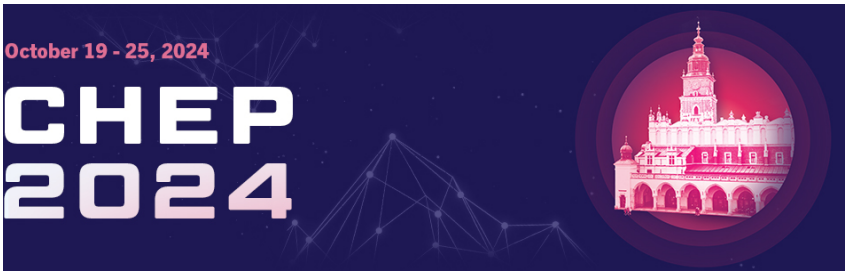

Contribution ID: **532** Type: **Talk**

Addressing tokens dynamic generation, propagation, storage and renewal to secure the GlideinWMS pilot based jobs and system.

Wednesday 23 October 2024 15:00 (18 minutes)

GlideinWMS has been one of the first middleware in the WLCG community to transition from X.509 to support also tokens. The first step was to get from the prototype in 2019 to using tokens in production in 2022. This paper will present the challenges introduced by the wider adoption of tokens and the evolution plans for securing the pilot infrastructure of GlideinWMS and supporting the new requirements.
In the last couple of years, the GlideinWMS team supported the migration to tokens of experiments and resources. Inadequate support in the current infrastructure, more stringent requirements, and the higher spatial and temporal granularity forced GlideinWMS to revisit once more how credentials are generated, used, and propagated.
The new credential modules have been designed to be used in multiple systems (GWMS, HC) and use a model where credentials have type, purpose, and different flows.
Credentials are dynamically generated in order to customize the duration and limit the scope to the targeted resource. This allows to enforce the least privilege principle. Finally, we also considered adding credential storage, renewal, and invalidation mechanisms within the GlideinWMS infrastructure to serve better the experiments' needs.

Primary authors: MOREIRA COIMBRA, Bruno (Fermi National Accelerator Lab. (US)); MAMBELLI, Marco (Fermilab (US))

Presenter: KNOEPFEL, Kyle (Fermi National Accelerator Laboratory)

Session Classification: Parallel (Track 4)

Track Classification: Track 4 - Distributed Computing