Open Science Grid ISO Position Paper on

Let’s Encrypt CA for Host Certificate Signing

Executive Summary:

By approving use of Let’s Encrypt within OSG, we can reduce overhead for resource providers, reduce our own overhead, and gain some security benefits with regard to certificate revocation for very little risk and no cost.

Problem Statement:

Every host that is part of Open Science Grid (OSG) requires a host certificate in order to authenticate itself when interacting with clients and other hosts. The overhead of acquiring, revoking, and replacing host certificates is currently much higher than necessary, and unreliability of revocation presents a security weakness. The issue is especially timely now, as the impending operations team spin-down increases the need to lower OSG’s certificate signing burdens as much as possible.

History:

OSG has thus far used only traditional IGTF-Classic (https://www.igtf.net/ap/classic/) Certificate Authorities (CAs) for signing host certificates. Depending on the implementation, these CAs rely on manual, multi-step processes for signing certificates. Certificates procured this way have long lifetimes, and rely on failure-prone revocation lists to let consumers know when they have been compromised. Certificate procurement and revocation are both too slow and involve too much administration overhead to meet the needs of many modern operational environments, which would like to spin up hosts in response to changes in user demand.

Let’s Encrypt is an automated CA system which relies on a FQDN’s authoritative DNS records to identify and confirm host ownership, and provides short-lived certificates in a secure manner with a minimum of overhead. IGTF-Classic CAs focus on *organizational validation* (determining that the host is controlled by a particular organization) while Let’s Encrypt provides *domain validation* (determining the host is actually the one at a network domain). Because OSG use cases for grid services have an out-of-band registration step, OSG does not depend on the organizational validation. The domain validation from Let’s Encrypt is sufficient from a security perspective.

Analysis:

Please note that this document only approaches issues around signing *host certificates* and evaluating the required assurance levels for OSG services, and is not proposing any changes to how OSG handles user certificates.

The following factors were considered in deciding whether to recommend the Let's Encrypt CA being adopted by OSG for host certificate signing:

Goals:

- OSG clients rely on signed X509 certificates in order to authenticate services for TLS connections.
- X509 certificates are *not* designed to prove or imply trust level or authority, only to authenticate that the host one connects to is truly the owner of its FQDN.
- It is desired to reduce overhead of maintaining this authentication mechanism for both our resource providers and OSG staff.
- Automating the certificate issuance and revocation process would increase security as well, by allowing on-the-fly server spin-up and spin-down, and making it practical to use short-lived certificates.

Benefits:

- With Let's Encrypt in place, resource providers can automate host certificate issuance via ACME protocol. This will support automated server provisioning, remove incentives for poor user certificate handling[1]
- Let's Encrypt certificates have a maximum three month lifespan, which reduces the window of possible exploit of a compromised certificate even for applications incapable of consulting Certificate Revocation Lists (CRLs).
- Let's Encrypt's ACME protocol effectively verifies domain ownership in a fast, secure, automated way. This provides the same level of assurance with regard to matching the FQDN to the host as methods currently in use at OSG.
- While our European partners may not yet recognize Let's Encrypt certificates, this impacts the very few OSG resources with which those partners interact. Those hosts can continue to use IGTF-Classic CAs (such as the OSG CA or InCommon IGTF CA) for host certificates.
- The Let's Encrypt CA is accepted by default in the set of trust roots on all major OS platforms, language runtimes, and browsers. This will make our services simpler to use with non-grid tool sets.

[1] Administrators often share or improperly store their user certificates in violation of OSG certificate handling policy in order to facilitate the issuance of host certificates when they are not present at the keyboard.

Risks and Mitigations:

- 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.
    b. Good documentation and communication around this issue can help allay any related concerns, as we aren't actually losing any assurance we already had.
- Allowing Let's Encrypt by policy will have no meaningful impact unless we make the technology accessible to resource providers by:
    a. Providing relevant documentation
    b. Including Let's Encrypt's root cert in our CA bundle so that these certificates don't require any extra set-up on the relying party's part
    c. Informing resource providers that they have the option to use Let's Encrypt.
- Our European collaborators do not accept Let's Encrypt certificates as they are not accredited by the IGTF.
    a. As few OSG hosts regularly interface with European systems, these hosts will continue to use IGTF-based certificates while other hosts move to Let's Encrypt.
    b. We will pursue the addition of Let's Encrypt as an IGTF accredited CA, an argument which is bolstered once we have a track record of its successful use at OSG.
- Let's Encrypt could, someday, stop existing as a free service.
    a. Let's Encrypt is supported by over 55 supporting organizations, including Google, Akamai, Automattic, Mozilla, Cisco, and EFF, with a collective track record of giving more than adequate warning before spinning down services.

Recommendation:

Based on the information above, I recommend that OSG adopt Let's Encrypt as a host CA by taking the following steps:

- Update OSG documentation to include information on obtaining signed host certificates through Let's Encrypt's automated process, without removing information on obtaining CILogon-signed certificates.
- Include the Let's Encrypt signing certificate in all future OSG CA cert bundles.
- Publish a note to the security contacts list notifying them of this change, in order to reduce friction/surprises among our resource providers.

11Apr2018 // Susan Sons
OSG Information Security Officer