KI-Agenten entwickeln mit MCP, A2A und ACP

Offene Protokolle für Tool-Integration und Agenten-Interoperabilität: Architektur, Implementierung, Sicherheit und Best Practices

In diesem praxisorientierten Seminar lernst du, wie du moderne KI-Agenten entwickelst, die standardisiert mit Tools, Systemen und anderen Agenten zusammenarbeiten. Im Fokus stehen offene Protokolle wie das Model Context Protocol (MCP) sowie Agenten-Kommunikationsstandards wie A2A und ACP. Du entwickelst ein fundiertes Verständnis für Architektur, Design und Implementierung von Agentensystemen und setzt dieses Wissen direkt in praktischen Übungen um. Dabei entwirfst du Tool-Contracts, implementierst einen eigenen MCP-Server und baust ein Multi-Agent-Szenario, in dem Agenten Aufgaben delegieren, Ergebnisse austauschen und Prozesse koordinieren. Ein besonderer Schwerpunkt liegt auf Sicherheit und Governance. Du lernst, wie du Agentensysteme kontrollierbar, nachvollziehbar und produktionsfähig gestaltest – von Authentifizierung und Autorisierung bis hin zum Schutz vor Prompt Injection und Missbrauch.

Inhalte

1. Grundlagen und Protokollüberblick
- Herausforderungen bei Tool-Integration und Agenten-Interoperabilität.
- Überblick über MCP, A2A und ACP.
- Einsatzszenarien: Tool-Integration, Delegation, Multi-Agent-Systeme.

2. MCP-Design und Tool-Contracts
- Rollenmodell: Host, Client, Server.
- Gestaltung von Schnittstellen und Datenstrukturen.
- Definition von Inputs, Outputs und Fehlerfällen.
- Aufbau robuster und validierbarer Contracts.

3. MCP-Server implementieren
- Struktur und Aufbau eines MCP-Servers.
- Tool-Registry und Integration von Funktionen.
- Validierung, Timeouts und Edge Cases.
- Entwicklung erster Tools und Services.

4. Integration in Anwendungen und Workflows
- Tool-Discovery und Aufruf von Funktionen.
- Verarbeitung strukturierter Ergebnisse.
- Robustheit durch Retries, Rate Limits und Logging.
- Aufbau stabiler Integrationsflows.

5. Sicherheit und Governance
- Trust Boundaries und Datenklassifizierung.
- Authentifizierung und Autorisierung (Least Privilege).
- Schutz vor Prompt Injection und Missbrauch.
- Auditierbarkeit und Nachvollziehbarkeit.

6. Agentenkommunikation mit A2A
- Rollen und Aufgabenverteilung zwischen Agenten.
- Kommunikationsmuster: Anfrage, Status, Ergebnis.
- Steuerung von Aufgaben und Delegation.
- Umgang mit langlaufenden Prozessen.

7. ACP und API-Design für Agenten
- Gestaltung von Capability APIs.
- Job-Lifecycle und Zustandsmodelle.
- Fehlerstrategien und Idempotenz.
- Mapping auf Agentenkommunikation.

8. Referenzarchitektur für Agentensysteme

- Zusammenspiel von MCP, A2A und ACP.
- Architektur von Agent-Mesh-Systemen.
- Versionierung, Kompatibilität und Tests.
- Governance, Policies und Logging.

9. Multi-Agent-Systeme entwickeln (Capstone)
- Entwicklung eines End-to-End-Agentensystems.
- Kombination von Tools, Agenten und Workflows.
- Qualitätssicherung, Review und Dokumentation.

10. Produktionsreife und Betrieb
- Anforderungen an produktionsfähige Systeme.
- Monitoring, Incident-Handling und Betrieb.
- Governance-Prozesse und Rollout-Strategien.

Dein Nutzen

- Du lernst, wie du KI-Agenten strukturiert entwickelst und in bestehende Systeme integrierst.
- Du verstehst offene Protokolle wie MCP, A2A und ACP und setzt sie praxisnah ein.
- Du entwickelst eigene Tool-Integrationen und baust Multi-Agent-Systeme.
- Du kannst robuste, sichere und nachvollziehbare Agentenarchitekturen entwerfen.
- Du berücksichtigst Sicherheits- und Governance-Anforderungen von Anfang an.
- Du erhältst praxisnahe Best Practices für produktionsreife KI-Agentensysteme.

Methoden

Das Seminar kombiniert kompakte Theorie-Impulse mit intensivem Praxisanteil:
- Live-Demos und strukturierte Architektur-Einführungen
- Geführte Hands-on-Übungen und Code-along-Sessions
- Entwicklung eigener Komponenten wie MCP-Server und APIs
- Abschlussprojekt zur Umsetzung eines Multi-Agent-Systems

Für das Seminar wird eine MCP-fähige Übungsumgebung zur Verfügung gestellt.

Teilnehmer:innenkreis

Dieses Seminar richtet sich an alle, die KI-Agenten technisch umsetzen und in Unternehmen einsetzen möchten:
- Software- und Plattform-Teams, die Anwendungen für KI-Agenten öffnen
- AI-, Data- und ML-Teams, die Agenten mit Daten und Tools integrieren wollen
- Solution Architects und Tech Leads, die Agentenarchitekturen planen und bewerten
- Entwickler:innen mit Grundlagen in APIs (z. B. Python, JavaScript oder TypeScript)

haufe akademie

Buchungsnummer
42723

Open Badges - Zeige auch digital, was du kannst.

Open Badges sind anerkannte, digitale Teilnahmezertifikate. Diese verifizierbaren Nachweise sind der aktuelle Standard für die Einbindung in Karrierenetzwerken wie z.B. LinkedIn.

Damit zeigst du digital, über welche Kompetenzen du verfügst.

Nach erfolgreichem Abschluss erhältst du von uns ein Open Badge.

Mehr erfahren kannst du unter:
https://www.haufe-akademie.de/seminare-lehrgaenge/trending-topics/open-badges

Trainer:in

Derzeit keine Vita verfügbar

Details zur Weiterbildung

Seminar | Online

2 Tage
Zahl der Teilnehmenden begrenzt

Starttermine

15.-16.09.2026
Live-Online
Durchführung
zoom

Modulzeiten
Dienstag, 15.09.2026
09:00 Uhr - 17:00 Uhr
Mittwoch, 16.09.2026
09:00 Uhr - 17:00 Uhr

30.11.-01.12.2026
Live-Online
Durchführung
zoom

Modulzeiten
Montag, 30.11.2026
09:00 Uhr - 17:00 Uhr
Dienstag, 01.12.2026
09:00 Uhr - 17:00 Uhr

08.-09.03.2027
Live-Online
Durchführung
zoom

Modulzeiten
Montag, 08.03.2027
09:00 Uhr - 17:00 Uhr
Dienstag, 09.03.2027
09:00 Uhr - 17:00 Uhr

17.-18.06.2027
Live-Online
Durchführung
zoom

Modulzeiten
Donnerstag, 17.06.2027
09:00 Uhr - 17:00 Uhr
Freitag, 18.06.2027
09:00 Uhr - 17:00 Uhr

23.-24.09.2027
Live-Online
Durchführung
zoom

Modulzeiten
Donnerstag, 23.09.2027
09:00 Uhr - 17:00 Uhr
Freitag, 24.09.2027
09:00 Uhr - 17:00 Uhr

Aktuelle Termine und weitere Informationen findest du unter www.haufe-akademie.de/42723

Teilnahmegebühr

€ 1.390,- zzgl. MwSt.
€ 1.654,10 inkl. MwSt.

Deine Anmeldemöglichkeiten

Online: www.haufe-akademie.de/42723
E-Mail: anmelden@haufe-akademie.de

Buche deine Weiterbildung einfach und schnell online. Gib sonst bitte unbedingt den Namen des Teilnehmenden und die vollständige Rechnungsanschrift mit Telefonnummer sowie E-Mail-Adresse an.

In unserem Bereich Fragen & Antworten (FAQ) findest du alle Antworten auf die häufigsten Fragen rund um unsere Weiterbildungen:
https://www.haufe-akademie.de/faqs

Unsere ausführlichen Teilnahmebedingungen findest du auch im Internet unter www.haufe-akademie.de/agb oder im Gesamtprogramm.
Die vollständigen Datenschutzbestimmungen findest du unter www.haufe-akademie.de/datenschutz.