Science and
Technology
Facilities Council

# UK eScience CA Update
## [C/Sh]ould we be a Catch All CA for WLCG?

John Kewley and Jens Jensen
UK eScience CA

CERN 13/2/2023

# Background

*NB: JK’s paraphrasing of the issue – so this is just a general idea of their challenges*

- Fermilab are having issues with getting certificates from their certificate supplier.
- Their command line API interface (ACME?) is broken such that only 2 people can currently use it, possibly due to an issue with the certificates the other Admins have. Their web i/f still works.
- It is not expected that this situation will be solved soon.
- It was requested at a recent WLCG meeting that maybe another CA could help and the UK eScience CA name came up, so I thought I’d look at the possibilities.

# Scope

- This is an issue for host certs only, personal certs come from elsewhere
- As well as Fermilab it also affects some of the CMS Tier2 and Tier3s. But their certificate needs are a lot lower so they can manage with just the web access.
- Fermilab OTOH is dependent on command line management tools.

# Can/could/should/would

- Is it technically feasible for the UK eScience CA to support Fermilab without significant internal changes?
- Would what the UK CA be able to offer be acceptable to Fermilab and their RPs, technically or politically?
- Would the UK CA's relying parties (including their Management) be happy with this?
- If it is decided that another CA should provide such a "catch-all", is the UK eScience CA the best choice?

# What would be required technically?

*Assuming no change to UK CA s/w …*

- All New (but not Renewal) host CSRs need requesting by holders of UK eScience CA personal certificates
- Approval of CSRs (host and personal) is done through an RA so we’d need a FermiLab RA with associated RA Operator(s)
- All certificates would be issued under the current `namespaces` / `signing_policy` files
- Might need to do minor updates to CP/CPS policy files.

# Would FermiLab be able to use these

**Latest: while confusing, it would be tolerable**

Certificates would be issued within the UK eScience CA namespace, i.e. “/C=UK” in the DN, would this be acceptable to

- Fermilab staff and users (accessing a US system with a UK DN)
- TAGPMA?

*Technically, UK eScience CA does provide a command line i/f, but it is NOT ACME. So would there be much work involved at the Fermilab end?*

# Is this something WE should be doing?

- Would EUGridPMA be happy with this*?
- STFC/SCD management will need convincing:
  - It is a US problem, so should it not be sorted by others in TAGPMA?
  - Previous precedents for catch-alls were for new/small nations with limited infrastructure, this isn't the case here.
  - Although not considerable, more effort will still be needed, who will pay?

** Note: ASGCA catch-all has "/C=TW" for all certs*

# Fuller support?

Apart from minor changes such as to the `signing_policy` / `namespaces` files or CP/CPS, options for further support would take considerably more time, effort and cost:

- Provision of “/C=US” would involve changes at all levels of our systems
- Authenticating to our middleware with non-UK eScience CA personal certs to request host certs would involve a fair bit of extra work

I suspect this would be a non-starter

# ?Discussion