Enhancing Access Control to the Docker Daemon

Nigel Brown

@n_brownuk www.windsock.io

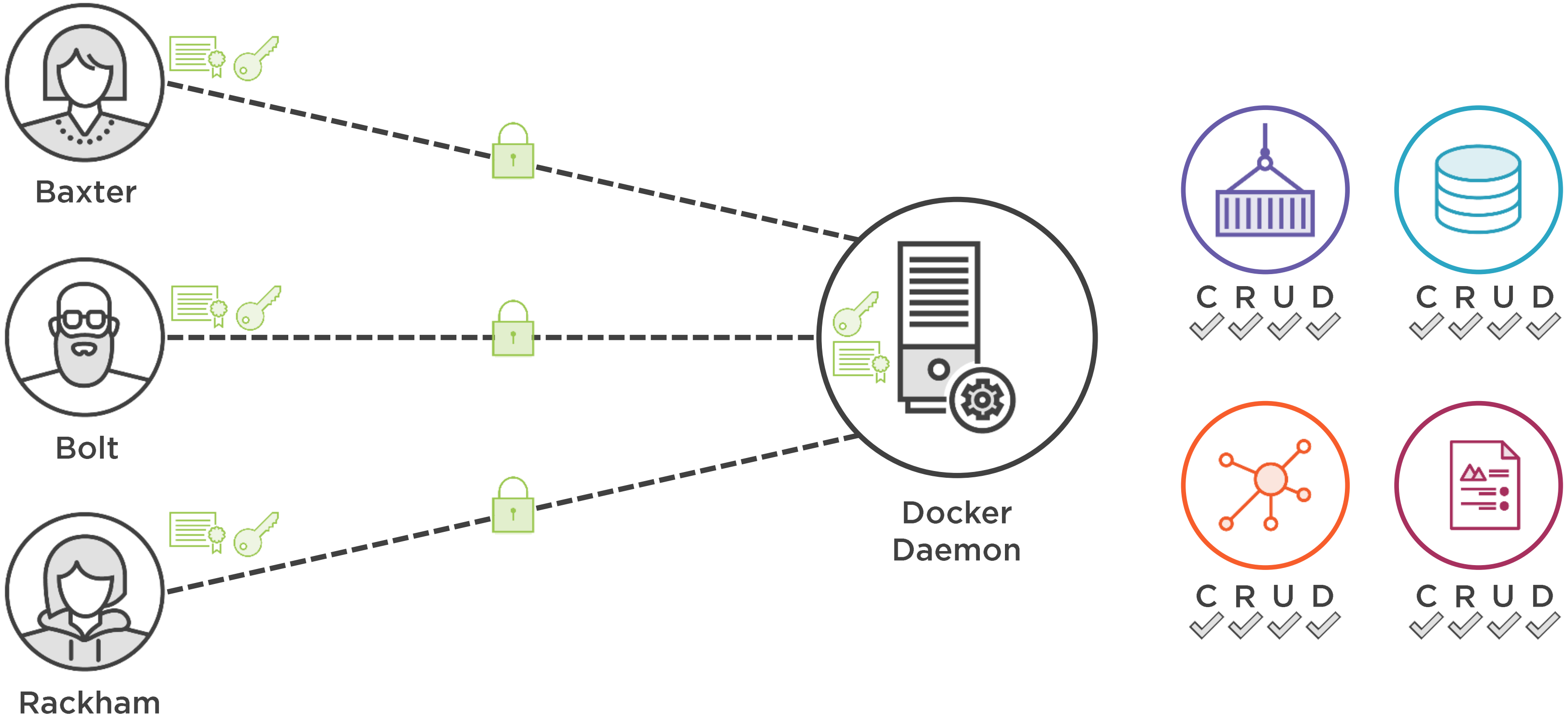
Module Outline

Using authorization to aid access control to the Docker daemon

Unravelling the Docker Engine plugin API

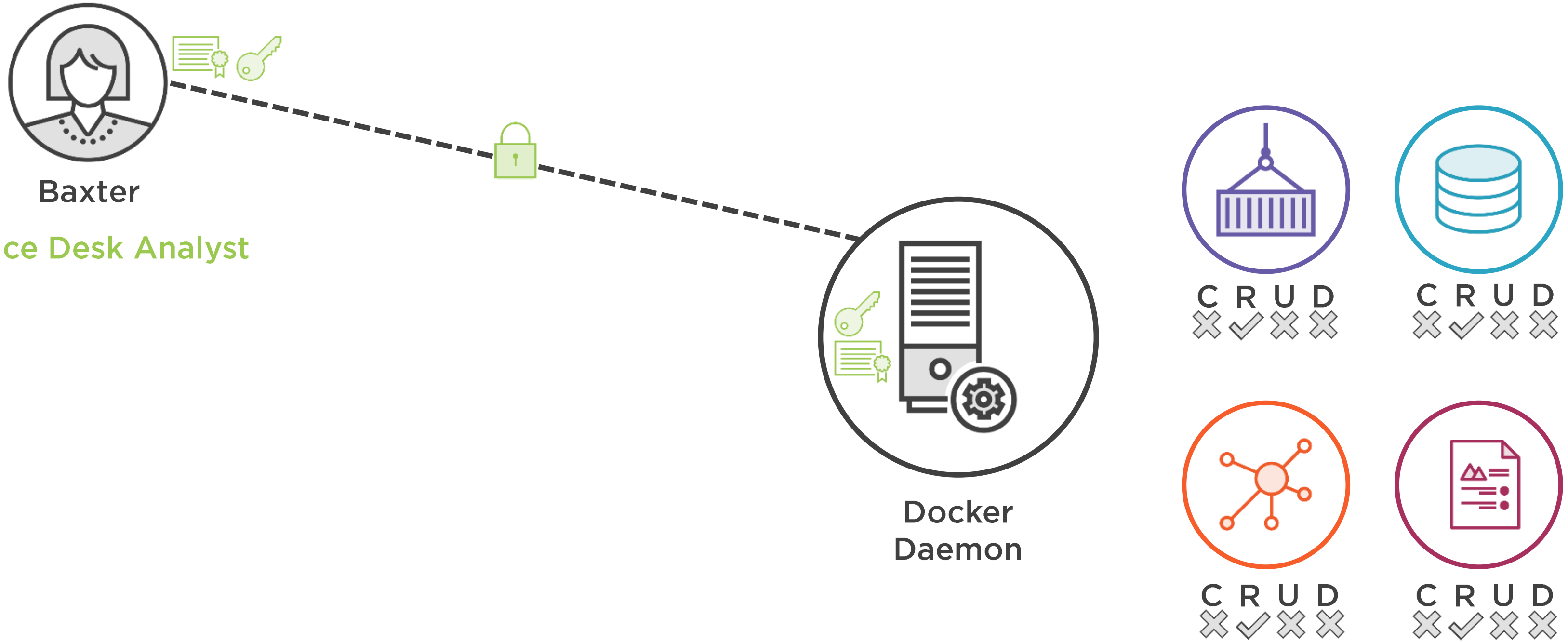
Making use of the Open Policy Agent to implement authorization by role

Authentication



Authorization

The act of determining what access privileges an identity has to an object or resource.



Baxter

Service Desk Analyst

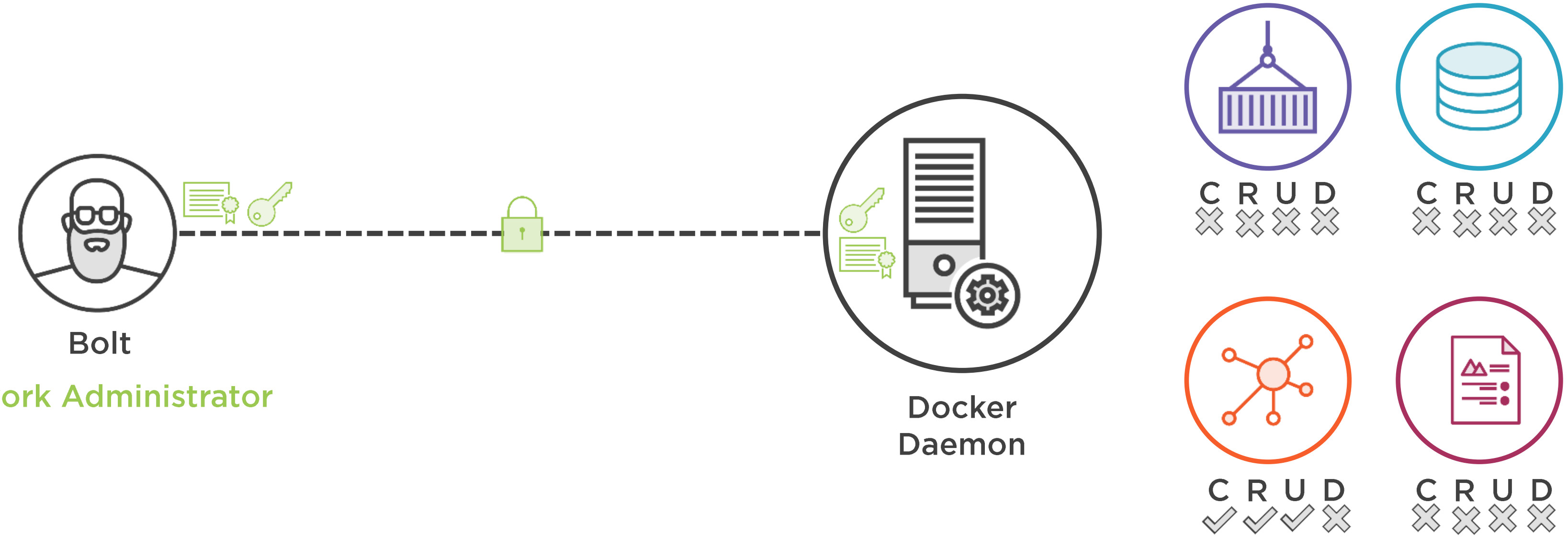
Docker Daemon

C R U D
✗ ✓ ✗ ✗

C R U D
✗ ✓ ✗ ✗

C R U D
✗ ✓ ✗ ✗

C R U D
✗ ✓ ✗ ✗



Bolt

Network Administrator

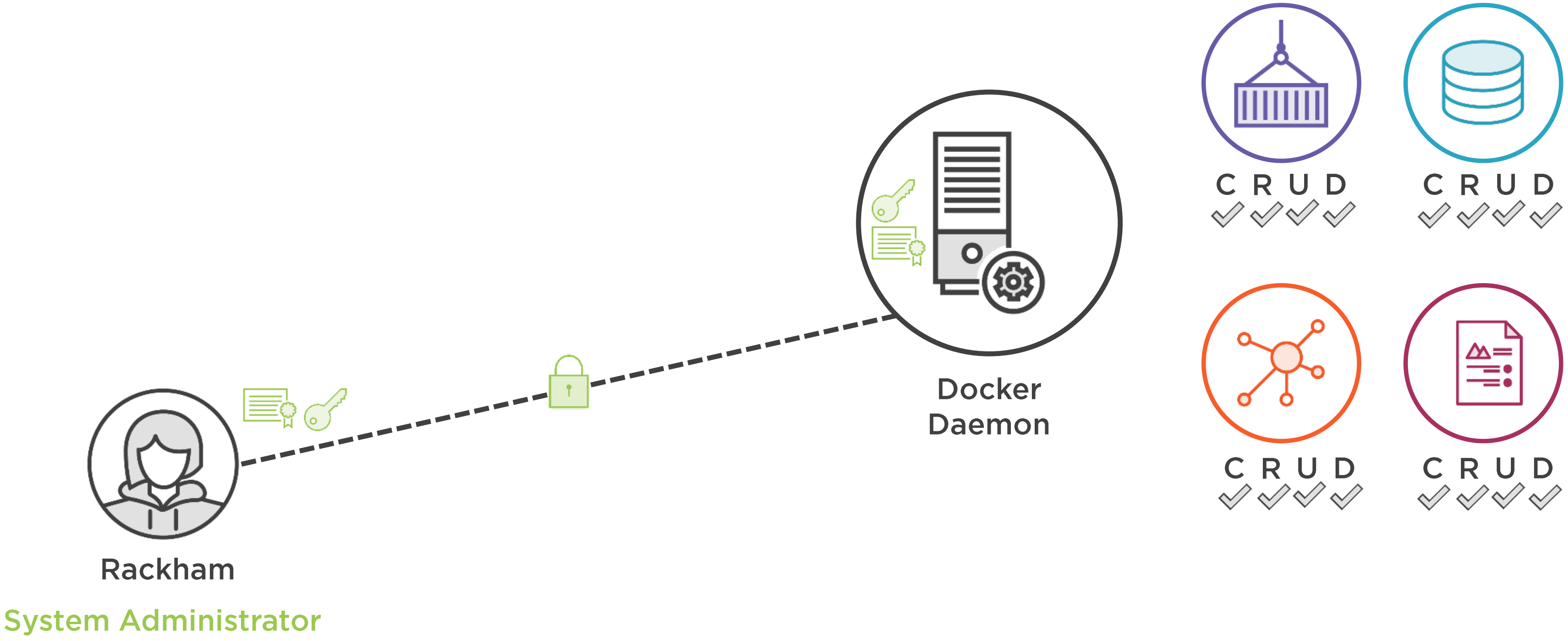
Docker Daemon

C R U D
✗ ✗ ✗ ✗

C R U D
✗ ✗ ✗ ✗

C R U D
✓ ✓ ✓ ✗

C R U D
✗ ✗ ✗ ✗


Rackham
System Administrator
Docker
Daemon
C R U D
C R U D
C R U D
C R U D

Authorization can be implemented using Docker’s plugin API

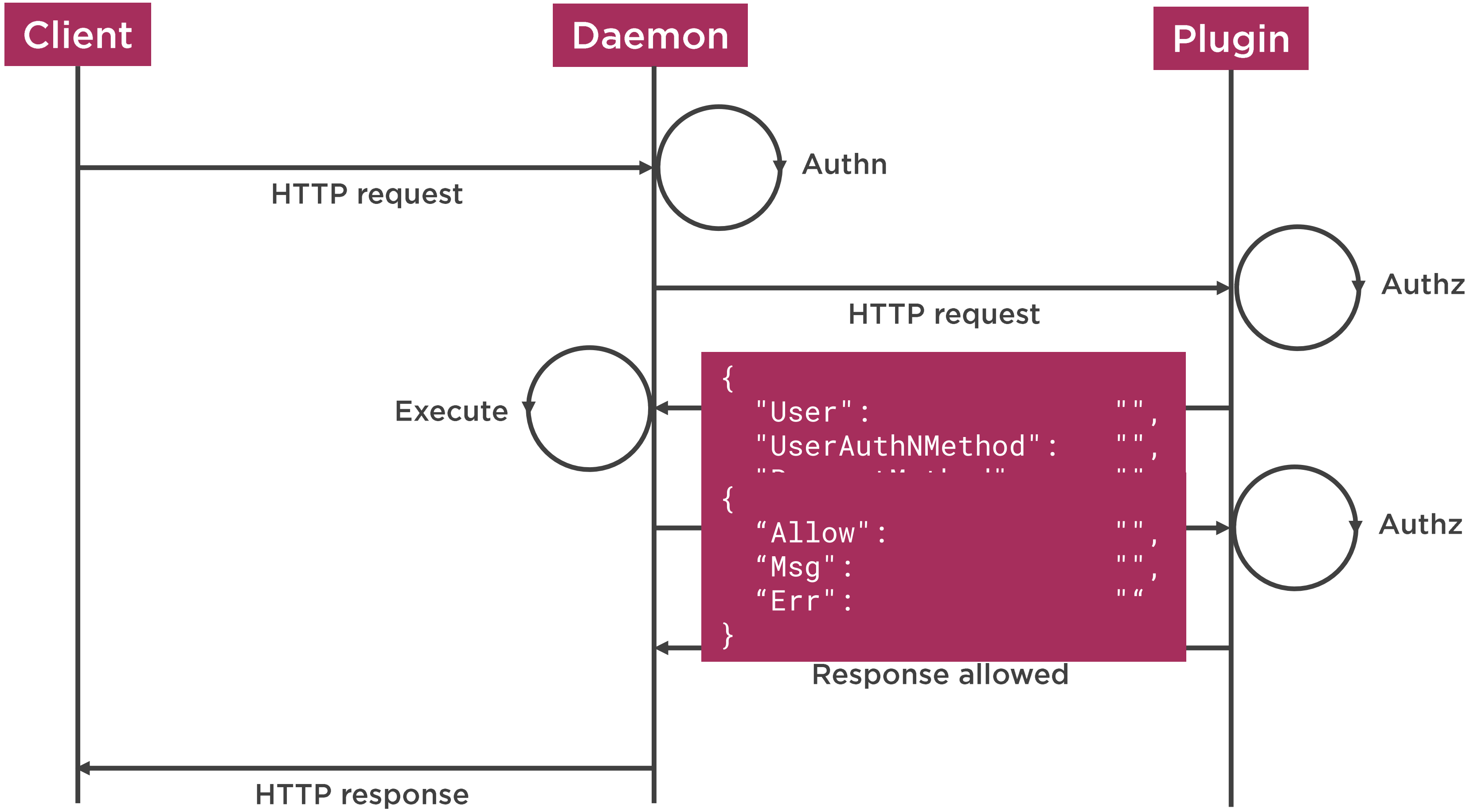
Docker's Plugin API

Allows the execution of external code at appropriate points

Plugins can be installed and managed as a Docker object

Plugins are usually implemented as Docker containers

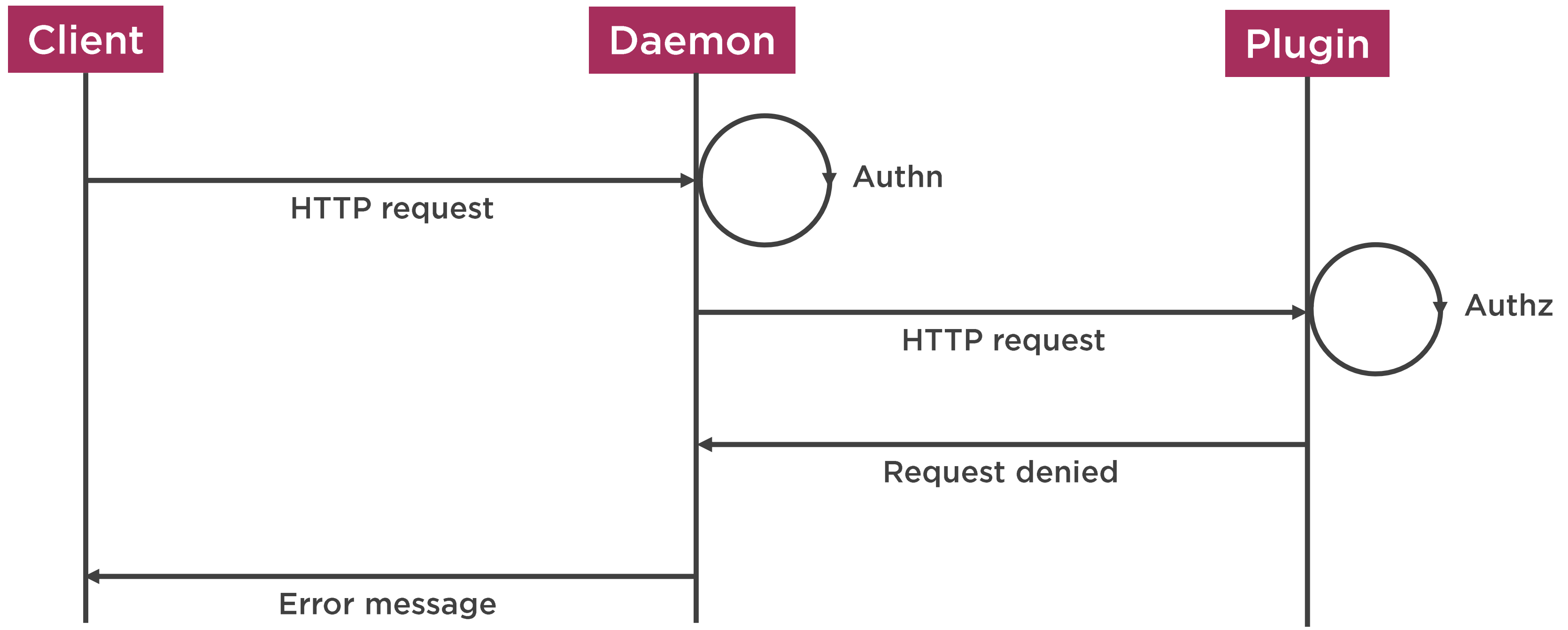
Successful Authorization



```
{
  "User":               "",
  "UserAuthNMethod":    "",
```

```
{
  “Allow":              "",
  “Msg":                "",
  “Err":                "“
}
```

Unsuccessful Authorization



Golang helper packages: https://github.com/docker/go-plugins-helpers

```
# Configure daemon to use authorization plugin(s)
--authorization-plugin=plugin-1,plugin-2, ...
```

Enabling an Authorization Plugin

Multiple plugins can be ‘chained’ together in a defined sequence

Open Policy Agent

The Open Policy Agent is a general-purpose policy engine that enables unified, context-aware policy enforcement.

What Is OPA?

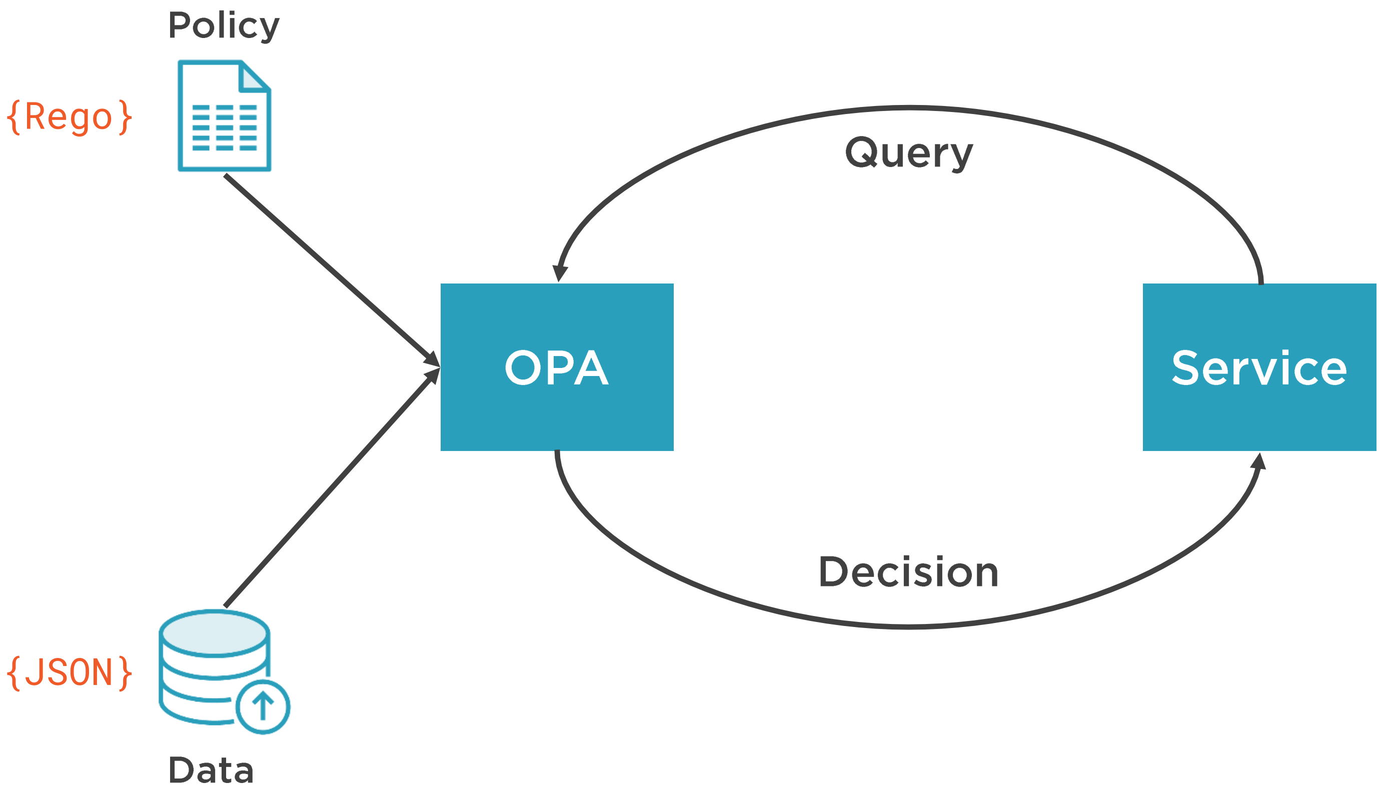
OPA is a sandbox project of the Cloud Native Computing Foundation

Decouples policy definition and enforcement from the application

OPA can be used to enforce policy across a wide range of use cases

OPA’s Docker authorization plugin is called ‘opa-docker-authz’

Overview of OPA



```
package httpapi.authz

import input as http_api

default allow = false

allow = true {
  http_api.method = "GET"
  http_api.path = [
    "finance",
    "salary",
    username
  ]
  username = http_api.user
}
```

◂ **Namespaces the module’s rules**

◂ **Import package as a variable** `http_api`

◂ **Defines the default outcome for the** `allow` **rule**

◂ **Rule ‘head’, followed by rule ‘body’**

◂ **The rule is evaluated by ANDing the statements in the rule body**

Module Summary

The Docker daemon provides ‘all or nothing’ access

Access control can be implemented with an authorization plugin

Plugins can be self-authored

Access control with authorization requires careful planning