WLCG Resource Trust Evolution TF

Kick-off meeting live notes/initial mandate and scope document

Problem statement (draft/proposed)

WLCG is seeing an increasing number of resources it would like to use that are available with host certificates issued by a non-IGTF CA, and where WLCG cannot influence the service provider's choice of CA. There are grid sites for whom obtaining a host certificate from an IGTF-approved CA presents an unreasonable cost burden. Sites that provide resources to both WLCG and non-WLCG communities are forced to provide services that present host certificates issued by an IGTF CA and host certificates issued by some other CA (typically CAB Forum), which increases the cost of providing those services. User communities that wish to collaborate with WLCG are forced to furnish their community-specific services with host certificates from IGTF approved CAs, presenting a barrier to such collaboration. Experience from onboarding new grid or cloud sites has shown that obtaining host certificates from an IGTF-approved CA is a significant barrier for that site's participation.

Statements contributing to scope

1. Resources that are shared between WLCG and other communities. Facilities providing services to other communities are presenting an IGTF certificate to non-grid services. People have to do tricks to sort this out or services have to provide two endpoints, or use certificates from a provider that has both public trust and IGTF assurance.
2. US sites need new certificates
3. The German cloud of sites are looking for a replacement for GermanGrid (their current IGTF CA). DFN TCS (just like InCommon IGTF server) has both public trust and IGTF assurance and unique naming.
4. RAL-Tier1: LSST uses cloud resources and would like to offer S3 storage direct to them (no grid technology involved): this is the same as point 1, I think → can serve as a real-world example.
5. WLCG would like to be an example that can be imitated by other big data infras. A sustainable trust model.
6. Experiment: trying to integrate with other services that are not in the grid world. 6 months R&D, run in widely distributed X509 worlds, practically impossible to add new root CA to IGTF trust store. Something more dynamic. (focus on R&D here, for now)
7. Changes needed on the middleware side to support two trust stores?
    a. This means having one store for the service acting as a client and one store for the service acting as a host/server
    b. For each of these roles also have your own identity. This means helping your peers trust you rather than you trusting them
8. Separating user/host cert handling. Question of who the site trusts? Question of who the experiment/user trusts? Do we want to delegate trust? A site trusts a VO that trusts its

members. But if the user certificate is used to access a service, the site still has to trust it directly. This will be less of an issue with tokens, because then users and services are no longer married to the same, single trust store and can be dealt with separately.
9. Services and systems managed at sites vs external things like other research communities/commercial providers. Trust is more than just certificates. Basis of trust.
10. What does trust really mean?
11. Traceability is always essential.
12. [EUGridPMA] Evaluate CAs in a way that is compatible with IGTF (with support from IGTF)
13. [EUGridPMA] Being clear about separation between HOST trust stores and CLIENT trust stores is essential

Goals

14. Find a set of questions/conversations for site/facility security teams?

Solution pool

- TCS/Sectigo
  - ACME like end point for IGTF+CAB not in place: DG: REST API in place with ACME endpoint scheduled.
- [EUGridPMA] Tools like HAPROXY can allow services to present different certificates to different communities based on hostname Used in RCauth

Notes

AF: more sites need to switch to S3 endpoints - these sites already support ATLAS and Belle.
DK: Support the idea that it’s important it works for everyone. Not easy to define the trust for specific parts of a site/service.
DK: lack of clarity: TAGPMA: Digicert rep was confused, went away with a mission to understand what the status is.
PM: Other examples of IGTF? Where are the peers?
ML: Unique? We spearheaded this, set out to make the trust basis very reliable. You will not get focused traceability support from other CAs. Using only CAB …
DG: Considerations: Distinguish between host certs and client certs. Assurance levels are very different. A single trust store → we cannot distinguish. In client (and host) certs we ensure namespacing. 2. Assurance: a couple of peers. Most you will not see in science env. Healthcare, finance, aerospace. If you look at the eIDAS framework, similarly defined by a set of CAs that are trusted. Adobe. Document signing defines its own ecosystem. Most visible in non-classified domains (e.g. the military do their own thing).
ML: For historical reasons, host/client certs are mixed. Want to make things “easier” for host certs…

DG: Imagine tokens with an IGTF-like trust framework. Trust derives from a different source. Not true here. In the token world many of these things will go away if you have a way of transferring trust anchors. It will make things easier at the service level but move the complexity to federation level. Source of trust in domain names comes from somewhere else (cf. GOC DB).
DK: More like this came from the infrastructures.
PM: Limit the scope of trust to R&D projects?
RW: Need to not splinter.
PM: Separate truststores? Software would need to be updated.
DK: Can we solve the client problem at authZ level?
RW: this is what we do anyway for IR.
DG: This works for WLCG, but not necessarily for others?
ML: Another VO might allow use of LE - what is the impact of that? It may be the easiest just to forbid that by policy.
DG: Architecturally correct thing would be for LE not to offer client certs. (ML: for some use cases, client usage may be needed). Also hostcerts used as Robots.
PM: client - is that a person?
DG: LE - you will never know if it was at one point a human.
TH: LE - for all services, or some aspects? I would say trust difference between CE/SE and between worker node/data.

US status: similar to the situation a few months ago: JD had no update (JT the one to ask) - thinks that some T2/T3 sites are affected.

DK: lack of clarity: TAGPMA: Digicert rep was confused, went away with a mission to understand what the status is.

Actions

- Ask JT for more details (JD/DC?)
- Find out what the Digicert status is (DK)
- DC/ML refine the scope statements - others can of course edit as well. Need to make sure we’re on the same page of what matters.
- DC: make a new poll for January

Notes from EUGridPMA
DavidG: Often found cases where the same cert was used for several purposes.
DavidG: Everything is moving to a year: and likely 90 days
Maarten: need to automate it
Discussion: Managing different packaging of IGTF root CAs

Jens: talking about having a hook into openssl to enforce policy.

Next steps: Document use cases and compare to existing technologies.