Resource Trust Evolution TF meeting

M. Litmaath

Feb 1, 2023

v1.1

What are the issues?

- Traditional CAs run by our institutes are steadily being discontinued
- Generic e-science CAs are taking over, but may be expensive
- In a few years, *users* should no longer need certificates at all
  - Thanks to the move to tokens and federated identities
- *Host* certificates will remain crucial
  - To allow clients to check the actual identity of a service
  - To allow encrypted communication channels to be set up easily
- Cloud (and HPC) resources are becoming ever more important
- Our institutes do not own the domains of such resources and hence cannot easily obtain IGTF certificates for them
  - Workarounds exist, but are not sustainable
- There are other potential concerns about cloud / HPC resources that we can look into later

Can we just add more CAs to IGTF?

- IGTF CAs have always been our *partners*, providing services at agreed QoS levels
  - User vetting
  - Collaboration on incident response
- That has been important for the *user* certificate use case
  - Which will go away, but only in a few years
- For other CAs we are just ordinary customers
- That should be fine for *host* certificates
- But our certificate verification machinery does not distinguish between user and host certificates
  - There is a single /etc/grid-security/certificates or $X509_CERT_DIR directory and our MW does not even support such distinctions
- But those other CAs should only be used for host certificates!
  - We can define such a *policy*, but cannot enforce it today
- Our sites also need to support other communities on their services
  - Any changes made for us will also affect others

Discussion items

- Should we try and make our MW more flexible?
  - Could be a lot of development work in various places
  - And deployment would not be fast either
  - For just those few years we actually have these issues?
- Can we aim for policies instead?
- How may we work with IGTF on these matters?
  - IGTF is about trust between R&E partners, not just CAs
  - The landscape is evolving for other communities too
  - Projects like AARC3 will try to tackle these questions as well
    - See EUGridPMA meeting, Feb 13, 2023
  - But their timelines do not necessarily match ours