

# Exploring token authorization enforcements on Grid middleware with Open Policy Agent

*Thursday, 3 October 2024 10:40 (20 minutes)*

Open Policy Agent (OPA) is an open-source, general-purpose authorization engine that provides a high-level declarative language, called Rego, which allows the expression of policies as code, using a combination of data manipulation and logical operators. OPA takes policy decisions by evaluating the query input against policies and data. The OPA RESTful APIs allow the service to be integrated into any application, making it a versatile tool for authorization and access control.

One of the main advantages of using OPA is its performance optimization capabilities. The OPA policy evaluation engine is designed to handle large volumes of requests, making it an ideal choice for the Grid middleware. Additionally, the OPA caching mechanism allows it to minimize the number of policy evaluations, further improving performance. Moreover, the OPA declarative approach to policy management allows for a more intuitive and straightforward policy development process.

With this contribution, we want to highlight the potential of this framework in the context of our Grid middleware and to illustrate how we are exploring the use of OPA in two use cases: to implement the authorization rules defined in the WLCG JWT profile for StoRM Tape and StoRM WebDAV, and to replace the home-made scope policy engine within INDIGO IAM. The appropriate comparison in terms of performance and compliance between the previous solutions and those based on OPA will also be illustrated.

## Topic

Trust and Security: Access control

**Primary author:** Mrs AGOSTINI, Federica (INFN)

**Co-authors:** MARCATO, Davide (INFN); VIANELLO, Enrico (INFN); GIACOMINI, Francesco (INFN); GAS-PARETTO, Jacopo (INFN); BASSI, Luca; MICCOLI, Roberta (INFN); ZOTTI, Stefano Enrico

**Presenter:** Mrs AGOSTINI, Federica (INFN)

**Session Classification:** Trust & Security