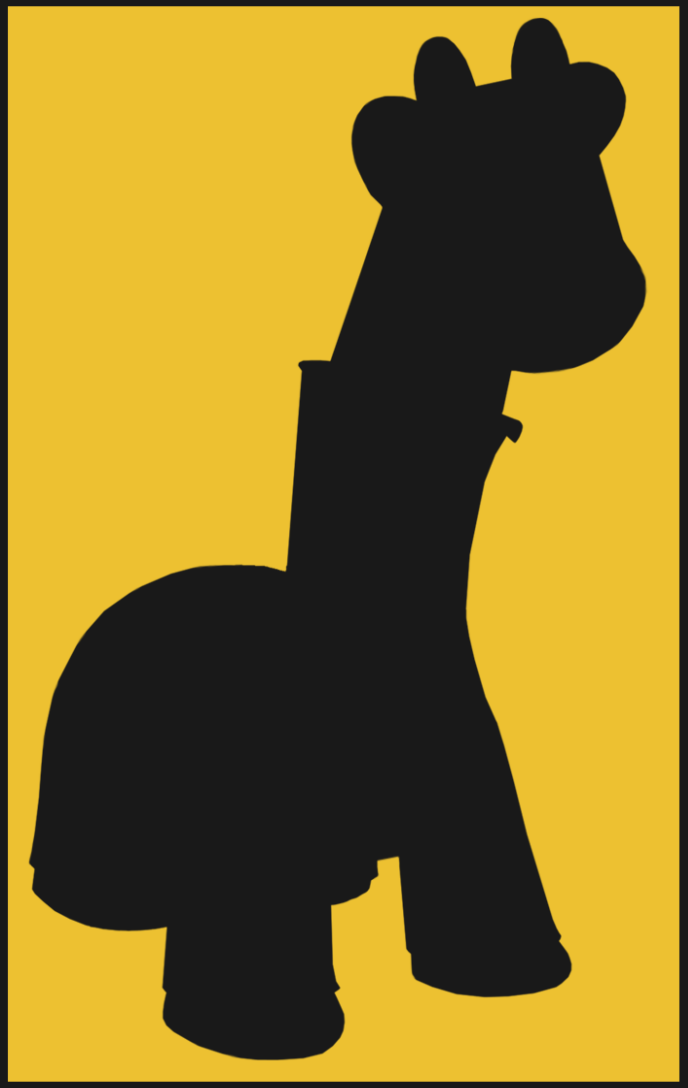
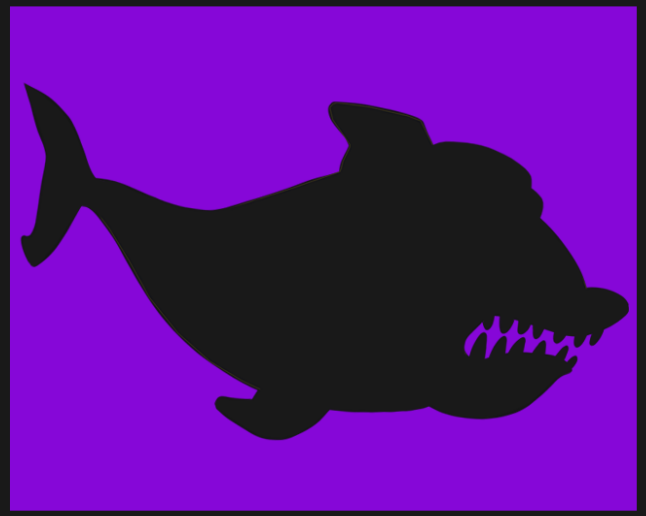
FROM 00-K8S, WITH LOVE





Brought to you by...

Written by: Matt Butcher, Karen Chu, & Lachlan Evenson

Illustrated by: Loretta Ford

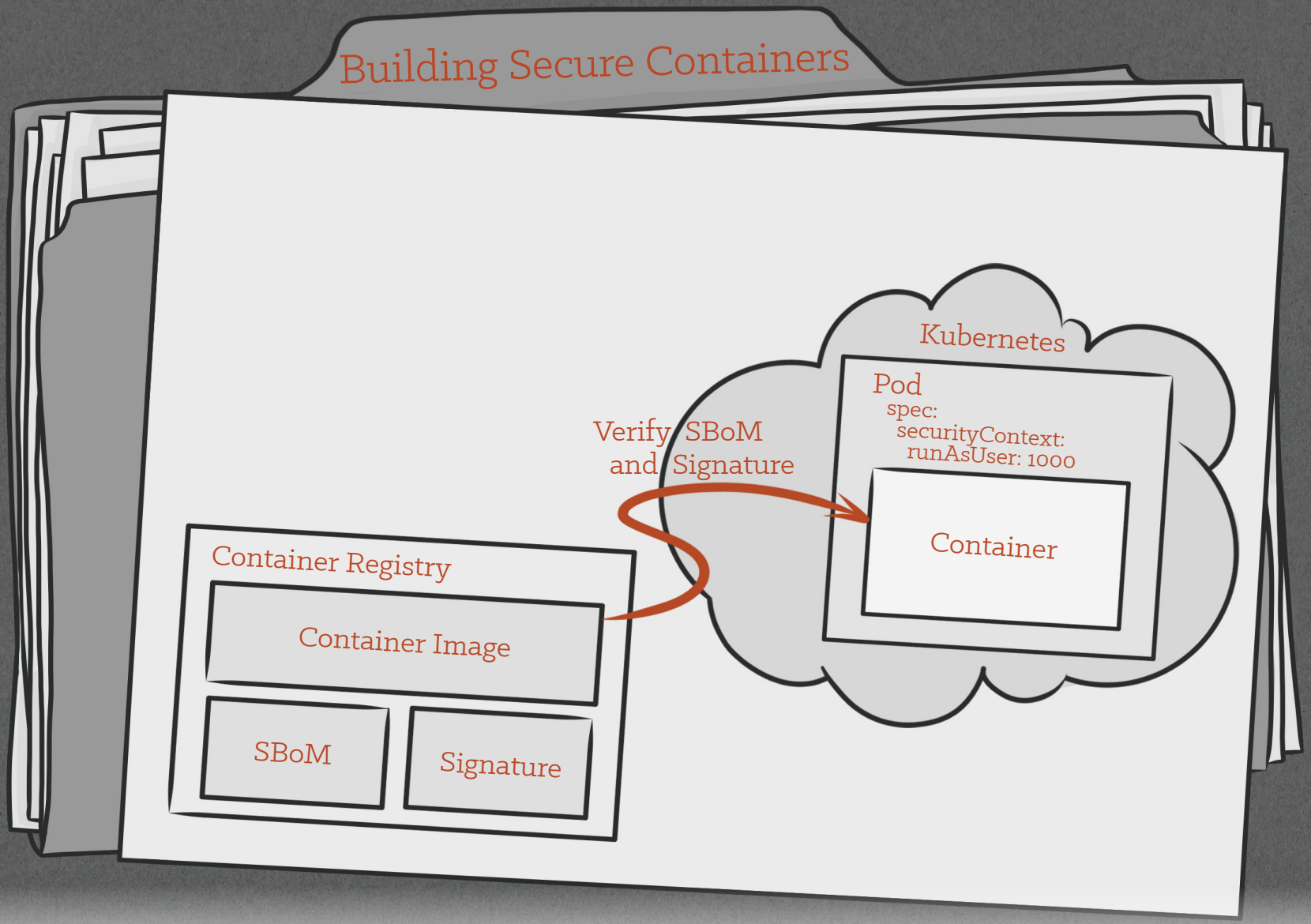
Designed by: Karen Chu

“This must be it!” Agent 00-K8s says to herself as her secret spy watch starts buzzing.

She lifts her wrist to read the message from Agent Zee: “Agent 00-K8s, we need you to deliver the super secret package as quickly and safely as possible. Good luck!”

Agent 00-K8s looks at the shining item on the desk in the room and at the open box. “Let’s get to work!” she says in a determined voice.

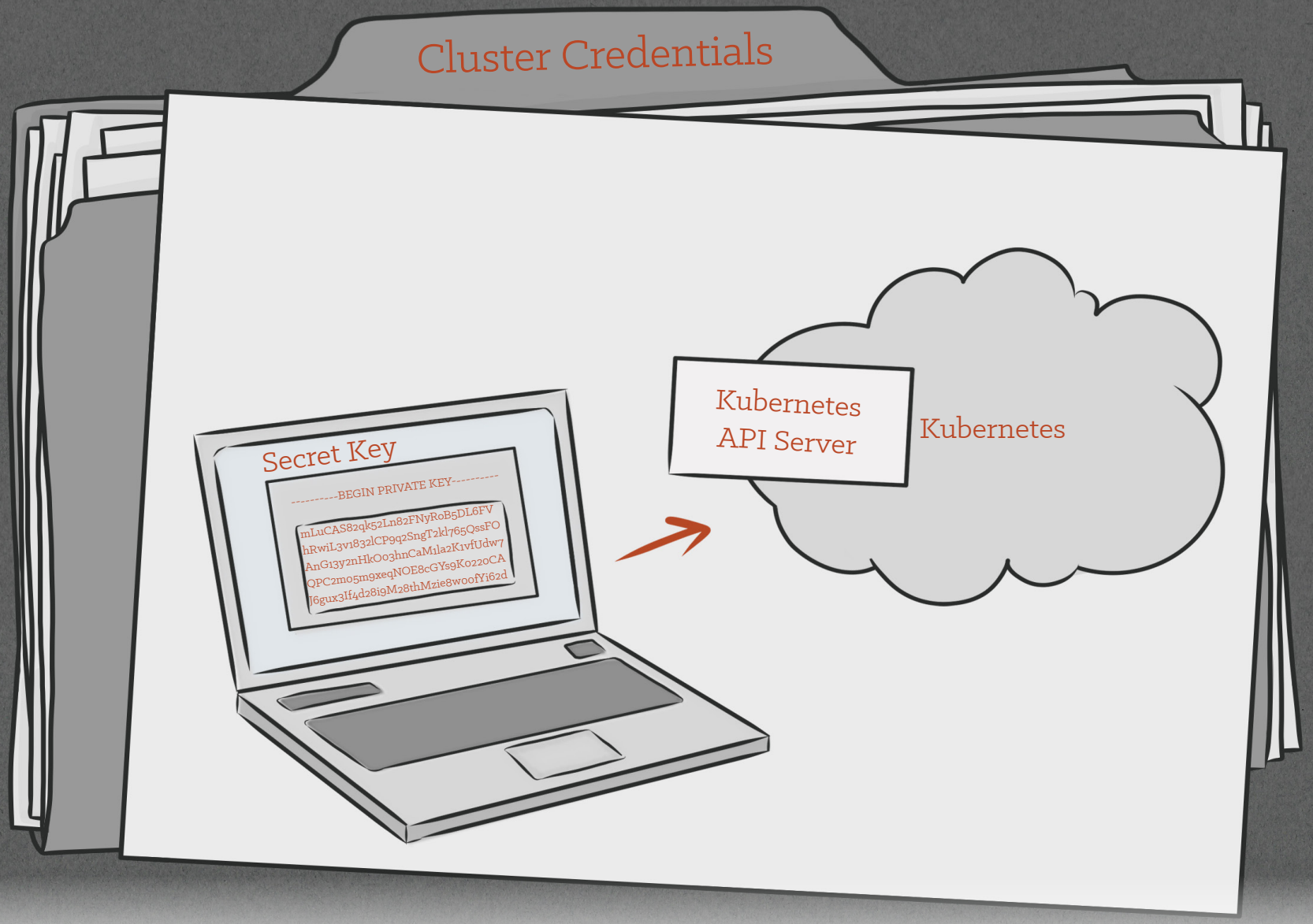
Agent 00-K8s places the shining item into the box. She reaches for her utility belt and grabs two small keypad devices. On the first device, she types “runAsUser: 1000”. On the other device, she types “1 super secret package”. The second device scans her face and responds “successfully signed” in a robotic tone. She places both devices into the box, shuts the lid, and ties it up.



- securityContext is where you will find all the security sensitive configuration for your pod
- A Software Bill of Materials (SBoM) is an inventory of application components
- Image signing allows you to verify that the image came from a specific source

Secure Kubernetes starts with secure containers, including getting your containers into the cluster without being tampered with.

Agent 00-K8s takes the package to the tube with a strange but familiar blue logo. She places her badge on the control panel and takes a deep breath. The panel scans her badge, the screen lights up green, and the top of the tube opens making a vacuuming sound. The package disappears into the tube. Deciding to personally make sure the package is safely delivered, Agent 00-K8s jumps in.



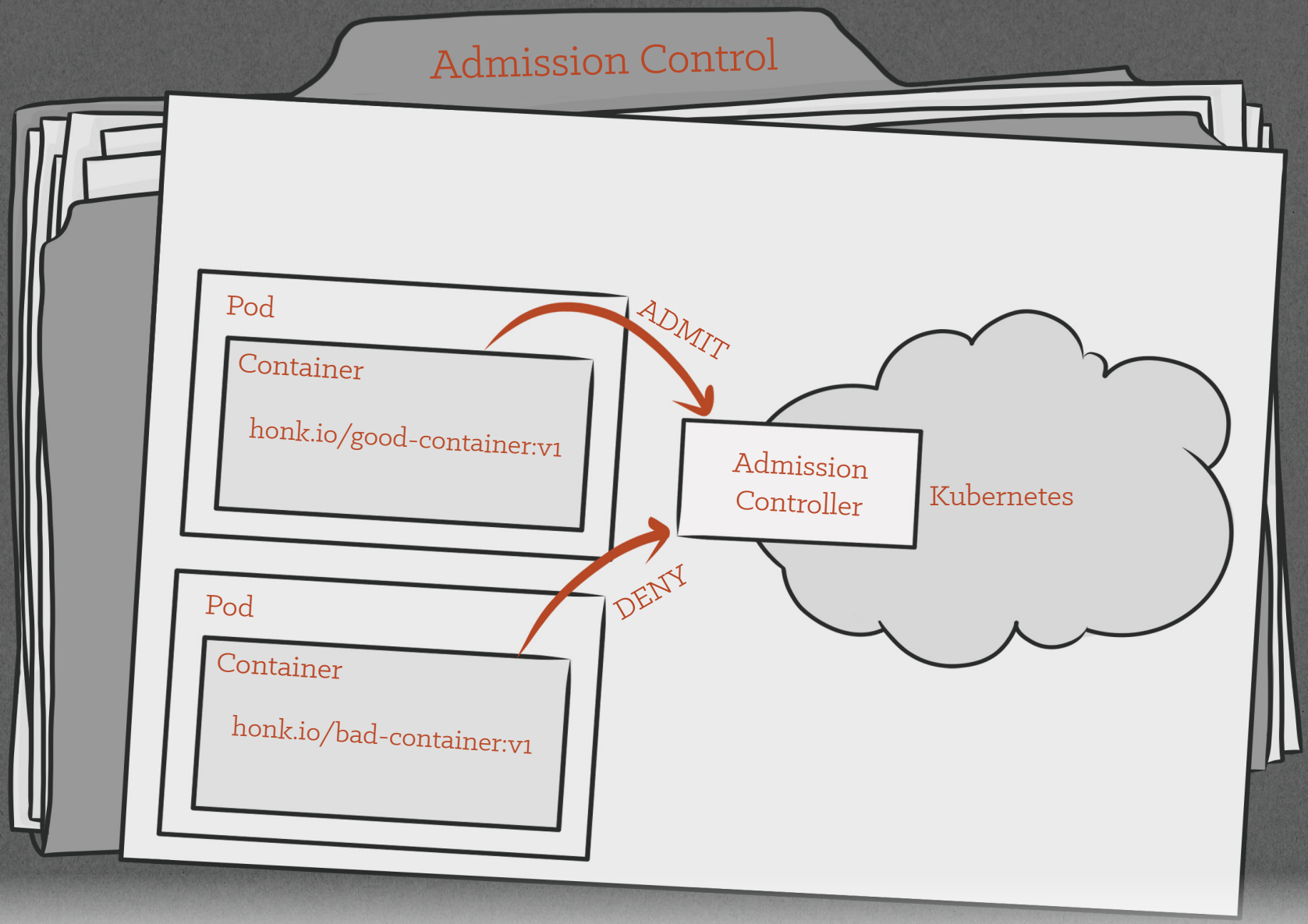
- Cluster credentials provide the information necessary to authenticate to Kubernetes
- There are different kinds of credentials, from username/password to cryptographic certificates
- Users must protect their credentials

When connecting to a Kubernetes cluster, a user must supply valid credentials for authentication.

Agent 00-K8s uses her grappling gun to avoid falling onto a conveyor belt. As she looks down, she sees the package pass through an x-ray machine. A dubious looking character appears from the shadows.

“Goldiefinger!” yells Agent 00-K8s.

“You’ll never stop me,” says Goldiefinger, firing a plunger toward the package. The door of the X-ray machine slams shut, blocking the plunger. Swinging to the ground, Agent 00-K8S follows the package.



- Admission controllers decide whether to admit or deny Kubernetes resources
- Make a decision based on policy
- May be dynamically configured on a running cluster

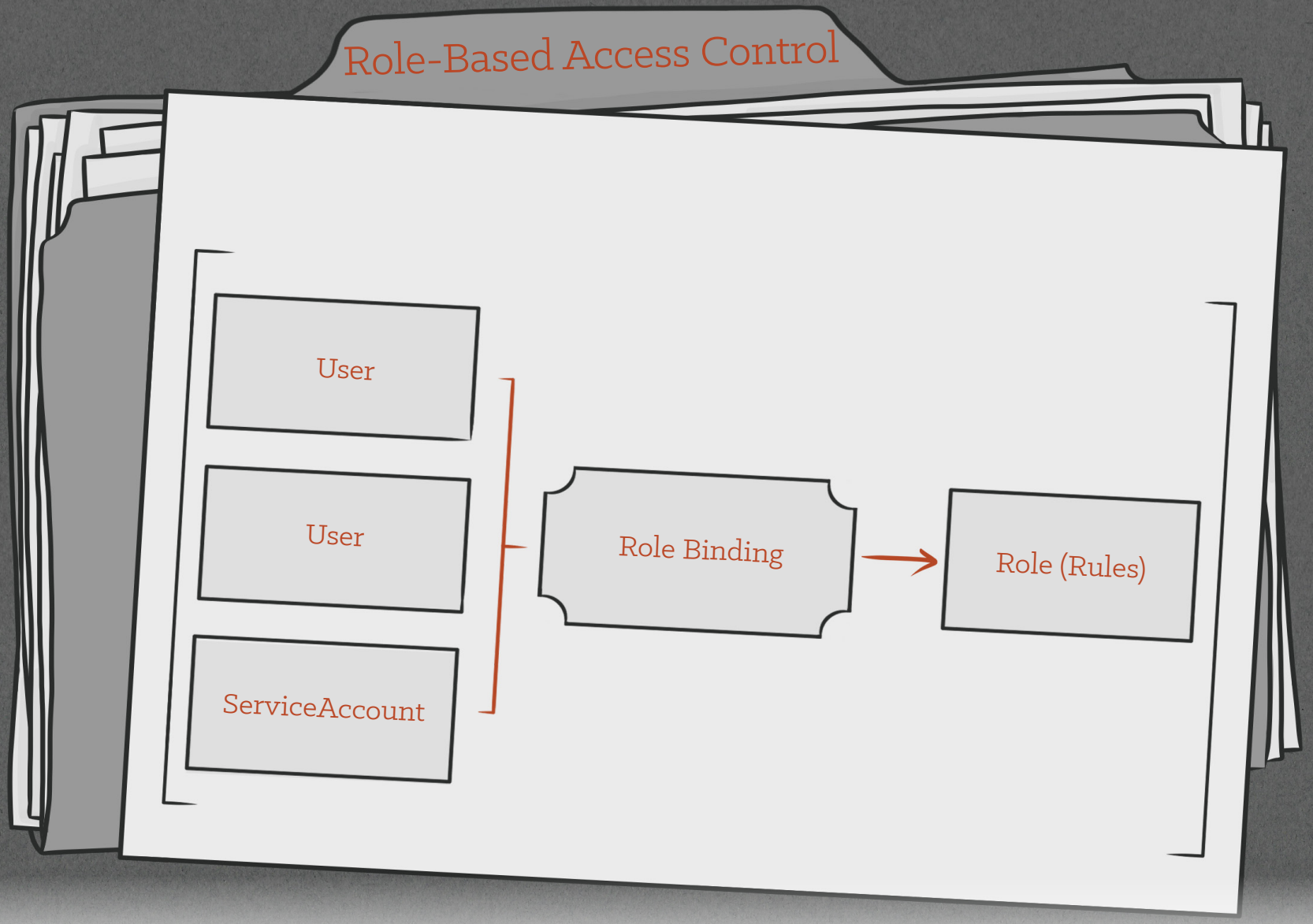
Admission controllers allow you to enforce policy on what resources can be created on your Kubernetes cluster.

“Captain Cronjob! Now there’s a name to die for!” says Agent 00-K8s as she dashes to the door.

“You’ll never win, Phippy!” says Captain Cronjob.

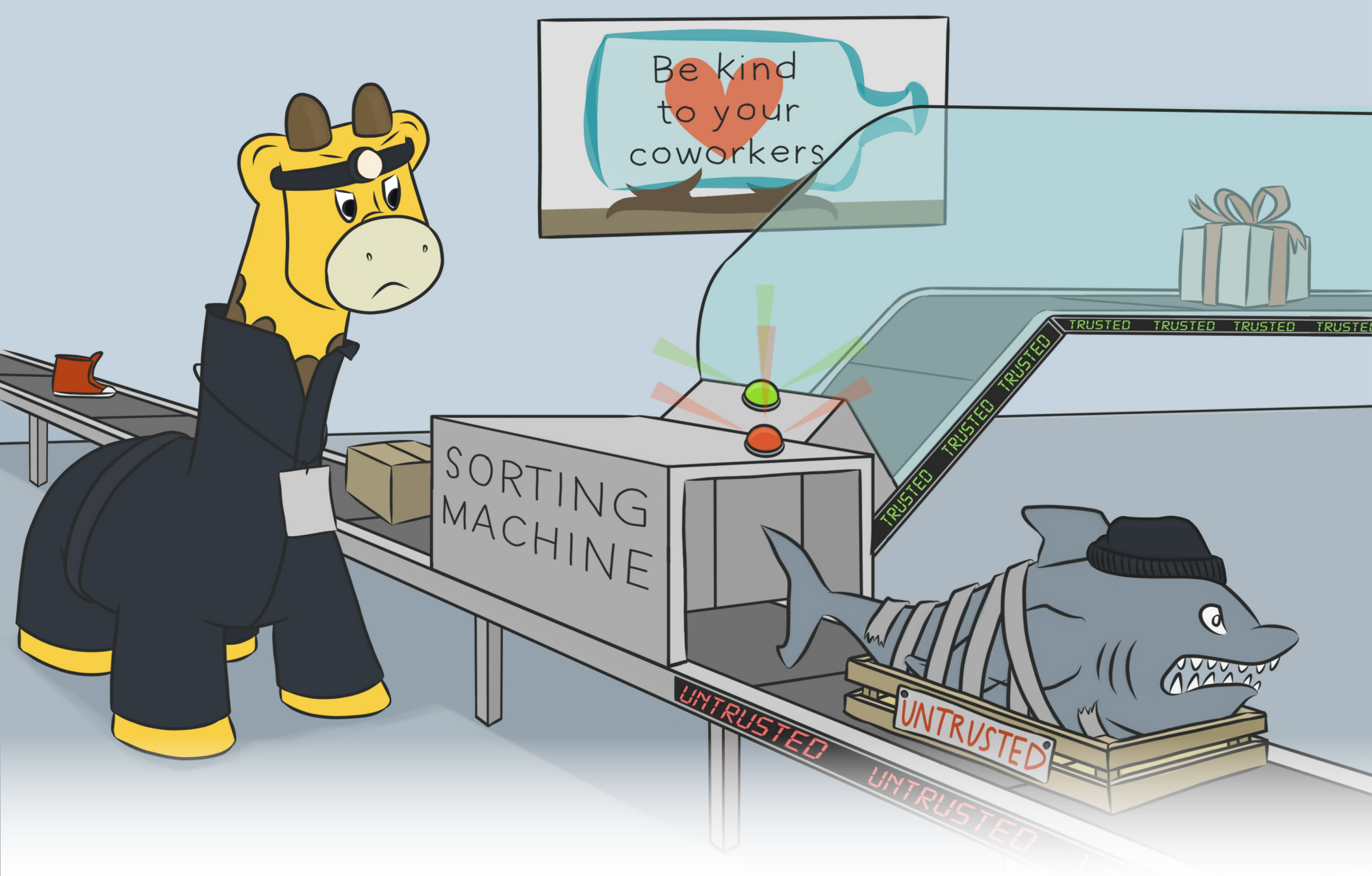
“The name’s K8s, Agent 00-K8s!” Agent 00-K8s replies as she raises her hoof to the scanner and the door pops open.

Captain Cronjob raises his wing, and the scanner says, “Forbidden: User Captain Cronjob cannot open resource door.”



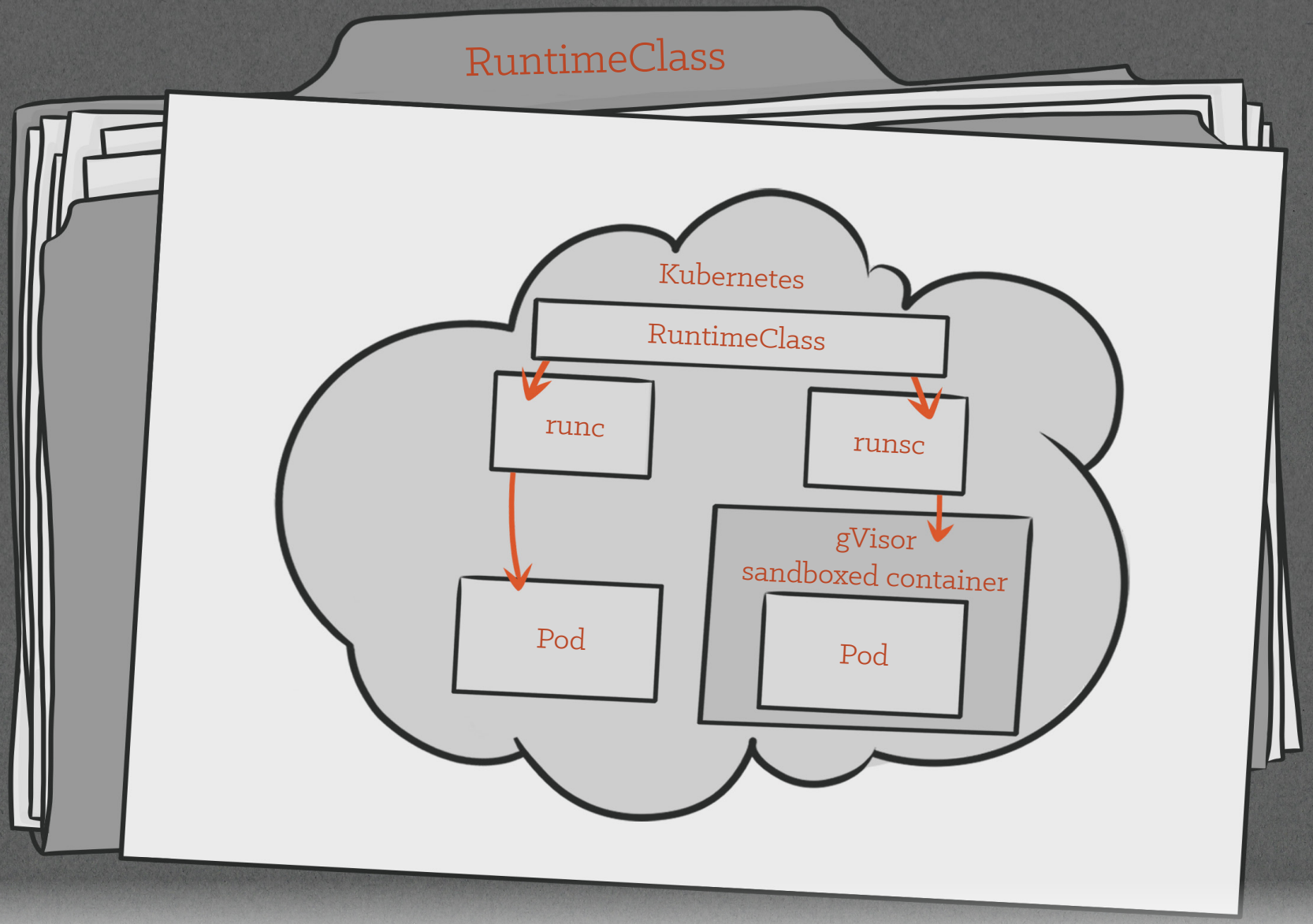
- Kubernetes uses roles and role bindings to provide authorization to resources
- Roles define what can and cannot be accessed
- Role bindings attach one or more users to a role

Role-based access control (RBAC) provides a way to attach users to roles, and roles to permissions.



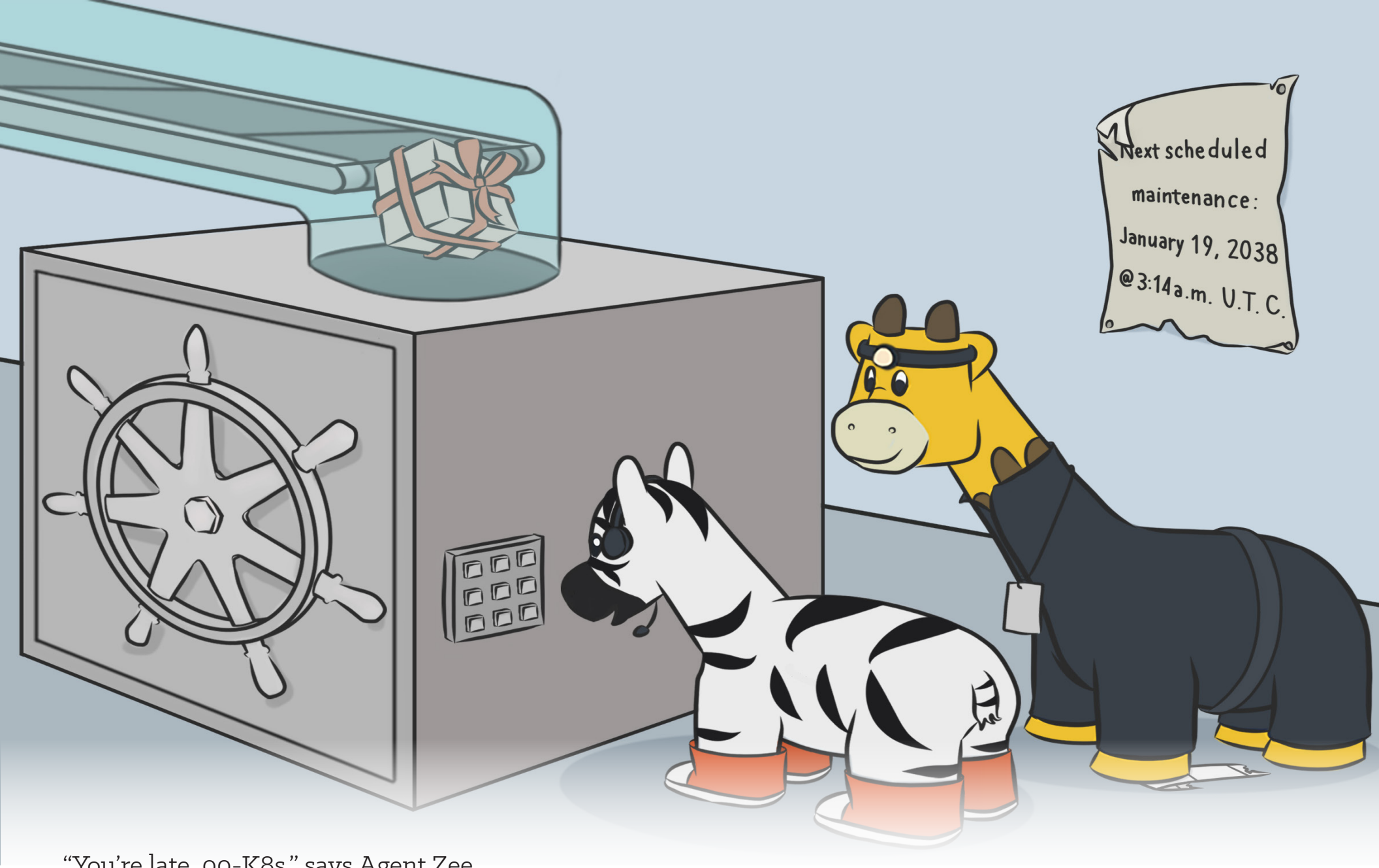
“Didn’t think I’d be seeing you so soon, Chompy!” says Agent 00-K8s. She dives to tackle Chompy, pushing him onto the conveyer belt.

The sorting machine flashes “untrusted”. It binds Chompy in duct tape and puts him in a sandbox. “You’ll regret this, Agent 00-K8s!” yells Chompy.



- RuntimeClass enables you to select between different container runtime configurations
- Run untrusted applications in container runtimes with stronger security guarantees like nested virtualization
- Allows you to balance security, cost, and performance per application

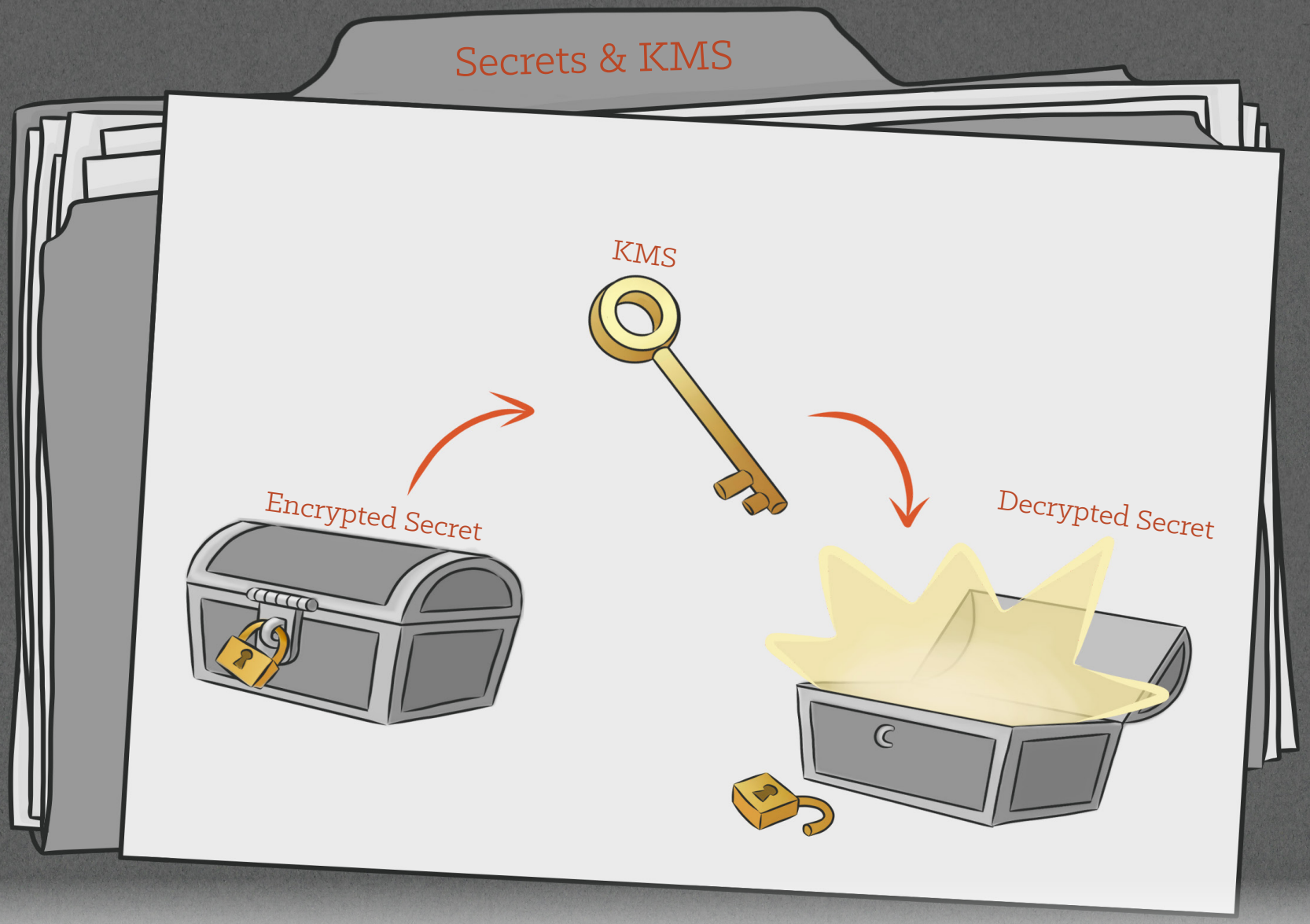
RuntimeClass provides a way to select different container runtimes based on the security needs for your application.



“You’re late, 00-K8s,” says Agent Zee.

“I had to use the bathroom,” replied Agent 00-K8s. Looking at the locked vault, she says “We need a code.”

“I know just whom to call,” says Agent Zee, tapping her headset. Agent Zee types a code into the keypad. The vault door springs open. Agent Zee reaches for the package inside the vault and grabs it.



- Kubernetes Secrets are used to store confidential information
- By default, Secrets are not encrypted
- A Key Management Service (KMS) provides an encryption and decryption service for Secrets

For truly encrypted Secrets, use a KMS system to encrypt records at rest, and decrypt them only when necessary.

And with that, the super secret package had finally made it quickly and safely to its destination. Agent Zee and Agent 00-K8s opened it to reveal a….


PROPERTY OF
Goldie