



Automatic OAuth Client Registration

With SPIFFE Credentials

Pieter Kasselman
Dag Sneegeen
Ismael Kazzouzi

Why Automatic Client Registration

1. Operational Cost - Toil, error, maintenance
2. Heterogeneous Environment - Org+Technical Complexity
3. Velocity - Market demand, team responsiveness, ephemeral workload
4. Exponential growth - Scaling up, AI
5. Security - Secrets Sprawl

What is SPIFFE?

- Solves for the “Bottom Turtle”
 - Bootstrap Credentials without secrets
- Attested workloads (aka clients)
 - Identity Proofing
- Assigns Identifiers
 - SPIFFE ID - `spiffe://domain/path`
- Issues and Provisions Credentials
 - X.509 SVID, JWT-SVID
 - Short lived
- Continuous Lifecycle Management
 - Built-in rotation
 - Accountless
- Deployed at Scale
 - OSS, Commercial



Learn more: <https://spiffe.io>

Why SPIFFE for Auto-registration?

Get Authorization servers out of the business of managing client identities

1. Replace labour intensive process with automated workload attestation.
2. Client/Workload providence is deferred to the SPIFFE Issuer.
3. Credentials are managed by a platform, short lived, high availability, scalable.

Simple, Scalable, Secure

A tale of two approaches (or at least a sketch)

Register on First Use

1. No additional registration protocol
2. Efficient, low latency
3. Suited to Client Credential Flows
4. Redirect Flow customisations
5. Metadata Management



DCR with Trusted Issuer Credentials

1. JWT-SVID as Software Statement
2. Compatible with DCR
3. MCP Enablement
4. JWT only
5. Generalised to other cred types



What next?

- Does this problem interest the working group?
- Are these approaches of interest the working group?
- Please reach out, add comments, open issues, create PRs.

Simple
Scalable
Secure

