



Agentic Starter Kit

Dieses Basisdokument dient als Ausgangspunkt für die Entwicklung agentischer Systeme auf Basis von MCP und A2A. Es stellt eine minimal vollständige Struktur bereit, mit der Teams erste Agenten definieren, Kontext anbinden und Interaktionen orchestrieren können. Ziel ist es, einen schnellen Einstieg in Prototyping und erste produktive Szenarien zu ermöglichen – ohne dabei auf klare Architekturprinzipien zu verzichten. Das Dokument folgt einem einfachen Prinzip:

Definiere Agenten → strukturiere Kontext → standardisiere Interaktion → sichere Verhalten durch Policies.

Agent-Definition (Beispiel)

agent:

name: "AnomalyDetectionAgent"

role: "Analyse von Sensordaten zur Erkennung von Abweichungen"

capabilities:

- "Load sensor data via MCP"
- "Detect anomalies based on thresholds and patterns"
- "Trigger maintenance workflow"

allowed_tools:

- "SensorDataAPI"
- "AnomalyModel"

policies:

- "No direct system changes"
- "Escalate if confidence < 80%"

Dieser Agent ist klar abgegrenzt: Er analysiert Daten, trifft jedoch keine direkten operativen Entscheidungen.

2. MCP Resource Schema (Beispiel)

```
{
  "resource_id": "machine_123",
  "type": "sensor_data",
  "attributes": {
    "temperature": 85,
    "vibration": 0.7,
    "timestamp": "2026-03-27T10:00:00Z"
  },
  "metadata": {
    "source": "edge_device",
    "access_level": "restricted"
  }
}
```

Das Schema zeigt, wie Kontext strukturiert und mit Metadaten versehen wird. Wichtig ist die klare Trennung von Daten und Zugriffsinformationen.

A2A Message Template (Beispiel)

```
{
  "message_type": "intent",
  "sender": "AnomalyDetectionAgent",
  "receiver": "MaintenanceAgent",
```

```
"payload": {  
  "task": "schedule_maintenance",  
  "context_ref": "machine_123",  
  "priority": "high"  
}  
}
```

Die Nachricht enthält keine vollständigen Daten, sondern verweist auf den Kontext im MCP.

Prompt & Guardrail (Beispiel)

Prompt:

```
Analysiere die Sensordaten und identifiziere mögliche Anomalien.  
Berücksichtige historische Werte und bekannte Muster.  
Gib eine Wahrscheinlichkeit für eine Störung an.
```

Guardrails:

- Keine Spekulation ohne Kontextbasis
- Keine Aktion ohne definierte Schwelle
- Eskalation bei Unsicherheit

Typischer Ablauf (End-to-End)

1. Agent lädt Sensordaten über MCP
2. Agent analysiert Kontext (Execution)
3. Bei Anomalie: A2A-Call an Maintenance-Agent

4. Wartungsprozess wird initiiert
5. Ergebnis wird im MCP-Kontext aktualisiert

Die Kernaussage: Dieses Basisdokument zeigt, wie sich agentische Systeme strukturiert aufbauen lassen.

- Agenten sind klar definiert
- Kontext ist strukturiert und referenzierbar
- Kommunikation ist standardisiert
- Verhalten ist kontrolliert

Damit entsteht eine belastbare Grundlage für skalierbare, nachvollziehbare und erweiterbare agentische Systeme.

Mehr zum Thema MCP und A2A

Der vollständige Leitfaden „MCP & A2A als Orchestrierungsinfrastruktur“



[Jetzt bei Amazon bestellen](#)