Funktionsbeschreibung
MCP-Schnittstelle

1 Überblick

Die MCP-Schnittstelle stellt Funktionen und Inhalte von d.velop Produkten über das offene Model Context Protocol (MCP) für KI-Agenten bereit.

Neben dem Applikationsfrontend für Endanwender und der öffentlichen REST-API für Systemintegrationen stellt die MCP-Schnittstelle damit einen dritten, speziell für KI-Agenten (MCP-Clients) optimierten Zugriffskanal auf d.velop documents dar.

2 Begriffsbestimmung

a. Model Context Protocol (nachfolgend „MCP") MCP ist ein offener Standard, über den KI-Agenten strukturiert auf externe Datenquellen und Funktionen zugreifen können.

b. MCP-Server Die MCP-Schnittstelle stellt die Funktionen und Inhalte von d.velop Produkten für MCP-Clients zur Verfügung.

c. MCP-Client Der MCP-Client verbindet einen KI-Agenten, z. B. in einer Entwicklungsumgebung, einem Chat- oder Assistenzsystem, mit einem oder mehreren MCP-Servern.

d. Tool Ein Tool ist eine vom MCP-Server bereitgestellte Aktion. Der KI-Agent wählt ein Tool anhand von dessen Name und Beschreibung aus und führt es – i. d. R. nach Bestätigung durch den Anwender – aus.

e. Resource Eine Resource ist ein vom MCP-Server bereitgestellter Inhalt, z. B. ein Dokument, der dem Kontext eines KI-Agenten hinzugefügt werden kann.

f. Prompt Ein Prompt ist eine vom MCP-Server bereitgestellte Vorlage, die dem Anwender die Formulierung einer Anfrage für ein bestimmtes Tool erleichtert.

3 Funktionsumfang MCP-Schnittstelle

Die MCP-Schnittstelle stellt Funktionen von d.velop Produkten über die drei Hauptfunktionalitäten Tools, Resources und Prompts bereit.

Tools

Der KI-Agent kann im Auftrag des Anwenders Aufgaben in d.velop Produkten erledigen, zum Beispiel:

- Dokumente und Akten finden, auch wenn der genaue Suchbegriff nicht bekannt ist: Die Suche erkennt auch inhaltlich passende Treffer.
- Fragen zu Dokumenten beantworten: Inhalte lassen sich in natürlicher Sprache abfragen, zusammenfassen oder auswerten.

Welche Funktionen zur Verfügung stehen, legt d.velop fest. Der Funktionsumfang wird kontinuierlich erweitert.

Resources

Über Resources können Dokumente aus d.velop Produkten dem Kontext eines KI-Agenten hinzugefügt werden, damit dieser bei der Bearbeitung einer Anfrage direkt darauf zugreifen kann.

Prompts

Die MCP-Schnittstelle stellt vordefinierte Prompt-Vorlagen bereit, die dem Anwender helfen, eine Anfrage mit den für ein Tool erforderlichen Angaben zu formulieren.

4 Zugriffssteuerung

Der Zugriff über die MCP-Schnittstelle ist an einen authentifizierten Einzelbenutzer gebunden; ein Zugriff über technische Servicebenutzer ist nicht vorgesehen. Der KI-Agent kann dabei ausschließlich auf die Daten und Funktionen zugreifen, für die der jeweilige Benutzer in den d.velop Produkten berechtigt ist.

5 Voraussetzungen

- Ein MCP-Client, der OAuth 2.1 oder eine Bearer-Token-Authentifizierung unterstützt
- Eine d.velop documents Umgebung mit aktivierter MCP-Schnittstelle
- Eine d.velop documents Umgebung mit aktiviertem & konfiguriertem d.velop pilot
- Ein Benutzerkonto mit den für die gewünschten Funktionen erforderlichen Berechtigungen in d.velop documents