Science and Technology Facilities Council
Scientific Computing

GridPP
UK Computing for Particle Physics

WLCG
Worldwide LHC Computing Grid

Host certificates in the modern landscape

David Crooks, Dave Kelsey, Jens Jensen, Will Furnell, John Kewley (STFC)

Maarten Litmaath, Stefan Lüders (CERN)

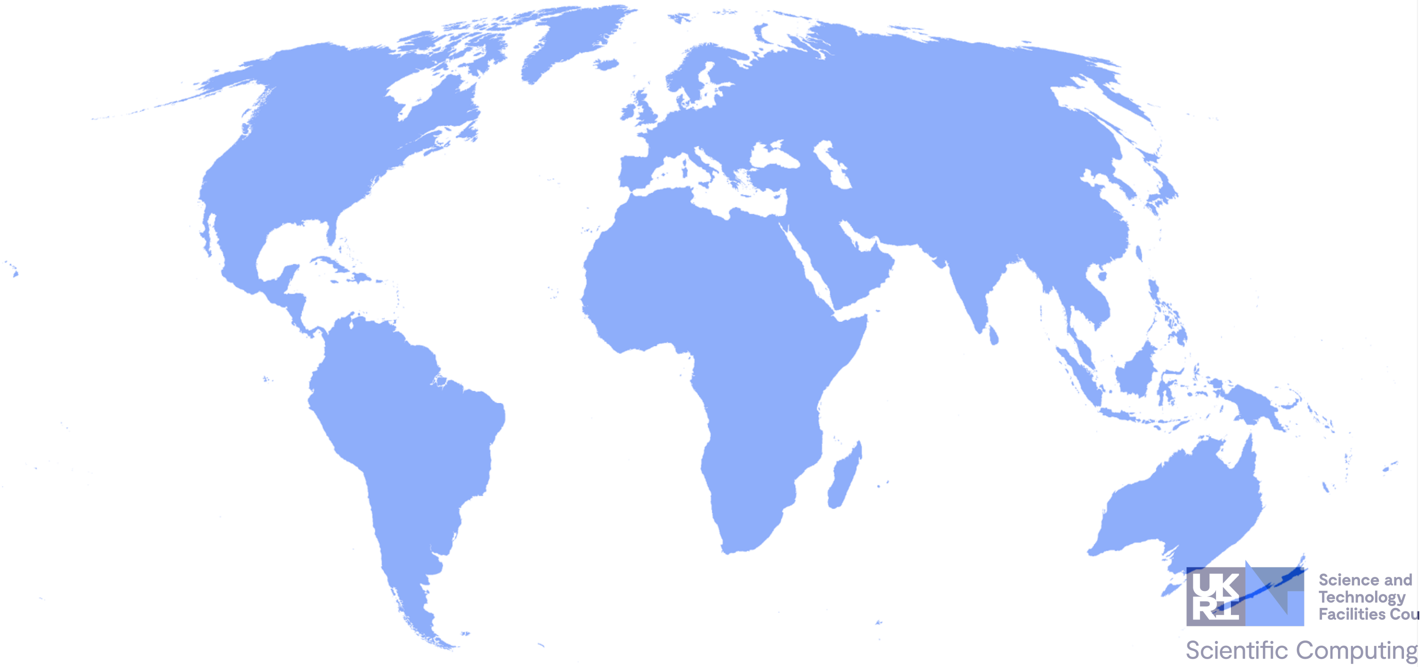
GridPP 46, September 2021, Ambleside

Introduction

- Aim of this afternoon is to discuss the challenge
- Identify key stakeholders and perspectives
  - Frame the question, **not** try to answer it today!
- Important precursor to GDB discussion a week today
  - Maarten Litmaath and Stefan Lüders contributed to these slides
  - I’ll give an updated set at the GDB incorporating our discussion today
    - Not exactly a Pre-GDB but serves a similar purpose
- Particularly welcome a note-taker for this discussion!

Background

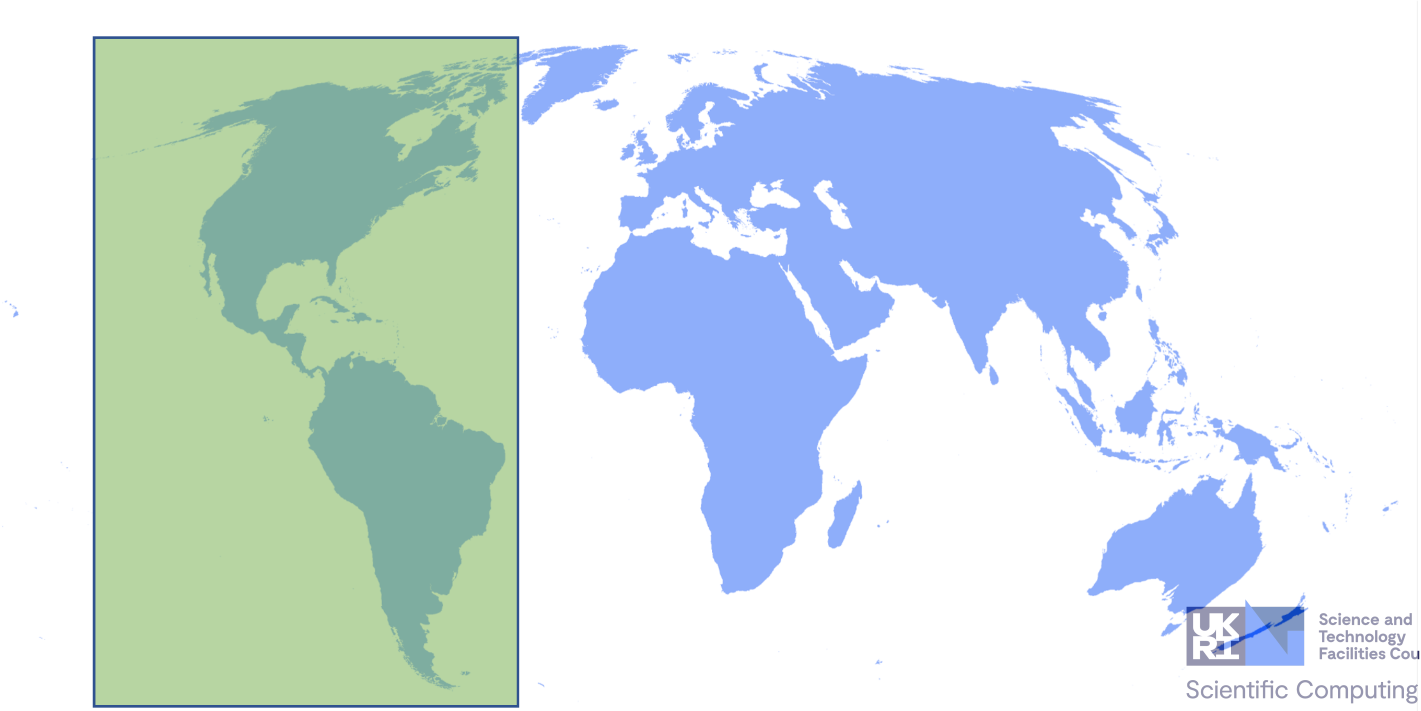
- Historically, all certificates used by GridPP have been provided by part of the Interoperable Global Trust Federation (IGTF) trust framework
  - In turn made up of three Policy Management Authorities (PMAs)



Background

- Historically, all certificates used by GridPP have been provided by part of the Interoperable Global Trust Federation (IGTF) trust framework
  - In turn made up of three Policy Management Authorities

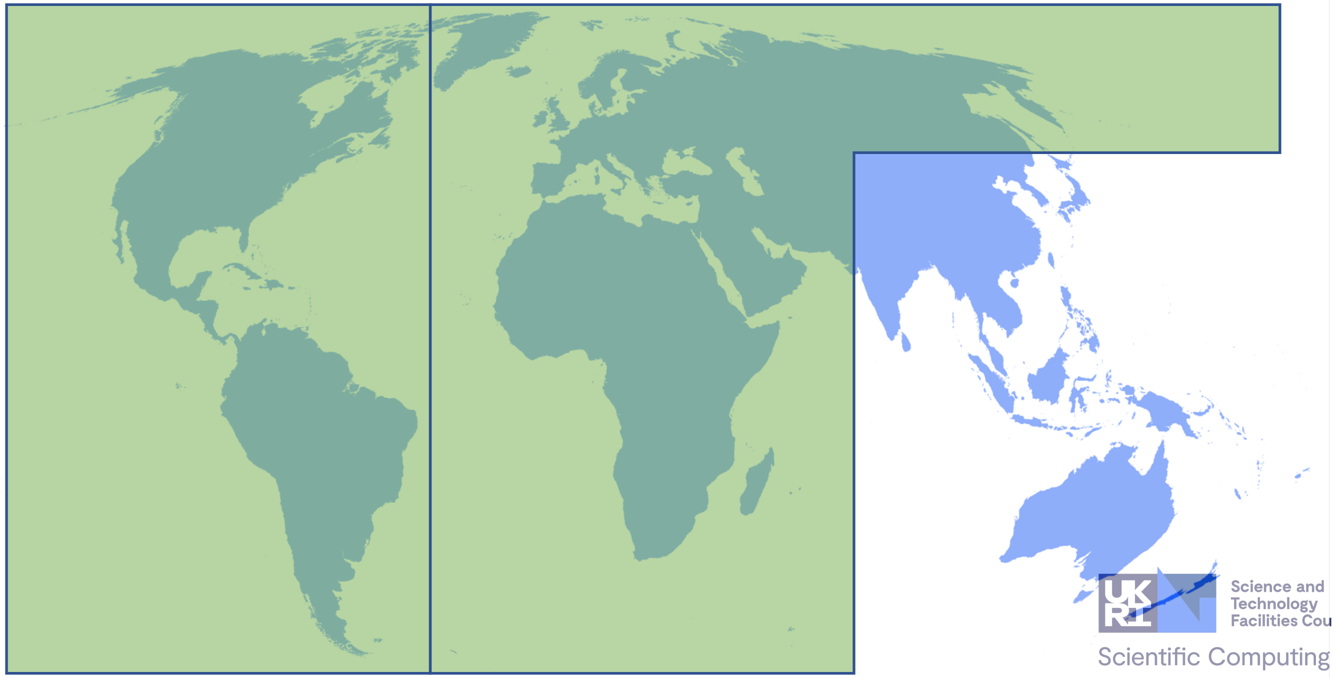
- TAGPMA



Background

- Historically, all certificates used by GridPP have been provided by part of the Interoperable Global Trust Federation (IGTF) trust framework
  - In turn made up of three Policy Management Authorities

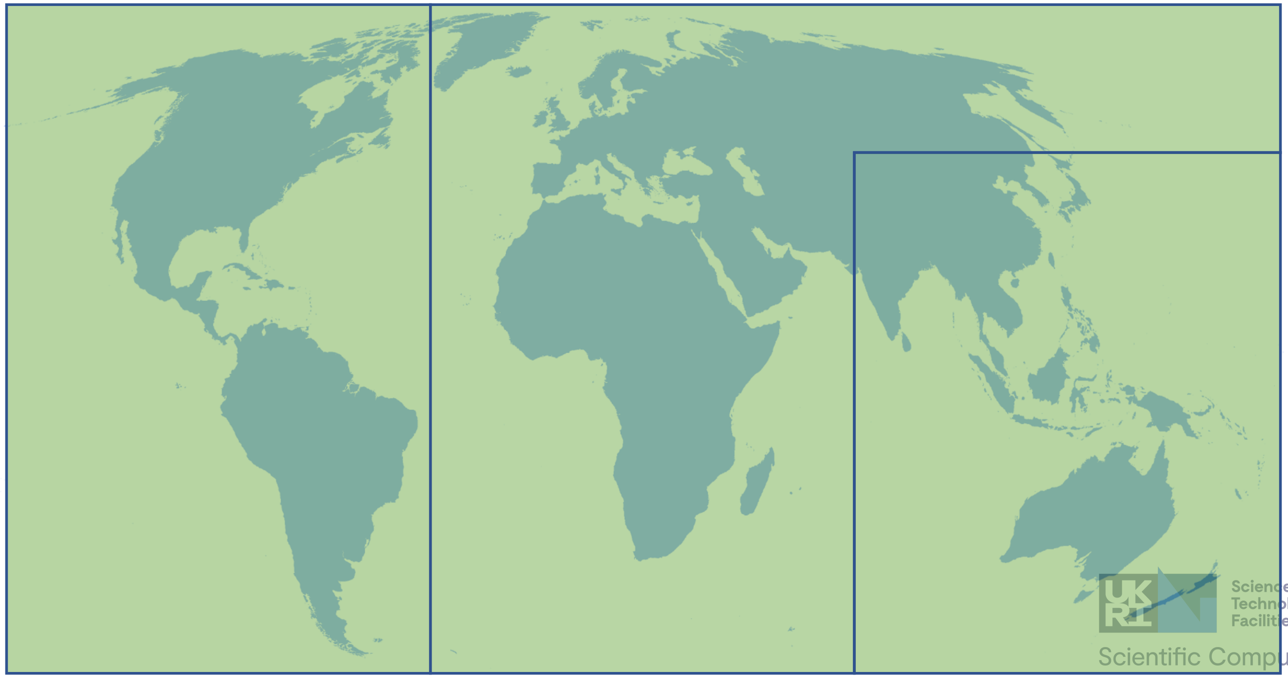
- TAGPMA
- EUGRIDPMA



Background

- Historically, all certificates used by GridPP have been provided by part of the Interoperable Global Trust Federation (IGTF) trust framework
  - In turn made up of three Policy Management Authorities

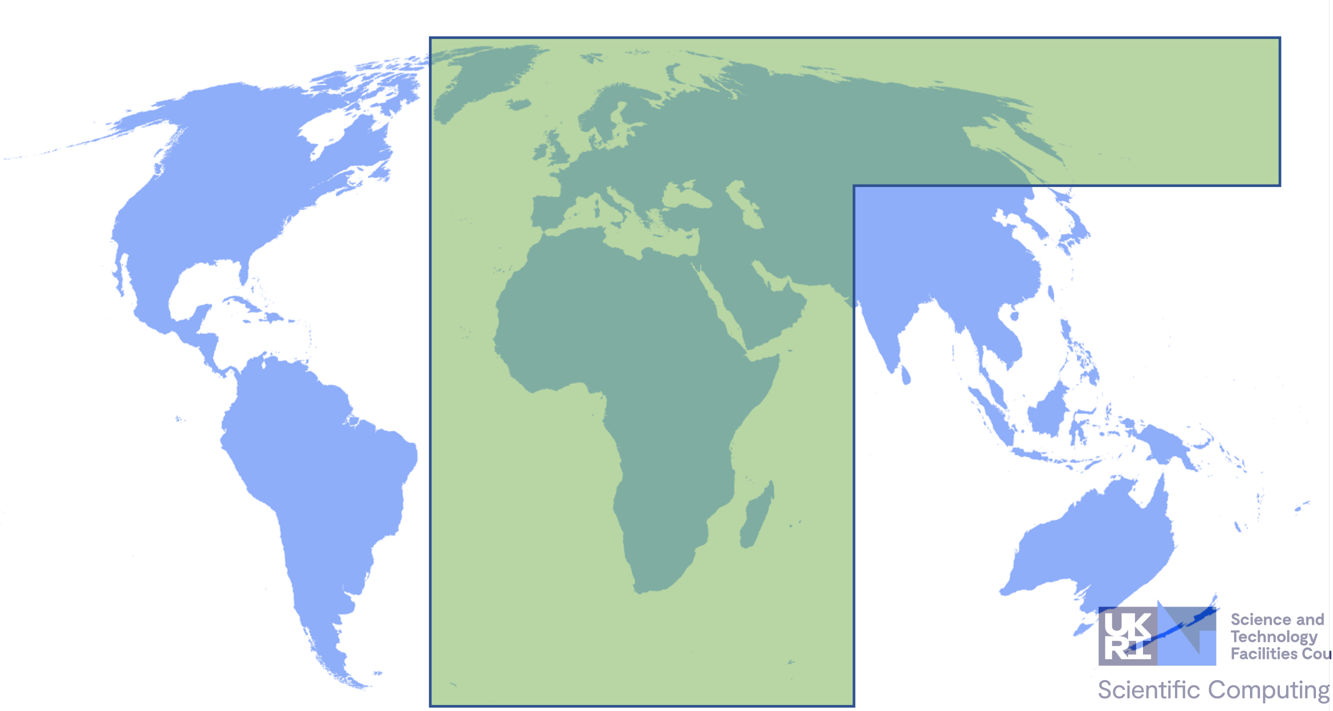
- TAGPMA
- EUGRIDPMA
- APGRIDPMA



Background

- Historically, all certificates used by GridPP have been provided by part of the Interoperable Global Trust Federation (IGTF) trust framework
  - In turn made up of three Policy Management Authorities

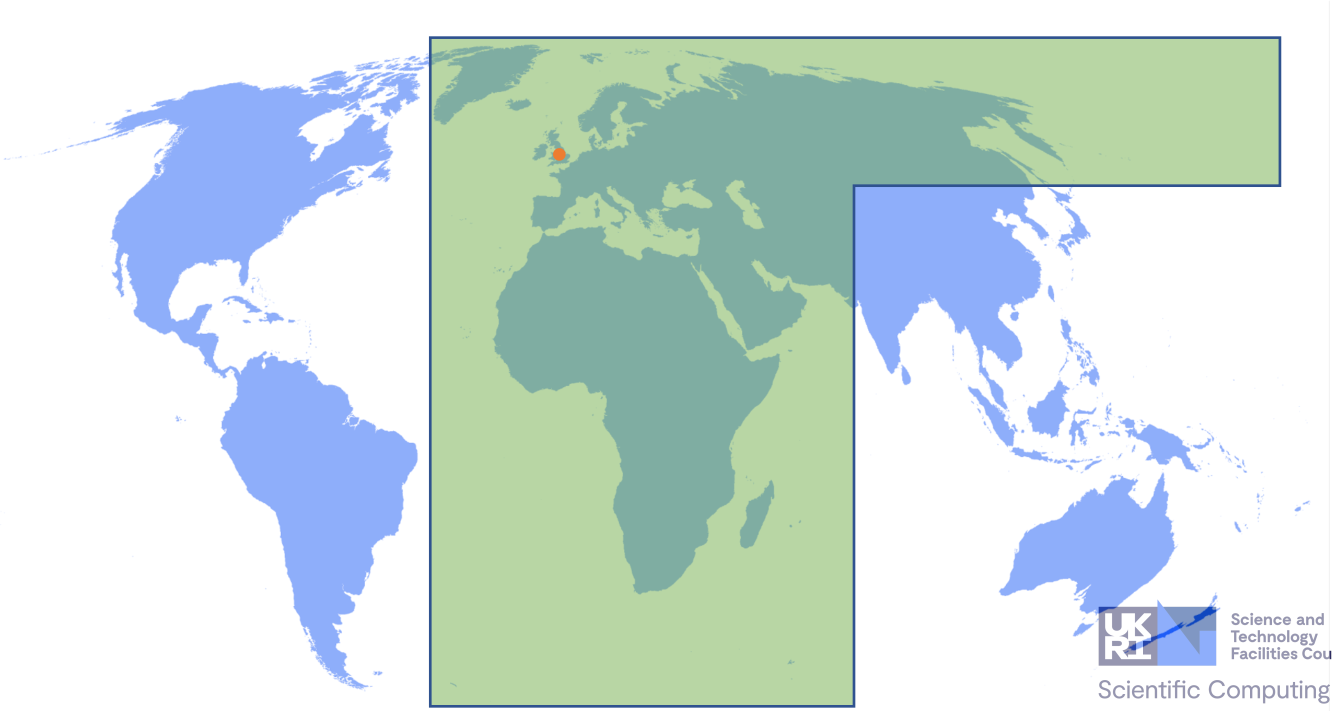
- EUGRIDPMA



Background

- Historically, all certificates used by GridPP have been provided by part of the Interoperable Global Trust Federation (IGTF) trust framework
  - In turn made up of three Policy Management Authorities

- EUGRIDPMA
  - UK eScience CA



UK eScience CA update

- Will Furnell has joined the CA team
  - ~40% of his time is spent working on the CA
  - His roles include
    - Administering the CA systems and the HSMs
    - Software development: upgrading the CA software
      - Fixing bugs, refactoring the code and adding new features for SANs
    - Also been working on upgrading hardware, improving power redundancy, increasing security and setting up a test environment
- Tom Dack has also recently joined the CA team as well
  - Important strengthening of link between x509 and token experience
    - Tom manages the very successful IRIS IAM identity proxy

UK eScience CA short term roadmap

- Current work in progress
  - Actively improving the host certificate lifecycle
    - Auto-approval of renewals
    - Simple renewal of certs with extra SANs
  - New CA hierarchy
  - Looking at auto-issue of some types of certificate
  - Investigating ACME interface

Background

- These Certificate Authorities provide user and host certificates according to a specific set of requirements, peer-reviewed at regular intervals
- To obtain Host certificates you first need to provide a User certificate
- These User certificates have Medium assurance
  - Require F2F (or remote equivalent) ID

The Challenge

- The challenge is NOT User certificates; the token transition being discussed elsewhere
- We ARE talking about Host certificates which will continue to be required
- The challenge is in how our workflows are changing

The Challenge (Operational Perspective)

- Discussions in DOMA on the use of google, amazon and azure cloud resources: there’s a desire to
  - Set these up efficiently
  - Avoid hacks to work with these providers
- This led to a question of the use of IGTF host certificates vs the use of Let’s Encrypt or the Google CA, etc…

The Challenge (Operational Perspective)

- Let’s Encrypt/Google CAs part of web browser trust chain
  - NOT part of IGTF distribution
- Let’s Encrypt (for example) offers programmatic APIs: Automated Certificate Management Environment (ACME) which can be advantageous
  - “Ease of provisioning”
  - IGTF CAs DO offer programmatic interfaces, with ACME being investigated
- Wildcards are of importance in the use of dynamic resources

- Now: need to include identity management and security perspectives…

IGTF Perspective

- Resource Providers have Assurance requirements
  - To what extent have these been discussed at this stage?
- Need detailed consideration of impact of certificates like Let's Encrypt
- An IGTF Working Group has been proposed
- Need to understand approval/renewal/revocation process in all cases
- TCS (Sectigo) certificates (see later) are an obvious option in the UK
  - In the web trust group and IGTF distribution (being careful of which product is used)
  - UK specific: CERN may not be able to use these
- Are certs provided by other CAs drop-in replacements for IGTF certs?

Security Perspective

- Overriding security concern is traceability
- Need to track activity in the context of an incident
    - Increasingly complex in the context of dynamic resources
- Need to understand how this works regardless of way forward
- Examine particular CA workflows in our context
    - Need clear picture of which CAs are included in discussion

Certificate Authorities: Pros and Cons

Let’s Encrypt

- Let’s Encrypt is a free, automated, and open certificate authority (CA), run for the public’s benefit. It is a service provided by the Internet Security Research Group (ISRG).

Pros

- Works with web browser trust chain
- No need for a personal certificate
- Programmatic interface: ACME
  - Variety of clients
- “Ease of renewal” (in fact fresh provisioning)
- Admin ease of use – free, don't have to get approval

Cons

- Uncertainties regarding long-term sustainability
  - Dangers of lock-in
- Rate limits
- Who applies for them (no personal certificate involved)
- “Ease of renewal” may in fact not be that easy
  - Systems inside firewalls
  - Possibility for bulk requests
  - Whether extra SANs/wildcards are all tested
- Trust means trust for any usage **including as client certs**
- Possibility of DNS spoofing
- Not IGTF trusted
- Reapply every 90 days

TCS (Sectigo)

- TCS allows participating national research and education networking organisations (NRENs) to issue unlimited numbers of certificates provided by a commercial CA at a significantly reduced price.

Pros

- Automatically work in both Grid and Browser trust frameworks.
  - if you get the right ones
  - IGTF accredited – with GFD.225 compliance
- EU service, linked to GÉANT
  - Good sustainability
- Also moving to ACME protocol
  - Already have a programmatic interface

Cons

- Funding model may change, and may be different for Universities, UKRI and industry partners.
- Easier in other countries (Paid for service in UK)
  - Can we discuss with Jisc?
- Exact attributes present in DNs have changed over time (eg email addresses)
  - Is this a problem?

UK eScience CA

- A certificate from the UK eScience CA can be used to authenticate to securely access resources worldwide. Certificates are trusted by the IGTF. Any host can have a eScience cert as long as the user controls the host

Pros

- Certificate requests approved by local humans
- Know who made the initial request
- No need for firewall/proxy configuration changes for local certs
- Can apply for a "bulk" of 10s or hundreds in one go – with only 1 approval required.
- Last a year before renewal (rekeying).
- (Largely) common procedures and tools for both host and user certs
- "Better the devil you know" - people are used to their tools and procedures.

Cons

- Certificate requests approved by local humans
    - Adds delay
- Not by default in the Browser Trust Domain (aren't intended to be web-certs)

Wider Landscape: OSG

- Uses Let’s Encrypt for non-WLCG use cases
- Susan Sons, then OSG Security Officer, wrote position paper on Let’s Encrypt
  - One extract:

“Perception of lower assurance level from Let’s Encrypt could make some stakeholders feel exposed.

a. We have separate registration procedures for services on the OSG that verifies the certain organizations; no access is given solely based on the possession of a host certificate.”

Wider Landscape: WLCG

- WLCG does have a current acceptable authentication assurance policy
    - Need to examine this in the context of this ongoing discussion

Questions for Discussion

- Who are the stakeholders
  - Operations, Identity management, Security
- Have we captured the challenge?
- What do we need to add to the perspectives?
- How do we move forward
  - Working group containing **all** perspectives to find common way forward
  - Nuanced discussion – need to have common discussion rather than separate silos that interact occasionally

Over to you!

Science and Technology Facilities Council

Scientific Computing

GridPP

UK Computing for Particle Physics

WLCG

Worldwide LHC Computing Grid