

# Resource Trust Evolution and Cloud-based Provisioning

David Crooks, David Kelsey (UKRI STFC)  
EGI Conference, 20 October 2021

# Introduction

---

- With many thanks to David Crooks (main author)
  - And also to Jens Jensen, Will Furnell, John Kewley (STFC)
  - And to Maarten Litmaath, Stefan Lüders, Hannah Short, Romain Wartel (CERN)
- Aim is to present the main challenges regarding use of host certificates
  - Acceptable authentication assurance policy
- Identify key stakeholders and perspectives
  - Frame some of the questions, **not** try to answer them today!
- A WLCG task force is being formed to work on this
  - Inviting participation to cover all viewpoints and experience

# Background

- EGI (and WLCG) has a policy on “Acceptable Authentication Assurance”
  - <https://documents.egi.eu/document/2930>
- Historically, all certificates used by EGI/WLCG have been provided by the Interoperable Global Trust Federation (IGTF) trust framework



# 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 often need to provide a user certificate
- The user certificates have “medium” assurance
  - Require F2F (or remote equivalent) with photo 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 include Let's Encrypt
  - But also Google CA, Amazon, Azure, etc...
  - Larger question of cloud workflows
- Should we trust these?

# 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

# 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 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
- Trust means **trust for any usage including as client certs**
- Possibility of DNS spoofing
- Not IGTF trusted
- Reapply every 90 days

# GÉANT Trusted Certificate Service (TCS)

- [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, research labs and industry partners
- Easier in some countries (paid for service in others)
- 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)

# The WLCG task force:

<https://twiki.cern.ch/twiki/bin/view/LCG/ResourceTrustEvolution>

---

- Stakeholders
  - Experiments, Operations, Identity management, Security
  - Include **EGI Operations and other stakeholders** - contact David Crooks (STFC)
- Capture specific use cases
- Capture specific security requirements
- WLCG task force is being formed
  - Contain all perspectives to find common way forward
  - 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

---