Reference	IT-CM-86
Project/ Activity	Secrets management enhancements
Duration	1 year, renewable (maximum 2 years)
Description	We use Puppet, an open source software configuration management and deployment tool, to manage over 30K nodes in CERN's Data Centre. For obvious reasons, some data in Puppet needs to be secret, and should be restricted to as few people as possible. Secrets can be whole files such as keytabs, special certificates or private keys. They can also be small passwords embedded in files. Unfortunately for our purposes, having these managed directly in Puppet via the Puppet master is insufficiently secure. Too many people have access to the execution path of the Puppet masters, or read access to repositories. Therefore we have developed tools to help manage those secrets for services managers that is integrated with Puppet without being subject to its security model. This project would consist on migrating some those tools (TBAG and TELLME) from using a home built service (Teigi) into using HashiCorp VAULT.
Profile	Requirements: Linux operating system and Python. We envisage the implementation of that VAULT service using Kubernetes for deployment and Flux for the automation and configuration of that deployment, so experience with any of those would be a plus.
Specific details	0