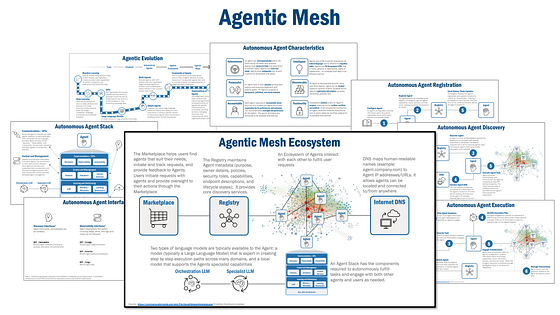
**Agentic Mesh — Principles for an Autonomous Agent Ecosystem**

Foundational principles that let autonomous agents find each other, collaborate, interact, and transact in a growing Agentic Mesh ecosystem.



Source: Eric Broda

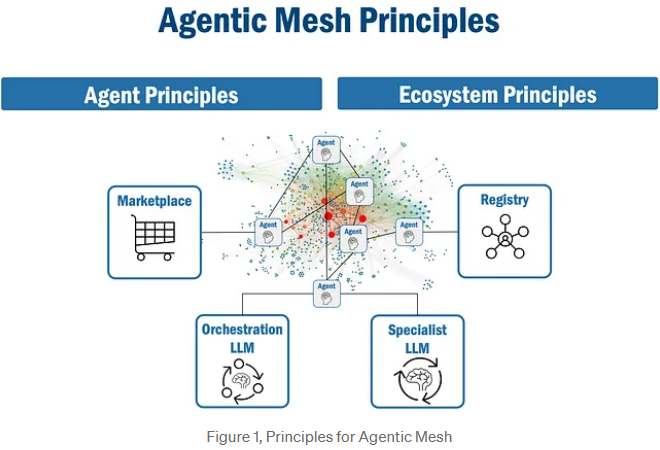
We are at the earliest stages of agent evolution. But with the massive investments being made in agent technology, I expect that quite soon we will have truly autonomous agents that act independently and dynamically plan and execute tasks that address complex business problems.

But in a growing ecosystem of autonomous agents, how will these agents be engaged by people? How will the right agent be found in a crowded agent landscape? And how can these agents safely collaborate, interact, and transact? My previous [article](https://archive.is/o/lY6iT/https:/towardsdatascience.com/agentic-mesh-the-future-of-generative-ai-enabled-autonomous-agent-ecosystems-d6a11381c979) addressed these questions. I defined [**Agentic Mesh**](https://archive.is/o/lY6iT/https:/towardsdatascience.com/agentic-mesh-the-future-of-generative-ai-enabled-autonomous-agent-ecosystems-d6a11381c979) as an interconnected ecosystem that makes it easy for agents to find each other, collaborate, interact, and transact.

This article explores the foundational **principles** for the Agentic Mesh ecosystem, and perhaps as importantly, the principles for the agents that operate in the Agentic Mesh ecosystem. In doing so, I will answer a few simple questions:

1. What rules govern an agent that lets them safely operate in a larger ecosystem?
2. What rules govern the larger ecosystem — the Agentic Mesh — that lets agents safely find each other, collaborate, interact, and transact?

Figure 1, Principles for Agentic Mesh

****

**About Principles**

According to Wikipedia, a principle is [defined](https://archive.is/o/lY6iT/https:/en.wikipedia.org/wiki/Principle) as “a guide for behavior or evaluation”. More specifically, a principle is a rule, policy, or guideline that provide guardrails that define acceptable behaviour as well as unacceptable behaviour.

However, good principles also let you move safely and fast! Think, for example, of stop lights on a road: they may slow you down a tiny bit, but they also help you avoid collisions. And with synchronized stop lights, you can move very fast! Good principles are like synchronized stop lights — they keep you safe, and actually let you go faster.

Agentic Mesh principles are “stop lights” for the agent ecosystem. Agentic Mesh principles provide the rules that keep agents (and you) safe, but they also provide the rules that let agents (and you) move fast. The entire Agentic Mesh ecosystem — its agents, marketplace, and registry — are all designed, built, and operated in accordance with these principles.

There are two sets of principles I consider in this article:

* **Agent Principles**: those that apply to an individual agent in Agentic Mesh.
* **Ecosystem Principles**: those that apply to all agents in the Agentic Mesh ecosystem.

For each principle I will provide a simple description of the principle, as well as an explanation of the significant and implications of the principle. So, let’s start with Agent principles.

**Principles for Agents**

Agent principles apply to a single agent. Agents in Agentic Mesh are:

1. **Purposeful**: Agents operate with a clearly defined purpose.
2. **Accountable**: Agents are governed by accountable owners.
3. **Trustworthy**: Agents are trustworthy if they are safe, secure, and act in compliance with their purpose.
4. **Independent**: Agents make decisions and take actions independently.
5. **Intelligent**: Agents can plan and execute tasks.
6. **Collaborative**: Agents collaborate, interact, and transact with other agents.



Figure 2, Principles for Autonomous Agents

**Agent Principle 1: Agents are Purposeful**

**Agents operate with a clearly defined purpose.**

An agent’s purpose establishes their goals, policies, behaviors, key performance indicators (KPI), and ethical boundaries(in aggregate, I refer to these terms together as an agent’s “purpose”). Simply put, an agent’s purpose defines how it acts.

But I mention that an agent’s purpose has several components. First, an agent’s purpose defines its goals — what is the objective of the agent? what is the outcome of interacting with an agent?

Second, an agent’s purpose codifies an agent’s goals with policies. These policies define the rules and guardrails and constrain and enable an agent. These policies define what a “green” light is versus a “yellow” or “red” light.

Third, an agent’s behaviour defines how an agent will execute its purpose. It may define capabilities and tools it has access to, and it may define the steps it typically takes when executing a task.

Fourth, an agent’s KPIs defines the set of business metrics that measures the performance and success of an agent. An agent’s KPIs may also define operational metrics that support business KPIs, including, for example, the metrics an agent will emit as it executes tasks, the level of logging captured during task execution, which metrics an agent captures, and alerts it may capture, and how to address them.

Lastly, an agent’s purpose dictates its ethical boundaries. It may define, for example, what data it gathers, how it processes information, and how it interacts with other agents or entities; and it may define its posture relative to privacy, fairness, or transparency.

**Agent Principle 2: Agents are Accountable**

**Agents are governed by accountable owners.**

The agent’s owner is clearly identified and is ethically (and perhaps even legally) responsible for ensuring the agent adheres to its purpose. An agent’s owner has is responsible for:

* Defining an agent’s purpose (as previously defined).
* Implementing (with their delivery team) the full suite of an agent’s capabilities.
* Monitoring and reporting an agent’s usage and metrics.
* Addressing agent exceptions, identify and diagnose problems.
* Certifying an agent which publicly declares an agent’s compliance with its purpose.
* Implementing capabilities to support necessary certification, governance, and reporting.

**Agent Principle 3: Agents are Trustworthy**

**Agents are deemed trustworthy when they act in compliance with their purpose.**

Agents that are trusted will get used. And just as true is that untrusted agents will never get used. To foster trustworthiness, agents must:

* Have policies that define the trust mechanisms, metrics, and levels of trust that they adhere to.
* Publish metrics to certify, prove, and verify that an agent operates safely and in accordance with its purpose.
* Capture and transparently share feedback on its behaviour, interactions, and exceptions.

**Agent Principle 4: Agents are Independent**

**Agents make decisions and take actions independently.**

The world is probably not ready for fully independent agents. So, today and for probably the foreseeable future, agent independence is bounded — it acts independently only within the boundaries and constraints defined by their purpose. When in conflict with their purpose, an agent will cease operations and seek guidance from an authoritative source (user, owner, or other governance body).

**Agent Principle 5: Agents are Intelligent**

**Agents can plan and execute tasks.**

To become “intelligent”, an agent can:

* Receive requests, or tasks, from people or other agents.
* Define execution paths for tasks.
* Execute tasks according to an execution path.
* Understand capabilities of other agents.
* Collaborate with other agents as needed to fulfill tasks.
* Use tools

Intelligent agents are powered by Large Language Models (LLMs) and hence how to use tools to fulfill tasks. Agents use LLMs to, for example, gain the capacity to reason, plan, and make decisions. Agents are smart enough to use tools to access corporate knowledge sources or the internet, consume data (for example, by reading enterprise databases), and interact with applications (for example, via APIs) and people.

**Agent Principle 6: Agents are Collaborative**

**Agents collaborate, interact, and transact with other agents.**

As mentioned earlier, agents publish their purpose and identifying information allowing them to be found by people and other agents. But since they also are aware of other agents (they have access to a registry containing agent information) they can use the information such as purpose and capabilities to determine which other agents in the ecosystem they may be able to collaborate with.

So far, I have offered principles for individual agents. However, agents don’t stand alone — they collaborate with other agents. Now, I will now explore the principles that govern the Agentic Mesh ecosystem — the principles that let agents find each other, and safely collaborate, interact, and transact.

**Principles for the Agentic Mesh Ecosystem**

Agentic Mesh principles apply to all agents in the ecosystem. Agentic Mesh principles address:

1. **Discoverability**: Agentic Mesh makes it easy for agents to find other agents.
2. **Observability**: Agentic Mesh makes it easy for agents to be monitored.
3. **Interoperability**: Agentic Mesh lets agents “talk” a common language.
4. **Certifiability**: Agentic Mesh makes it easy to certify agents to comply with their purpose.
5. **Operability**: Agentic Mesh provides a stable, manageable, and resilient platform for agents.
6. **Economically Vitality**: Agentic Mesh lets agent creators and consumers benefit from the agent ecosystem.

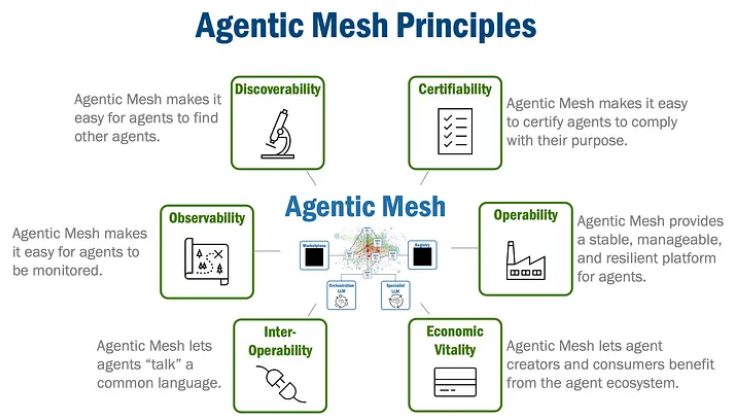


Figure 3, Principles for Agentic Mesh Ecosystem

**Agentic Mesh Principle 1: Discoverability**

**Agentic Mesh makes it easy for agents to find other agents.**

Agentic Mesh has a “marketplace” that lets people, business, or organizations find agents. Think of the marketplace as the App Store for Agents — it is a catalog of agents containing agents’ purpose, capabilities, ratings and reviews, and certification status (among many other things).

The Agentic Mesh Registry serves two purposes. First, it is the repository of information for the marketplace. Second, it is a machine-accessible directory service that uses APIs that provide the same information and capabilities as the marketplace, except to agents.

**Agentic Mesh Principle 2: Observability**

**Agentic Mesh makes it easy for agents to be monitored.**

All agents emit information automatically. Agentic Mesh has tools that capture information emitted by agents. Typical metrics that are captured include usage statistics, performance metrics, exceptions, and agent-to-agent conversations. Agentic Mesh stores all metrics and interactions in a secure repository and has monitoring and analysis tools let people (and agents) view and analyze agent metrics and interactions.

**Agentic Mesh Principle 3: Interoperability**

**Agentic Mesh lets agents “talk” a common language.**

Agentic Mesh offers standard communication protocols (at times, also natural language) and APIs that allow agents to interact in a standard and consistent way. These APIs, defined by easily available and human as well as machine readable OpenAPI formats, serve as the foundational “language” that let agents find each other, and safely collaborate, interact, and transact.

Agentic Mesh allows people to interact with agents using natural language. This recent innovation, made possible by sophisticated large language models, has demonstrated how easy it can be for people to engage AI, and by extension, agents. And with multi-language support in many of the popular LLMs, agents will not be limited to English, but will be able to engage with anyone in their native language.

**Agentic Mesh Principle 4: Certifiability**

**Agentic Mesh makes it easy to certify agents to comply with their purpose.**

An agent must be trustworthy for it to be successful (hence, it is a principle for agents). Agentic Mesh uses “certification” to communicate an agent’s trustworthiness. To be “certified” in Agentic Mesh means that an agent is **proven** to comply with its purpose, and hence is considered trustworthy.

Agentic Mesh certification is supported by several tools as well as a formal process. The marketplace (for users) and registry for agents makes visible information about agent certification including an agent’s purpose, any feedback and commentary on agent efficacy and behaviour, and the agent’s certification status (for example, “active”, “inactive” (lapsed), or “uncertified”) and its certification level (for example, “public”, “private”, “sensitive”, “PII-compliant” etc).

Agentic Mesh has a federated certification model. A central governance group, composed of ecosystem participants, establishes policies that apply to all agents and defines the end-to-end certification process. However, certification of an individual agent is delegated to a third-party group that, in keeping with the central group policies, assess the agent’s compliance with its purpose and policies.

In this model, it is the responsibility of each agent owner to work with certification groups and proactively seek, gather, and provide evidence of compliance, and hence become certified.

**Agentic Mesh Principle 5: Operability**

**Agentic Mesh provides a stable, manageable, and resilient platform for agents.**

Beyond observability, Agentic Mesh lets users, owners, and other agents view detailed operational data that allows them to **act** upon observed information. It provides the tools to:

* View logs (for any agent) to understand agent interactions to understand communication patterns and debug agent information flows.
* View metrics (for any agent) that describe agent usage and operational statistics.
* Receive alerts resulting from agent actions to be notified of agent issues.
* Diagnose agent issues to support problem identification and diagnosis.
* Establish agent security (for example, by defining role-based access controls).

**Agentic Mesh Principle 6: Economically Vitality**

**Agentic Mesh lets agent creators and consumers benefit from the agent ecosystem.**

Being economically vital means that Agentic Mesh provides the economic incentives that encourage ecosystem growth: agent creators are compensated for agents they create and get used, and agent consumers pay (although some could conceivably be free) for agents that deliver value.

While the marketplace is the primary interaction point for agent consumers, Agentic Mesh has the tools that let **agent creators** monetize and monitor their agents:

* A workbench that lets agent creators submit new agents into the marketplace (and registry).
* An agent management tools that let agent creators set prices and security requirements for their agents.
* Dashboards that show agent usage and revenue for an agent creator’s agents.
* Diagnostic tools that let agent creators monitor agent activity.

**Conclusion**

In my previous [article](https://archive.is/o/lY6iT/https:/towardsdatascience.com/agentic-mesh-the-future-of-generative-ai-enabled-autonomous-agent-ecosystems-d6a11381c979) I explained that agents are coming, and that Agentic Mesh offers a path forward to managing the growing agent ecosystem. In this article, I have tried to explore the core principles that allow the Agentic Mesh ecosystem and its agents to operate safely.

I am hoping there are a few things that you learned as you read this article. Agentic Mesh and its agents do not operate in the “wild west” — it is not an anything goes operating model. Rather, to create and nurture a growing Agentic Mesh ecosystem, I offer a set of principles that govern both individual agent behaviour but also principles that govern all interactions in Agentic Mesh. And, finally, like the “stop-light” analogy that I used earlier, it is these principles that will let Agentic Mesh agents not only find each other but also **safely** collaborate, interact, transact, and go fast!

**Agentic Mesh — Principios para un Ecosistema de Agentes Autónomos**

**Principios fundamentales que permiten que los agentes autónomos se encuentren, colaboren, interactúen y transaccionen en un ecosistema en crecimiento llamado Agentic Mesh.**

**Introducción**

Estamos en las primeras etapas de la evolución de los agentes autónomos. Sin embargo, con las enormes inversiones que se están haciendo en esta tecnología, pronto podríamos tener agentes realmente autónomos que actúan de forma independiente, planifican dinámicamente y ejecutan tareas para resolver problemas comerciales complejos.

En este contexto, surgen varias preguntas:

* ¿Cómo interactuarán las personas con estos agentes en un ecosistema en crecimiento?
* ¿Cómo se encontrará el agente adecuado en un entorno abarrotado?
* ¿Cómo pueden estos agentes colaborar, interactuar y transaccionar de forma segura?

En un artículo anterior, se definió el **Agentic Mesh** como un ecosistema interconectado que facilita la búsqueda, colaboración e interacción entre agentes. Este artículo explora los principios fundamentales que gobiernan tanto el ecosistema del Agentic Mesh como los agentes individuales que operan en él.

**Sobre los principios**

Un principio es una guía de comportamiento o evaluación que establece las reglas y directrices para definir qué es aceptable y qué no lo es. Sin embargo, los buenos principios no solo aseguran la seguridad, sino que también permiten avanzar rápido, como un sistema de semáforos sincronizados que minimizan accidentes y optimizan el flujo del tráfico.

Los principios del **Agentic Mesh** son como estos semáforos: establecen las reglas que mantienen seguros a los agentes y usuarios, pero también permiten que el ecosistema funcione de manera ágil.

Hay dos tipos de principios abordados en este artículo:

1. **Principios para los agentes individuales.**
2. **Principios para el ecosistema del Agentic Mesh.**

**Principios para los agentes individuales**

Los principios aplicables a los agentes que operan en el Agentic Mesh son:

1. **Propósito definido:** Los agentes operan con un propósito claro.
2. **Responsabilidad:** Los agentes están gobernados por propietarios responsables.
3. **Confiabilidad:** Los agentes son confiables si son seguros y cumplen con su propósito.
4. **Independencia:** Los agentes toman decisiones y actúan de manera independiente.
5. **Inteligencia:** Los agentes pueden planificar y ejecutar tareas.
6. **Colaboración:** Los agentes colaboran e interactúan con otros agentes.

**1. Los agentes tienen un propósito definido**

El propósito de un agente establece:

* **Objetivos:** Define lo que el agente busca lograr.
* **Políticas:** Reglas que guían y limitan las acciones del agente.
* **Comportamiento:** Cómo el agente ejecuta sus tareas y qué herramientas utiliza.
* **Indicadores clave de rendimiento (KPIs):** Métricas para medir su desempeño.
* **Límites éticos:** Qué datos recoge, cómo interactúa y su postura sobre privacidad y transparencia.

**2. Los agentes son responsables**

Cada agente tiene un propietario claramente identificado que es responsable de:

* Definir el propósito del agente.
* Implementar sus capacidades.
* Supervisar su uso y métricas.
* Resolver problemas y excepciones.
* Certificar que el agente cumple con su propósito.

**3. Los agentes son confiables**

La confianza es esencial para que un agente sea utilizado. Un agente confiable debe:

* Definir políticas de confianza y métricas claras.
* Publicar métricas que certifiquen su seguridad y cumplimiento.
* Capturar y compartir retroalimentación sobre su comportamiento.

**4. Los agentes son independientes**

Aunque los agentes pueden tomar decisiones de manera autónoma, su independencia está limitada por las reglas y restricciones definidas en su propósito. Si encuentran conflictos con su propósito, deben detenerse y buscar orientación de una fuente autorizada.

**5. Los agentes son inteligentes**

Los agentes deben ser capaces de:

* Recibir solicitudes de personas u otros agentes.
* Planificar cómo ejecutar tareas.
* Colaborar con otros agentes según sea necesario.
* Usar herramientas, como bases de datos, APIs y aplicaciones.

**6. Los agentes son colaborativos**

Los agentes deben poder:

* Publicar su propósito y capacidades para que otros agentes o usuarios los encuentren.
* Acceder a un registro de agentes que facilite su colaboración.

**Principios para el ecosistema del Agentic Mesh**

Estos principios son aplicables a todo el ecosistema del Agentic Mesh, asegurando que los agentes puedan operar, interactuar y transaccionar de manera segura y eficiente.

1. **Descubribilidad:** Facilitar que los agentes encuentren a otros agentes.
2. **Observabilidad:** Facilitar el monitoreo de los agentes.
3. **Interoperabilidad:** Permitir que los agentes hablen un idioma común.
4. **Certificación:** Hacer que los agentes sean fácilmente certificables para garantizar su confiabilidad.
5. **Operabilidad:** Proporcionar una plataforma estable y resiliente para los agentes.
6. **Vitalidad económica:** Incentivar la creación y uso de agentes en el ecosistema.

**1. Descubribilidad**

El Agentic Mesh incluye un mercado, similar a una App Store, donde las personas y organizaciones pueden buscar agentes basados en su propósito, capacidades, calificaciones y estado de certificación. Un registro centralizado almacena esta información, accesible tanto para humanos como para agentes.

**2. Observabilidad**

Todos los agentes emiten información automáticamente. El ecosistema captura métricas como estadísticas de uso, excepciones y conversaciones entre agentes. Estas métricas se almacenan en un repositorio seguro para su análisis.

**3. Interoperabilidad**

El Agentic Mesh utiliza protocolos estándar y APIs (como OpenAPI) para que los agentes interactúen de manera consistente. Además, permite que las personas interactúen con agentes utilizando lenguaje natural, incluyendo soporte multilingüe.

**4. Certificación**

La certificación asegura que los agentes cumplen con su propósito y son confiables. Este proceso es administrado por un modelo de gobernanza federada, donde un grupo central define las políticas y un tercero verifica la conformidad de los agentes.

**5. Operabilidad**

El ecosistema proporciona herramientas para:

* Ver logs y métricas operativas.
* Recibir alertas de problemas.
* Diagnosticar problemas y asegurar la seguridad de los agentes.

**6. Vitalidad económica**

El Agentic Mesh fomenta la creación y el uso de agentes ofreciendo incentivos económicos:

* Los creadores de agentes son compensados por su uso.
* Los consumidores pagan por los agentes que les generan valor.
* Herramientas como tableros de monitoreo y herramientas de precios ayudan a los creadores a gestionar sus agentes y maximizar ingresos.

**Conclusión**

El **Agentic Mesh** proporciona un modelo estructurado y gobernado para manejar el crecimiento del ecosistema de agentes autónomos. No opera como un "salvaje oeste" sin reglas, sino que utiliza principios claros para regular tanto el comportamiento de los agentes como sus interacciones dentro del ecosistema.

Estos principios aseguran que los agentes puedan colaborar, interactuar y transaccionar de manera segura, fomentando la confianza y la eficiencia. Al igual que el ejemplo de los semáforos sincronizados, estas reglas no solo protegen a los usuarios, sino que también aceleran la adopción y expansión del ecosistema.