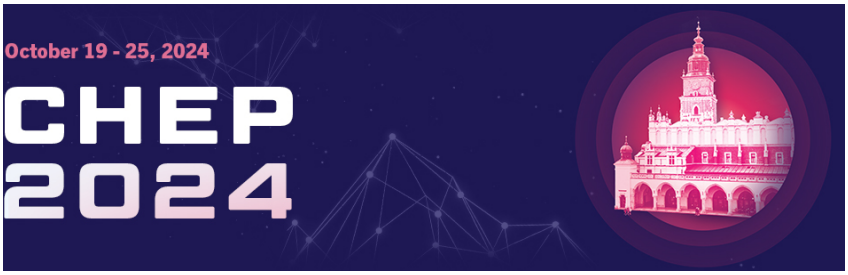

Contribution ID: **489** Contribution code: **THU 06** Type: **Poster**

A Managed Tokens Service for Securely Keeping and Distributing Grid Tokens

Thursday 24 October 2024 16:00 (15 minutes)

Fermilab is transitioning authentication and authorization for grid operations to using bearer tokens based on the WLCG Common JWT (JSON Web Token) Profile. One of the functionalities that Fermilab experimenters rely on is the ability to automate batch job submission, which in turn depends on the ability to securely refresh and distribute the necessary credentials to experiment job submit points. Thus, with the transition to using tokens for grid operations, we needed to create a service that would obtain, refresh, and distribute tokens for experimenters'use. This service would avoid the need for experimenters to be experts in obtaining their own tokens and would better protect the most sensitive long-lived credentials. Further, the service needed to be widely scalable, as we are currently keeping credentials active for approximately 15 experiments, each with 1-3 different credentials, and distributing those credentials to 2-20 submit points per experiment, with those numbers steadily increasing. To address these issues, we created and deployed a *Managed Tokens* service. The service is written in Go, taking advantage of that language's native concurrency primitives to easily be able to scale operations as we onboard experiments. The service uses as its first credentials a set of kerberos keytabs, stored on the same secure machine that the *Managed Tokens* service runs on. These kerberos credentials allow the service to use *htgettoken* via condor_vault_storer to store vault tokens in the *HTCondor* credential managers (credds) that run on the batch system scheduler machines (*HTCondor* schedds); as well as downloading a local, shorter-lived copy of the vault token. The kerberos credentials are then also used to distribute copies of the locally-stored vault tokens to experiment submit points. When experimenters schedule jobs to be submitted, these distributed vault tokens are used to access a *Hashicorp Vault* instance (run separately from the *Managed Tokens* service), and previously-stored refresh tokens there are used to obtain the bearer token that is submitted with the job. We will discuss here the design of the *Managed Tokens* service, including elaborating on certain choices we made with regards to concurrent operations, configuration, monitoring, and deployment.

Primary authors: BHAT, Shreyas (Fermi National Accelerator Laboratory (US)); DYKSTRA, Dave (Fermi National Accelerator Lab. (US))

Presenter: SMITH, Nick (Fermi National Accelerator Lab. (US))

Session Classification: Poster session

Track Classification: Track 4 - Distributed Computing