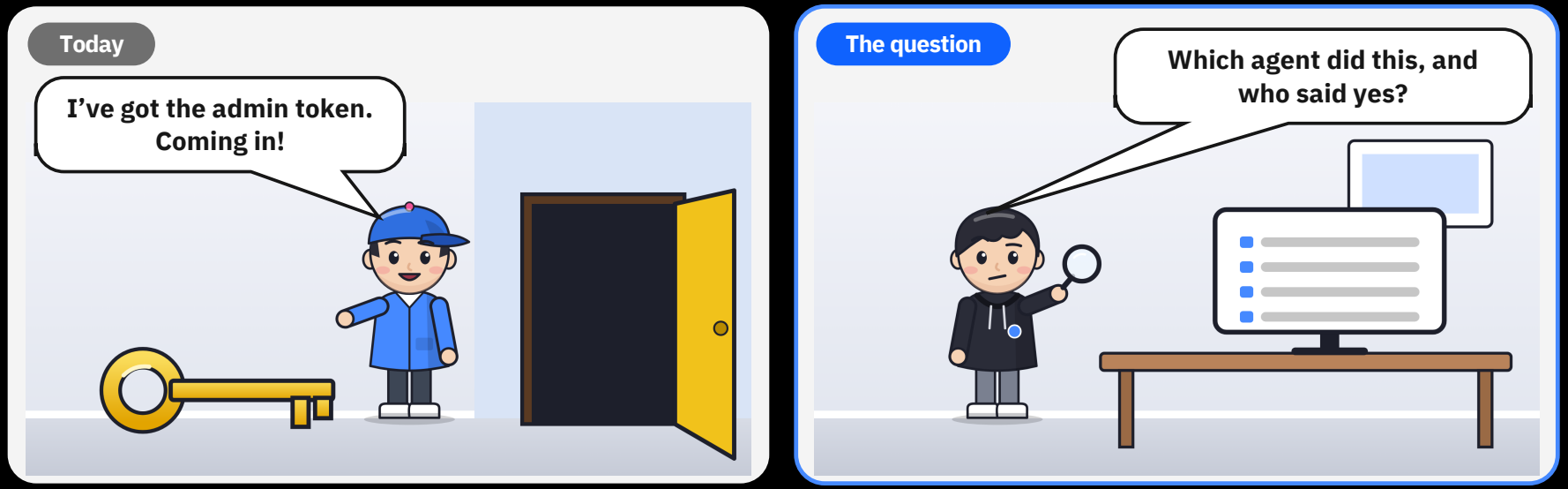
CLOUD NATIVE AI +
INFERENCE DAY
NORTH AMERICA

Who let the agent in?

Securing agentic AI with non-human identity in cloud native infrastructure



“Which agent did this, whose keys did it use, and who said yes?”



Hands up if an agent acts in your cluster today. **Keep it up** if you know its credential. **Still up** if your logs prove who asked.

Mahendran Selvakumar

Cloud and DevSecOps Engineer
@Tata Consultancy Services (TCS)



Cloud Native Community Group
ORGANIZER
2025
CLOUD NATIVE COMPUTING FOUNDATION

AAIF
AMBASSADOR

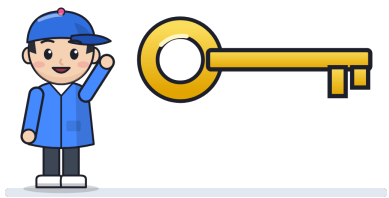
IBM Champion 2026
Awarded through the program
IBM Champion

AWS community builders

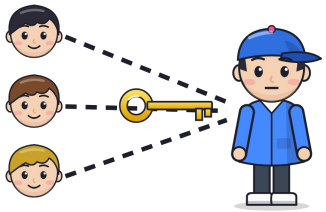
aws
AMBASSADOR

Standing access: one master key, four risks

Agents now act across Kubernetes, CI/CD, observability, security and platform workflows, mostly on shared tokens, broad roles or inherited human permissions.



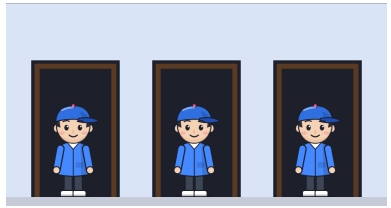
Over-authorization: a triage agent holds cluster-admin all day for a five-minute task



Invisible delegation: three engineers share one agent token, so nobody knows who asked



Weak auditability: the API server log shows one service account, not which agent or why



Uncontrolled access: agents call the Kubernetes API, Argo CD and cloud APIs directly

So how do we let an agent in without handing it the master key?

From master key to visitor pass

Five building blocks of a verified agent, told as a building with a front desk



1 Pass: SPIRE issues a JWT-SVID carrying the agent's SPIFFE ID. The token expires after 300 seconds

2 Door check: Envoy Gateway verifies that pass on every tool call

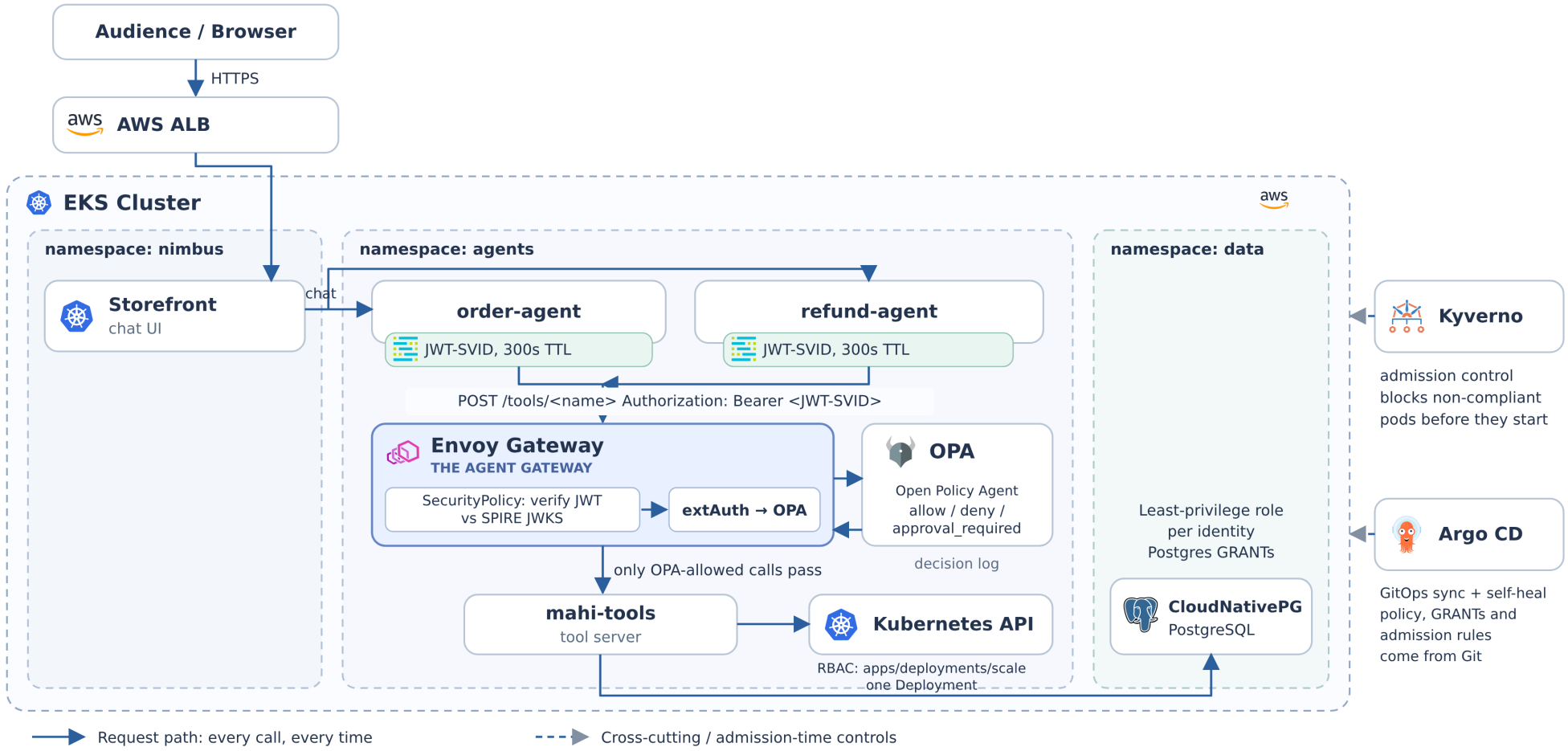
3 Rulebook: OPA enforces least privilege: allow, deny or approval required

4 Sign-off: risky actions wait for a human in the chat UI

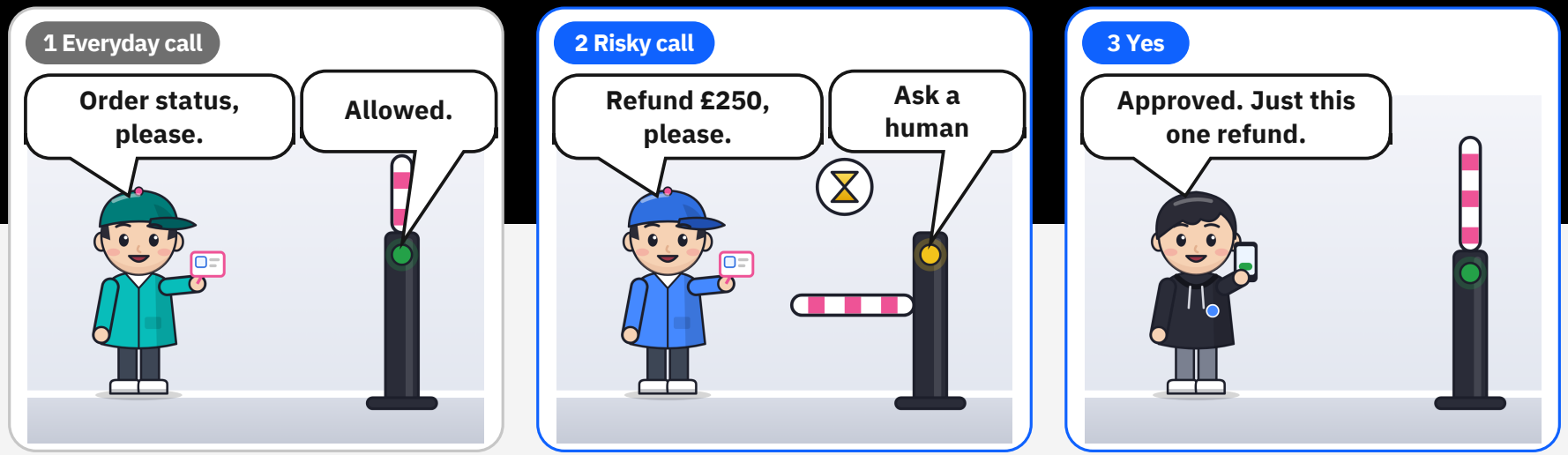
5 Guest book: every decision is recorded for investigation

The fence: Kyverno checks workloads at admission. NetworkPolicy restricts runtime routes (it needs a CNI that enforces it). Rules are reviewed in Git and applied through Argo CD.

Securing agent access on Kubernetes



Every tool call is checked, not trusted



Everyday call: order-agent's pass is verified, OPA allows the read-only call, and the gate opens at once

Risky call: refund-agent's pass is valid too, but OPA returns approval required, so the refund waits

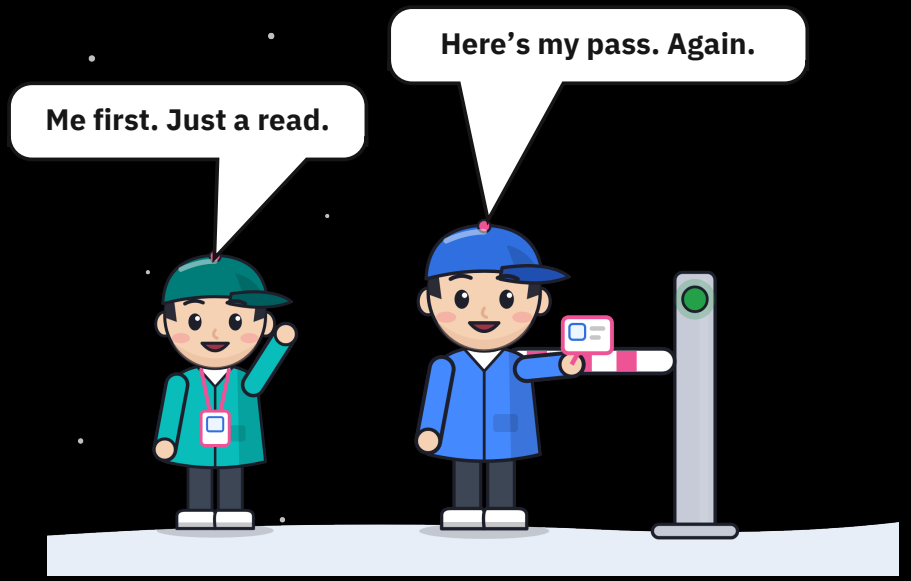
Approve: the app checks the approval matches this agent, order, amount and expiry, then rechecks OPA

No identity, no call: the gateway stands in front of every tool, API and MCP server.

Demo

From standing access to a verified agent

Two agents. One door. Three minutes, live on EKS.



1 Before
The master key
0:00 · 30s

2 Verify
Pass, door check, rulebook
0:30 · 60s

3 Approve
Sign-off in chat
1:30 · 60s

4 Prove
The guest book
2:30 · 30s

Mahi Stores

Ask Gemini

Not Secure kubecon-agent-demo-storefront-857460817.eu-west-1.elb.amazonaws.com

Finish update

All Bookmarks

Mahi Stores

Shop | Agentic Workflow | Reset

MAHI STORES

KubeCon swag for the cloud native community

Checkout works fine. Refunds are handled by an AI agent that's (mostly) not allowed to do anything stupid.

CATALOG



Custom Kubernetes Full Zip Hoodie
Embroidered Kubernetes wheel, fleece-lined
£78.00



Samsonite Arcway Laptop Backpack
Professional travel backpack, CNCF embroidery
£204.00



Eddie Bauer Hooded Soft Shell Parka
Insulated, water-resistant, CNCF embroidery
£122.00



CNCF Richardson Low Pro Trucker
Low-profile trucker cap, snapback
£24.00



Heritage Corduroy Trucker Cap
Classic corduroy trucker, adjustable
£34.00



Kubernetes Custom Woven Beanie
Knit winter beanie, woven wheel logo
£18.00



Kruger Fleece Crew
Casual fleece crewneck
£44.00



Helm - Embossed Midweight Crewneck
Embossed Helm ship-wheel logo
£100.00



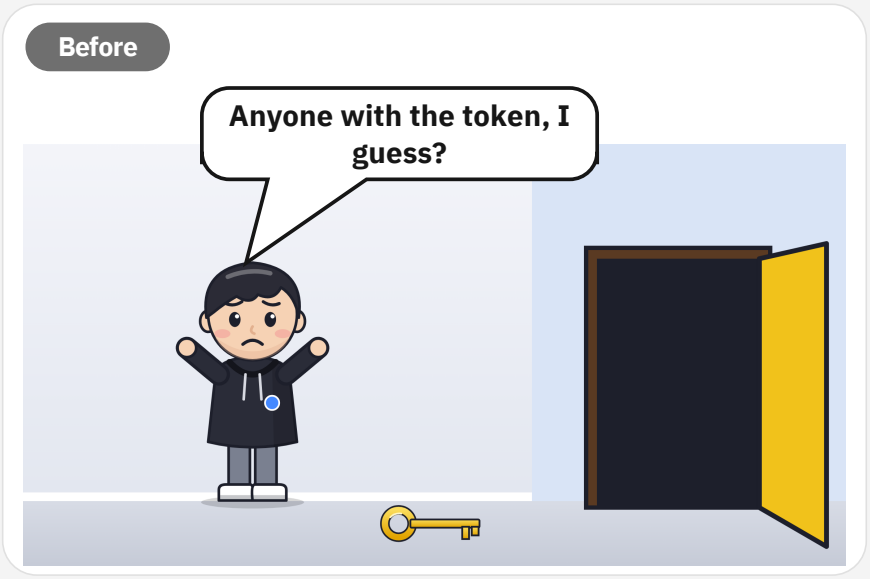
Phippy & Friends Core Cotton Tee
Phippy the giraffe, soft cotton tee
£21.00



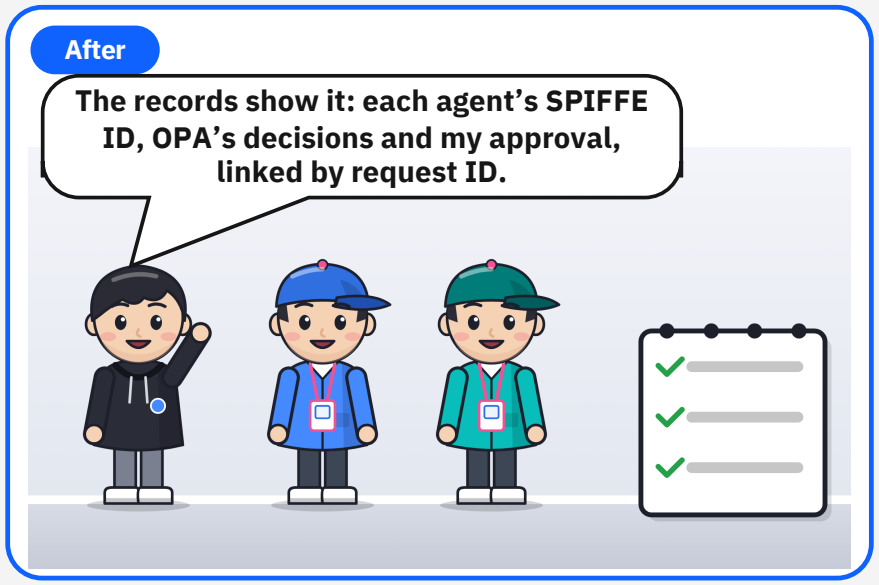
SOMOTO Eco Long Sleeve Tee
Sustainable fabric, long sleeve
£44.00

AI Assistant

So, who let the agent in?



Before: standing access, so the honest answer is a shrug



After: order-agent went straight through, refund-agent waited for a yes, and every call left a record

No identity, no call.

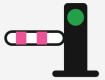
Your blueprint: trusted to verified

1



Give every agent an identity: its own ServiceAccount and SPIFFE ID, never a shared token

2



Route every call through one gate: a gateway, with Kyverno and NetworkPolicy closing side doors

3



Decide per call, not per login: OPA for least privilege, short-lived credentials, no standing access

4



Approve risk, audit everything: human approval for risky ops, policy from Git, a decision log for every call

Thank you

No identity, no call.

Verify the agent. Scope the call. Approve the risk. Audit everything.

devopstronaut.com · github.com/skmahe1077



