SECURITY

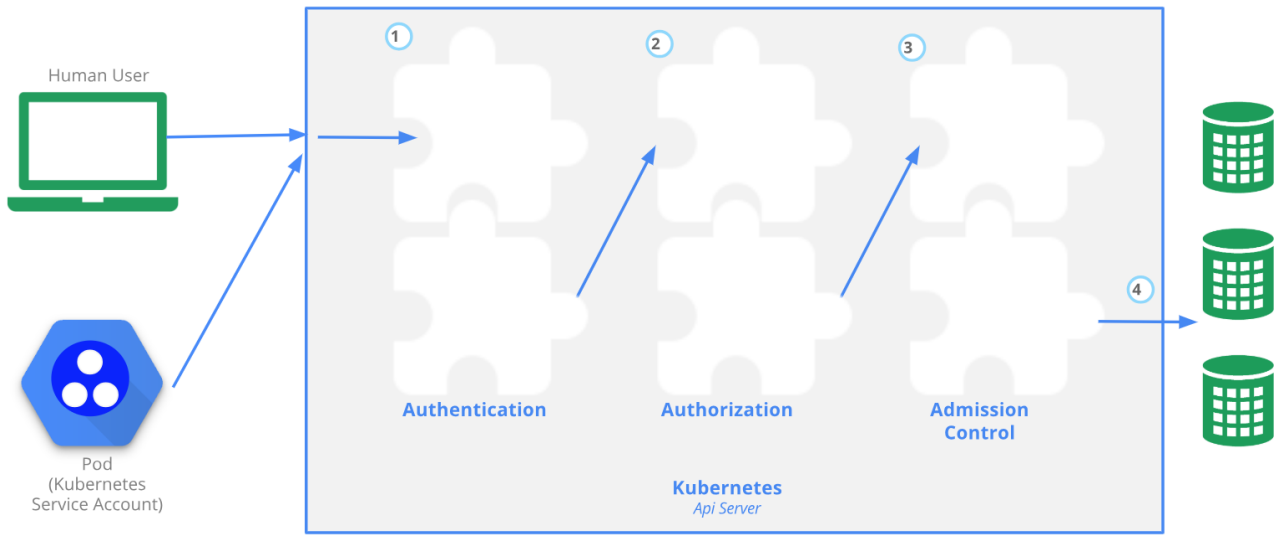
# Security

# Accessing the API

To perform any action in a Kubernetes cluster, you need to access the API and go through three main steps:

- Authentication (token):
- Authorization (RBAC):
- Admission Controllers.

These steps are described in more detail in the official documentation about controlling access to the Kubernetes API and illustrated by the diagram below.




**Accessing the API**
Retrieved from the Kubernetes website

Once a request reaches the API server securely, it will first go through any authentication module that has been configured. The request can be rejected if authentication fails or it gets authenticated and passed to the authorization step.

At the authorization step, the request will be checked against existing policies. It will be authorized if the user has the permissions to perform the requested actions. Then, the requests will go through the last step of admission. In general, admission controllers will check the actual content of the objects being created and validate them before admitting the request.

In addition to these steps, the requests reaching the API server over the network are encrypted using TLS. This needs to be properly configured using SSL certificates. If you use **kubeadm**, this configuration is done for you; otherwise, follow *Kubernetes the Hard Way* by Kelsey Hightower, or review the API server configuration options.