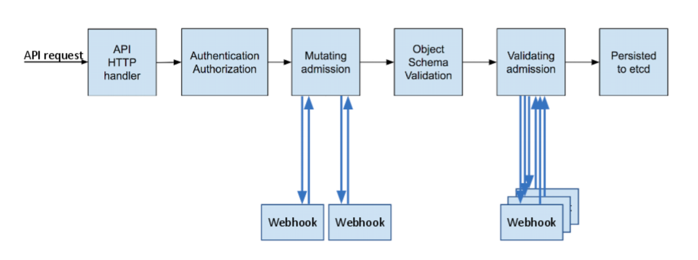
EKS에서 기존에 Pod에 IAM Role을 부여하기 위해선 Kube2IAM과 KIAM을 사용했다.

* KIAM: 하나의 노드에서 Assume Role를 가지고 모든 SDK의 응답을 대신해서 처리해주는 방식.
* Kube2IAM: 모든 노드가 Assume Role을 가지고 각 파드들의 응답을 처리하는 방식.



우선 쿠버네티스 API는 위와 같은 절차를 거쳐 처리된다. API 서버로 들어오는 모든 요청은 etcd에 저장되는데, 이 전에 auth를 거치며, JWT or Certificate를 통해 클라이언트를 인증 후 RBAC 권한과 매칭되는지 검사한다. 해당 요청이 권한이 있다고 판단되면, Mutate, Validate 과정을 거쳐 etcd에 저장하는 구조다.

ServiceAccount는 이러한 Admission Controller에 대한 하나의 플러그인이다. 또한, Kubernetes는 OpenID Connect (OIDC)를 지원하기 때문에, Service Account와 OIDC를 매핑하여 인증절차로 사용할 수 있다. 다만 이를 WebHook에서 이전에는 Pod Identity WebHook으로 따로 구성하여서 사용했다. 하지만 이제는 AWS에서 IAM이 OIDC와 연동이가능하게 제공하고있다.

