KI-Agenten entwickeln mit MCP, A2A und ACP

ID: 0069

In diesem Seminar lernen die Teilnehmenden offene Protokolle für die Tool-Integration und die Interoperabilität von KI-Agenten kennen. Behandelt werden Architektur und Implementierung ebenso wie Sicherheitsaspekte und bewährte Best Practices für den produktiven Einsatz.

online
2 Tage
Einsteiger
1490€ p.P. zzgl. MwSt.

Beschreibung

In diesem praxisorientierten Seminar lernen die Teilnehmenden, wie moderne KI-Agenten standardisiert mit Software, Tools und anderen Agenten zusammenarbeiten. Im Fokus stehen das Model Context Protocol (MCP) für die Anbindung von Tools und Kontext sowie A2A und ACP für Koordination, Kommunikation und interoperable Agenten-Architekturen.

Der Kurs ist hands-on aufgebaut: Die Teilnehmenden entwerfen robuste Tool-Contracts, implementieren einen MCP-Server und entwickeln ein Multi-Agent-Szenario mit Delegation, Statusaustausch und nachvollziehbarer Ergebnisübergabe. Ein Schwerpunkt liegt auf Sicherheit und Governance (AuthN/AuthZ, Trust Boundaries, Prompt-Injection-Schutz, Auditing), damit Lösungen produktionsnah und kontrollierbar umgesetzt werden können.

Inhalte

- Protokoll-Landkarte: MCP, A2A, ACP
- Einsatzmuster für Agenten-Systeme
- MCP-Rollenmodell (Host, Client, Server)
- Tool-/Resource-Contracts und Schemas
- Validierung und Fehlertypen
- MCP-Server: Struktur und Tool-Registry
- Tool-Calls und strukturierte Ergebnisse
- Robustheit: Retries, Rate Limits, Caching
- Observability: Logging, Nachvollziehbarkeit
- A2A-Kommunikation und Delegation
- ACP-Capabilities und Job-Lifecycle
- Referenzarchitektur MCP + A2A/ACP
- Versionierung und Kompatibilität
- Security und Governance
- Capstone: Multi-Agent-System

Lernziele

Die Teilnehmenden lernen, MCP, A2A und ACP fachlich sicher einzuordnen und je nach Anwendungsfall das passende Protokoll auszuwählen. Sie können Tool-Contracts strukturiert und nachvollziehbar spezifizieren sowie einen MCP-Server mit ersten Tools praktisch umsetzen. Darüber hinaus sind sie in der Lage, Agenten- und Message-Flows zu entwerfen und typische A2A-/ACP-Patterns in der Praxis anzuwenden. Ein weiterer Schwerpunkt liegt darauf, Sicherheitsrisiken frühzeitig zu erkennen und geeignete Schutzmaßnahmen umzusetzen. Zusätzlich lernen die Teilnehmenden, eine Referenzarchitektur für Pilotprojekte zu erstellen und einen PoC- bzw. Pilot-Rollout strukturiert zu planen.

Zielgruppe

Der Kurs richtet sich an Software- und Plattform-Teams, die Anwendungen für KI-Agenten öffnen oder KI-Funktionen integrieren möchten, sowie an AI/ML- und Data-Teams, die Agenten sicher an Unternehmensdaten und Tools anbinden wollen. Ebenfalls angesprochen sind Solution Architects und Tech Leads, die Agenten-Architekturen vendor-neutral planen und Standards bewerten. Grundlagen in HTTP/APIs sind hilfreich (Python, JavaScript oder TypeScript von Vorteil).

Kontakt

+49 5254 9496500 | info@qualidy.de | qualidy.de