

~~Tech Talks~~

KCD Austria 2nd Chance Edition

SSO for Kubernetes Using Dex

Let's get authenticated!



\$ whoami

Martin Nirtl

Solution Architect



I am an IT engineer 🏠 with strong backgrounds in software, DevOps/platform and electronic engineering working for **Mirantis** as a pre-sales solution architect. Next to my job, my main side-hustles are all around Kubernetes 🚢, IaC and automating things. From time to time, I even build little apps in Go or other languages.



[**martinnirtl**](https://twitter.com/martinnirtl)



[**martinnirtl**](https://www.linkedin.com/in/martinnirtl)



[**martinnirtl**](https://github.com/martinnirtl)



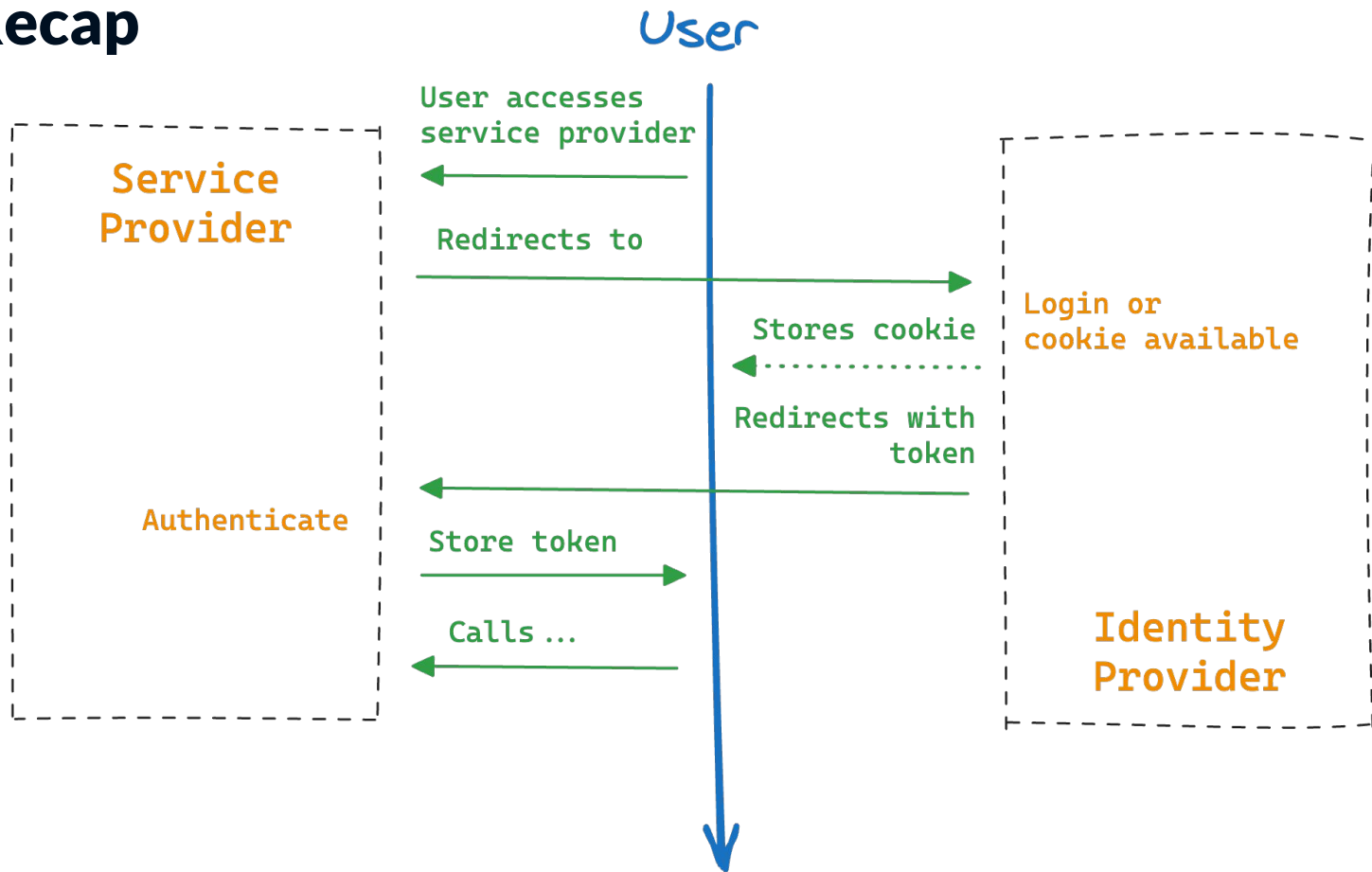
Slides, Code and more!

Single Sign-On Recap

Let's do a quick refresher!



SSO Recap



Kubernetes Authentication

Reminder for Martin: Don't talk too much!

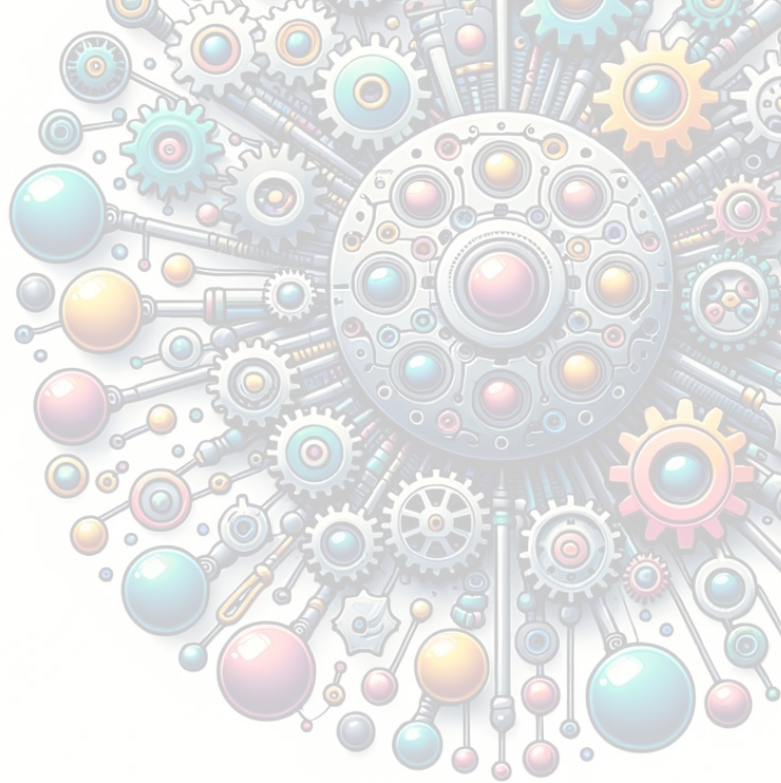
X509 Client Certs

- User Info stored in Cert Subject
 - Username: Common Name (CN=)
 - Groups: Organization fields (O=)
- Requires API-Server Params
 - client-ca-file
 - tls-cert-file
 - tls-private-key-file
- Generate certificates manually
- Use certificates.k8s.io API

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 8937326423629948540 (0x7c07c307c22ce67c)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: CN=kubernetes
  Validity
    Not Before: Oct 17 18:17:59 2023 GMT
    Not After : Oct 16 18:18:00 2024 GMT
  Subject: O=system:masters, CN=kubernetes-admin
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
      00:e1:7d:72:4a:a8:3f:08:c4:fe:fd:21:23:96:ca:
      88:ad:04:a4:0e:90:b8:b1:2f:4a:5c:c9:8e:5c:f6:
      06:ae:9b:4a:67:65:40:18:3e:f2:78:03:ba:95:73:
      3a:f7:d5:18:98:d0:32:25:2c:8a:97:79:1c:14:79:
      d5:84:97:05:d9:b7:fa:f0:d7:e9:35:8e:4f:e0:92:
      2d:f7:a8:42:e6:27:78:6c:74:52:88:71:16:0a:6f:
      ab:c0:e2:ea:35:48:42:91:6e:27:85:09:4f:9c:d9:
      3b:07:c4:ac:cd:59:7e:6b:1d:ce:09:1b:07:8b:7b:
      93:28:32:d7:ca:0d:bd:16:75:11:82:52:c9:54:f6:
      0a:9a:e2:40:ed:e5:51:83:c8:aa:41:33:f5:63:6e:
      5b:5a:00:ea:50:88:3b:99:bb:1e:a2:d8:1b:a5:18:
      ea:0e:3d:a7:94:c9:f1:6e:ed:a1:e4:98:0c:d3:4e:
      86:c2:eb:c2:9e:3a:35:d7:b4:86:70:af:78:b1:c5:
      61:b2:36:b4:25:31:1a:71:65:f3:bc:50:5d:41:08:
      45:d3:af:a7:2d:c7:ba:44:7b:8e:89:15:6f:52:91:
      21:11:d4:42:9c:e0:ea:a7:ca:1a:f6:f9:a2:1b:08:
      61:b6:03:a3:50:97:60:a6:cc:ab:8f:ec:b2:1f:0a:
      b3:59
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Key Usage: critical
      Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
      TLS Web Client Authentication
    X509v3 Basic Constraints: critical
      CA:FALSE
    X509v3 Authority Key Identifier:
      keyid:08:28:09:E2:4B:F4:F5:EC:E3:EB:D2:C0:08:3F:FF:39:A5:2E:A
Signature Algorithm: sha256WithRSAEncryption
10:f2:2d:80:58:18:5b:28:2b:2a:9b:9c:2a:61:00:41:b0:0b:
f3:4a:0d:c2:9e:6b:b6:c8:06:ea:09:b4:7b:20:f0:ae:91:63:
0f:d7:54:c9:7f:ea:22:16:9b:b1:e8:72:43:32:df:0a:79:2d:
07:51:95:e2:b7:7c:ef:e4:17:01:de:38:59:f8:1c:3a:a6:f4:
6a:4a:32:df:5d:46:a1:99:45:c5:ae:ee:76:c4:87:fd:1f:86:
a1:16:32:7b:87:ec:0c:05:38:67:d6:f1:94:63:4f:8b:ed:e6:
a3:4a:3e:50:b6:a6:30:cc:04:c0:4a:6e:c7:9b:dd:64:04:62:
5d:8d:a4:96:04:12:2a:26:52:af:09:d0:a8:4c:64:c6:8a:51:
69:71:57:8d:6d:63:62:da:f6:43:06:0f:e5:01:ba:96:a9:77:
a7:ce:17:56:6f:e4:59:f7:65:77:ca:9f:d3:98:5a:41:e7:05:
ed:cd:d4:1f:7e:3c:4e:a9:b6:a4:c5:25:84:bb:c2:85:08:c7:
a9:87:78:f6:88:e0:5f:84:75:f3:a4:ef:bc:7a:61:dc:5a:bb:
77:fb:54:16:52:cf:47:56:7c:05:27:24:a8:6a:ff:6a:0d:6e:
ae:75:53:6a:36:f8:88:50:a0:ee:37:20:3c:72:91:5f:e0:53:
1e:3d:4c:b2
```

Bootstrap Tokens

- Bootstrapping new Clusters
 - Joining nodes, etc.
- Token Format
 - `<token-id>.<token-secret>`
 - `[a-z0-9]{6}\.[a-z0-9]{16}`
 - `abcdef.0123456789abcdef`
- Requires API-Server Params
 - `Enable-bootstrap-token-auth`
- Authorization
 - Bearer `<token>`



Sample Bootstrap Token

Source: <https://kubernetes.io/...>

```
apiVersion: v1
kind: Secret
metadata:
  # Name MUST be of form "bootstrap-token-<token id>"
  name: bootstrap-token-07401b
  namespace: kube-system
# Type MUST be 'bootstrap.kubernetes.io/token'
type: bootstrap.kubernetes.io/token
stringData:
  # Human readable description. Optional.
  description: "The default bootstrap token generated by 'kubeadm init'."
  # Token ID and secret. Required.
  token-id: 07401b
  token-secret: f395accd246ae52d
  # Expiration. Optional.
  expiration: 2017-03-10T03:22:11Z
  # Allowed usages.
  usage-bootstrap-authentication: "true"
  usage-bootstrap-signing: "true"
  # Extra groups to authenticate the token as. Must start with "system:bootstrappers:"
  auth-extra-groups: system:bootstrappers:worker,system:bootstrappers:ingress
```

Static Token File

- Indefinitely lasting Tokens
- CSV File
 - `<token>,<username>,<uid>,<groups...>`
 - File on controller nodes
- Requires API-Server Params
 - `token-auth-file`
- API restart after update required
- Authorization Header
 - `Authorization: Bearer <token>`



Webhook Token Auth

- Arbitrary Auth-API
 - Receives TokenReview Object holding opaque token
 - Responds with TokenReview Object
- User fields in TokenReview
 - Required: username
 - Optional: uid, groups, extra
- Required API-Server Params
 - authentication-token-webhook-config-file

Source: <https://kubernetes.io/>

```
{
  "apiVersion": "authentication.k8s.io/v1beta1",
  "kind": "TokenReview",
  "status": {
    "authenticated": true,
    "user": {
      # Required
      "username": "janedoe@example.com",
      # Optional
      "uid": "42",
      # Optional group memberships
      "groups": ["developers", "qa"],
      # Optional additional information provided by
      # This should not contain confidential data,
      # or API objects, and is made available to all
      "extra": {
        "extrafield1": [
          "extravalue1",
          "extravalue2"
        ]
      }
    }
  },
  # Optional list audience-aware token authentications
  # containing the audiences from the `spec.audiences` field
  # If this is omitted, the token is considered to be valid for all audiences
  "audiences": ["https://myserver.example.com"]
}
```

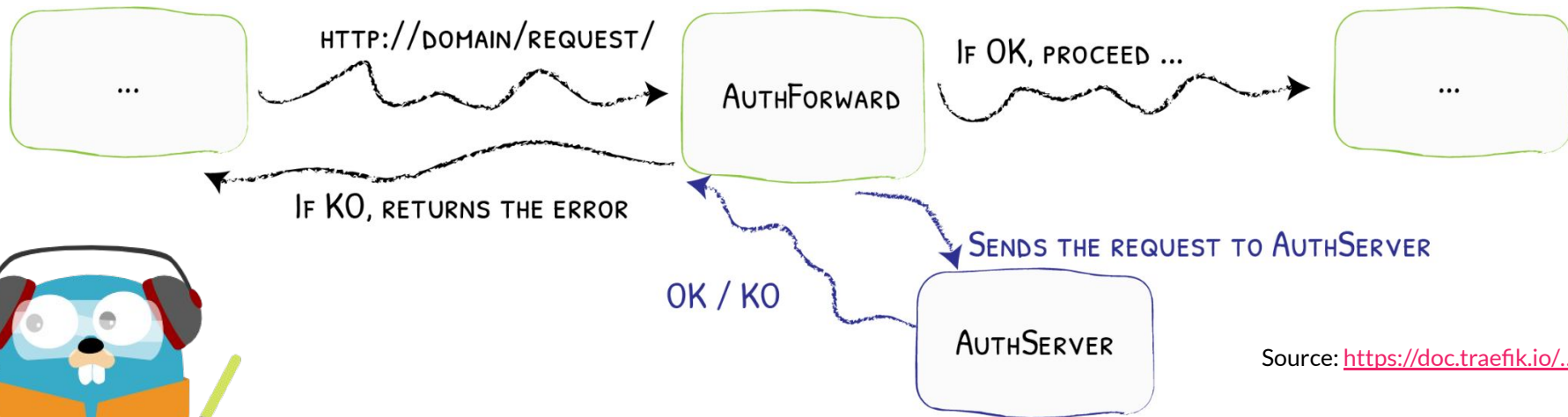
Authenticating Proxy

- Reverse Proxy in front of API-Server
- Example below: Traefik

- API-Server Params

- Required: requestheader-username-headers
- requestheader-group-headers
- requestheader-extra-headers-prefix
- Required: requestheader-client-ca-file
- requestheader-allowed-names

Sorry for the slide

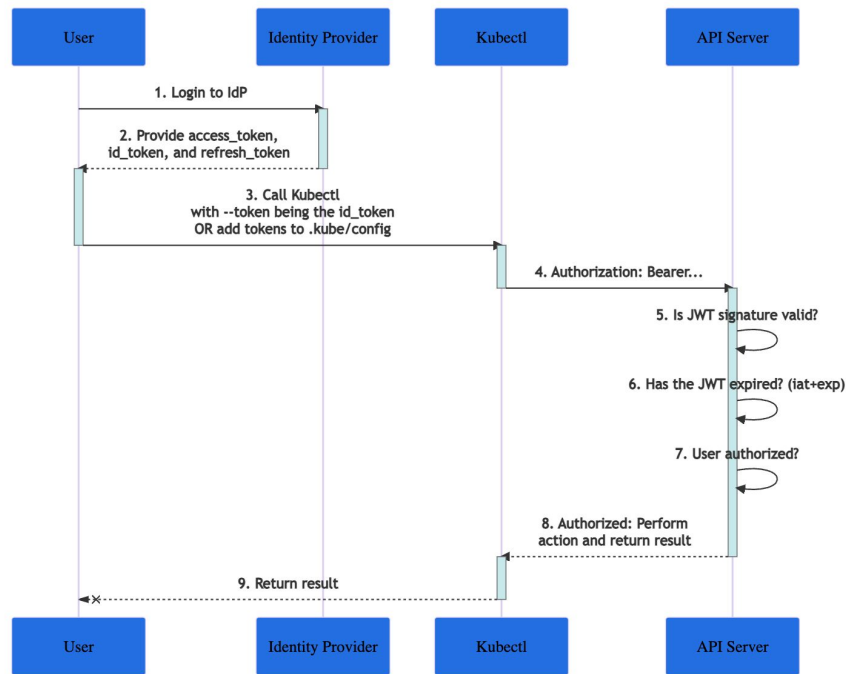


Source: <https://doc.traefik.io/...>



OpenID Connect Tokens

- Allows SSO Flow
 - Integrate Directory Services & IAM
 - Central User Management
- OIDC extends OAuth2
 - Uses `id_token` (not `access_token`)
 - JSON Web Token (JWT)
- API-Server Params
 - `oidc-issuer-url`
 - `oidc-client-id`



Service Account Tokens

- Associated with Pods
 - Operators, Controllers, etc.
- Workload Identity
 - `service-account-issuer`
 - `service-account-jwks-uri`
- Optional API-Server Params
 - `service-account-key-file`
 - `service-account-lookup`
- JSON Web Token (JWT)
- Can be stored in Secrets!



Kube Auth Strategies

- X509 Client Certs
- Bootstrap Tokens
- Static Token File
- Webhook Token Auth
- Authenticating Proxy
- OpenID Connect Tokens
- Service Account Tokens
- Anonymous Requests

Good to know:

- Multiple modules possible
- First success short-circuits evaluation
- API server does not guarantee order
- Enable at least SA tokens and one user auth module



Comparison

OpenID Connect Tokens

- ✓ Central
- ✓ Short living
- ✓ Easy to manage
- ✓ No

Enterprise-grade Tooling 🕶️

X509 Client Certs

- ✗ Distributed
- ✗ Long-living
- ✗ Hard to manage
- ✗ Easy to lose

Can be automated 😄💧

Dex

A Federated OpenID Connect Provider

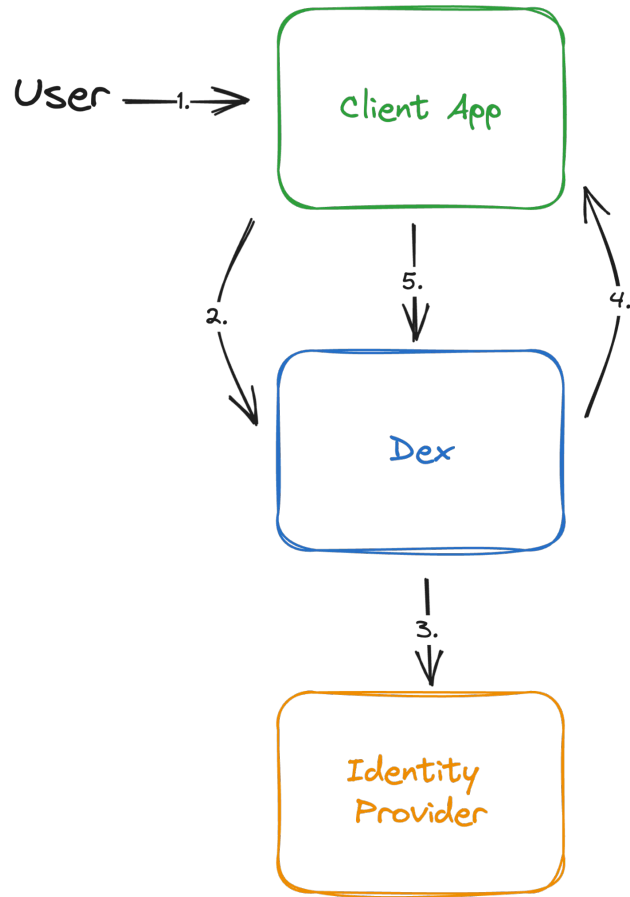
- CNCF Project
- Federated OIDC Provider
- Integrate any Identity Provider
 - One Tool to Rule Them All 💍
 - Easy ✌️
- Integrates with Kubernetes
 - Via [kubelogin](#)

Source: <https://dexidp.io/>

Name	supports refresh tokens	supports groups claim	supports preferred_username claim	status	notes
LDAP	yes	yes	yes	stable	
GitHub	yes	yes	yes	stable	
SAML 2.0	no	yes	no	stable	
GitLab	yes	yes	yes	beta	
OpenID Connect	yes	yes	yes	beta	Includes Salesforce, Azure, etc.
OAuth 2.0	no	yes	yes	alpha	
Google	yes	yes	yes	alpha	
LinkedIn	yes	no	no	beta	
Microsoft	yes	yes	no	beta	
AuthProxy	no	no	no	alpha	Authentication proxies such as Apache2 mod_auth, etc.
Bitbucket Cloud	yes	yes	no	alpha	
OpenShift	no	yes	no	stable	
Atlassian Crowd	yes	yes	yes *	beta	preferred_username claim must be configured through config
Gitea	yes	no	yes	alpha	
OpenStack Keystone	yes	yes	no	alpha	



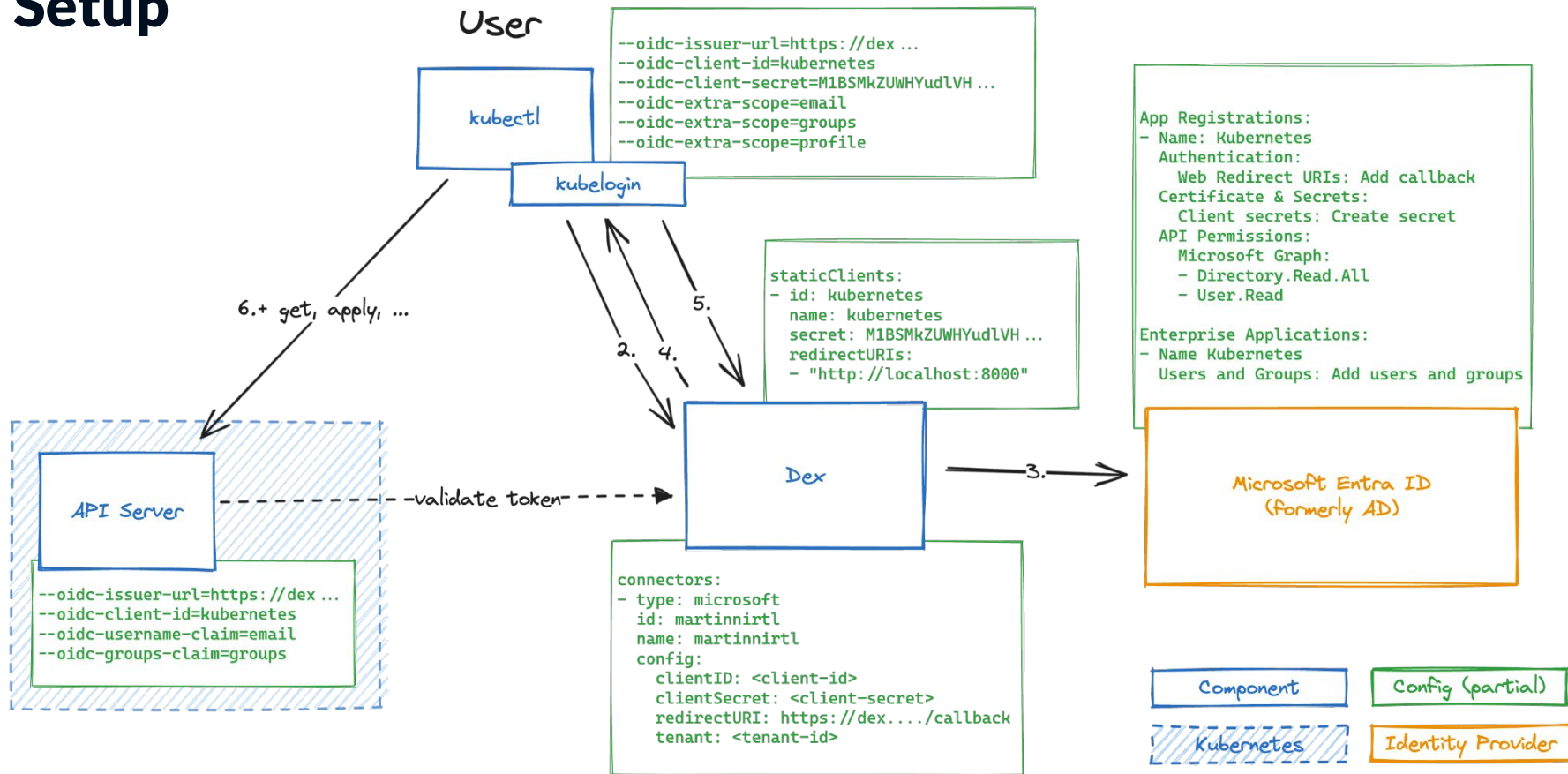
1. User visits client app
2. App redirects user to Dex with OAuth2 request
3. Dex determines user's ID
4. Dex redirects user back with a code
5. App uses code to exchange for a token (ID token)



Demo

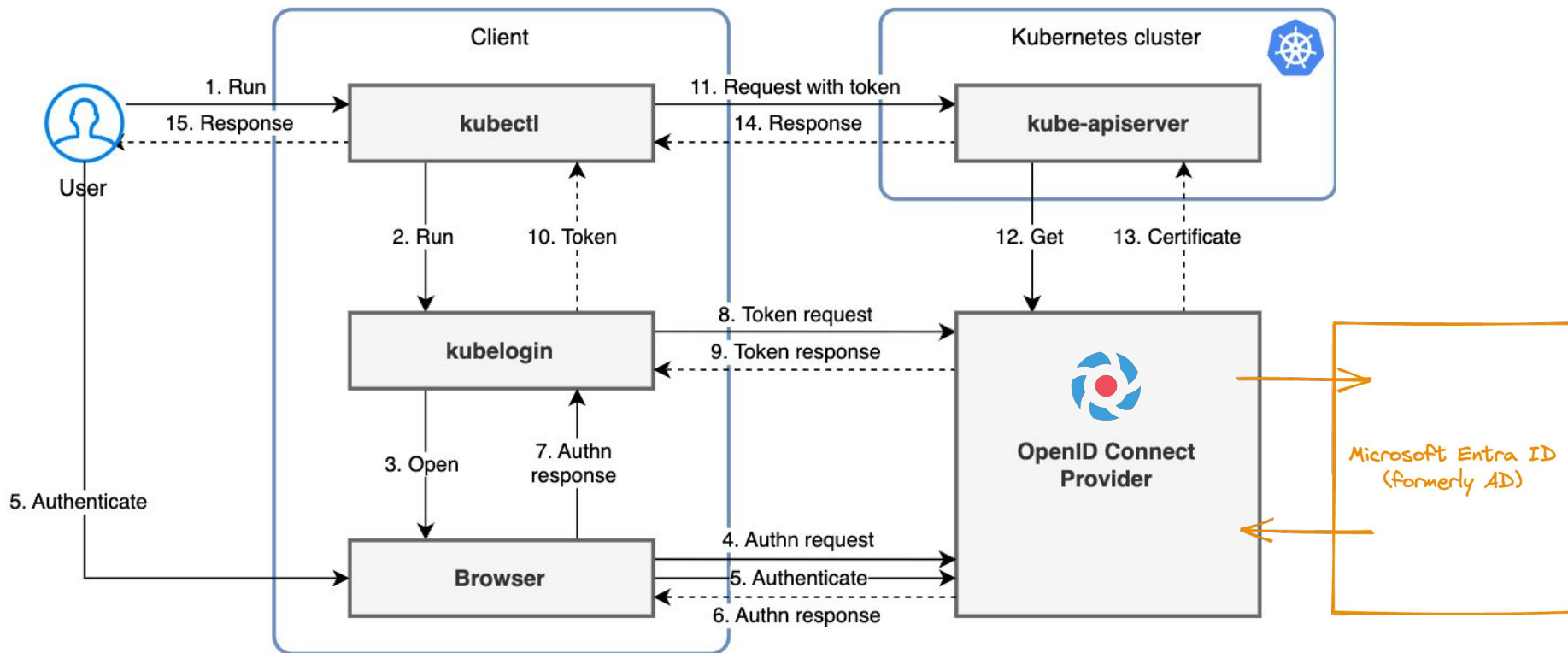
Let's get authenticated!

Setup



Kubelogin Flow

(Source: <https://github.com/int128/kubelogin>)



Beyond Authentication

Hmm... What else could there be?

Authorization

- AUTH, AUTHN, AUTHZ
- Central Management and Standardized Roles are Key!
- Nice tools to keep you sane (and reduce effort) 🕶️
 - Fairwinds' [RBAC Manager](#) - Roles and Bindings on Steroids
 - Fairwinds' [RBAC Lookup](#) - Search roles for a user, service-account or group
 - [Audit2RBAC](#) - Create roles from audit logs
 - [Paralus](#) - Zero trust Kubernetes with zero friction
 - [Teleport](#) - Open Infrastructure Access Platform

Beyond Authentication - Workload Identity

- Assign identities to Workloads
 - E.g. Assume IAM role on AWS
 - No credentials needed
- OIDC used to verify token
 - OpenID Config Doc
 - JSON Web Key Set (JWKS)
- Uses SA token to retrieve credentials
- Examples
 - External-DNS
 - External Secrets Operator

Example: IAM Roles for Service-Accounts (IRSA, AWS)

1. External-DNS reads SA and asks for AWS credentials
2. External-DNS retrieves credentials and assumes role
3. External-DNS updates and manages Route53 entries

GKE and AKS call it Workload Identity

Logout

Signed out successfully!