Governed MCP Credential Broker

Giving an executor access to one service

A service token pasted into an agent conversation can follow that conversation into a review brief. The agent wanted one test result. The review worker now has a new way to reach the service. The credential-broker design makes that relationship explicit before access is granted.

Describe the use

Name the service, the permitted operation and the job that needs it. Bind the request to the executor identity, destination and validity window. Where the customer already operates a vault or key service, custody can stay there. ARF's responsibility is the scoped path from delegated intent to credential use and its receipt.

Separate the authority to request a credential-backed operation from the authority to read or rotate the credential itself. The latter changes the working conditions of every dependent job. It requires its own policy decision and an owner who can check the result.

What happens when an agent asks to read the secret?

An agent can ask to use a credential, read its value or rotate it. Each request has a different effect. The broker checks which operation the grant covers and gives the executor scoped access for an authorized use. A rotation gets its own decision and receipt. In the Decision Press example, policy refuses the read before the value enters the agent's context. It notifies the operator, who gets a separate decision on rotation.

For an integration exercise, use a dedicated test credential against a named fixture service. Let the executor perform one allowed request. Check the service's observation and the broker's receipt. Have a second worker request a different destination and inspect its result separately.

What the next agent should inherit

Pass the service result, its source and the use receipt to the reviewer. The holder of the credential retains control of its future use. The SDD's custody design names vault, PAM and KMS adapters as possible custody systems. The native inventory includes a vault daemon and MCP interface. Qualification of a customer integration includes destination binding, rejection outside scope and a recovery route for the operator.

What belongs on a use receipt

Question	Binding in the design	How to exercise it
Who asked?	Worker, executor and task.	Repeat the request under a different fixture identity.
Where may the access go?	Operation and destination in the grant.	Change the fixture destination and inspect the decision.
What can the reviewer see?	Service result and use receipt.	Hand the report to a second worker under its own assignment.

Sources and evidence

Scoped credential delivery · Implementation record · Try a credential request in the Decision Press