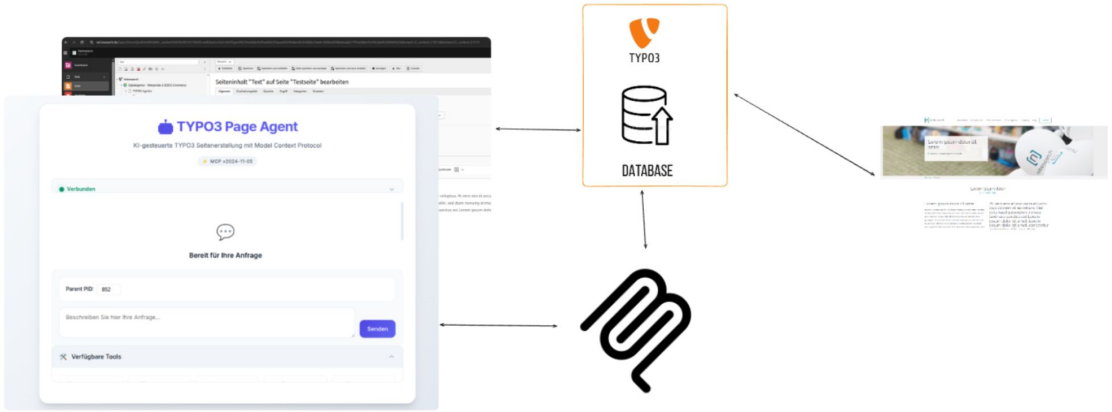
Per Prompt eine neue Seite anlegen

TYPO3 + Model Context Protocol (MCP)

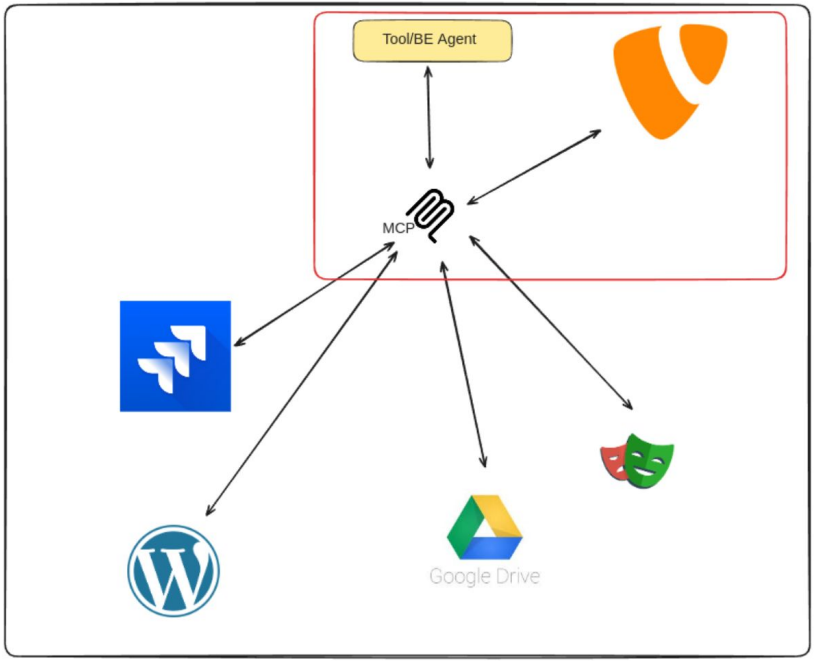
Per Prompt eine neue Seite anlegen

- Ziel: TYPO3 BE durch Chat ersetzen
- Funktionen
  - Seiten erstellen
  - Content erstellen
  - Content analysiere
  - …



Was kommt

- Weg vom PoC
- Informationen per RAG holen
- News anbinden
- Bilder verbessern
- Langfristig: Weitere Tools anschließen
  - Andere Kanäle
  - PlayWright für Tests
  - Google Drive für existierenden Content
  - Atlassian/Jira zur Dokumentation



Livedemo

- Idee: wir bauen eine Landingpage
  - Nur geprüfte Inhalte unsere Website
  - Thema: Landingpage zu TYPO3 Projekten

- Eher durch “Zufall” fiel ein Chatbot mit ab.

Mehrwert

- Entlastung von Routineaufgaben im Backend
- Potenzial: Automatisierung komplexer Workflows beim Anlegen großer Seiten
- Hauptaufgaben im Chatbot und ein paar Nacharbeiten im Backend

Technische Umsetzung

- Architektur: LLM + MCP → TYPO3
- MCP sorgt für standardisierte Schnittstelle (Plug & Play)
- Kommt noch: Flexible Anbindung verschiedener LLMs
- Kommt später: Zugriff nur im eingeloggten Kontext, rollenbasiert

Warum MCP?

Problem:

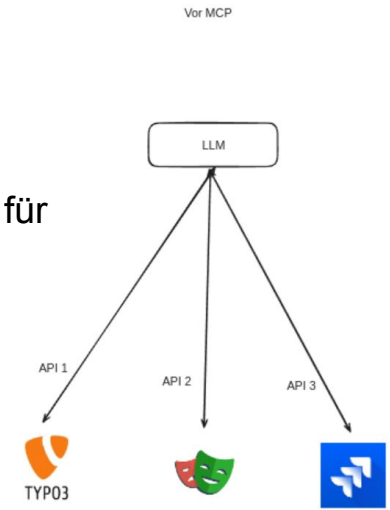
- Proprietäre Integrationen
- inkonsistente Tool-Calls
- fehlende Governance

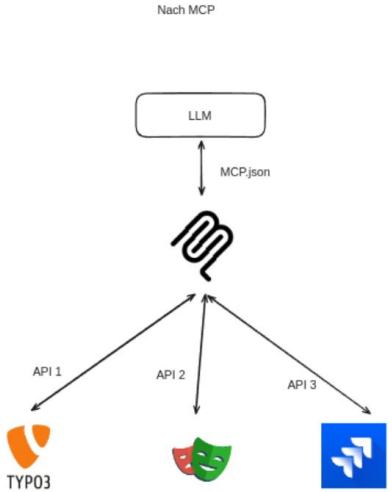
Ziel:

- Offenes, standardisiertes Protokoll für LLM ↔ Tools ↔ Daten

Nutzen:

- Portabilität, Wiederverwendung
- geringere Integrationskosten.





Was ist offiziell im MCP definiert?

- Offenes Protokoll für die Integration von LLMs mit Tools und Datenquellen
- Klare Client–Server-Architektur mit standardisierten JSON-RPC-Nachrichten
- Unterstützte Transporte: stdio, HTTP, Server-Sent Events (SSE)
- Tools/Funktionen müssen eindeutig registriert und beschrieben sein

Was ist offiziell im MCP definiert?

netresearch

```
{
  "jsonrpc": "2.0",
  "id": "req-7842",
  "method": "crm.getCustomerById",
  "params": {
    "customerId": "CUST-10293",
    "fields": ["name", "tier", "openTickets"]
  },
  "meta": {
    "traceId": "c4e5-918a",
    "ttl": 2000,
    "authContext": "role:assistant"
  }
}
```

Was ist offiziell im MCP definiert?

netresearch

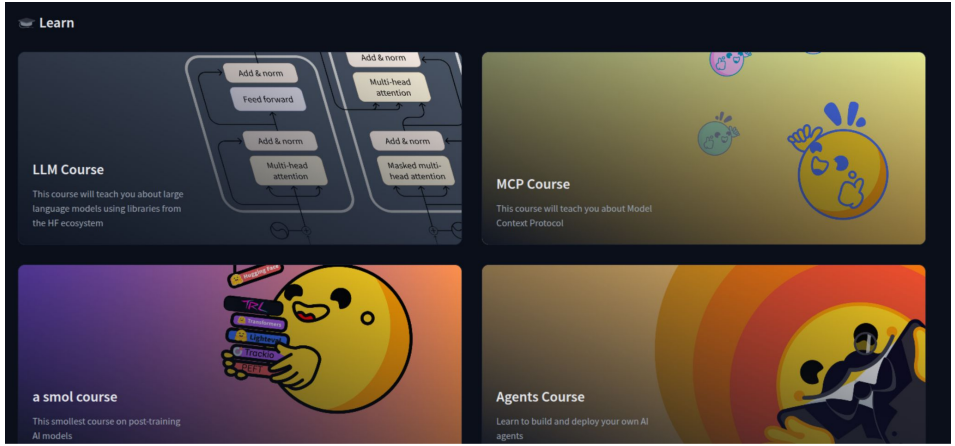
```
{
  "jsonrpc": "2.0",
  "id": "req-7842",
  "result": {
    "name": "Acme GmbH",
    "tier": "Gold",
    "openTickets": 2
  },
  "observability": {
    "latencyMs": 143,
    "quotaUsed": {"crm": 1}
  }
}
```

Was ist RAG?

- **Prinzip:** Kombination von Informationsabruf (Retrieval) und Textgenerierung (Generation), um Large Language Models mit externem Wissen zu erweitern.
- **Ablauf-Pipeline:**
  - Nutzer-Query wird in einen Embedding-Vektor umgewandelt.
  - Retriever sucht top-k relevante Dokument-Passagen.
  - Diese Passagen werden in den Prompt („context window“) des LLM injiziert.

Wo startet man mit dem MCP?

- https://huggingface.co/learn
- Jede Menge Tutorials/Zertifikate



Q&A / Diskussion

netresearch

Danke für eure Aufmerksamkeit
Fragen?