



SECURING KUBERNETES WITH OPENID CONNECT

WHY ?

- ▶ We don't need to maintain multiple usernames/passwords
- ▶ We don't need to manage another user management system
- ▶ We want to accelerate sign in process
- ▶ We want to use the best method of authorization in Kubernetes !

HOW DOES KUBERNETES AUTH/RBAC WORK ?

KUBECTL/
HTTP

AUTHENTICATION

AUTHORIZATION/
RBAC



ADMISSION
CONTROLLERS

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  namespace: default
  name: pod-reader
rules:
- apiGroups: ["" ] # "" indicates the core API
  group
  resources: ["pods"]
  verbs: ["get", "watch", "list"]
```

WHAT IS OPENID CONNECT ?

- ▶ OAuth2 - "Login with Facebook"
- ▶ Discovery - .well-known/openid-configuration
- ▶ JWT Token



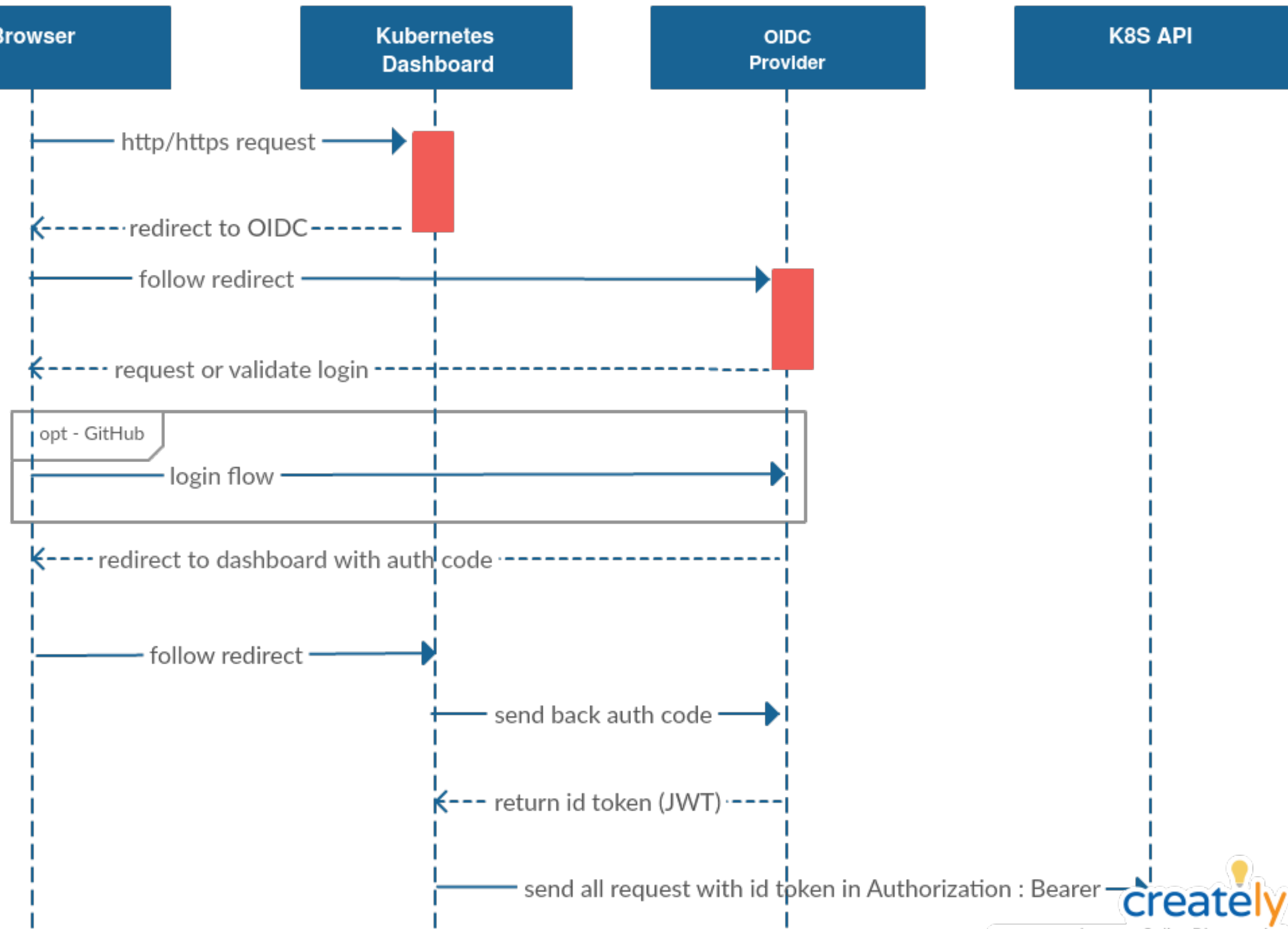
AUTHORIZATION: BEARER/JWT TOKEN

PAYLOAD: DATA

```
{
  "iss": "https://192.168.99.100:32000",
  "sub": "CggzMDU5MjQ1NRIGZ2l0aHVi",
  "aud": "kubernetes",
  "exp": 1519312060,
  "iat": 1519225660,
  "nonce": "MQQEOWWKPZAUOBVZ",
  "at_hash": "1pe2o7-mipBTMGbzsrkWSg",
  "email": "adamdrozd1@gmail.com",
  "email_verified": true
}
```



HOW OIDC WORKS ?



DEX & PROVIDERS

- ▶ LDAP
- ▶ GitHub/GitLab
- ▶ SAML 2.0
- ▶ OpenID Connect (Google)
- ▶ LinkedIn
- ▶ Microsoft
- ▶ AuthProxy



VIA 9GAG.COM

Q&A ?

Q&A

THANK YOU!

- ▶ github.com/lintops-tech
- ▶ Email: `adamdrozdz@lintops.tech`
- ▶ <https://lintops.tech>

