Contribution ID: **54** Type: **not specified**

dCache, towards Federated Identities and Anonymized Delegation

Thursday, March 9, 2017 4:40 PM (20 minutes)

For over a decade, X509 Proxy Certificates are used in High Energy Physics (HEP) to authenticate users and guarantee their membership in
Virtual Organizations, on which subsequent authorization, e.g. for data access, is based upon. Although the established infrastructure worked well and provided sufficient security, the implementation of procedures and the underlying software is often seen as a burden, especially by smaller communities trying to adopt existing HEP software stacks. In addition, it is more efficient to guarantee the identity of a scientist at his home institute, since the necessary identity validation has already been performed. Scientists also depend on service portals for data access and processing, on their behalf. As a result, it is imperative for the infrastructure providers to support delegation of access to these portals for their end-users without compromising data security and identity privacy.

The growing usage of distributed services for similar data sharing and processing have led to the development of novel solutions like OpenID Connect, SAML etc. OpenID Connect is a mechanism for establishing the identity of an end-user based on authentication performed by a trusted third-party identity provider, which thereof can be used by infrastructures to delegate the identity verification and establishment to the trusted entity. After a successful authentication, the portal is in possession of an authenticated token, which can be further used to operate on infrastructure services on behalf of the scientist. Furthermore, these authenticated tokens can be exchanged for more flexible authorized credentials, like Macaroons. Macaroons are bearer tokens and can be used by services to ascertain whether a request is originating from an authorized portal. They are cryptographically verifiable entities and can be embedded with caveats to attenuate their scope before delegation.

In this presentation, we describe how OpenID Connect is integrated with dCache and how it can be used by a service portal to obtain a token for an end-user, based on authentication performed with a trusted third-party identity-provider. We also propose how this token can be exchanged for a Macaroon by an end-user and we show how dCache can be enabled to accept requests bearing delegated Macaroons.

Primary authors: Dr ROSSI, Albert (FNAL); Mr ASHISH, Anupam (DESY); Dr LITVINTSEV, Dmitry (FNAL); Dr BEHRMANN, Gerd (NDGF); Ms SAHAKYAN, Marina (DESY); Mr ADEYEMI, Olufemi (DESY); Dr FUHRMANN, Patrick (DESY/dCache.org); Dr MILLAR, Paul (DESY); Mr MKRTCHYAN, Tigran (DESY)

Presenter: Dr MILLAR, Paul (DESY)

Session Classification: Netwok, Scurity, Infrastructure &Operations IV

Track Classification: Networking, Security, Infrastructure & Operations