The EurValve Portal, an entry point for the EurValve research platform, provides a Web Application type environment where computational pipelines can be prepared, executed and controlled. As each pipeline obtains access to a potentially sensitive set of medical data, and is also permitted to schedule computational tasks on supercomputing facilities (including the Prometheus cluster at ACC CYFRONET AGH), a comprehensive security system has been envisioned. Invoking computational tasks or accessing EurValve data requires proper authentication and authorization as explained below. This infrastructure also protects access to services external to the Portal, which are equipped with the Policy Enforcement Point (PEP). It should be noted that in addition to human actors the system may also be interfaced by machine/robot actors (e.g. one service accessing another using a token obtained with the standard login/password mechanism via the Portal API).



EurValve security infrastructure – conceptual view

**Identity Provider**

An Identity Provider (IdP) is a service which is capable of validating that users are actually who they claim to be. Thus, Identity Providers perform authentication for lower layers of the software stack. A set of trusted external Identity Providers based on the OpenID standard, including the PL-Grid IdP (required for accessing HPC resources at CYFRONET), has been integrated with the system. Additional IdPs can be plugged in and activated as required.

**System core**

The core of the security system comprises the EurValve Security Web Platform (EV SWP), which includes an IdP assertion consumer, a JSON Web Token issuer, a Policy Decision Point and a Policy Retrieval Point. JSON Web Tokens are a popular standard for authorizing requests to RESTful Web Services (such as those exposed by the EurValve platform) and ensuring that only authenticated and authorized users can initiate the relevant actions.

**Policy Decision Point**

A Policy Decision Point (PDP) is a subcomponent of the core service which makes authorization-related decisions. Each request received by the Portal must be accompanied by a valid user token which confirms the user’s identity. It should be noted that authenticating with EurValve does not entail the right to invoke arbitrary operations – the user must also be authorized for a given operation in accordance with **Policies**, which are stored and maintained by the portal. A separate Policy Retrieval Point (PRP) is built into the system to facilitate management of policies.

**Policy Enforcement Point**

A Policy Enforcement Point (PEP) contacts the PDP when a new request arrives, and obtains a decision on whether access to the selected service is permitted for the requestor. As the name implies, the task of the PEP is to *enforce* policy decisions – either by allowing the request to proceed or by preventing activation of a given operation. Within the EurValve research environment Policy Enforcement Points for HTTP(s) services are being implemented as NginX extensions.

**File access security**

The EurValve File Store represents a special type of service where more fine-grained access control is required. Specifically, each user may be granted access to a subsection of the overall project binary file tree. While the data storage component externally mimics a simple WebDAV server, fine-grained access control is implemented behind the scenes to ensure that user data is not viewable by unauthorized parties.

**Technologies**

Following careful consideration, a decision has been made to implement the core of the EurValve Security Platform as a Web Application exposing a simple REST service mechanism. The platform includes a versatile security module which supports a variety of authentication and authorization methods, including integration with many different Identity Provider services.

**Obtaining an EurValve account**

The EurValve portal is available at <https://valve.cyfronet.pl> – simply navigate to the portal and enter your login credentials. All users of the PL-Grid Infrastructure are automatically recognized. If you do not have a PL-Grid account, you can request a dedicated EurValve account by accessing the Portal registration feature (you will need to be approved by one of the Portal’s administrators).

**Up-to-Date API Documentation**

The most recent documentation of the REST API can be found at the following addresses:

* Authentication / Token retrieval: <https://valve.cyfronet.pl/help/api/sessions>
* Policy Decision Point (PDP): <https://valve.cyfronet.pl/help/api/pdp>
* Policy management: <https://valve.cyfronet.pl/help/api/policies>