



FAIRD

Eine RAG-AI für die HS-KL und darüber hinaus
Ein Exposé

Was ist FAIRD?

FAIRD ist eine lokale Chat-Anwendung, die entwickelt wurde, um Large Language Models (LLMs) für die Beantwortung von Fragen zu nutzen. Die Beantwortung kann dabei auch die Inhalte aus selbst hochgeladenen PDF-Dokumenten einbinden. Sowohl der Chat als auch die Dokumente werden dabei datenschutzkonform behandelt.

FAIRD vereinfacht mehrere wesentliche Aufgaben: es speichert Chatverläufe, erleichtert das Hochladen und Bearbeiten von Dokumenten und verwaltet einen lokalen Vektorspeicher. Mittels des Vektorspeichers können aus dem Fundus an Dokumenten die zu einer Frage passenden Dokumente effizient gefunden werden. Ziel des Projektes ist es, auf eine Frage möglichst zügig eine präzise, kontextbezogene Antwort zu liefern.

Das eingesetzte Open-Source-LLM wird auf leistungsstarker Infrastruktur der Hochschule betrieben.

Datenschutz im Fokus

▪ DSGVO-konform

Alle Daten, einschließlich des Chats und der hochgeladenen Dokumente, werden lokal auf Ihrem Rechner gespeichert, so dass Sie die volle Kontrolle über Ihre Informationen haben. Die einzige Übertragung der für eine Anfrage relevanten Daten findet mit dem Aufruf des LLMs statt. Die Daten werden auf dem Server allerdings nicht gespeichert und auch nicht für das künftige Trainieren des Modells genutzt.

▪ Zugriffsschutz

Die Server-Infrastruktur ist ausschließlich innerhalb des Netzes der Hochschule Kaiserslautern zugänglich, d.h. FAIRD arbeitet NUR innerhalb dieses Netzes. Dies gewährleistet, dass alle Daten innerhalb der vertrauenswürdigen Umgebung verbleiben.

Features

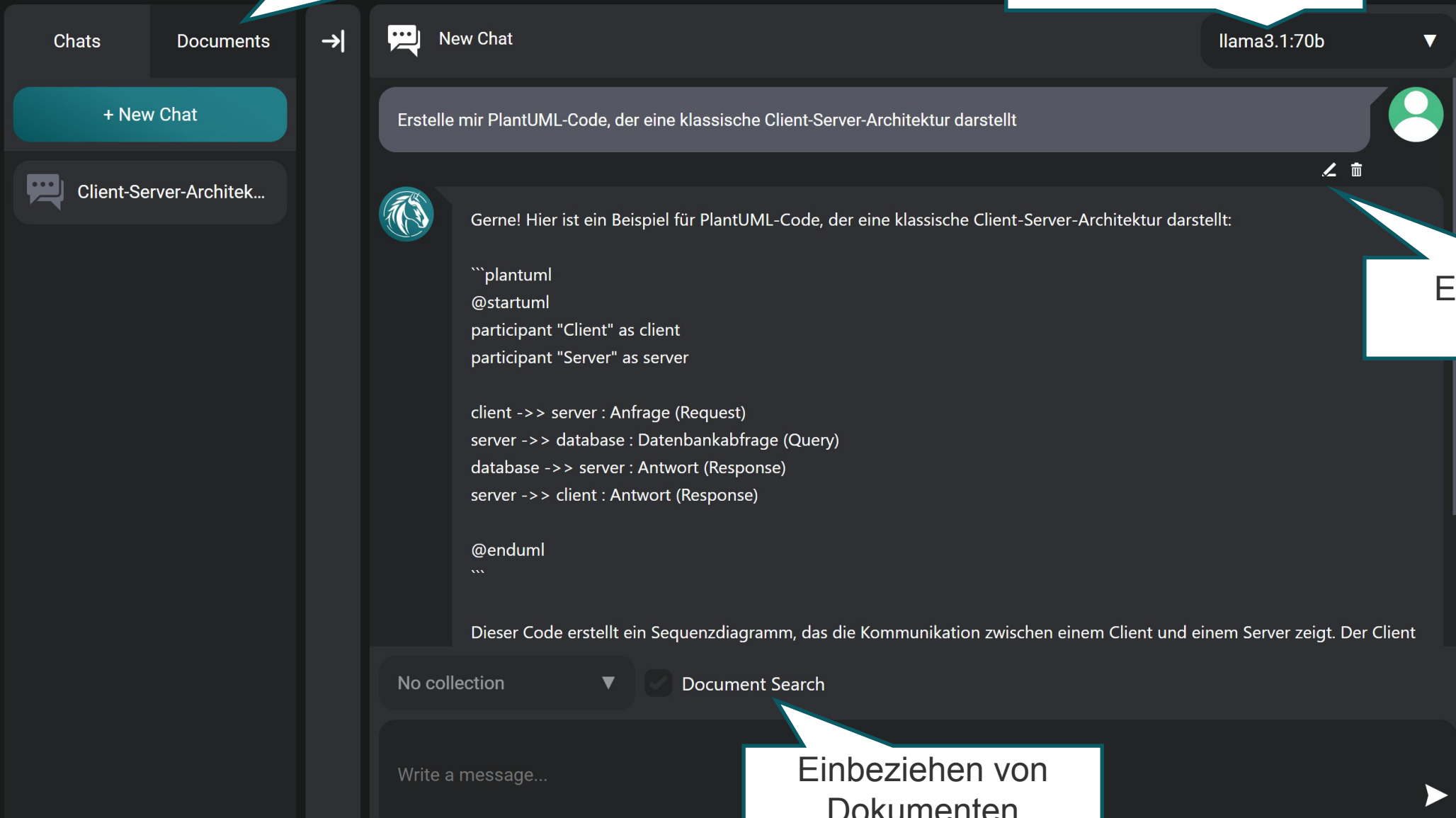
- DSGVO-konform
- Selbst gehostet
- Foundation Modell agnostisch
- Einbindung von PDF-Dokumenten
- Eigenes User-Interface mit der Möglichkeit, Dokumente hochzuladen

Zukünftige Features

- Architektur, die kein Update bedarf
- Advanced RAG (<https://pub.towardsai.net/advanced-rag-techniques-an-illustrated-overview-04d193d8fec6>)
- Headless-Modus zur Integration in Webseiten der Hochschule
- RAG auf Server-Seite mit hochschulspezifischen Inhalten
- Custom FAIRDs – eigene Systemprompts hinterlegen
- Multi-Modalität

Hochladen von Dokumenten

Wählen eines Open-Source-LLMs



The screenshot shows the FAIRD chat interface. On the left, there are tabs for 'Chats' and 'Documents', a '+ New Chat' button, and a chat titled 'Client-Server-Architek...'. The main chat area is titled 'New Chat' and shows a conversation with 'llama3.1:70b'. The user's message is 'Erstelle mir PlantUML-Code, der eine klassische Client-Server-Architektur darstellt'. The AI's response is: 'Gerne! Hier ist ein Beispiel für PlantUML-Code, der eine klassische Client-Server-Architektur darstellt:'. Below this is a code block for PlantUML:

```
``plantuml
@startuml
participant "Client" as client
participant "Server" as server

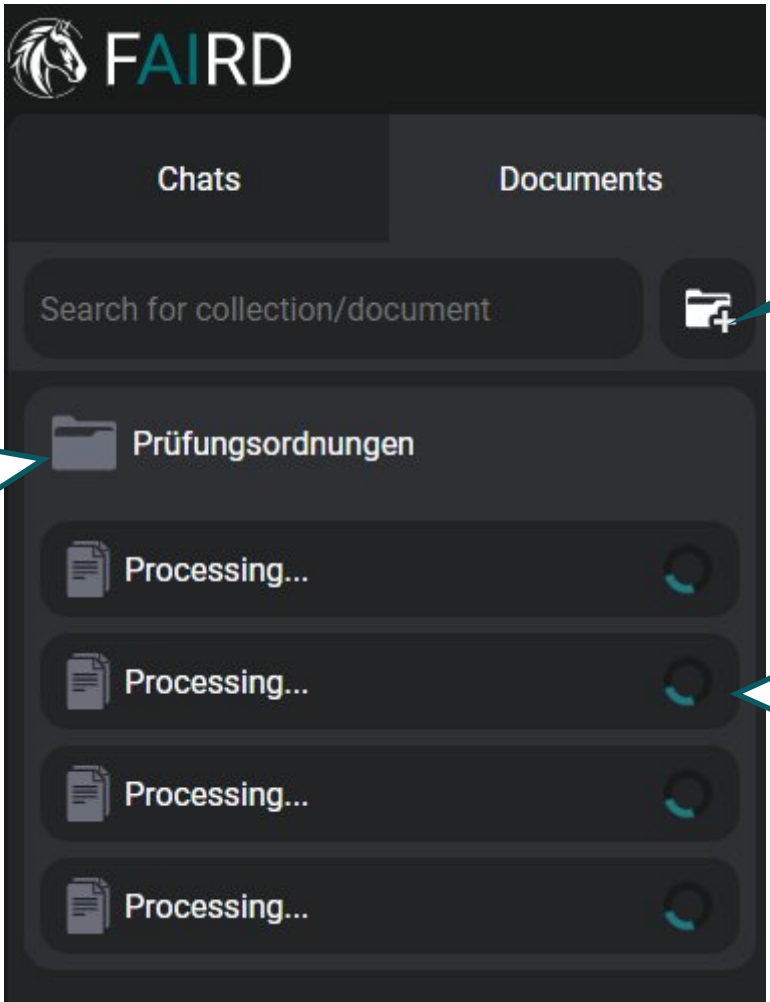
client ->> server : Anfrage (Request)
server ->> database : Datenbankabfrage (Query)
database ->> server : Antwort (Response)
server ->> client : Antwort (Response)

@enduml
``
```

 Below the code, it says 'Dieser Code erstellt ein Sequenzdiagramm, das die Kommunikation zwischen einem Client und einem Server zeigt. Der Client'. At the bottom, there is a 'No collection' dropdown, a checked 'Document Search' checkbox, and a 'Write a message...' input field.

Editieren einer Anfrage

Einbeziehen von Dokumenten



The screenshot shows the FAIRD mobile application interface. At the top, there is a header with the FAIRD logo (a horse head) and the text "FAIRD". Below the header, there are two tabs: "Chats" and "Documents". Under the "Documents" tab, there is a search bar with the placeholder text "Search for collection/document". To the right of the search bar is a folder icon with a plus sign. Below the search bar, there is a list of items. The first item is a folder icon followed by the text "Prüfungsordnungen". Below this, there are four items, each consisting of a document icon followed by the text "Processing..." and a circular progress indicator on the right. Three callout boxes are present: one on the left pointing to the "Prüfungsordnungen" folder with the text "Sammlung"; one on the top right pointing to the folder icon with a plus sign with the text "Anlegen neuer Sammlungen („Collections“)"; and one on the bottom right pointing to the progress indicators with the text "Vorbereiten gerade hochgeladener neuer Dokumente".

Sammlung

Anlegen neuer Sammlungen („Collections“)

Vorbereiten gerade hochgeladener neuer Dokumente

Roadmap

Milestone 1: Einzelnutzung mit lokalen sensiblen Daten (Private Store, lokal)

1. Update-Problematik lösen (sowas wie Electron)
2. Prüfen, ob Ollama Prompts in ein Log schreibt (€ Datenschutz)
3. UI auf Deutsch

Milestone 2: Öffentliche Nutzung im Intranet

1. Headless-Modus-API ohne Historie (€ Ziel: einen REST-Endpoint haben, der getestet werden kann)
2. RAG-Evaluations-Pipeline einrichten (auch für Electron)
3. Golden Dataset erstellen
4. RAG verbessern
5. Nutzungsspezifische Endpoints
6. Systemprompts (fest hinterlegt)
7. Typo3-Plugin

Milestone 3: Nutzung im Team mit einem Shared Space (auf dem Server)

1. UI, um Gruppen zusammenzustellen
2. Authentifizierung mit Shibboleth

Milestone 4: Öffentliche Nutzung im Internet

1. Datenschutz-Disclaimer von DSB ausarbeiten lassen
2. Server nach außen verfügbar machen
3. Server isolieren

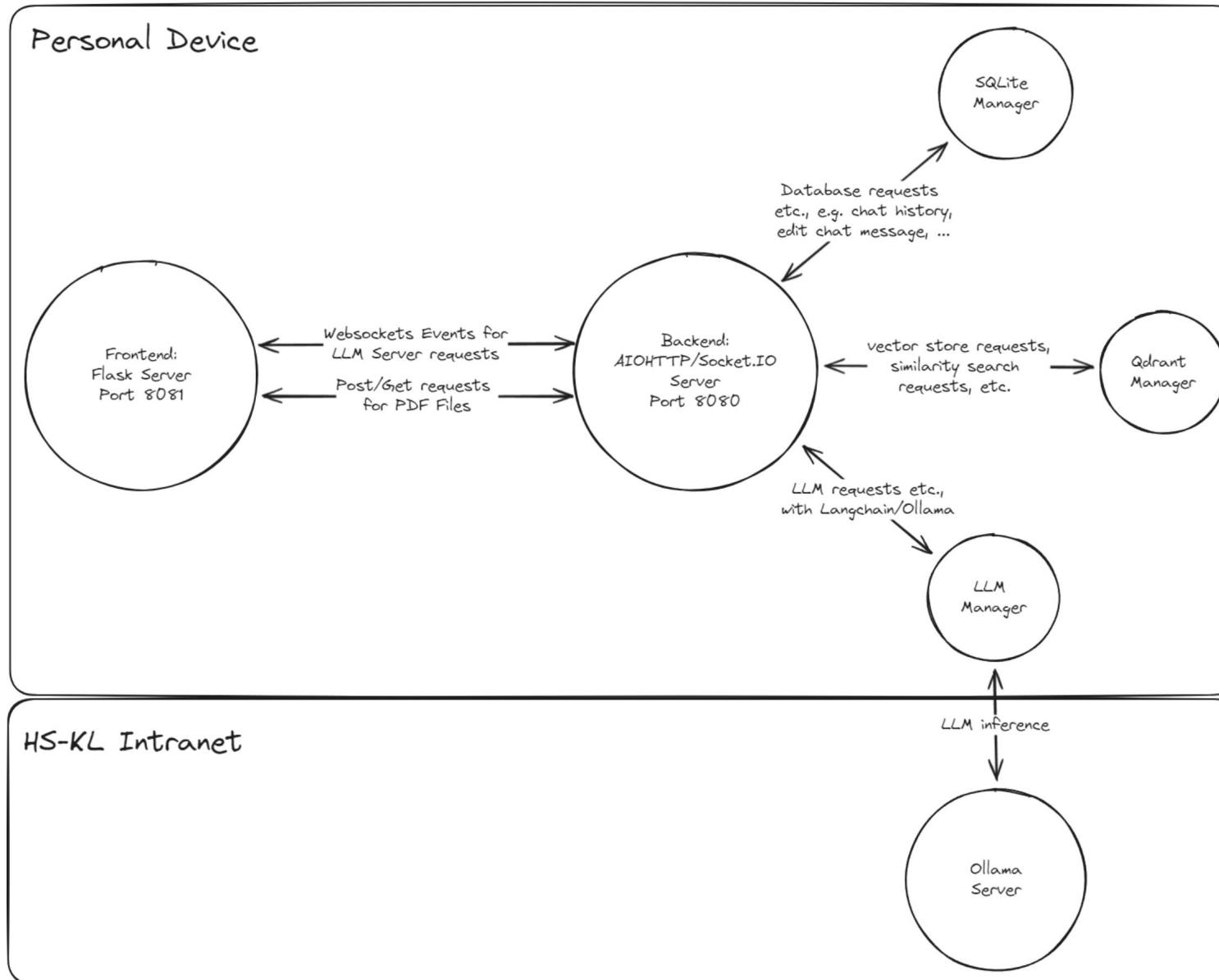
Benutzungsszenarien

- Milestone 1: Einzelnutzung mit lokalen sensiblen Daten (Private Store, lokal)
- Milestone 2: Öffentliche Nutzung mit Systemprompts und öffentlichen Daten (auf dem Server) ohne Chathistorie im Intranet
- Milestone 3: Öffentliche Nutzung im Internet (Typo3-Plugin, Datenschutz, Security, Rate-Limiter)
- Milestone 4: Nutzung im Team mit einem Shared Space (auf dem Server)

Eine Auswahl an Use-Cases

- Dozent*innen
 - Allgemein: GenAI in der Lehre
 - Anfragen zu vergangenen Abschlussarbeiten, ggf. auch mit Sperrvermerk
 - Analyse von Texten
- Studierende
 - Anfragen zu Prüfungsordnungen
 - Feedback zu eigenen Texten
- Potenzielle Bewerber
 - Informationen zu Studiengängen
 - Studiengangsempfehlungen

Architektur



Team

- Contributors
 - Eric Gaida (development lead)
 - Nicholas Grund
 - Nicolas Sand
 - Niklas Borresch
 - Jens Müller
- Projektleitung
 - Prof. Dr. Jan Conrad
 - Prof. Dr. Eugen Staab



FAIRD

Eine RAG-AI für die HS-KL und darüber hinaus
Ein Exposé