Hochschule Kaiserslautern
University of Applied Sciences

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

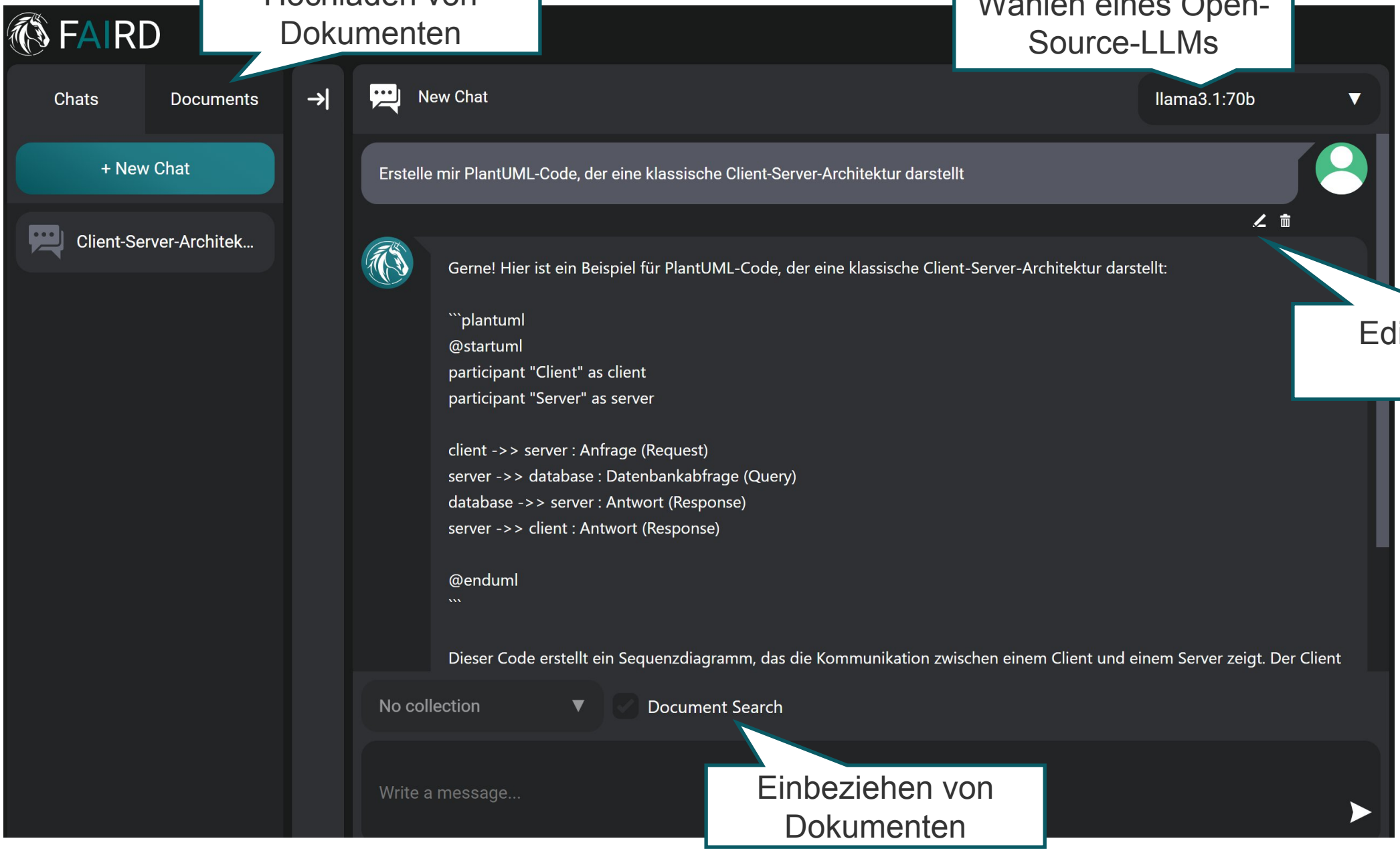
- **DSGVO-konform**
  Alle Daten, einschließlich des Chats und der hochgeladenen Dokumente, werden lokal auf Ihrem Rechner gespeichert, so dass Sie die volle Kontrolle über Ihre Informationen haben. Die einzige Übertragung der für eine Anfrage relevanten Daten findet mit dem Aufruf des LLMs statt. Die Daten werden auf dem Server allerdings nicht gespeichert und auch nicht für das künftiges Trainieren des Modells genutzt.
- **Zugriffsschutz**
  Die Server-Infrastruktur ist ausschließlich innerhalb des Netzes der Hochschule Kaiserlautern zugänglich, d.h. FAIRD arbeitet NUR innerhalb dieses Netzes. Dies gewährleistet, dass alle Daten innerhalb der vertrauenswürdigen Umgebung verbleiben.

Features

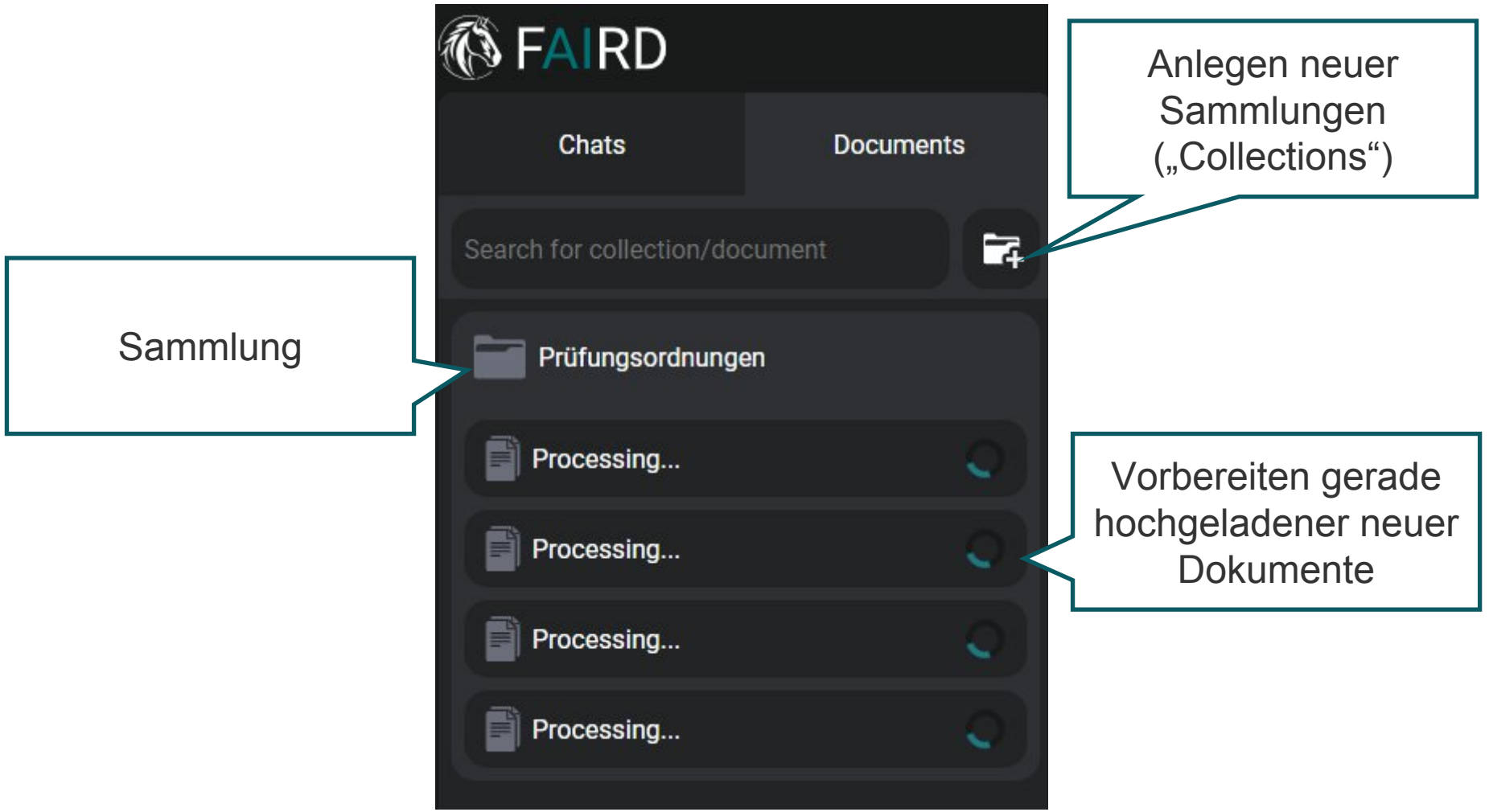
- DSGVO-konform
- Selbst gehostet
- Foundation Modell agnostisch
- Einbindung von PDF-Dokumenten
- Eigenes User-Interface mit der Möglichkeit, Dokumente hochzuladen

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



Hochschule Kaiserslautern
University of Applied Sciences


FAIRD
Chats
Documents
Search for collection/document
Prüfungsordnungen
Processing...
Processing...
Processing...
Processing...
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

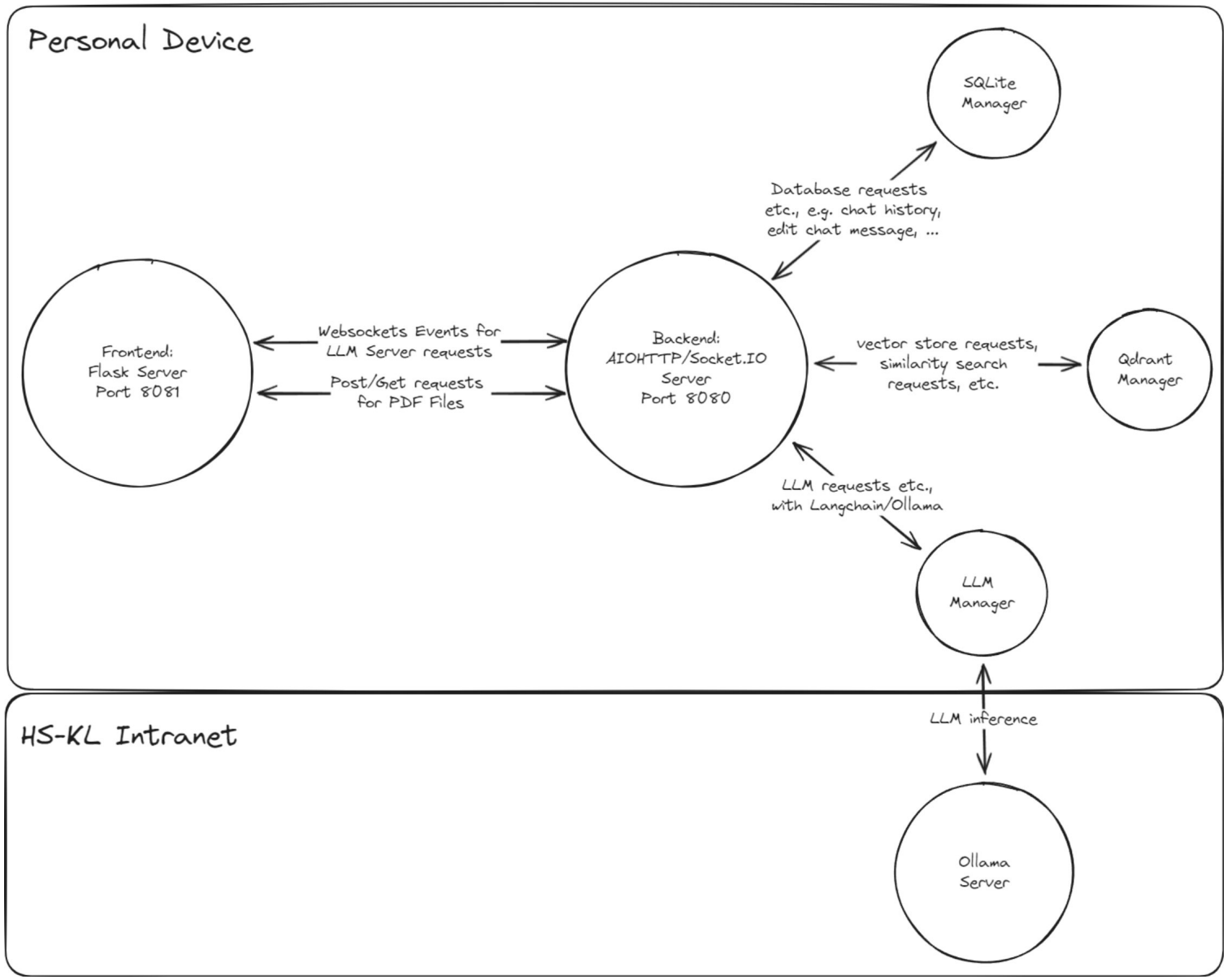
Benutzungsszenarien

- 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

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

Hochschule Kaiserslautern
University of Applied Sciences

FAIRD

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

Ein Exposé