



Contribution ID: 335

Type: **Talk**

CMS Token Transition

Tuesday 22 October 2024 16:51 (18 minutes)

Within the LHC community, a momentous transition has been occurring in authorization. For nearly 20 years, services within the Worldwide LHC Computing Grid (WLCG) have authorized based on mapping an identity, derived from an X.509 credential, or a group/role derived from a VOMS extension issued by the experiment. A fundamental shift is occurring to capabilities: the credential, a bearer token, asserts the authorizations of the bearer, not the identity.

By the HL-LHC era, the CMS experiment plans for the transition to tokens, based on the WLCG Common JSON Web Token profile, to be complete. Services in the technology architecture include the INDIGO Identity and Access Management server to issue tokens; a HashiCorp Vault server to store and refresh access tokens for users and jobs; a managed token bastion server to push credentials to the HTCondor CredMon service; and HTCondor to maintain valid tokens in long-running batch jobs. We will describe the transition plans of the experiment, current status, configuration of the central authorization server, lessons learned in commissioning token-based access with sites, and operational experience using tokens for both job submissions and file transfers.

Primary authors: MALTA RODRIGUES, Alan (University of Notre Dame (US)); BOCKELMAN, Brian Paul (University of Wisconsin Madison (US)); RUNGPHITAKCHAI, Chan-Anun (University of Wisconsin Madison (US)); DYKSTRA, Dave (Fermi National Accelerator Lab. (US)); CIANGOTTINI, Diego (INFN, Perugia (IT)); KIZINEVIC, Edita (CERN); VAANDERING, Eric (Fermi National Accelerator Lab. (US)); MASCHERONI, Marco (Univ. of California San Diego (US)); PAPARRIGOPOULOS, Panos (CERN); CHAUHAN, Rahul (CERN); NUNTAVIRIYAKUL, Sarun (Chulalongkorn University (TH)); LAMMEL, Stephan (Fermi National Accelerator Lab. (US)); ZOKAITE, Vaiva (Vilnius University (LT))

Presenter: BOCKELMAN, Brian Paul (University of Wisconsin Madison (US))

Session Classification: Parallel (Track 4)

Track Classification: Track 4 - Distributed Computing