CREDENTIAL MANAGEMENT FOR AI AGENTS · ADD-ON TO LUMEN POET

Lumen POET Credential Broker

The policy decision point and policy enforcement point for agent credentials

Overview

Every credential an AI agent holds is a credential that can leak, sprawl, or outlive its purpose. Hard-coding API keys into agents recreates the worst habits of service-account sprawl at machine speed. The Lumen POET Credential Broker removes the problem at its root: agents hold no standing secrets at all.

An add-on service to Lumen POET, the broker front-ends generated MCP servers and A2A agents as the policy decision point and policy enforcement point for credentials. The application administrator defines the policy schema, mapping users, roles, and AI agents to the features and scope each may exercise. When an agent arrives, with no token, a just-in-time token, or a user bearer token, the broker validates the caller against enterprise IAM and exchanges the request for a vault-held non-human identity credential. Standing secrets live only in the vault. Agents hold nothing worth stealing.

Why it matters

Zero standing privileges
Agents carry no permanent secrets. Every credential is resolved per transaction from the vault and scoped by policy.

Policy the app admin owns
The administrator defines the PDP schema: which users, roles, and AI agents may reach which features, at what scope.

The vault stays in charge
Passwords and certificates never leave the external PAM vault, and rotation practices are preserved unchanged.

Audit evidence per transaction
Every exchange records the caller, the schema decision, the credential type, and the credential lifetime.

Capabilities

Credential PDP and PEP
Front-ends generated MCP servers and A2A agents, deciding and enforcing which credential, if any, each caller receives.

Admin-defined policy schema
The application administrator maps users, roles, and AI agents to features and scope. Policy lives with the application owner, not in agent code.

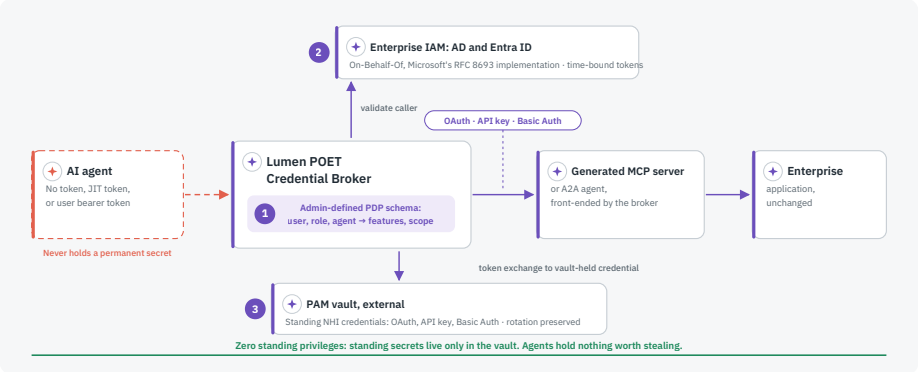
Flexible inbound identity
Accepts agents arriving with no token, a just-in-time token, or a user bearer token, and normalizes each against enterprise identity.

Enterprise IAM validation
Verifies callers with AD and Entra ID. On-Behalf-Of, Microsoft's implementation of RFC 8693 token exchange, yields a time-bound token; the broker registers as a directory application.

Vault-held credential swap
Exchanges the validated request for a vault-held NHI credential: OAuth, API key, or Basic Auth. The agent never sees the standing secret.

Legacy compliance, no code change
Applications that only speak API keys or Basic Auth become governed, agent-ready endpoints without modification.

Architecture



The broker validates the caller with enterprise IAM and swaps in a vault-held credential. The agent never holds a standing secret.

How it works

1. Define the schema. The application administrator maps users, roles, and AI agents to the features and scope each may exercise: the policy decision point.
2. Validate the caller. The agent arrives with no token, a JIT token, or a user bearer token. The broker verifies it against AD and Entra ID; On-Behalf-Of, Microsoft's RFC 8693 implementation, produces a time-bound token, with the broker registered as a directory application.
3. Swap the credential. The broker exchanges the validated request for the vault-held application credential, OAuth, API key, or Basic Auth, and completes the call. The secret never reaches the agent.
4. Evidence follows every transaction: caller, schema decision, credential type, and credential lifetime, recorded alongside the gateway's intent verdict when deployed with Lumen A2A Gateway.

Deployment

Delivered as an add-on to Lumen POET and enabled per generated MCP server or A2A agent. The broker sits in the request path inside the customer VPC.

Deploy behind Lumen A2A Gateway for defense in depth: the gateway authorizes intent, the broker authorizes credentials, and each transaction carries evidence from both.

Technical specifications

Function	Policy decision point (PDP) and policy enforcement point (PEP) for credentials
Packaging	Add-on service to Lumen POET; front-ends generated MCP servers and A2A agents
Policy schema	Admin-defined: users, roles, and AI agents mapped to features and scope
Inbound identity	No token, just-in-time token, or user bearer token
IAM validation	AD and Entra ID; On-Behalf-Of (Microsoft's RFC 8693 implementation); broker registered as a directory application; time-bound tokens
Credential types	Vault-held NHI credentials: OAuth, API key, Basic Auth
Secret handling	Passwords and certificates stay in the external PAM vault; rotation preserved; agents never hold permanent secrets
Standing privileges	Zero
Audit evidence	Per transaction: caller, schema decision, credential type, credential lifetime
Legacy applications	Governed with no application code change

Standards and interoperability

- **OAuth 2.0 token exchange:** RFC 8693, including Microsoft On-Behalf-Of
- **Identity providers:** Active Directory, Microsoft Entra ID
- **Credential types:** OAuth, API key, Basic Auth
- **Vault integration:** External PAM vault; rotation preserved
- **Zero trust:** Zero standing privileges, aligned with NIST SP 800-207

THE BACKFLIPT DIFFERENCE

No agent is re-coded. No application authorization is reworked. Enterprises scale AI on the identity and security investments they already have.

About Backflipt

Backflipt (Xenovus, Inc.) builds the Lumen product line for runtime authorization of AI agents. Lumen A2A Gateway authorizes agent intent, Lumen POET generates agent-ready MCP servers and A2A agents from the API specifications enterprises already have, and the Lumen POET Credential Broker keeps standing secrets in the vault and out of agents. www.backflipt.com · reachus@backflipt.com