Evolution of CAs for WLCG Ops

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

Maarten Litmaath, Stefan Lüders, Hannah Short,
Romain Wartel (CERN)

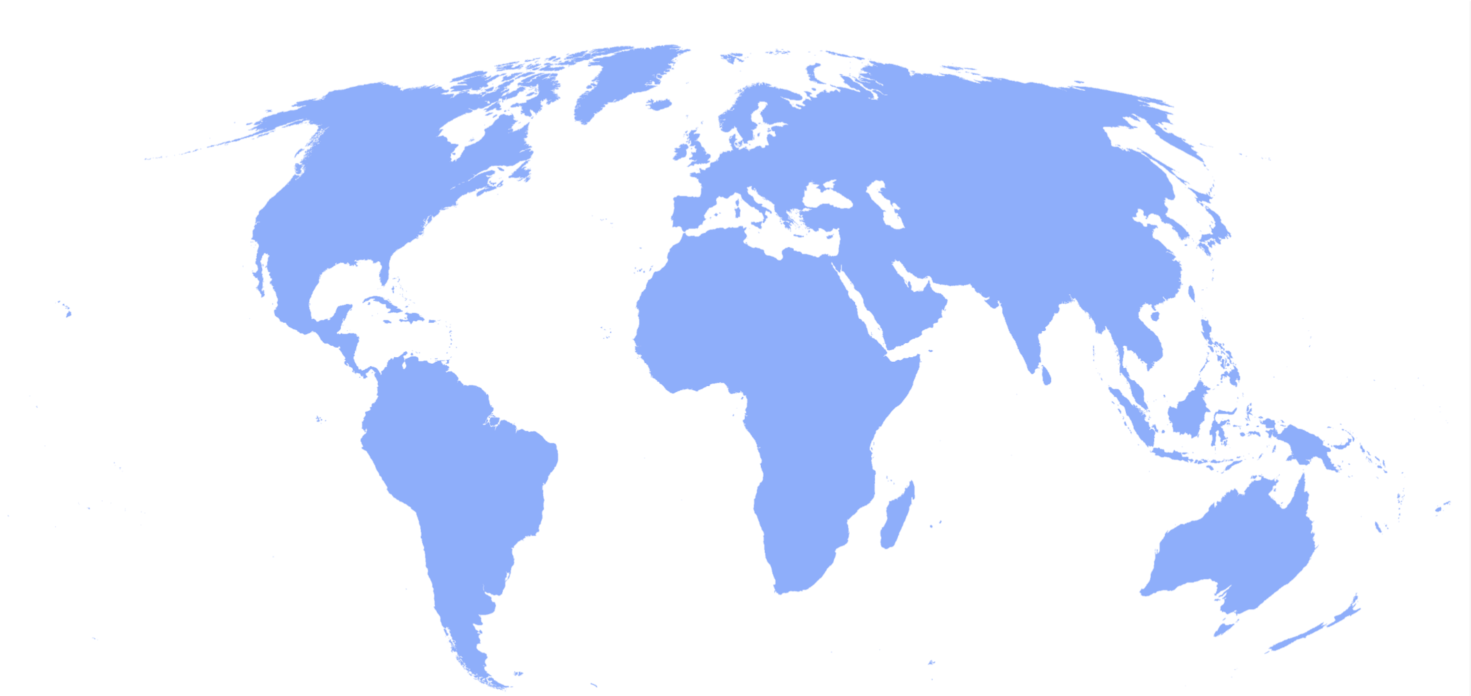
GDB, 8 September 2021

Introduction

- Aim of this afternoon is to discuss our challenge
- Identify key stakeholders and perspectives
  - Frame the question, **not** try to answer it today!
- Propose to have task force to work on this
  - Identify key participants
  - Invite participation to cover all viewpoints and experience

Background

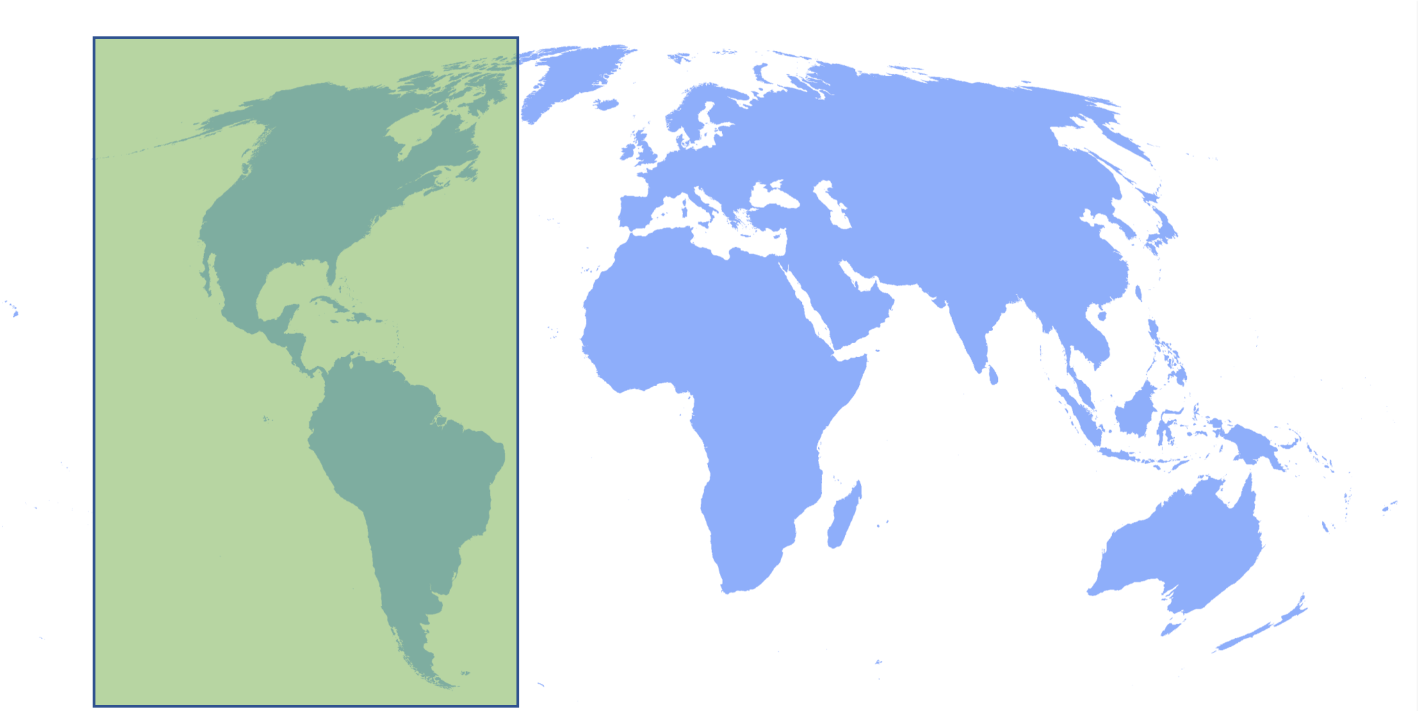
- Historically, all certificates used by WLCG have been provided by part of the Interoperable Global Trust Federation (IGTF) trust framework
  - In turn made up of three Policy Management Authorities (PMAs)



Background

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

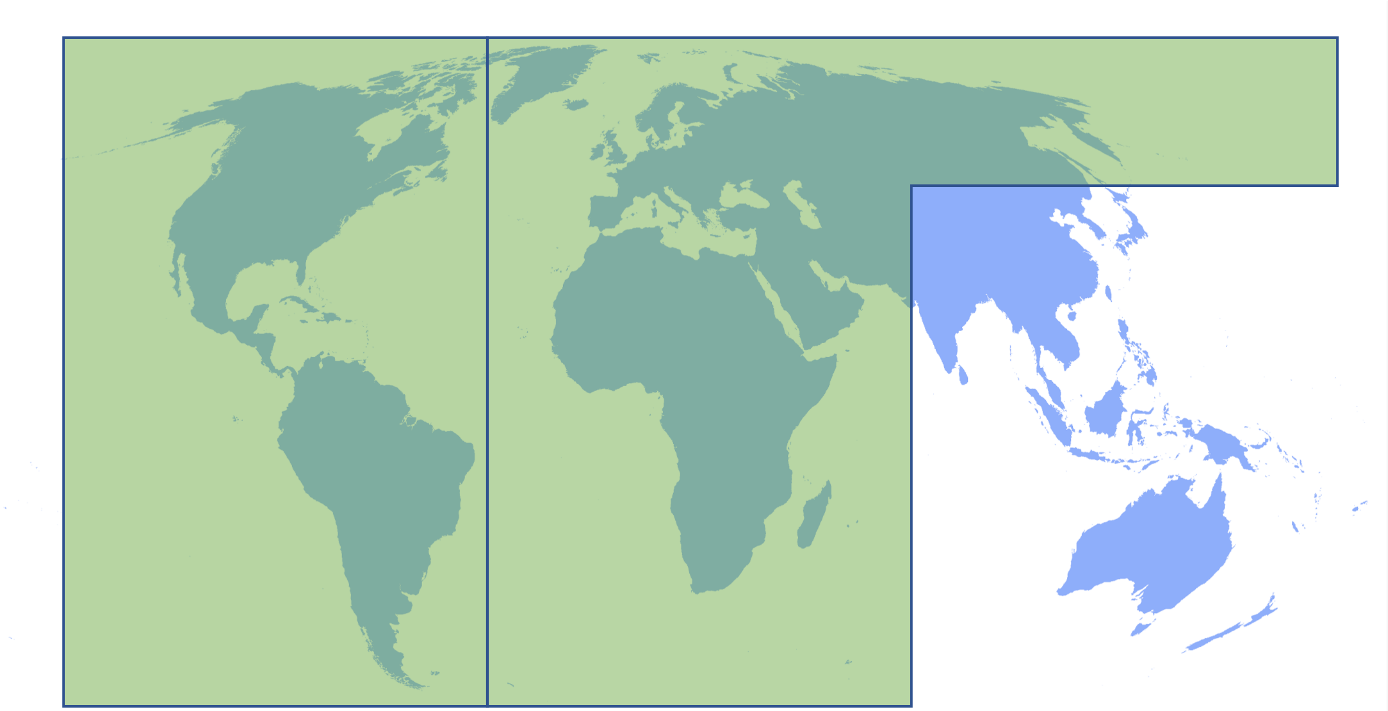
- TAGPMA



Background

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

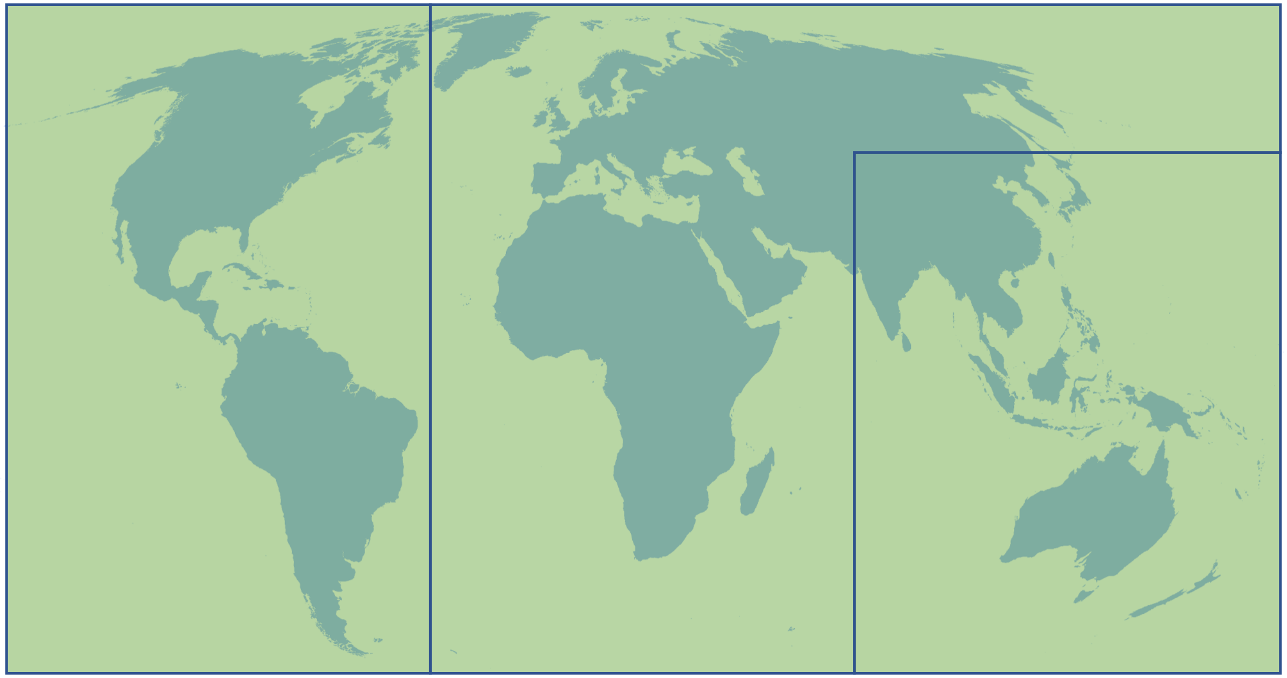
- TAGPMA
- EUGRIDPMA



Background

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

- TAGPMA
- EUGRIDPMA
- APGRIDPMA



Background

- IGTF 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

- This discussion is **not** around user certificates
  - the token transition is 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)

- Increasing use of cloud resources, and other developments in new workflows, has raised the question of which host certificates are appropriate for different use cases
- Particularly around dynamic provisioning
- CAs being discussed included Let's Encrypt
  - But also Google CA, Amazon, Azure, etc…
  - Larger question of cloud workflows

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 Automated Certificate Management Environment (ACME) interface which can be advantageous
  - “Ease of provisioning”
  - Some IGTF CAs DO offer programmatic interfaces
    - ACME being investigated
- Wildcards are of importance in the use of dynamic resources

Identity Management (IGTF) Perspective

- Relying Parties (including 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

Identity Management (IGTF) Perspective

- TCS (Sectigo) certificates (see later) are an obvious option
  - In the web trust group and IGTF distribution (being careful of which product is used)
  - CERN, eg, is investigating how to use these, Switch do not participate (RENATER)
- Are certs provided by other CAs drop-in replacements for IGTF certs?
- Important note: typically, any configuration of trust is carried out at a site level
  - Hard to do VO/experiment specific config
  - Need to be very careful of impact of WLCG decisions on broader community

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

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

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
  - Location/region may be added or removed
  - Impacts myproxy needed periodic updates

IGTF CA

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.”

WLCG

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

- How best to approach different use cases with common approach
  - That's consistent with broader landscape
  - Many providers support communities outside WLCG

Discussion

- Stakeholders
  - Experiments, Operations, Identity management, Security
- Capturing specific use cases
- Capturing specific security requirements
- How do we move forward
  - Propose working group containing all perspectives to find common way forward
  - Define clear starting point
    - May have short term and longer-term goals
    - Some of these workflow changes are very powerful
    - Host certs are only one part of the discussion

Discussion