Table of Contents

WLCG Resource Trust Evolution Task Force

Introduction

For many years, authentication in WLCG and related infrastructures and projects has relied on ***trust anchors*** vouched for by IGTF, the Interoperable Global Trust Federation. For practical reasons, those anchors covered both users and resources, which has served us nicely for many years. However, as the use of client-side X509 certificates is cumbersome for users, preparations are being made for users to be able to switch to more modern and convenient authentication mechanisms that are gradually being adopted in academia and industry: federated identities and tokens.

On the other hand, identity federation does not address a number of key server-side use cases, and the continued use of X509 certificates to authenticate *resources* is in line with common practice. However, the IGTF portfolio of trusted certificate authorities (CAs) does not include several CAs that have become popular for various reasons and are trusted by browsers. Particular examples are Let's Encrypt and the CAs that come with commercial cloud providers. While such CAs have not been part of the IGTF bundle as they would not match existing security and assurance profiles, there is the perception of a gap widening between our traditional best practices and what is happening elsewhere in the digital world.

As the ***trust*** between parties ultimately underlies all WLCG activities, opting for extra convenience and practical benefits must not be done in a way that is detrimental to the trust, security and collaboration between parties. The relevant aspects between the various stakeholders as well as the impact on the trust model need to be discussed, in order to fully understand how we can advance together: experiments, sites, infrastructures, identity management, operations, security. Another important consideration is that most WLCG sites need to support other, separate, communities, on the same resources, usually through the same middleware. A change implemented for WLCG may thus affect other customers as well.

The goal of this task force is to bring all stakeholders together to build consensus on the way forward. A short-term objective would be to see which CAs, if any, could be added to the portfolio and for which purposes. A possibly longer-term objective would be to see how cloud resources and workflows can be integrated such that the benefits greatly outweigh the additional risks.

Communication

- Mailing list: `wlcg-resource-trust-evolution` (at `cern.ch`)
    - You can contact `wlcg-resource-trust-evolution-admin` (at `cern.ch`) if you do not manage to subscribe.

- Meetings: Security Group category
    - June 29, 2023 - how to integrate cloud storage resources

Documentation

- GDB presentation, 8 Feb 2023
- GDB presentation, 13 July 2022
- HEPiX Autumn presentation, 28 October 2021
- EGI Conference presentation, 20 October 2021
- MB presentation, 14 September 2021
- GDB presentation, 8 September 2021

This topic: LCG > ResourceTrustEvolution
Topic revision: r10 - 2023-07-01 - MaartenLitmaath