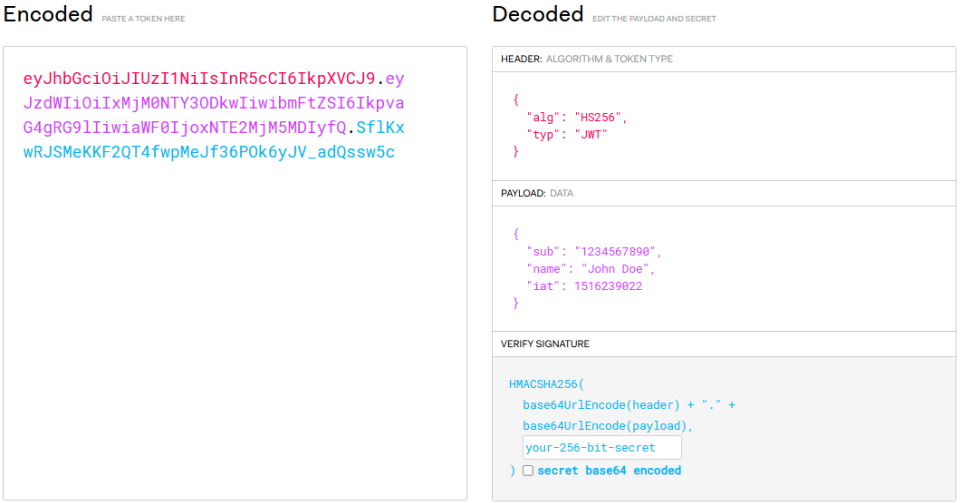
Enhancing Security with Istio: Realtime JWT Access Revocation

Josh Oberdick, Rocket Companies

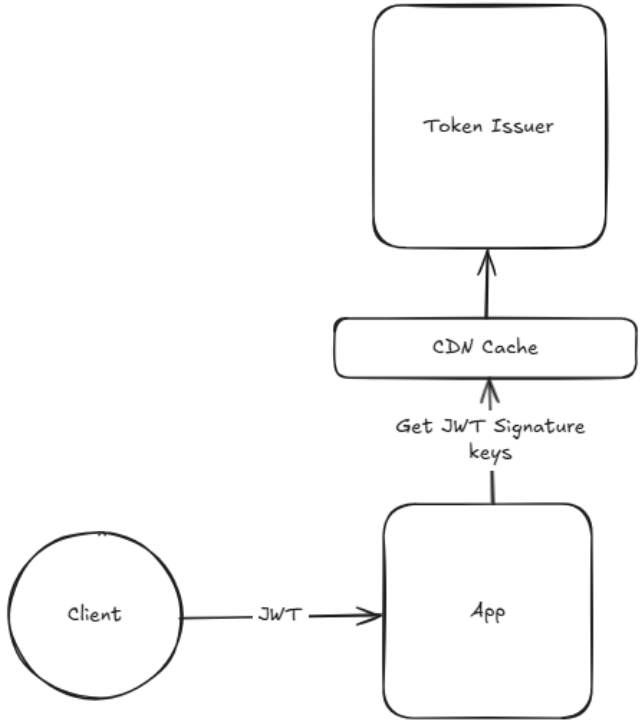
What are JWTs?

- Open standard for JSON based tokens
- Supports claims encoded in token
- Verifiable/tamper proof



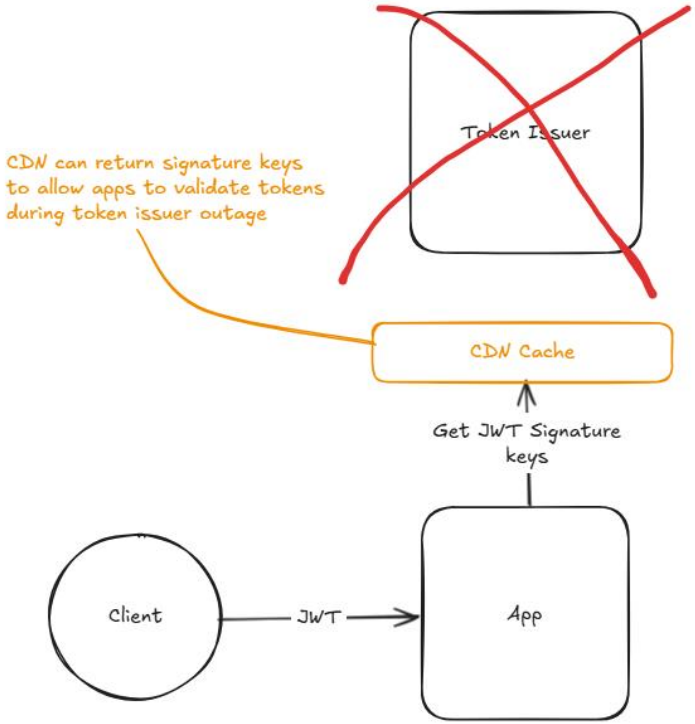
Advantage of JWTs

- Lightweight – can be less than 1kB
- Portable – SDK's for all platforms
- **Stateless** – tokens can be verified at unlimited scale, even when token issuer is offline
- Performance – signature keys can be cached in local apps



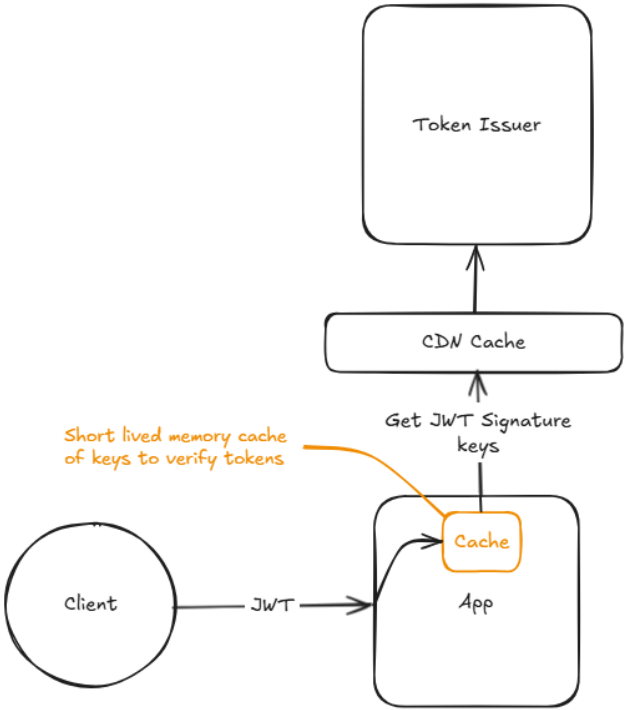
Advantage of JWTs

- Lightweight – can be less than 1kB
- Portable – SDK's for all platforms
- **Stateless** – tokens can be verified at unlimited scale, even when token issuer is offline
- Performance – signature keys can be cached in local apps

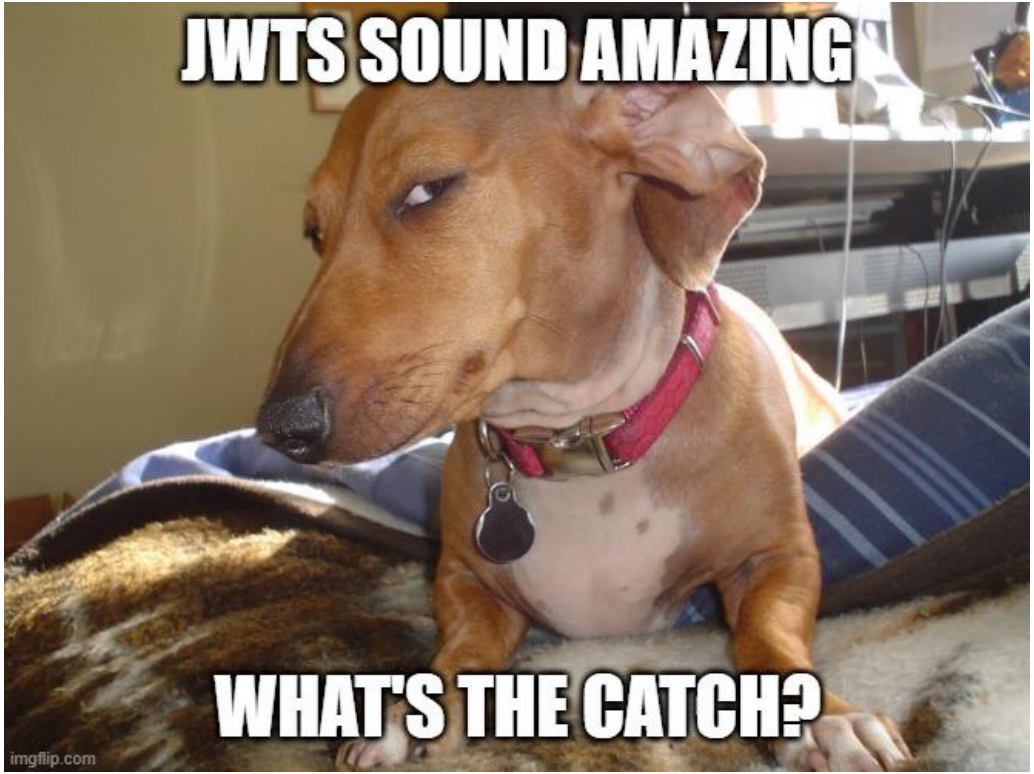


Advantage of JWTs

- Lightweight – can be less than 1kB
- Portable – SDK's for all platforms
- Stateless – tokens can be verified at unlimited scale, even when token issuer is offline
- **Performance** – signature keys can be cached in local apps



Advantage of JWTs



Biggest weakness of JWTs

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022,
  "exp": 1516249022
}
```

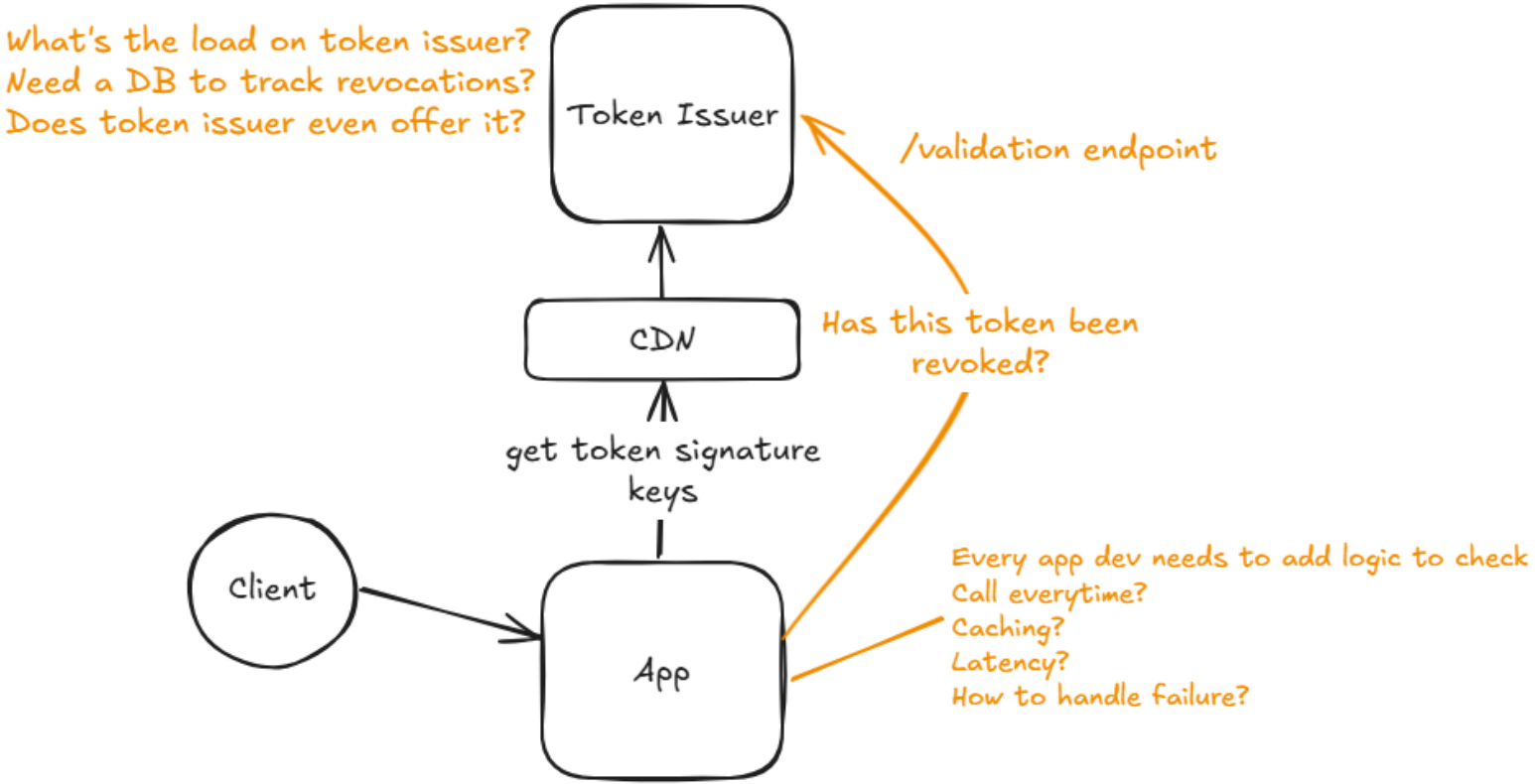
You have unlimited scale for your tokens

They can never be revoked before their expiration

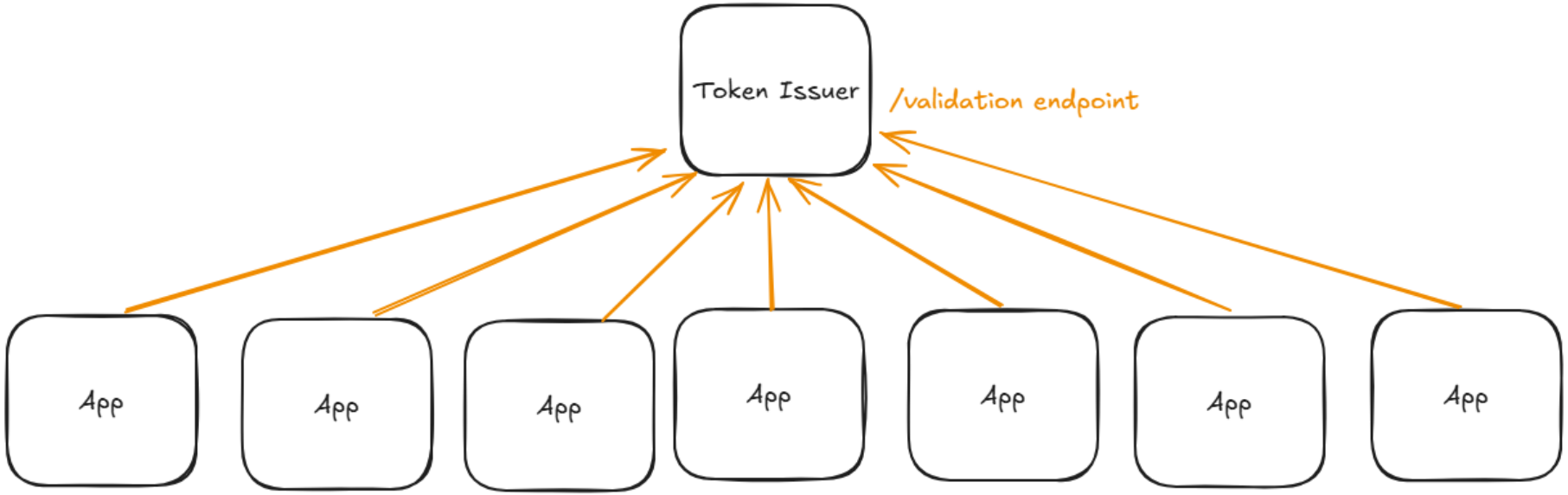
Should you care?

Security team – “Hi, we just found out Jane’s account was compromised. We need to disable all their access immediately!”
Ops team – “No problem, we will disable the account right now.”
Security team – “Thanks! All Their app access is removed then?
Ops team – Uh, well actually any app that had a token still has access for the next few hours 😬…
Security team – …
Security team – How is that possible!?
Ops team – we use JWTs🙂
< CIO has joined the chat >

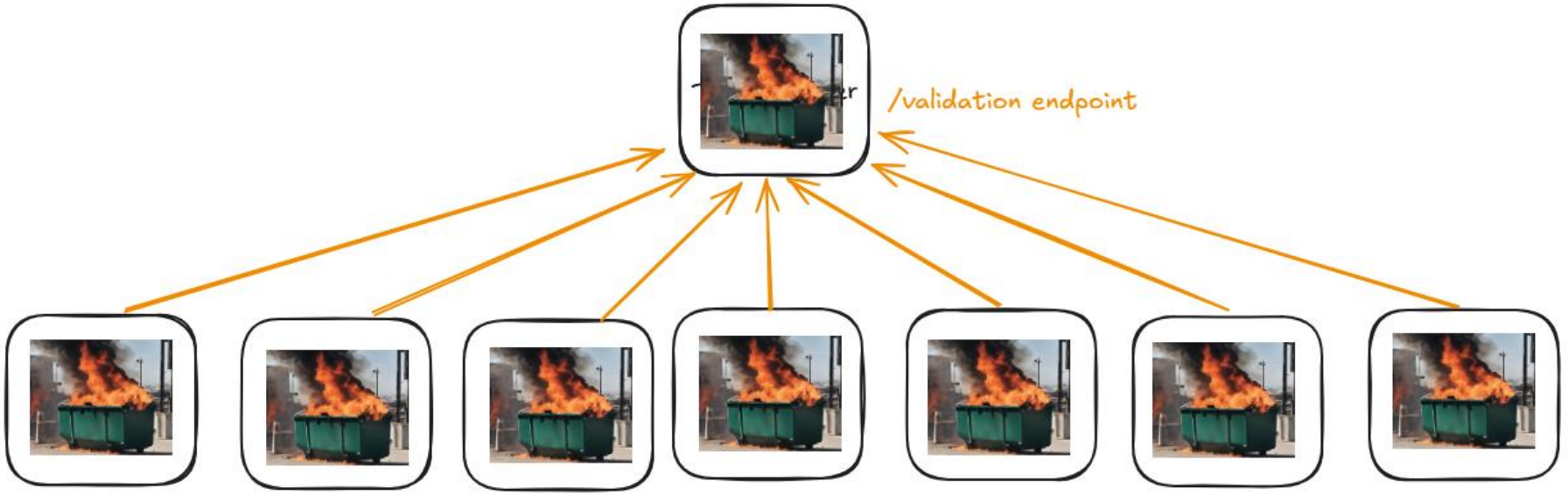
Asking your app dev teams to solve



Asking your app dev teams to solve

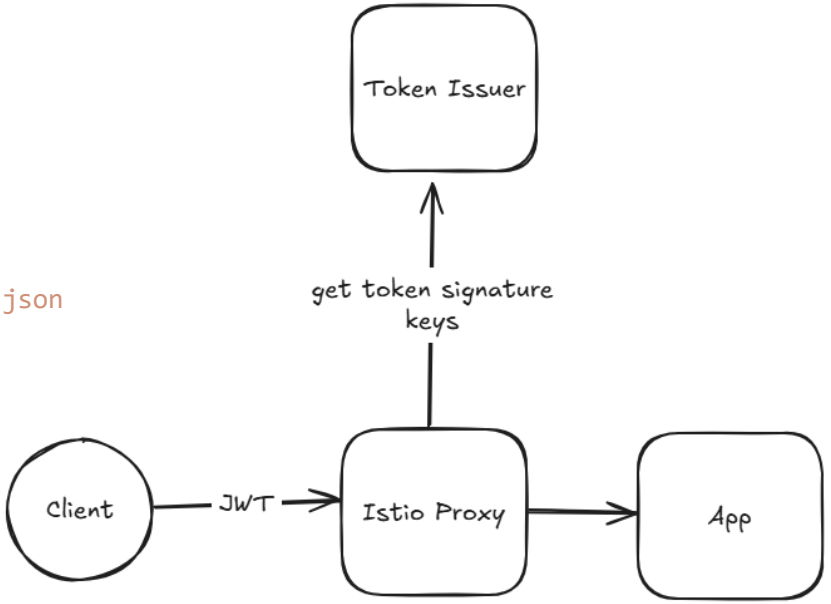


Asking your app dev teams to solve

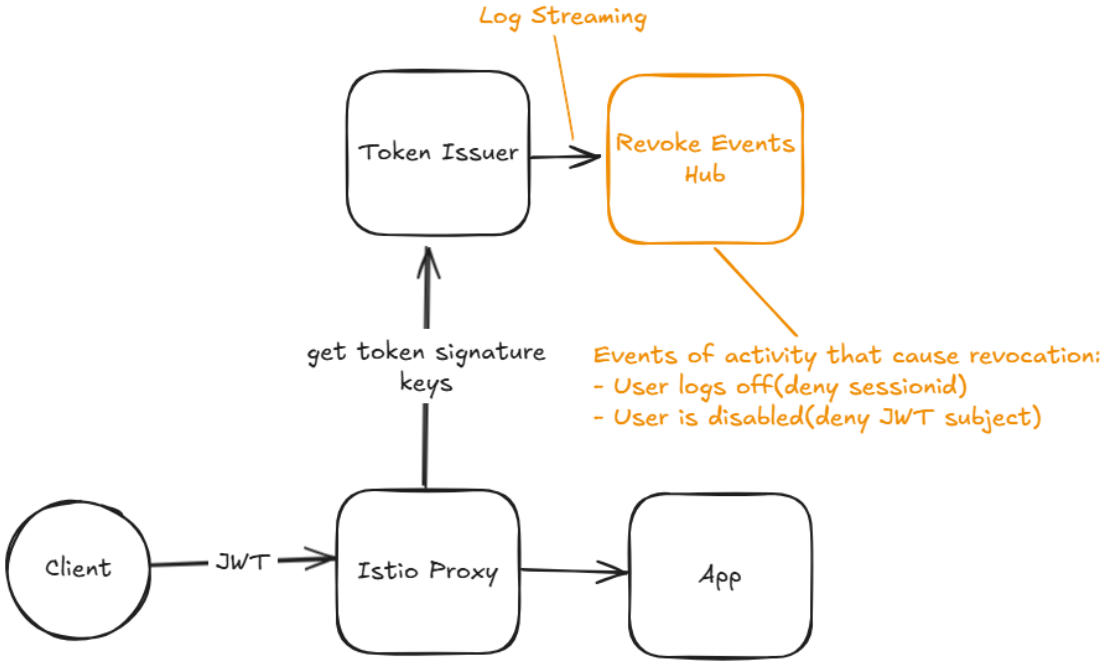


Istio to the rescue

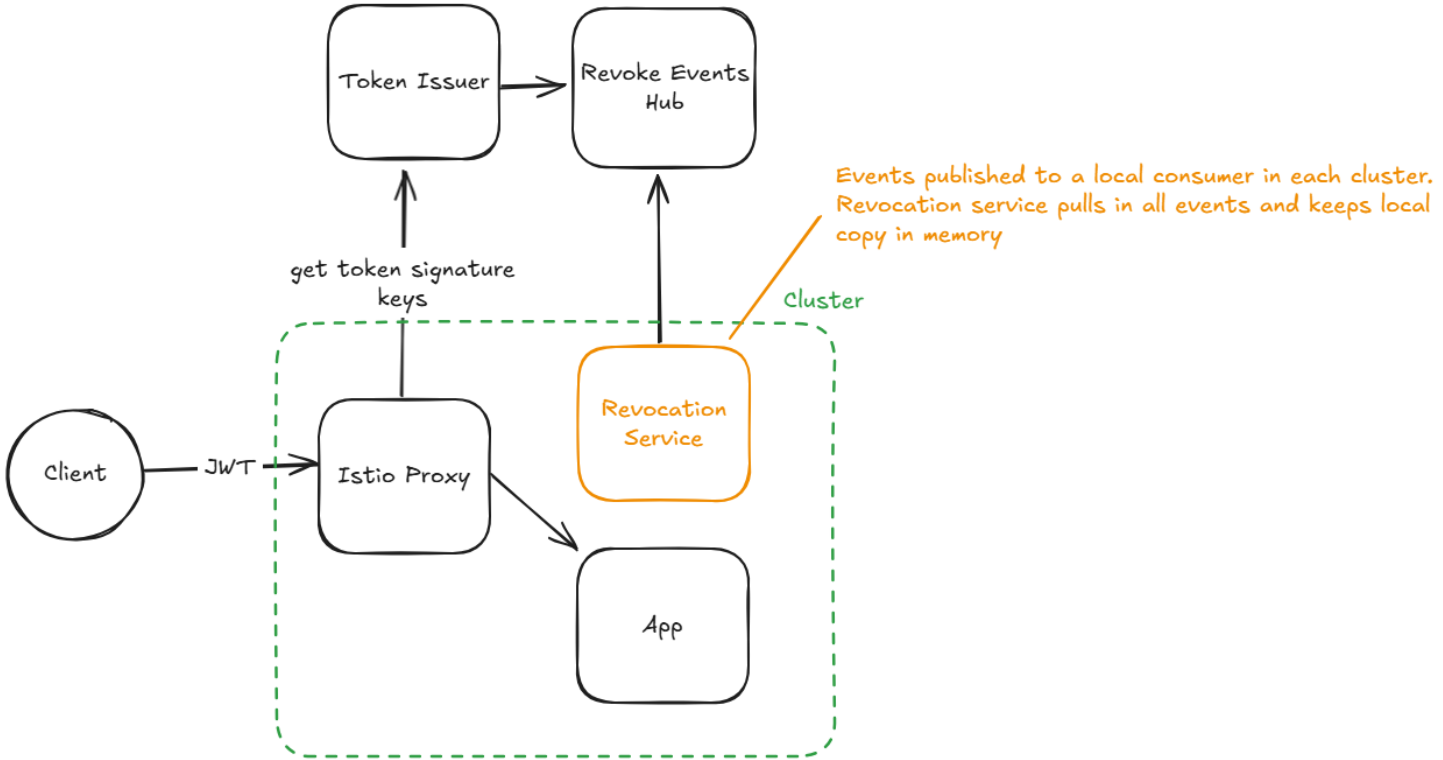

```yaml
apiVersion: security.istio.io/v1
kind: RequestAuthentication
metadata:
  name: httpbin
  namespace: foo
spec:
  selector:
    matchLabels:
      app: httpbin
  jwtRules:
  - issuer: "issuer-foo"
    jwksUri: https://example.com/.well-known/jwks.json
---
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: httpbin
  namespace: foo
spec:
  selector:
    matchLabels:
      app: httpbin
  rules:
  - from:
    - source:
        requestPrincipals: ["*"]
```



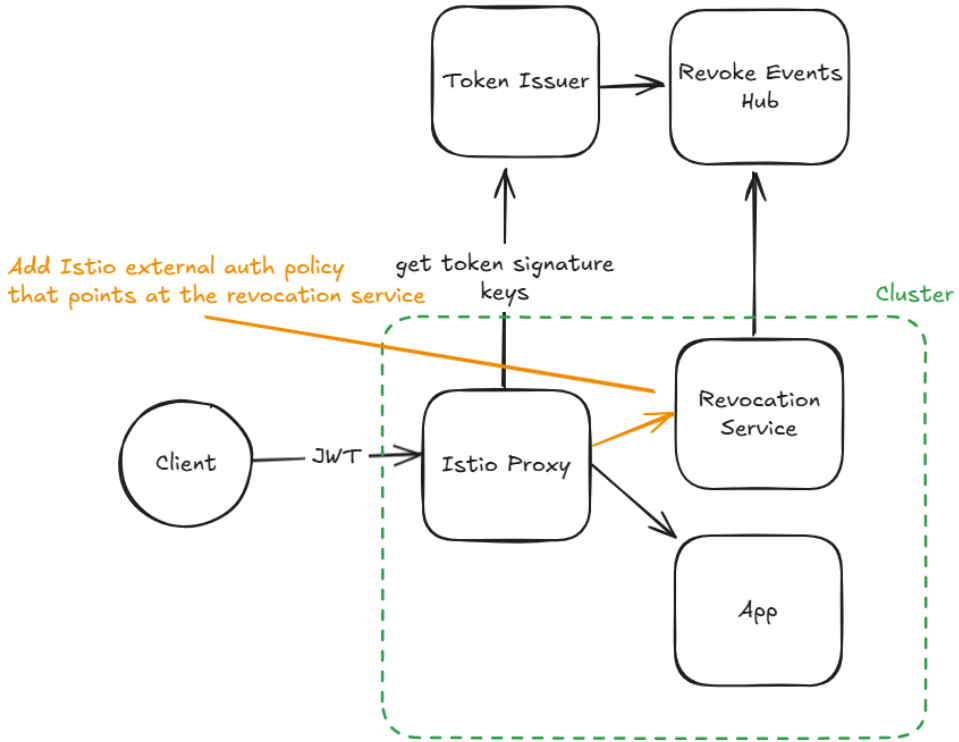
Istio to the rescue



Istio to the rescue

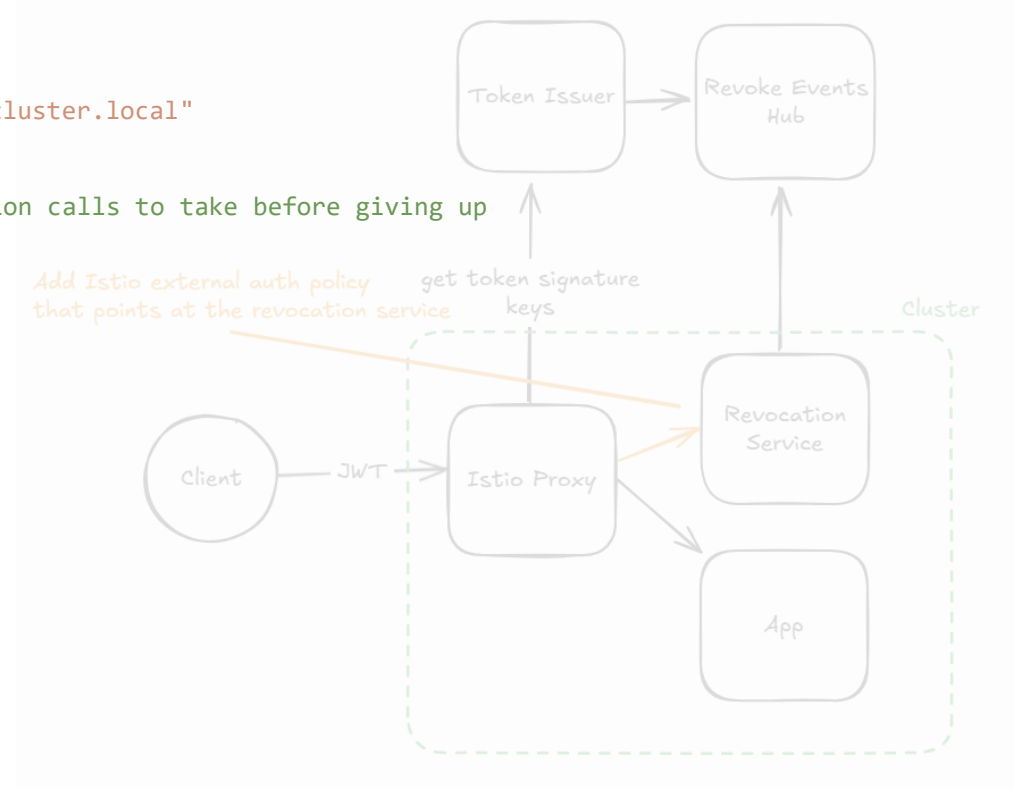


Istio to the rescue



Istio to the rescue

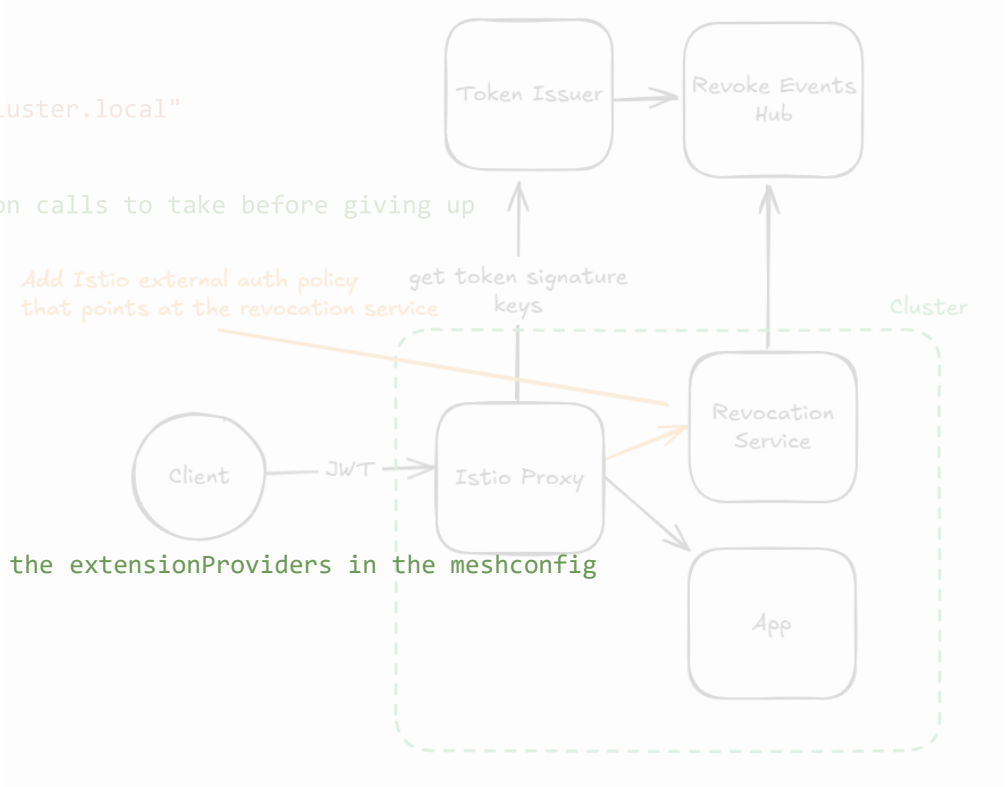

```yaml
meshConfig:
  extensionProviders:
  - name: "revocation-service"
    envoyExtAuthzHttp:
      service: "revocation-service.foo.svc.cluster.local"
      port: "80"
      failOpen: # true or false
      timeout: # time that we allow revocation calls to take before giving up
```



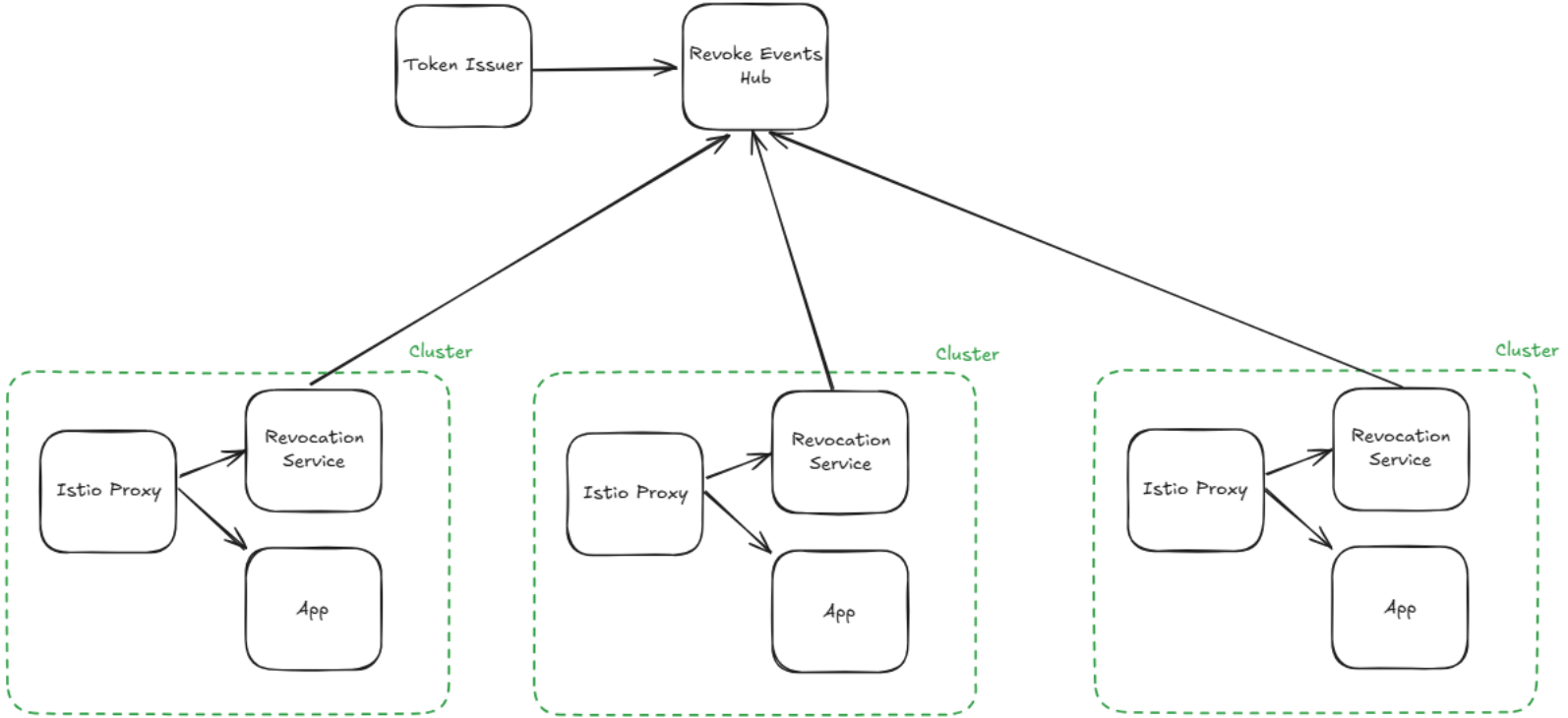
Istio to the rescue


```yaml
meshConfig:
  extensionProviders:
  - name: "revocation-service"
    envoyExtAuthzHttp:
      service: "revocation-service.foo.svc.cluster.local"
      port: "80"
      failOpen: # true or false
      timeout: # time that we allow revocation calls to take before giving up
```

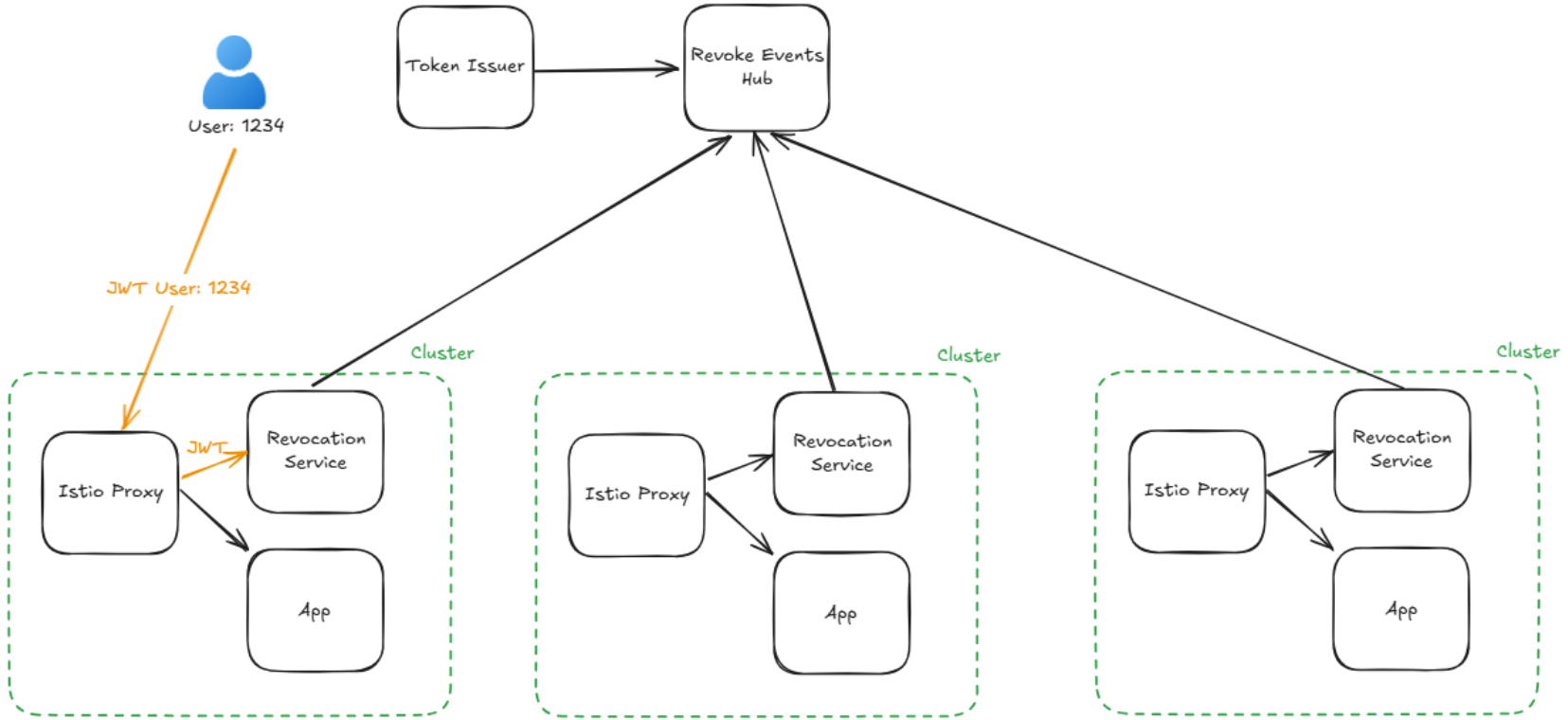
```yaml
apiVersion: security.istio.io/v1
kind: AuthorizationPolicy
metadata:
  name: revocation-check
spec:
  selector:
    matchLabels:
      app: httpbin
  action: CUSTOM
  provider:
    # The provider name matches the name of the extensionProviders in the meshconfig
    name: revocation-service
  rules:
  - to:
    - operation:
        paths: ["/*"]
```



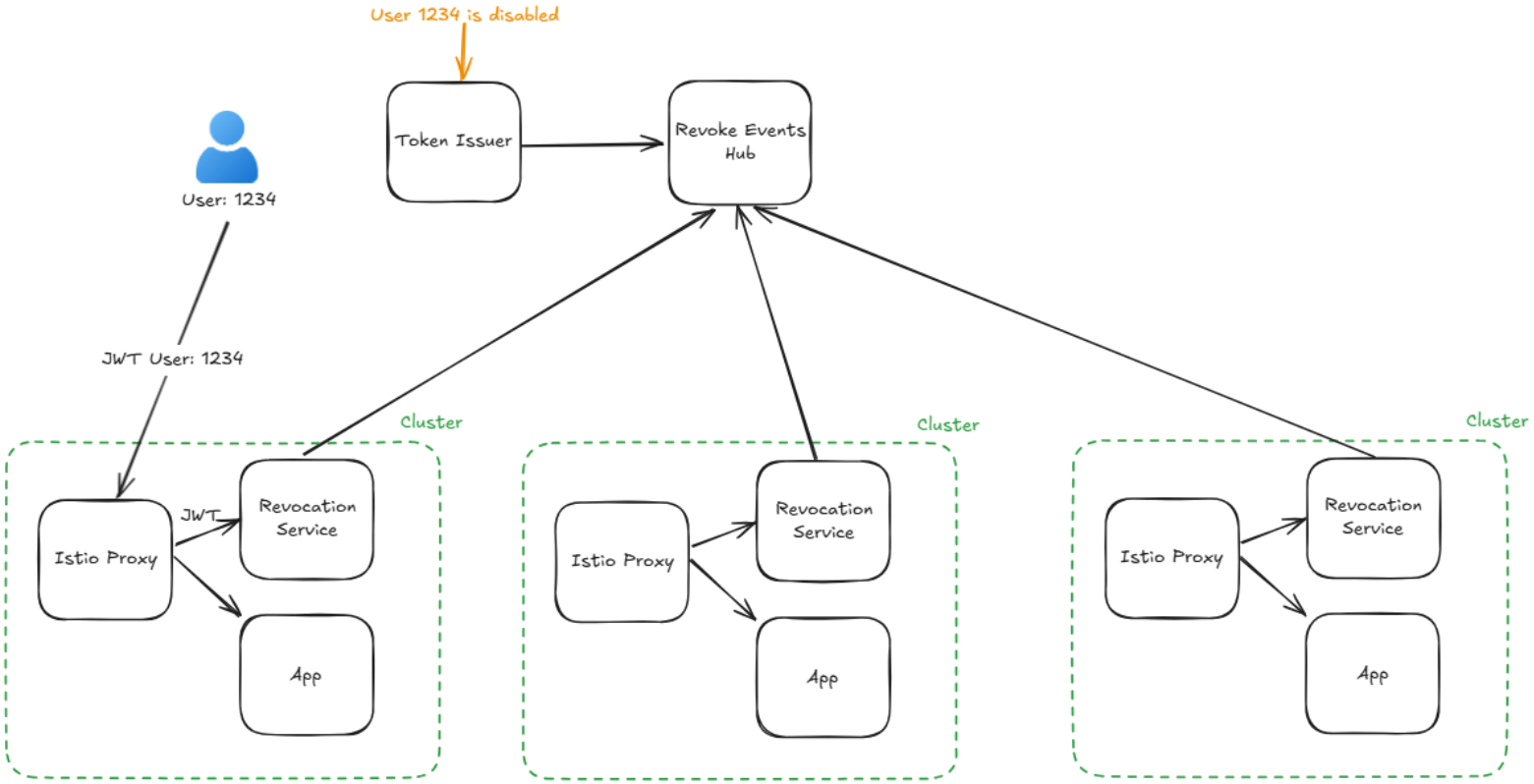
Istio to the rescue



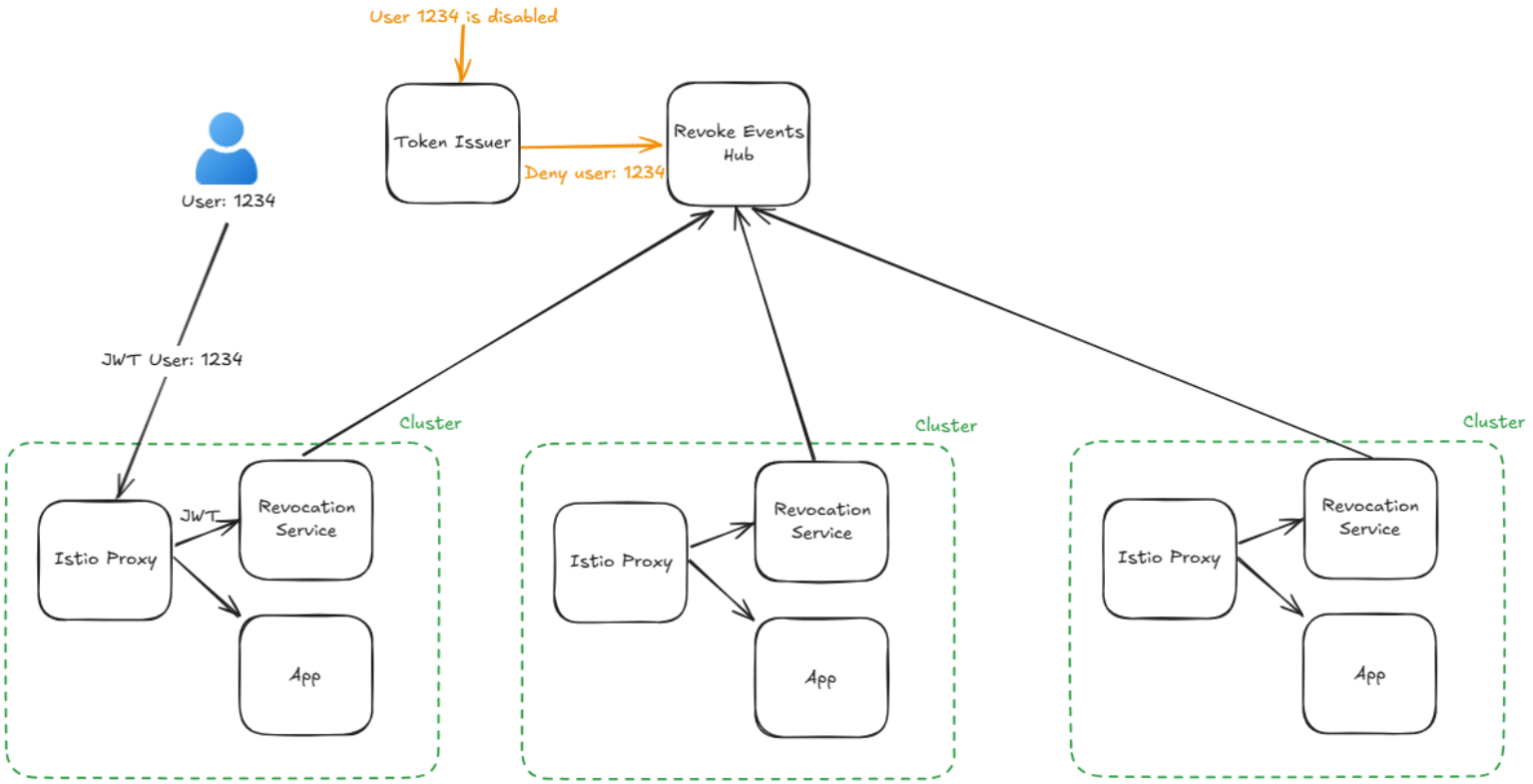
Istio to the rescue



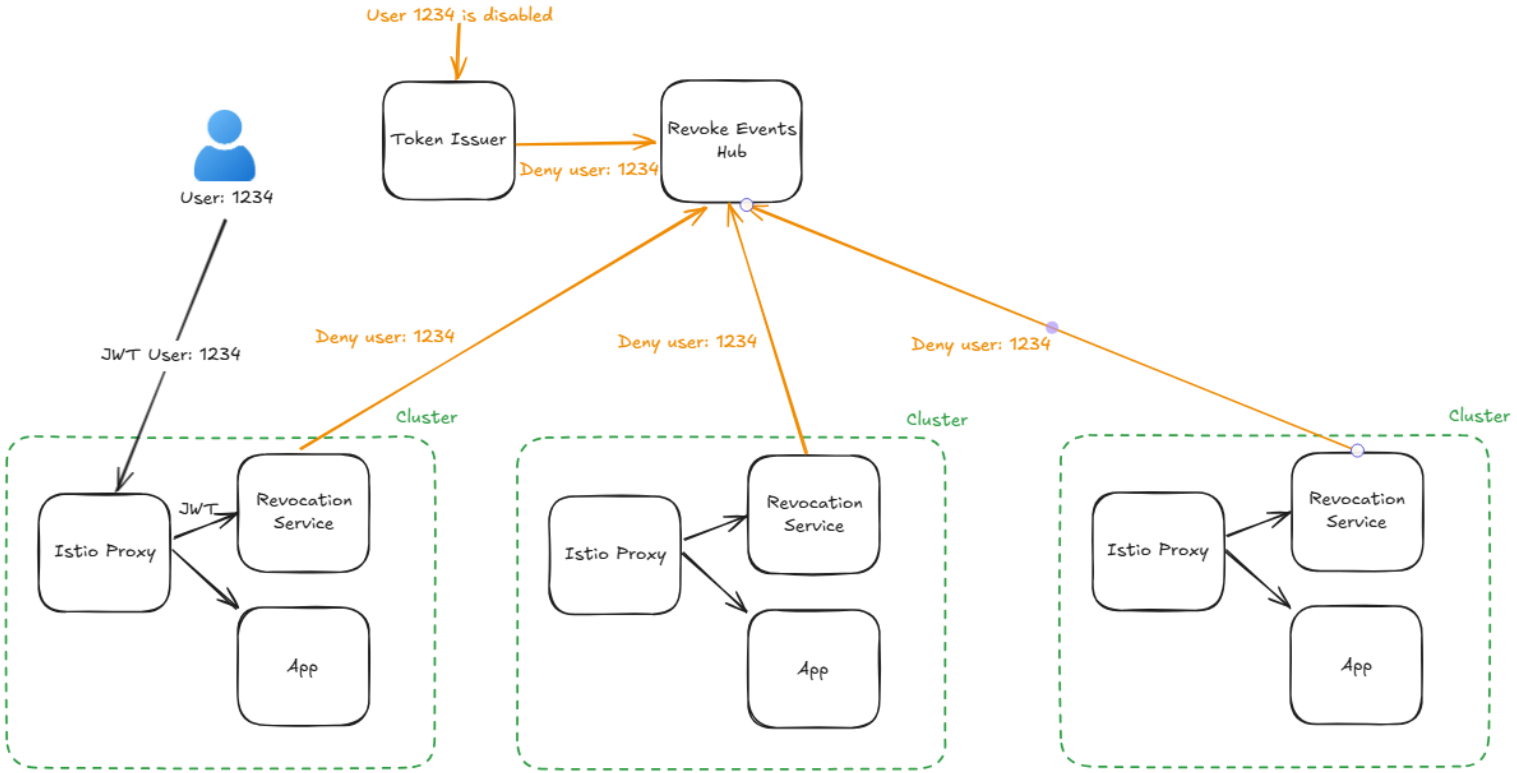
Istio to the rescue



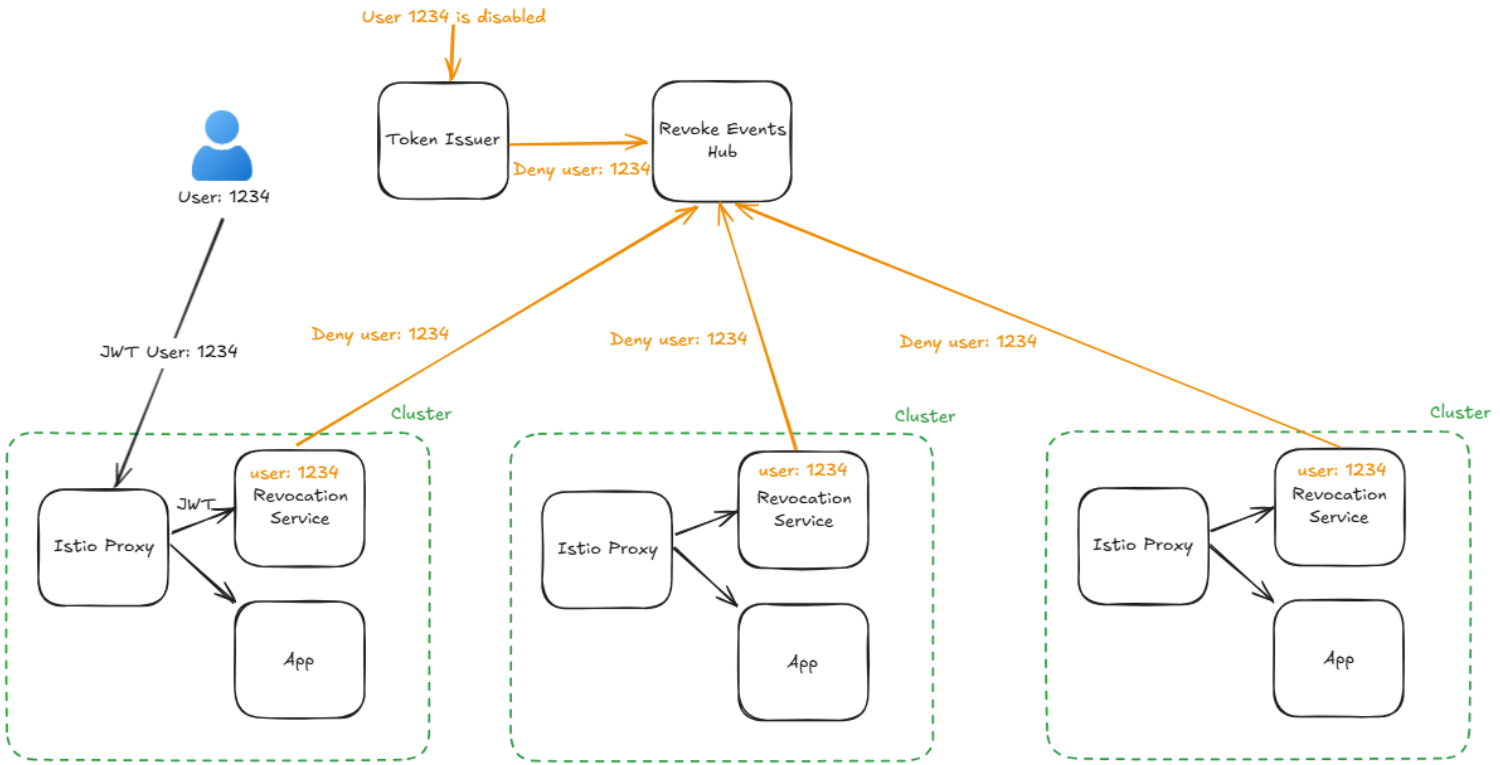
Istio to the rescue



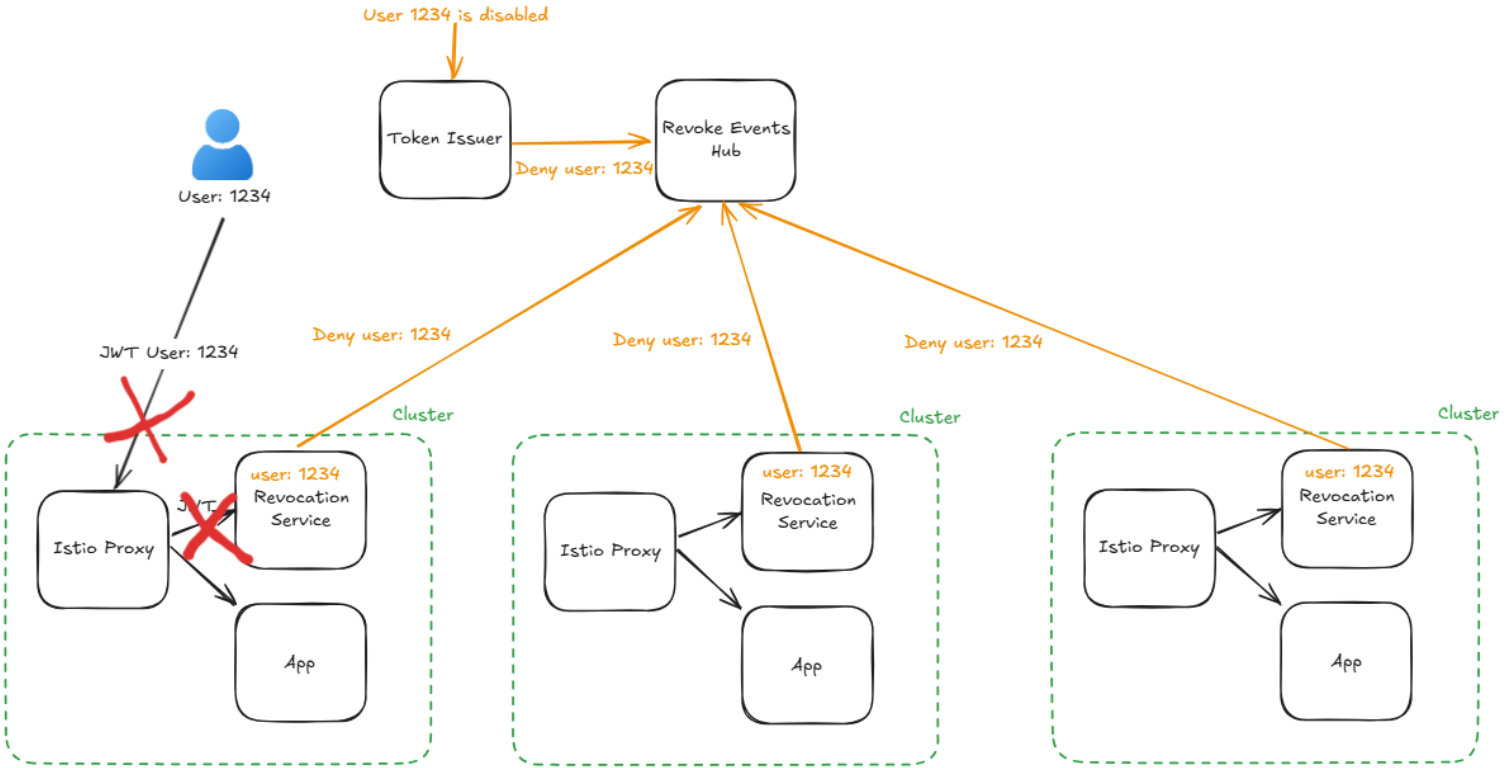
Istio to the rescue



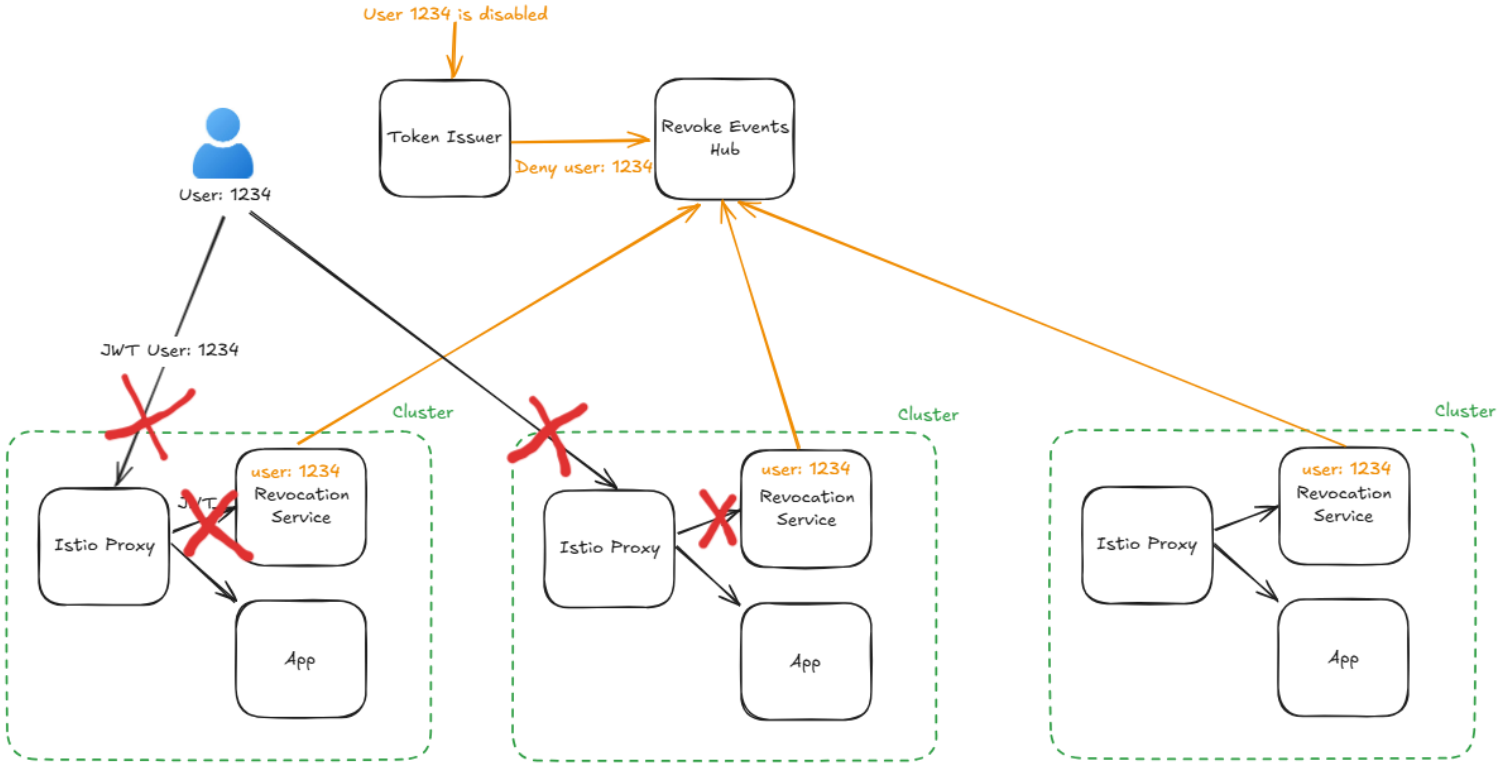
Istio to the rescue



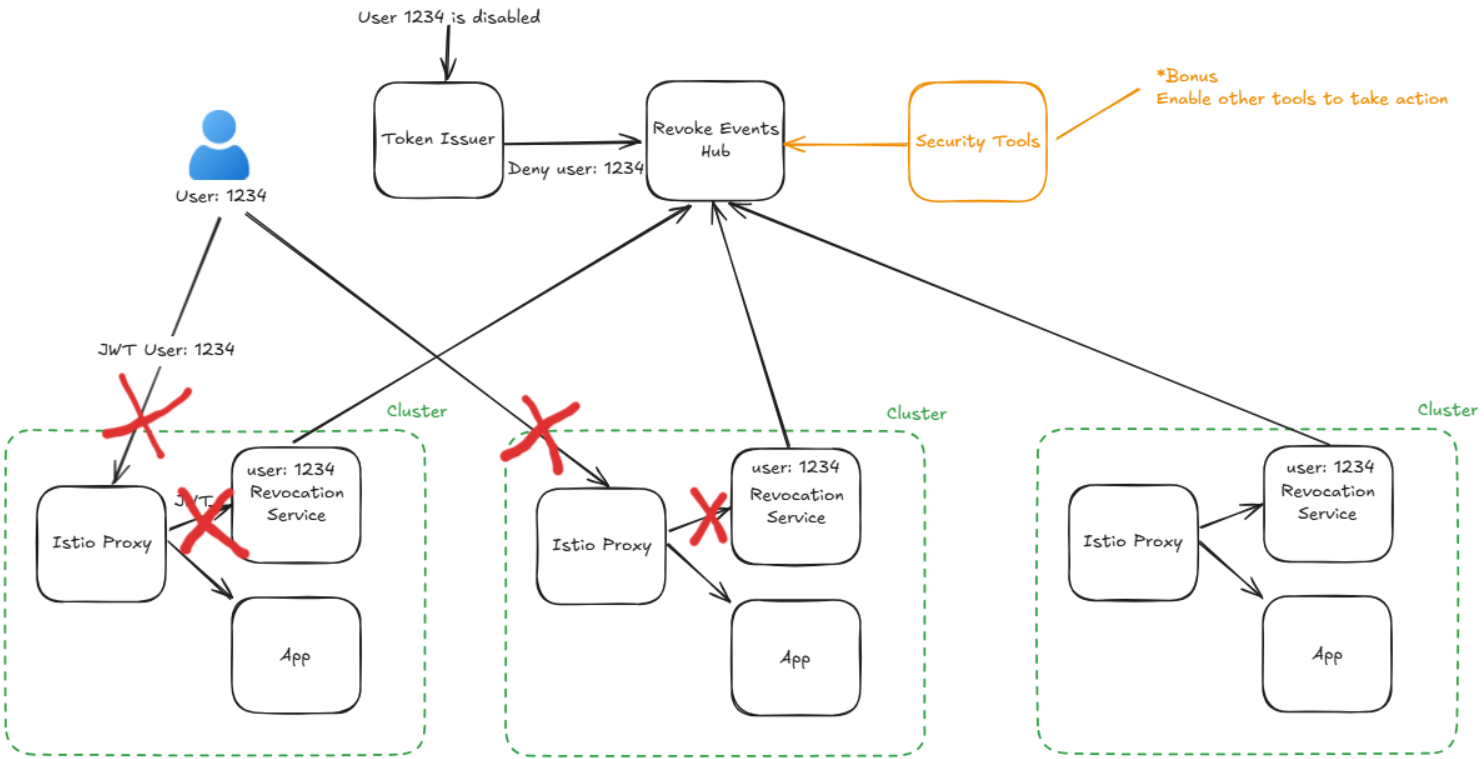
Istio to the rescue



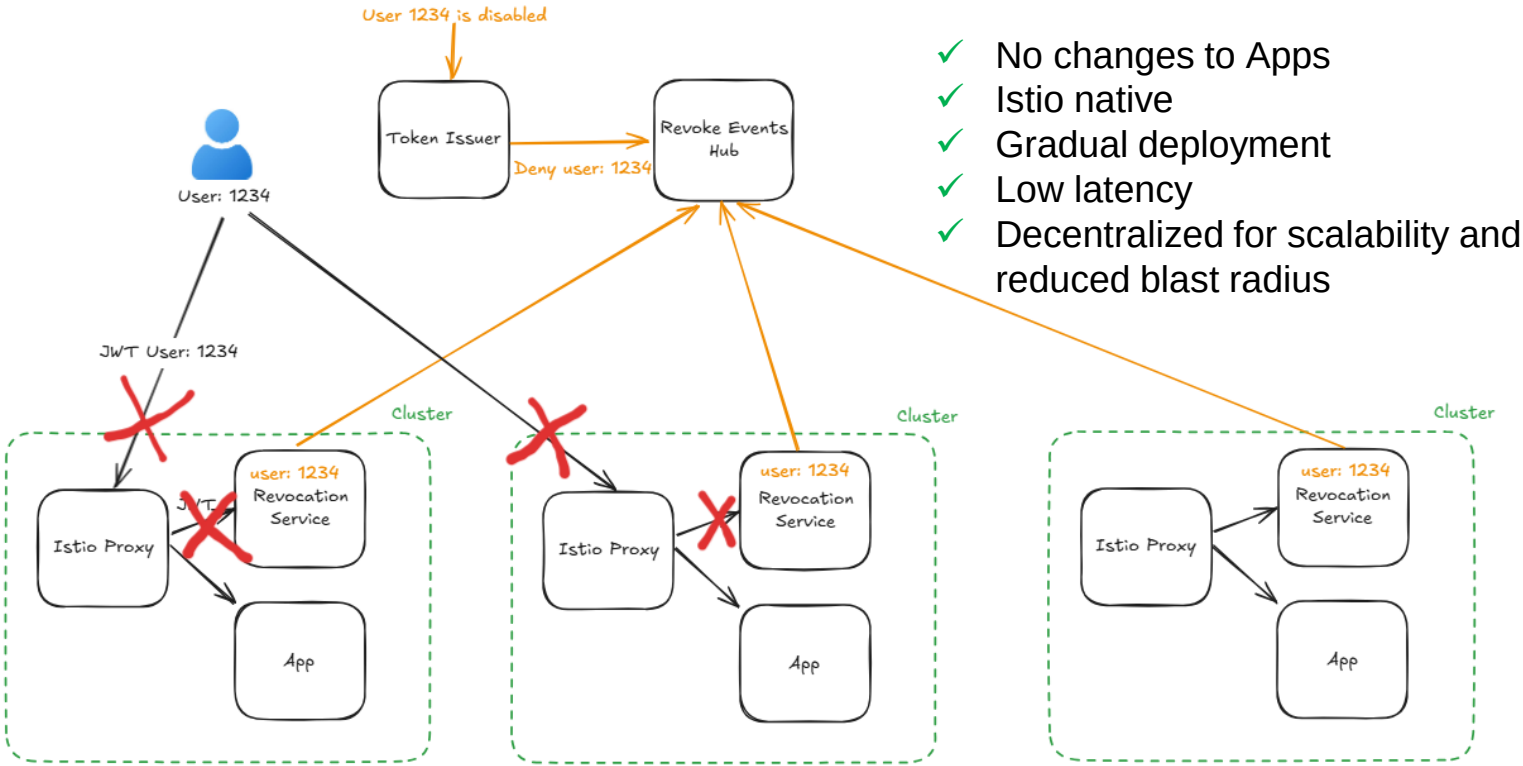
Istio to the rescue



Istio to the rescue



Istio to the rescue



- ✓ No changes to Apps
- ✓ Istio native
- ✓ Gradual deployment
- ✓ Low latency
- ✓ Decentralized for scalability and reduced blast radius

Closing

Things to keep in mind:

- Istio “Custom” authorization comes BEFORE standard authorization policies
- Canary and Locality based routing is not supported in external authorization

Inspiration:

- Continuous Access Evaluation By Microsoft
- Shared Signals by OpenID foundation: https://sharedsignals.guide/

Thanks to my colleague Matt Williams

Demo