

AI Agents Meet Data Spaces

How MCP and connectors give agents governed access to shared mobility data

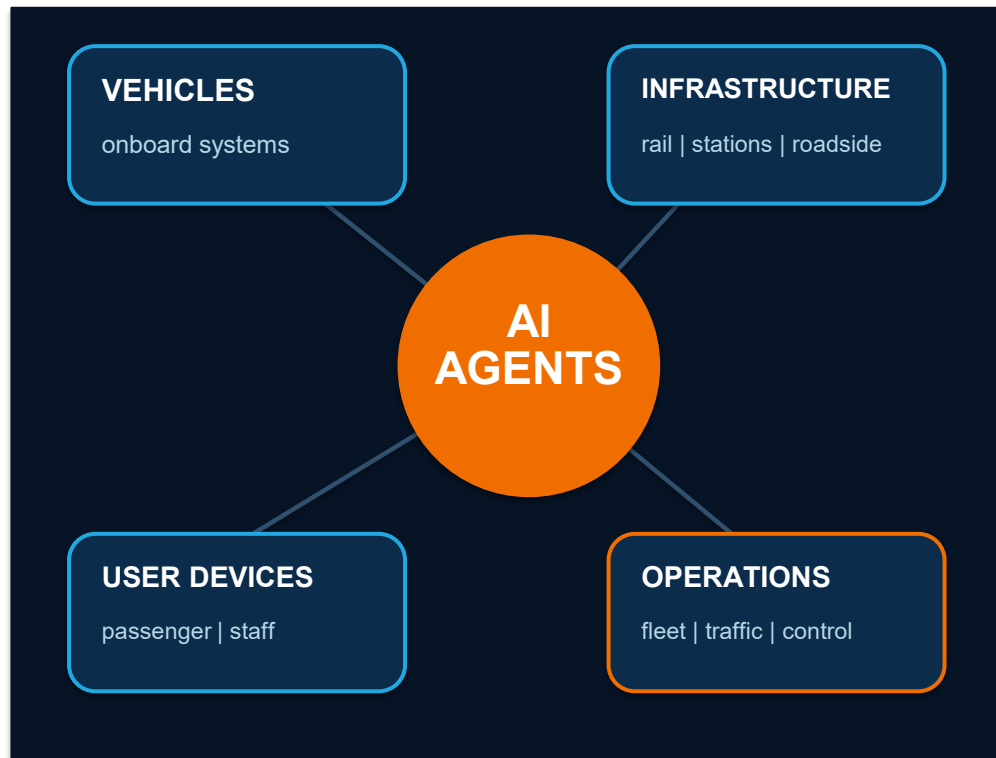
AI agents are entering mobility operations

Vehicles, infrastructure, operations platforms and user devices are becoming data sources and action environments.

**Agents increasingly
observe, reason,
coordinate and act across
mobility systems.**

USEFUL AUTONOMY

**Trusted data +
bounded authority**



AI agents are only as good as the data they can reach

- Agents can plan, coordinate and act across mobility systems, but the valuable data usually sits in other organisations: fleets, infrastructure, operators, cities, etc.
- The **opportunity**: agents that reason over live, distributed mobility data have good context
- The **constraint**: that data is owned by others, commercially sensitive and safety-relevant
- Open APIs are not enough. Organisations need control over who accesses what, for which purpose, under which terms

Mobility agents need data and action authority

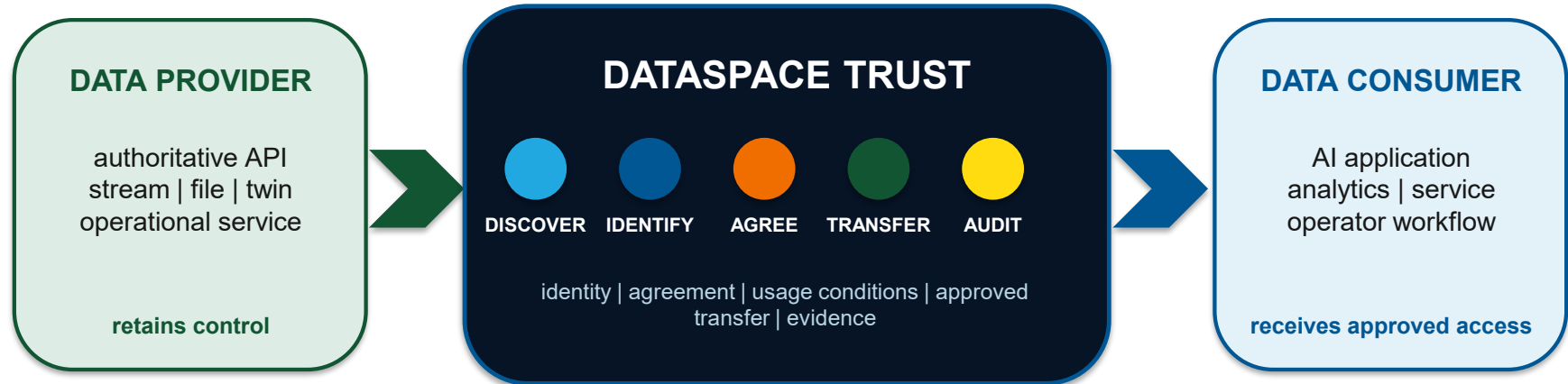
The same agent may observe, reason, recommend and act, but each step has a different risk profile.



The agent must see enough to help, without gaining a path around security, policy or operational control.

Data spaces provide the organisational trust layer

They support governed exchange between independent participants while providers retain control.



Data stays with its provider. Access is granted under explicit conditions.

WHAT THE DATA SPACE ADDS

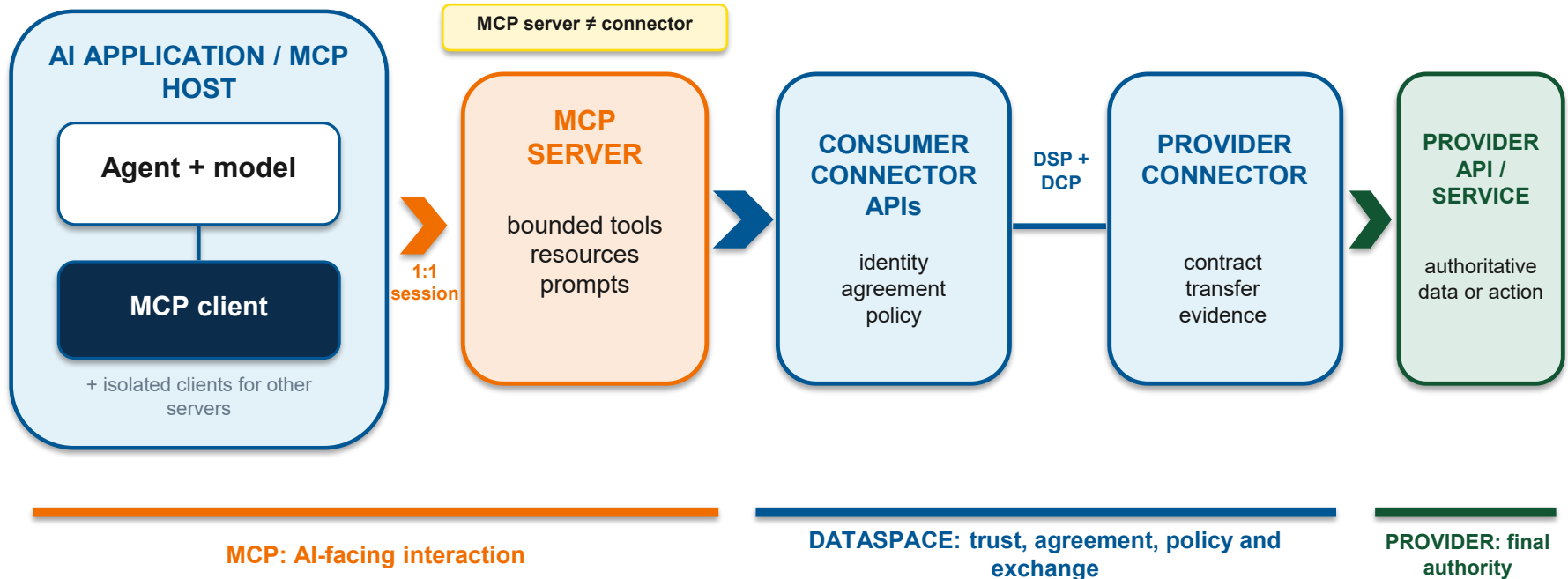
discovery | organisation identity | agreements | usage conditions | provenance

STILL REQUIRED

AI reliability | data quality | endpoint security | operational safety

MCP and data spaces solve different parts

MCP exposes bounded capabilities to the AI application. Connectors enforce organisational exchange.



An agent request enters the governed connector flow

The recorded VTT demonstration follows catalogue, identity, agreement and transfer before the agent receives data.

The screenshot displays the 'AI AGENT PLATFORM' interface. The main section is titled 'mcp-data' and shows 'MCP-DATA · READ MEMBRANE'. It describes the single governed gateway to all Lyyli telemetry. Below this, there are 'EXPOSED TOOLS' including 'timescale.query', 'realtime.latest', 'realtime.gtfs_rt', 'timescale.schema', and 'timescale.freshness'. A sidebar on the right shows 'SERVICES' (8/8), 'LLM TOKENS - TODAY' (233k), 'A2A CHECK-INS' (9), 'SECURITY POSTURE' (PASS), and 'RUUVI SENSORS'. At the bottom, the 'EDO Connector · API access' section is highlighted, showing a 'DATA SPACE' button and a 'view flow' link. A tooltip 'Open the data space flow' is visible over the 'DATA SPACE' button.

35 s

27/08/20

Operational actions require stronger assurance

The agent may be allowed to understand without being allowed to change.

SAME IDENTITY + POLICY FOUNDATION

READ PATH



- read-only provider role
- scoped fields + time range
- freshness + provenance
- usage-policy evaluation

ACTION PATH

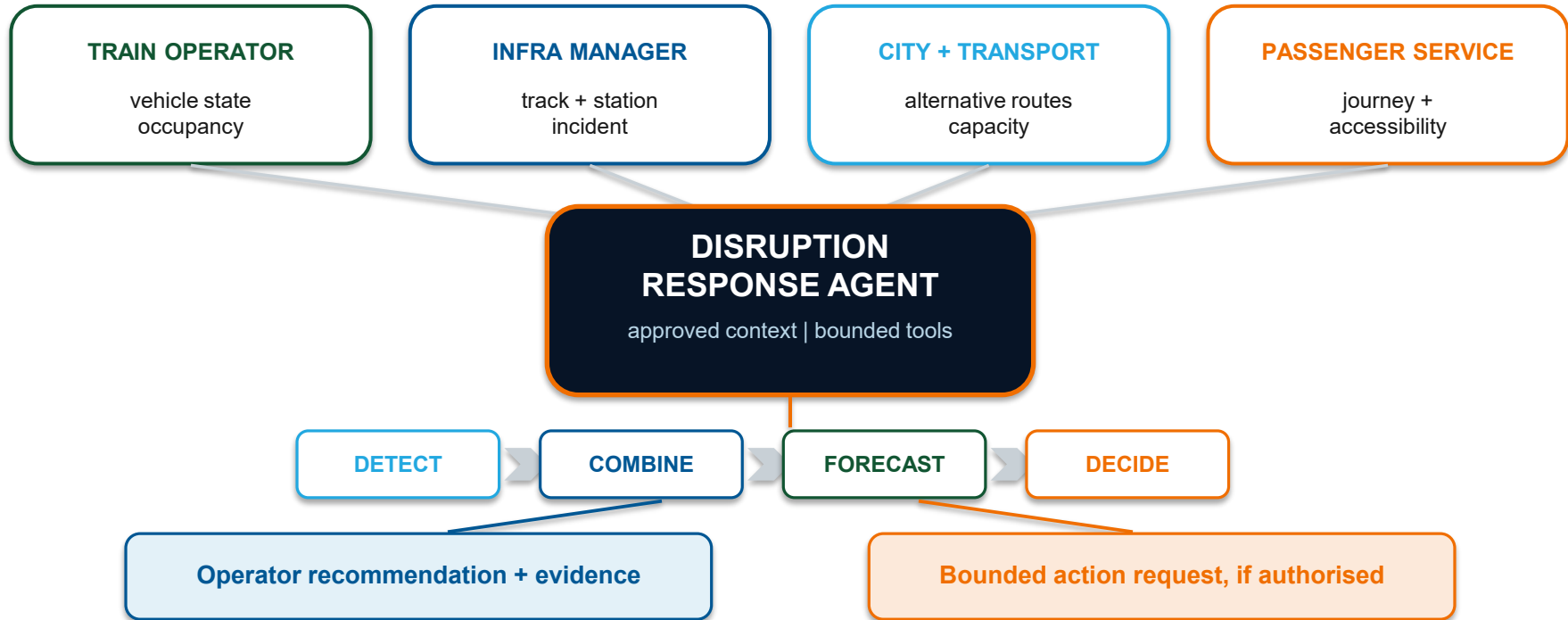


- validated parameters
- limited effects + rate limits
- simulation first
- approval where needed
- authoritative outcome log

Critical permissions, policy decisions and safety controls remain outside the language model.

Example: coordinated response to a rail disruption

The response combines governed data products from several participants without removing their control.



bey⁰nd

the obvious

Kiitos!

Janne.lahti@vtt.fi