KUBECON + CLOUDNATIVECON NA 2026 · SESSION #1234729 · GITHUB.COM/GOOGLE/AGENTMESH

Governing and Scaling Agents in Heterogeneous Environments

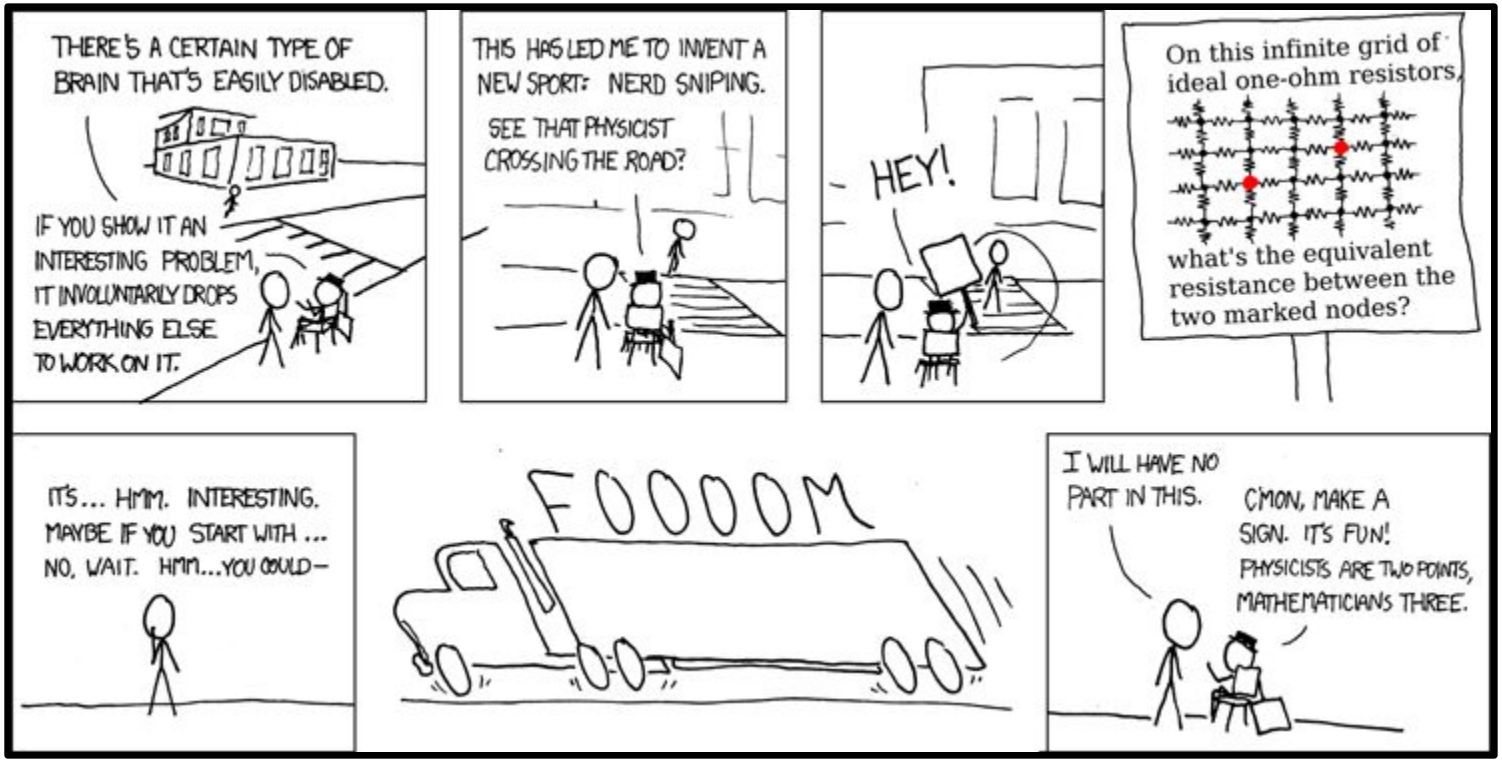
Identity-Bound libp2p P2P Dataplane · Task-Scoped Eclipse Biscuits · Connecting Platforms Without Competing





Governing and Scaling Agents in Heterogeneous Environments

Welcome to KubeCon! Grab a seat—we're about to get nerd-sniped across 3 platforms and 3 IdPs.

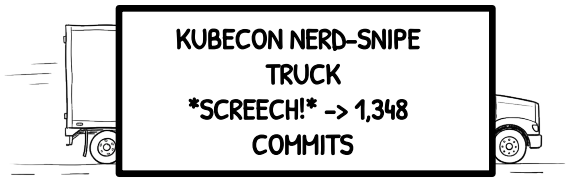


SOURCE: XKCD.COM/356 ("NERD SNIPING") BY RANDALL MUNROE · LICENSED UNDER CC BY-NC 2.5 (XKCD.COM/LICENSE.HTML)

KUBECON + CLOUDNATIVECON NA 2026 · #1: CONFESSIONS OF A SERIAL NERD-SNIPED ENGINEER (@AOJEA)

"WHAT IF AN AGENT ON A LAPTOP CALLS A PODMAN SANDBOX, WHICH CALLS K8S MCP ACROSS 3 INCOMPATIBLE IDPS?"
"WAIT... DON'T CROSS THE ROAD! IT'S A NERD SNIPE!"





@AOJEA
(CAN'T SLEEP UNTIL REFERENCE CODE SHIPS)

SNIPE #1: LOCAL & POLICY GAPS
KINDNET · CLOUD-PROVIDER-KIND · KUBE-NETWORK-POLICIES

↓

SNIPE #2: SCALE & AI NETWORKING
KEP-1880 SERVICECIDRS · KEP-6313 NETWORK-ISOLATED PODS · DRANET & KND

↓

SNIPE #3 (NOW): AGENT MESH v0.2.0
GITHUB.COM/GOOGLE/AGENTMESH (1,182+ STARS · DPUB-303524)
IDENTITY-BOUND LIBP2P + TASK BISCUITS ACROSS SILOS

INSPIRED BY XKCD.COM/356 ("NERD SNIPING") BY RANDALL MUNROE · CC BY-NC 2.5

KUBECON + CLOUDNATIVECON NA 2026 · MEET MY PARTNER IN CRIME: TOMAS TORMO (@KAISOZ)

"ANTONIO, YOUR NERD-SNIPED P2P + BISCUIT IDEA IS GREAT...
NOW LET'S MAKE IT SURVIVE REAL PLATFORM ADMINS & AI INFRASTRUCTURE!"
"DEAL! YOU GROUND THE ADMIN REALITY, AND WE SHIP IT TOGETHER."



Antonio Ojea (@aojea)
Software Engineer, Google
(Nerd-Sniped Instigator)



Tomas Tormo (@kaisoz)
Staff Platform Engineer, Nearform
(Partner in Crime & Admin Reality)

01 · CORE CONTRIBUTOR #2 ON AGENT MESH
Co-built the project with ideas, feedback & code from day one
(github.com/google/agentmesh · A2A · test-infra · Android)

02 · KUBERNETES & AI INFRASTRUCTURE VETERAN
Kubernetes (Job Controller, Scheduler) · Kueue (Batch) ·
Kubeflow Trainer · Staff DevOps & Platform Engineering

03 · GROUNDING IN ADMIN REALITY (DEMO LATER)
Shaped node rules, label floors (egress.require_labels)
& zero-trust boundaries—and leads our live demo!

Ideas + code + Platform Engineering & AI infra expertise = grounded for admins who deal with this daily.

KUBECON + CLOUDNATIVECON NA 2026 · INCEPTION, SHADOW AI & SIDECAR-TO-EDGE FLEXIBILITY

1: CHRISTMAS IN SPAIN

"You work at Google— can I ask you something?"

- EU gov/regulated contraints
- Wanted frontier models + MCP safely
- Stuck on existing on platforms
- Wrote Sovereign K8s Stack paper



2: SHADOW AI REALITY

"Wait... devs run agents WHERE?!"

- Non-Kubernetes platforms & harnesses!
- Single-cluster K8s wasn't enough!
- lack of security mechanisms and visibility



3: SIDECAR OR EDGE!

"Work inside OR across borders!"

- [✓] Sidecar / SDK inside sandboxes (Zero secrets in RAM!)
- [✓] Edge Gateway w/ Federation (Istio, Envoy ext_authz)
- Connect without competing!



4: FLEXIBLE DEPLOYMENT -> SIDECAR INSIDE PLATFORMS OR FEDERATED AT THE EDGE!

"Run as a Sidecar/SDK inside sandboxes (Substrate, OpenShell, Podman) with ZERO secrets inside, OR at the Edge with Federation (Envoy/Istio ext_authz + SPIFFE, K8s JWT & OIDC)!"

KUBECON + CLOUDNATIVECON NA 2026 · 3 SILOS, 5 AGENT NETWORKING NEEDS & WHY VPNs FALL SHORT

SILO 1: KUBERNETES CLUSTER

agent-sandbox · Agent Substrate

Istio · kgateway · agentgateway

[IdP #1: Local SPIFFE / K8s JWT]

SILO 2: NON-KUBERNETES PLATFORMS

OpenCode · Antigravity · Codex · Hermes

Docker · Podman · Dev Laptops · VMs

[IdP #2: Corp OIDC / Pairing]

SILO 3: CLOUD GPUS & APIS

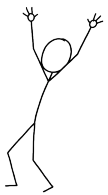
Gemini · vLLM · Modal

BigQuery · AWS S3

[IdP #3: GCP / AWS / Azure Cloud IAM]

"WHY NOT OVERLAY VPNs?!"

- Virtual IPs (100.x.y.z): IPAM management, Prompt injection port-scans SSH & DBs!
- Single IdP & Static Machine ACLs: Can't federate 3 IdPs or narrow per sub-agent hop!
- Blind to L7 models, MCP tools & data residency!



"THE 5 AGENT NETWORKING NEEDS!"

1. inference:// — LLM routing + EU residency check
2. mcp:// — Per-tool access (not full port access)
3. a2a:// — Multi-hop swarms w/ narrowing
4. egress:// — Secretless outbound API broker
5. /ingress/ — Policy-gated service publishing

VPNs connects machines at L3/L4; Agent Mesh governs the 5 agent primitives across IdPs with zero IPs.

KUBECON + CLOUDNATIVECON NA 2026 · UNIVERSAL P2P SECURE DATPLANE, KUBERNETES AGENTIG WGs & THE 5 PRIMITIVES

[X] OVERLAY VPN
(L3 Virtual IPs: 100.x.y.z)

Prompt-Injected Agent:
"Ooh, I'm on the IP network!"
|--> Scans SSH (:22) & DBs
|--> All-or-nothing MCP port
|--> Raw API keys in sandbox
+--> No GEO residency check!
[MACHINE ACL != AGENT POLICY]

"HOW DO YOU NETWORK CHAOS?" -> P2P (BitTorrent / eMule / Botnets)!

Lessons Learned from SIG-Network Agentic Projects:
1. MCP is unbounded over JSON-RPC -> static API schemas fail!
2. Bottleneck is LLM TPS (seconds), NOT proxy µs -> optimize for REACHABILITY!



1. inference://<model>
Model Routing + EU Residency Check

2. mcp://<service>
Per-Tool Access & Attenuation

3. a2a://<agent>
Swarm Delegation Across NATs

4. egress:// & 5. /ingress/
Secretless Egress + A2A Card Relay

Closed by default over libp2p mTLS 1.3 + Kademlia DHT: 5 agent primitives, zero IPs in policy!

KubeCon + CloudNativeCon NA 2026 · How Policies Work: Eclipse Biscuit, Datalog & Mesh Policy

1. [X] Remote L7 Webhooks
ingress-nginx Lua · Envoy Wasm
Remote ext_authz callouts:
Extra network hops & black-box code!

2. [!] Local CEL / Cedar / OPA
Non-Turing-complete & auditable,
but NOT a cryptographic token
that travels across hops!

3. [✓] Biscuit + Datalog
Google "Bakery" (Macaroons)
->
Ed25519 token + embedded Datalog
evaluated offline in µs!



```
// 1. Central Mesh Policy (roles & bindings)
roles:
  - name: "developer"
    allowed_services: ["mcp://*", "inference://*"]
    allowed_publish:  ["a2a://diagnoser"]
    allowed_labels:   ["region=eu"]
bindings:
  - role: "developer"
    members: ["group:eng",
"spiffe://k8s/ns/ai/sa/x"]
```

```
// 2. Compiled Datalog (Evaluated 100% Offline)
check if client_peer_id($id),
connection_peer_id($id);
check if label("region", "eu");
allow if role("developer"),
service("mcp", $s);
```

Localhost ext_authz into agentmesh-node is great (we support it!); Remote webhook hops are what hurt.

KUBECON + CLOUDNATIVECON NA 2026 · TWO-LAYER SECURITY: BLOCK 0 PEERID BINDING + OFFLINE TAR_BLOCK

BLOCK 0 · AUTHORITY
Control Plane (Off Hot Path!)

- Enrolls via OIDC / SPIFFE / K8s JWT + Ed25519 PoP (/register)
- Binds client_peer_id(PeerID)
- Signs label("region", "eu")

+ BLOCK 1 · ORCHESTRATOR
Appended Offline in RAM

- Fact: tar_block(proto)
- Narrows tool: get_q3_revenue
- Target: mcp://finance.report
- Max TTL: 5 minutes

+ BLOCK 2 · SUB-AGENT SANDBOX
Appended + biscuit.Seal()

- Fact: tar_block(proto)
- HTTP Method: GET Only
- Path: /v2/eu_sales/*
- Cryptographically Sealed!

"WHAT IF AN ATTACKER STEALS THE BISCUIT TOKEN?!" -> USELESS!

1. TLS connection_peer_id != Token client_peer_id (Zero Replayability on any other host).
2. Effective Authority = Block 0 Policy AND TAR Block 1 AND TAR Block 2 (Monotonic narrowing in O(1) RAM).



Standard JWTs at both borders (RFC 8693); channel-bound, offline-attenuatable Biscuits inside.

KUBECON + CLOUDNATIVECON NA 2026 · GUARANTEEING SOVEREIGNTY: 3-WAY NODE RULES & MUTUAL CHECK

1. PROVIDER REFUSES CALLERS

attenuation.checks:
check if label("app", "laptop");
Data owner restricts who can call!

2. OPERATOR IMMUTABLE FLOOR

egress.require_labels: region: eu
Admin enforces residency floor;
Prompt injection CANNOT lower it!

3. CALLER PER-REQUEST HEADER

X-Mesh-Required-Labels:
region=eu
Caller verifies provider
BEFORE 1 byte of data leaves!



```yaml
# agentmesh-node.yaml
version: v1alpha1
labels:
  - region: eu
  - app: diagnoser
attenuation:
  checks:
    - 'check if label("app", "laptop");'
egress:
  require_labels:
    region: eu
```

```
// 5-Step Mutual Call Check
1. Caller -> Provider: Caller Biscuit (0 bytes sent)
2. Provider checks Caller Biscuit & Policy offline
3. Provider -> Caller: Provider Biscuit (region=eu)
4. Caller checks Provider labels (Aborts if US!)
5. Both pass -> Service Call Payload moves!
```

"The model asks. The node decides." — Both caller and provider verify signed Biscuit facts offline before payload moves!

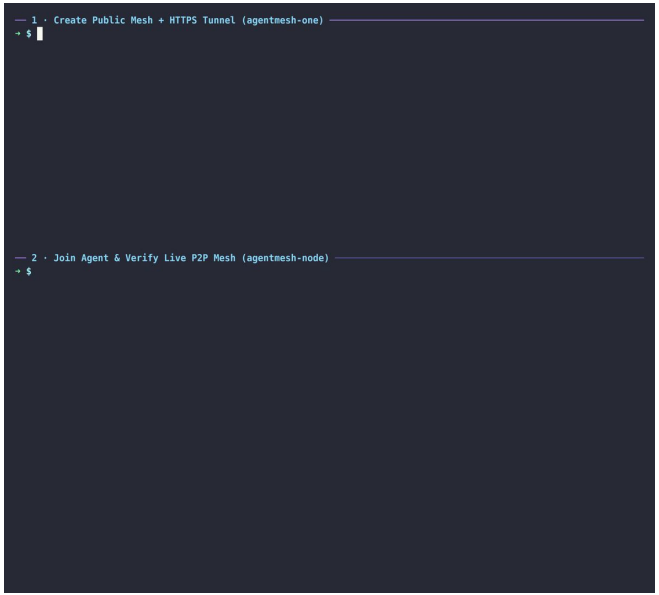
KUBECON + CLOUDNATIVECON NA 2026 · ARCHITECTURE: CONTROL PLANE & 2-TIER P2P DATA PLANE

CONTROL PLANE · ADMIN FRONTEND (OFF HOT PATH!)
HOSTS MESH POLICY · VALIDATES OIDC/K8S/SPIFFE · MINTS BLOCK 0 BISCUITS

DATAPLANE TIER 1 · ROUTERS (ADMIN / NETOPS CONCERN)
BOOTSTRAP NODES · KADEMLIA DHT · NAT SIGNALING & RELAY · /INGRESS/

DATAPLANE TIER 2 · NODES & SDKS (WORKLOADS & DEVS)
SIDECAR (AGENTMESH-NODE :8080) OR EMBEDDED SDKS (SDK/MESHNET)

ON-DEMAND / MINIMAL SCALE: AGENTMESH-ONE
CONTROL PLANE + ROUTER + CONSOLE IN 1 BINARY!





CONTROL PLANE HOSTS POLICIES & MINTS BISCUITS OFF THE HOT PATH; 2-TIER P2P DATAPLANE (ROUTERS + NODES/SDKS) KEEPS RUNNING!

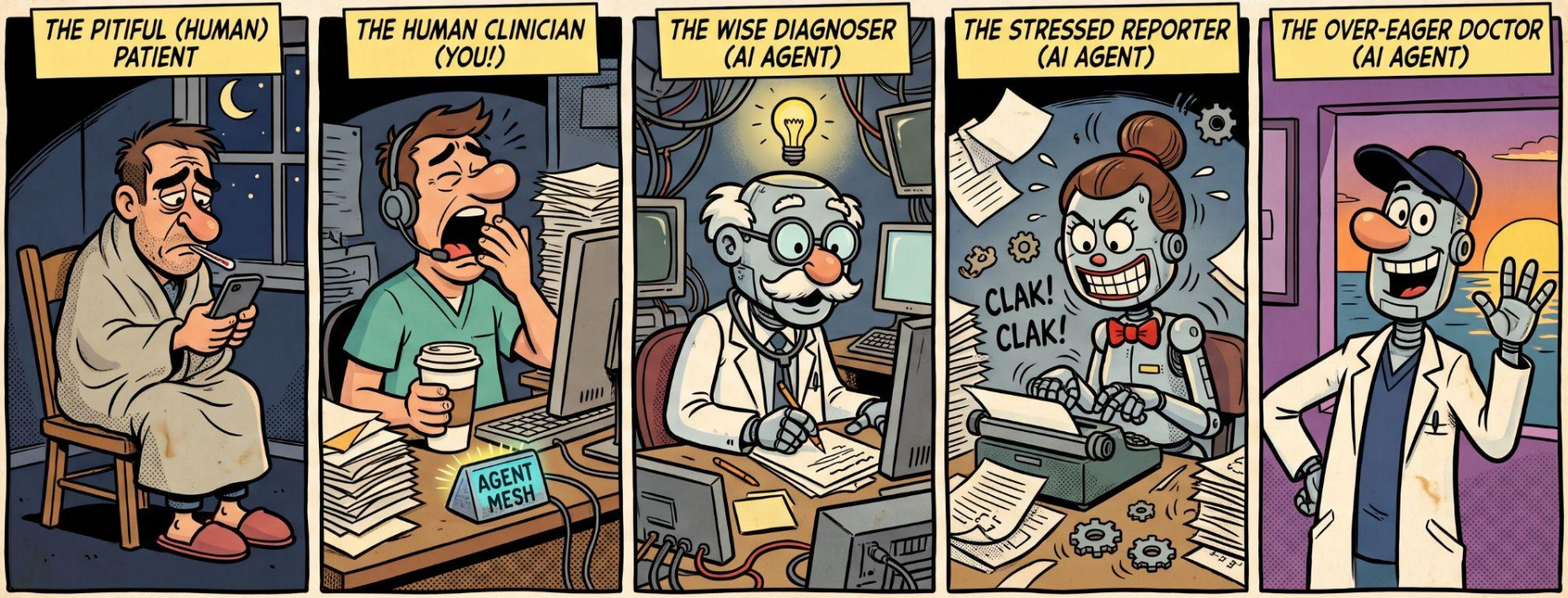
AGENT MESH DEMO

CASE 4711 – THE NIGHT SHIFT!

human oversight, AI efficiency

EUROPE REGION 🇪🇺 • 04:12

US WEST REGION 🇺🇸 • 19:12



KUBECON + CLOUDNATIVECON NA 2026 · WHAT'S NEW IN v0.2.0 AND WHAT's NEXT

01 · v0.2.0 CHANGELOG

- Go (sdk/meshnet), JS & Python SDKs
- Android: Experimental support
- External HTTP /ingress/ relay across NAT

02 · SOVEREIGN & RUNTIMES

- EU Sovereign Cloud & AI Act controls (Signed region=eu geo-fencing)
- Cross-runtime: Google ACE, Azure, AWS, Vercel Edge & Docker/Podman
- Gateways: Istio, kgateway & Envoy

03 · COLLAB: LLNL & HEURETES

- National Labs & HPC research project
- Hyperscheduling: graph scales across sites
- Secretary agents negotiate & dispatch
- Resource-manager agnostic (Flux + K8s)
- Trust fabric for multi-site placement

04 · COLLAB: LINUX FOUNDATION A2A PROJECT (github.com/a2aproject/a2a-serve)

"By embedding Agent Mesh v0.2.0's sdk/meshnet (--private agentmesh --public agentmesh), a2a-serve turns coding harnesses (opencode, Claude Code, Codex, Antigravity) into discoverable, sandboxed A2A agents across NATs—with zero SaaS lock-in, secretless egress:// key brokering, and offline Biscuit task attenuation."



v0.2.0 shipped today (Go/JS/Python SDKs + Android) + 2 immediate collaborations: LLNL HEURETES & Linux Foundation A2A.

KUBECON + CLOUDNATIVECON NA 2026 (Q&A) · OSS ACKNOWLEDGEMENTS & PROJECT ROOTS

[❖] LIBP2P PROJECT

libp2p.io · github.com/libp2p/go-libp2p

- Modular P2P networking stack born from IPFS & Filecoin ecosystem.
- Cryptographic PeerID binding + encrypted mTLS 1.3 & Noise handshakes.
- Kademlia DHT O(log N) decentralized routing & Circuit Relay v2 hole-punching.
- Huge appreciation to the libp2p maintainers & global community!

[*] ECLIPSE BISCUIT PROJECT

biscuitsec.org · github.com/eclipse-biscuit · Eclipse Foundation

- Next-gen authorization token standard (Eclipse technology.biscuit).
- Embedded Datalog logic engine for offline, non-Turing complete verification.
- Unforgeable offline attenuation in memory without central verifier callouts.
- Warm thanks to C. Delafargue (@divarvel) & team!

```
# TRY AGENT MESH TODAY:

$ curl -sL https://google.github.io/agentmesh/install.sh | bash
$ agentmesh-node join https://bananas.sam-mesh.dev
$ agentmesh-node skill install

Docs & GitHub: https://github.com/google/agentmesh
```



Governing and Scaling Agents in Heterogeneous Environments

SCAN FOR SLIDES & CODE

github.com/google/agentmesh

THANK YOU & QUESTIONS! · Antonio Ojea (@aojea) & Tomas Tormo (@kaisoz) · Apache-2.0 Open Source