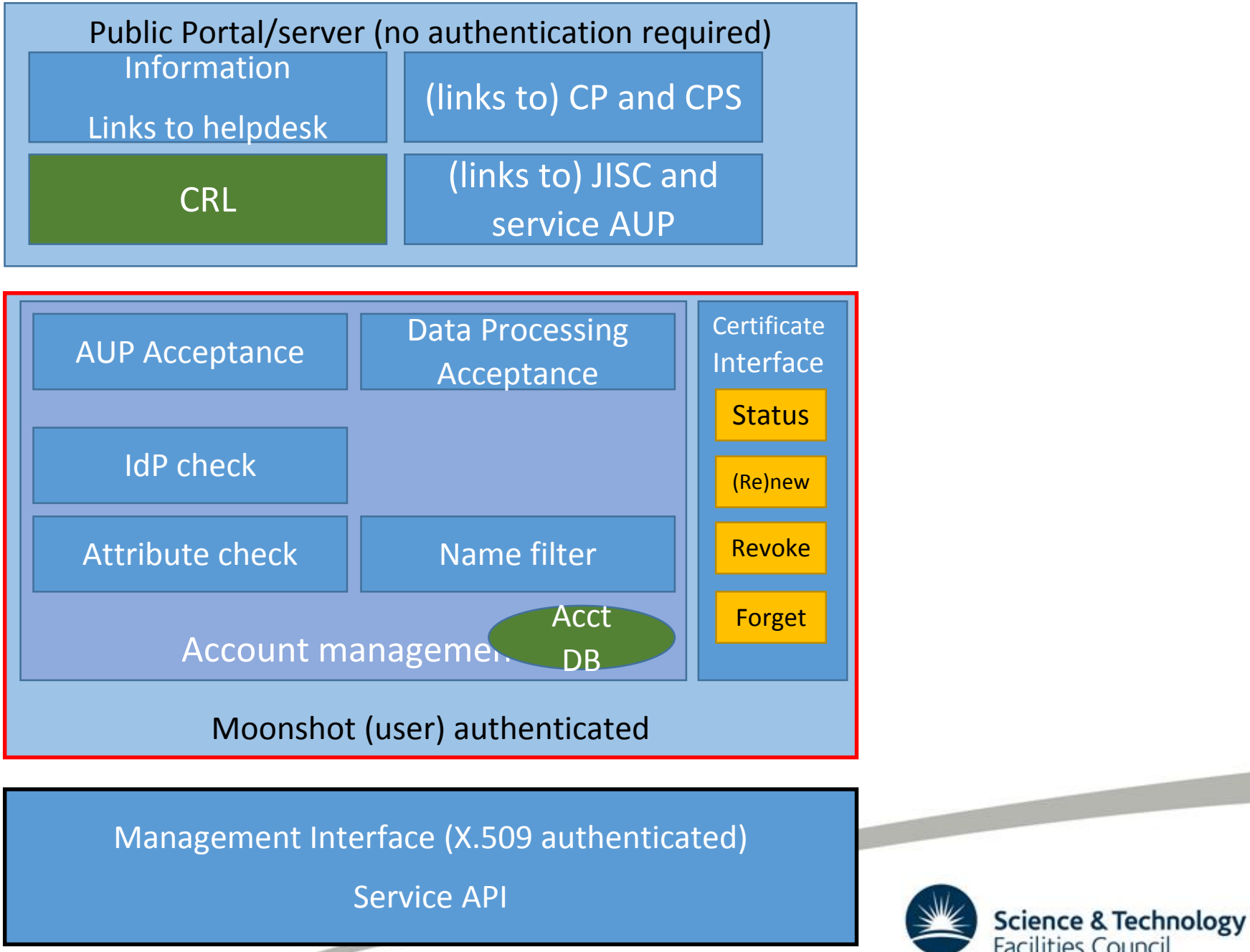
AAAI Pathfinder



Science & Technology Facilities Council



Science & Technology Facilities Council



Science & Technology Facilities Council

GridPP's participation

- Work with Suleman Tariq
- CA portal (user interface)
  - If you have an IdP in Assent, you can authenticate to https://pathfinder.stfc.ac.uk/moonshot/userreq.pl
- Not finished yet
  - You can't get a certificate (yet)
- Chose not to use the CTS code
  - No VOMS in interface; expecting attrs from Moonshot

Science & Technology Facilities Council

Visiony Stuff

- Single identity provided by home org.
  - Or a “homeless” org.
- Access to both web and non-web resources
- Chicken and egg takeup:
  - More resources make having an IdP more attractive
  - Use Pathfinder to provide resources

Science & Technology Facilities Council

Technical Points

- Moonshot requires client side libs (mech_eap.so)
- X.509 certificates require higher LoA
  - Aiming for BIRCH
  - Need for IdP to communicate “loss of traceability”
- Infrastructure managed private keys
  - Should improve usability

(Main) Risks

- (There is a proper risk register…)
- Not enough IdPs…
  - Of a sufficient LoA (IGTF BIRCH)
  - Need to sign a contract! (little assurance in Assent itself)
- IdP cannot notify on loss of traceability
- IGTF accreditation delayed
- Users *still* manage certs through browser!

Support for added extra supplementary additional

SUBJECT ALT NAMES

Science & Technology Facilities Council

Now supported via PeCR

- cli mode uses --san to request extra SANs
- Bulk mode uses extra lines in cnfiles
  - Comma separated (no spaces)
- Need a recent version of PeCR, see www.ngs.ac.uk

Still a few niggles

- Need to pre-authorise all SANs
  - By submitter DN
  - Through RA
  - (Because RA will not necessarily see the SANs during approval)
- Only works for NEW host requests
  - Otherwise submitter DN is not present
  - Need to fiddle old requests
- ~~cnfiles need single names to download~~ fixed!

Science & Technology Facilities Council

Additional Credits

- PeCR – Robert Frank
- Testing – John Kewley

Science & Technology Facilities Council

More information on both Pathfinder and Multi-SAN: dteam