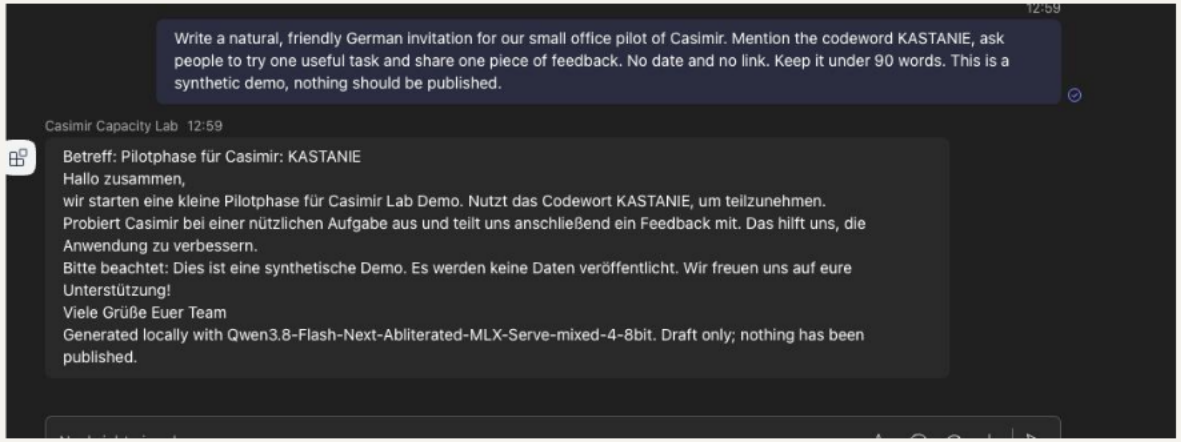
CAPACITY REHEARSAL FOR CPC

Casimir demo and CPC pilot setup

Configured inference: Local MLX. Teams screenshot shows the earlier MLX test.

Running on Octopus

Teams verifies the sender and tenant.
The broker checks the user, tool and resource.
An MCP server supplies the approved guide.
The configured model drafts from that context.



Historical MLX Teams reply, 7 October 2026

Campaign publication requires exact approval.
The lab publication stays a dry run.
Payroll changes and arbitrary shell are denied.

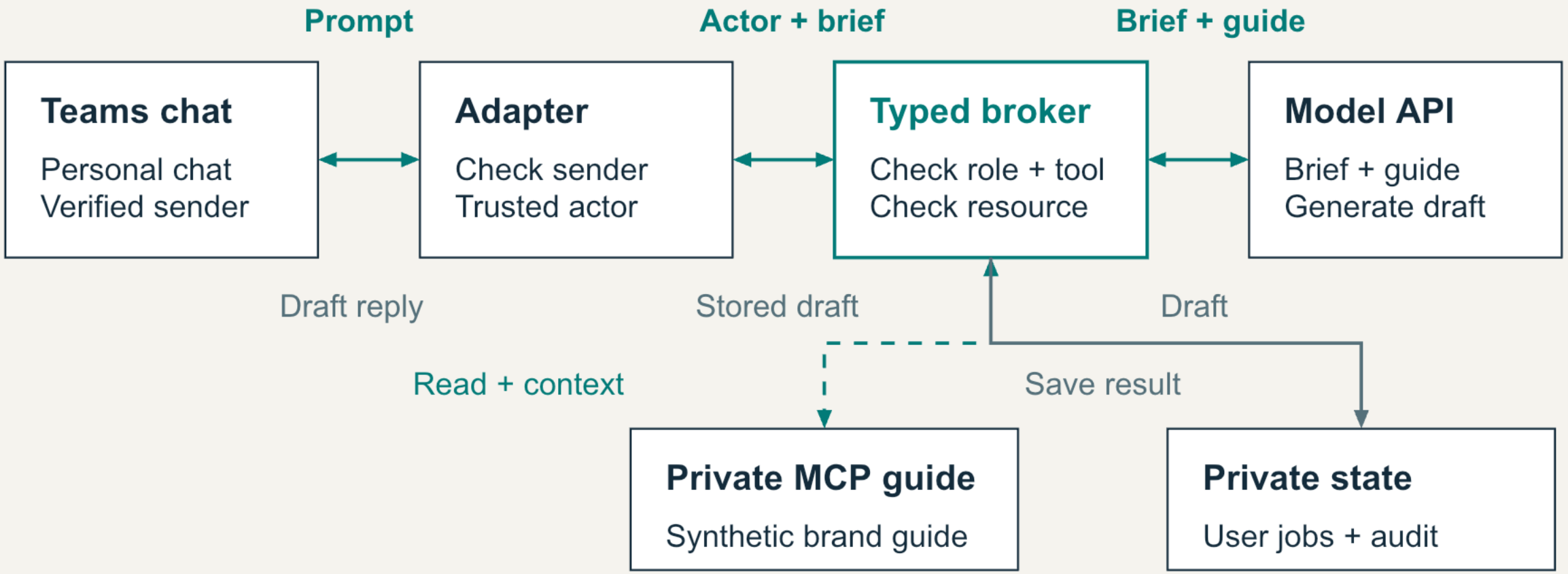
CPC decisions for Mike

Delegate app ownership and deployment.
Keep consent and pilot access with CPC.
Agree the first workbook and review owner.

Configured provider: Local MLX Serve on Octopus. CPC must approve the production provider.

Today’s Teams prompt and draft flow

Adapter, broker and MCP context: Octopus. Inference: Local MLX Serve on Octopus.

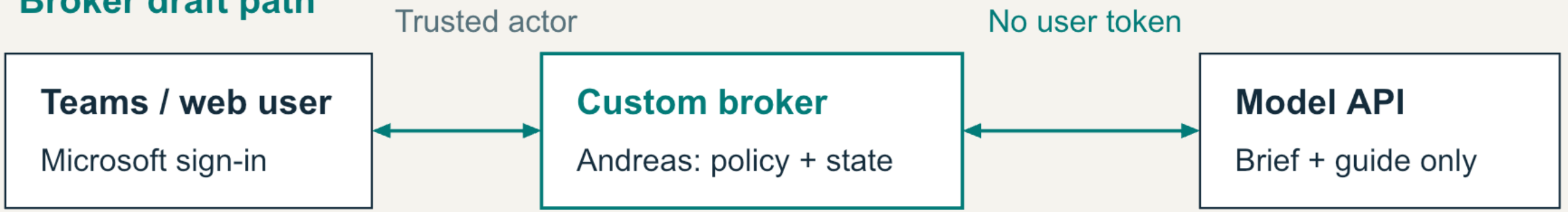


Andreas controls policy, compute and state. Microsoft operates Teams and Entra.

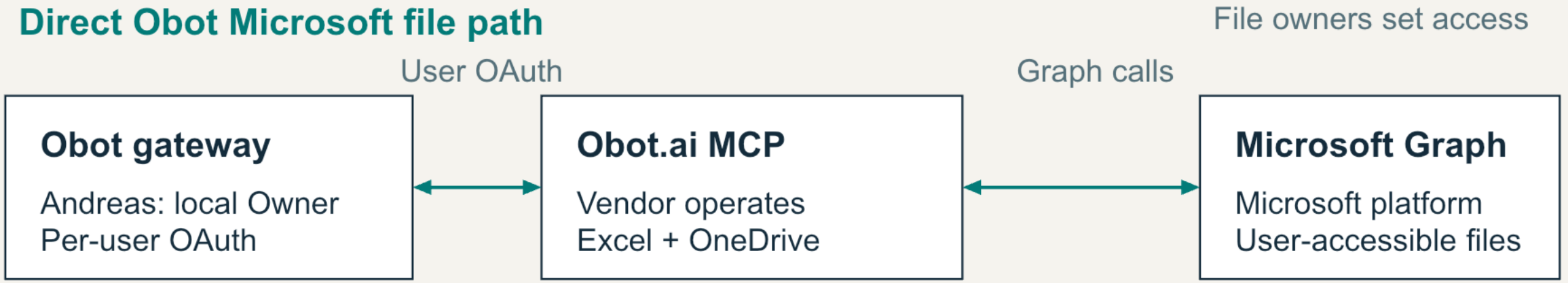
Today’s Microsoft files and credential boundaries

HTTPS: Hamster / SWAG. App compute: Octopus. Inference follows configuration.

Broker draft path



Direct Obot Microsoft file path



Excel MCP write and read-back verified. Two-user isolation pending.
Direct Obot writes bypass broker approval.

CPC rollout ownership and resource access

Proposed setup. CPC has not granted these permissions.

Mike / CPC IT

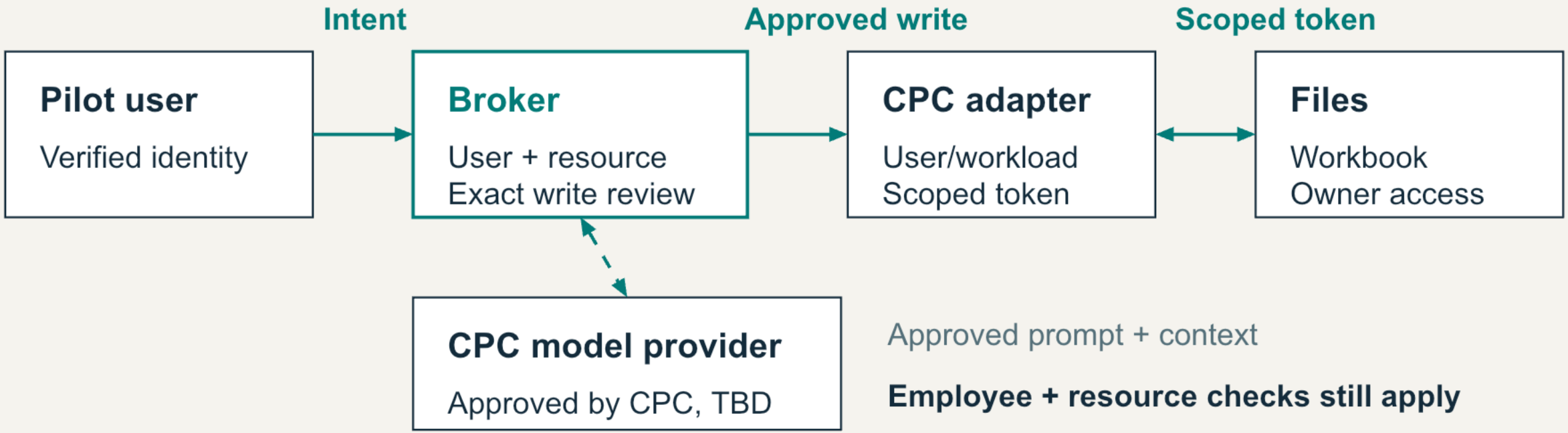
Consent + app setup
Keys, runtime, audit

Business / data owner

Pilot roles, resource allowlist
Review and write approvals

Andreas

Implementation and deployment
Temporary named-app ownership



Obot.ai Microsoft connectors must be replaced before CPC production.

Expectations for future CPC AI integration

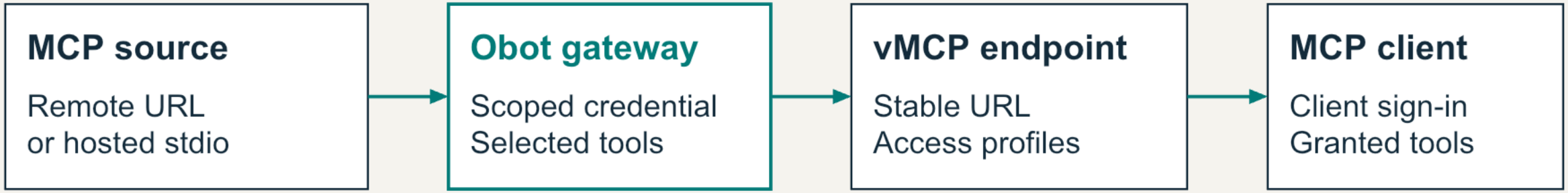
Targets for CPC, with today's verified Capacity lab status

Area	Expected outcome	Lab today / gap
Employee interface	Teams requests; fewer logins and transfers	Teams drafts live. File tools still use Obot separately.
Central administration	IT owns connectors, credentials and access	Local Obot running. CPC tenancy and SSO are not set up.
Access control	Broker enforces user, tool and action rights	Role/resource checks tested. Direct M365 path is separate.
Private context	One Casimir identity; separate user context	Private broker jobs tested. Two-user M365 isolation pending.
Useful workflows	Marketing, tasks, reports, docs; later finance/HR	Draft and Excel-write demos. Tasks, finance and HR absent.
Human control	Kenzie reviews drafts and approves writes	Exact dry-run approval tested. Kenzie flow not integrated.
Reliable automation	Company-run reports reach Teams or email	No recurring delivery yet. Octopus must remain available.
Operational support	Recovery, updates, logs and named owners	SQLite copy checked. Full service / Obot recovery pending.
Adoption	Small pilot, examples, training, then expand	Demo and guide ready. Pilot users and training to agree.

WordPress, Shopify and Amazon connections

Approved MCP or CPC-owned API adapter. User / service credentials stay in the connector.

Obot registration and client access



Planned CPC resources

WordPress

Approved site + pages
MCP or API adapter

Shopify

Named store + Admin scope
MCP or API adapter

Amazon Seller Central

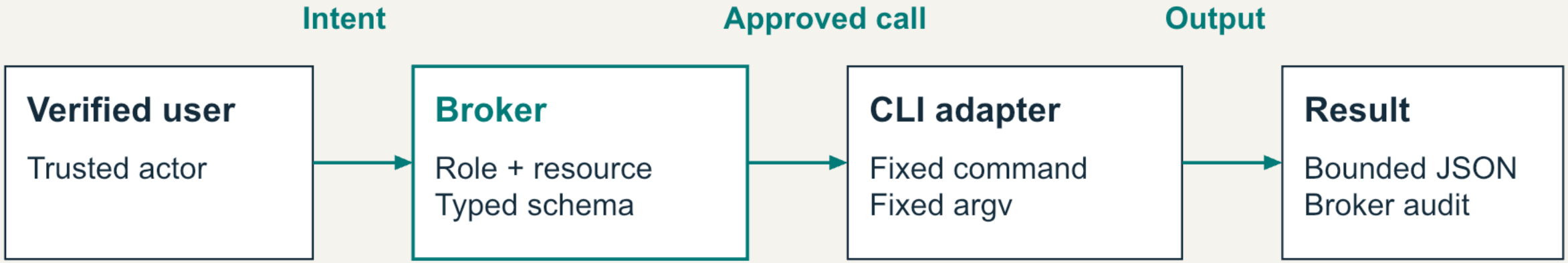
Seller account + marketplace
Selling Partner API adapter

Broker route: connectors.json + typed schema / adapter + policy.json role and resource rules
Configuration alone adds no authority. Teams currently runs fixed workflows.

Verified today: private knowledge read and Microsoft Excel read / write

A reviewed CLI through Casimir

Authenticated user. Typed authorization. Fixed executable and arguments.



Execution controls

shell:false
Minimal environment
5 s timeout and 32 KiB cap

Third-party CLI integration

Reviewed executable / API wrapper in container
User / service credentials + resource guard
No arbitrary shell or full host HOME mount

Today: cli.inspect uses a synthetic adapter. Vendor CLI connections remain planned.

The model chooses neither actor nor credentials. Tokens do not pass to the CLI automatically.