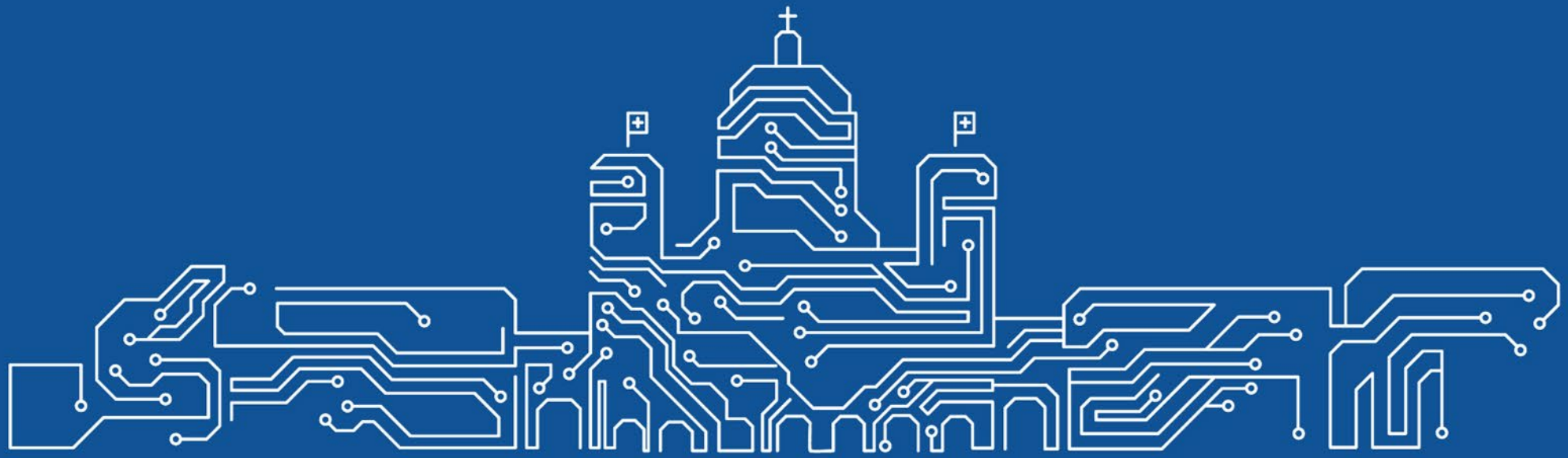
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
**Digitale Transformation und IKT-Lenkung (DTI)**

# Wie streichen wir das O von LOD?

5. November 2024



# Agenda

– Situation rund um Daten der natürlichen Person

– Lösungsansatz
  - ➢ gewählte Architektur
  - ➢ Funktionalität des Proxy

- Video zur Demo

- Herausforderungen und ungeklärte Punkte

- Fragen

# Was tun wir hier: Motivation

Aufgabe in der "Gemeinsamen Stammdatenverwaltung Bund" die Zielbild für Stammdaten der natürlichen Person zu entwickeln. Herausforderung der bisherigen Herangehensweise

- Daten an einer Stelle sammeln und bereitstellen ist verbunden mit Gesetzes-Revisionen bis zu Verfassungsartikel.
- Dezentrale Ansätze zu wenig untersucht
- **Bund kann das Problem für sich alleine nicht lösen**

Weitere Herausforderungen:

- Daten der natürlichen Person werden auf allen Verwaltungsebenen erstellt und genutzt
- Daten werden heute teils mehrfach geführt
- Bezug von Daten benötigt viele Schnittstellenintegrationen

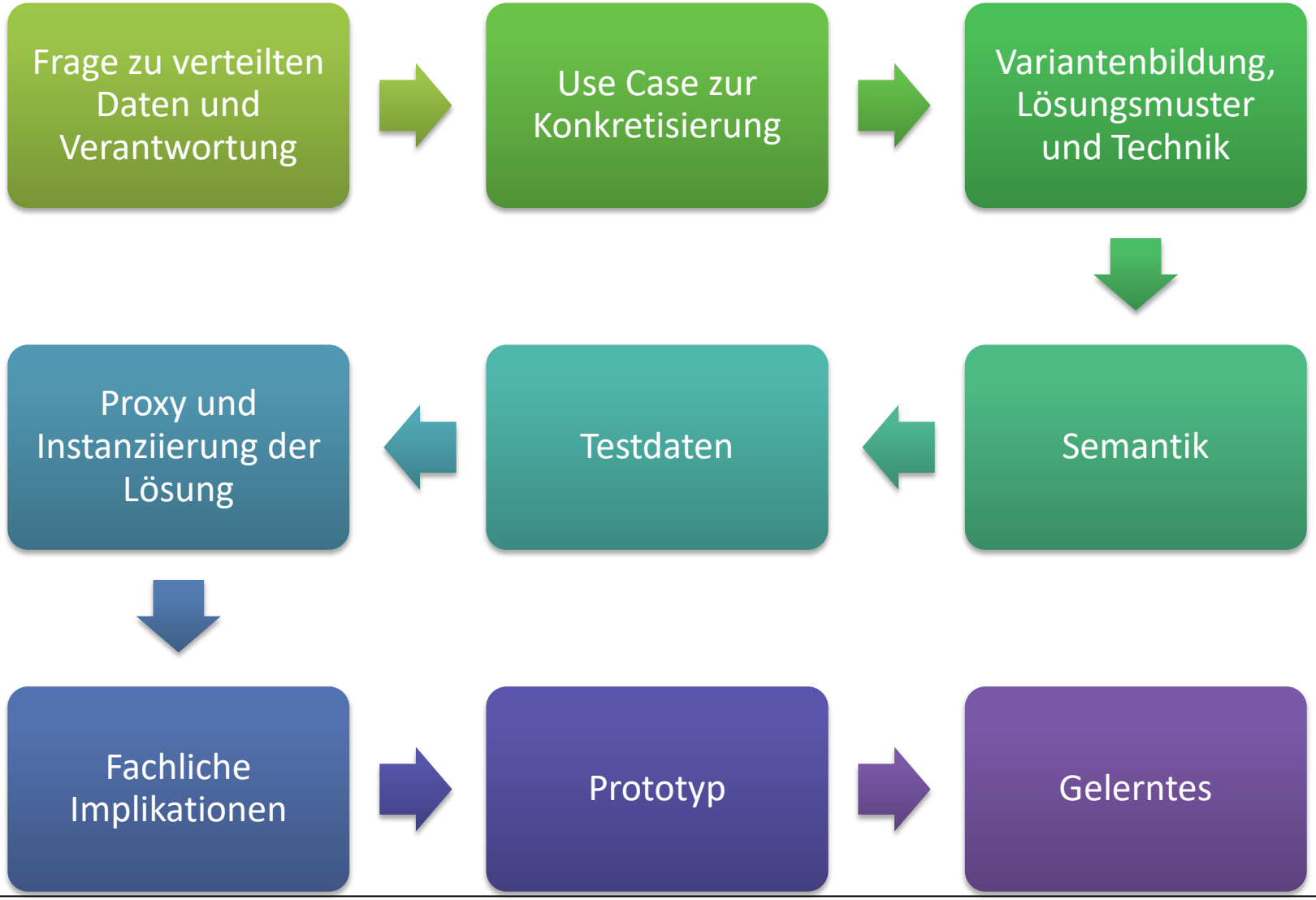
# Gelegenheit

- Im Projekt Datenökosystem der Digitalen Verwaltung Schweiz (DVS) werden Prototypen für das Datenökosystem entwickelt.

- **Idee:** In einem Prototyp Linked Data als Ansatz für föderal gehaltene Verwaltungsdaten einsetzen und mehr über die Technologie und deren Grenzen zu lernen.

- **Wir lernen** den Lösungsansatz Linked Data und die Herausforderungen einer föderalen Datenstruktur kennen

# Unser Weg

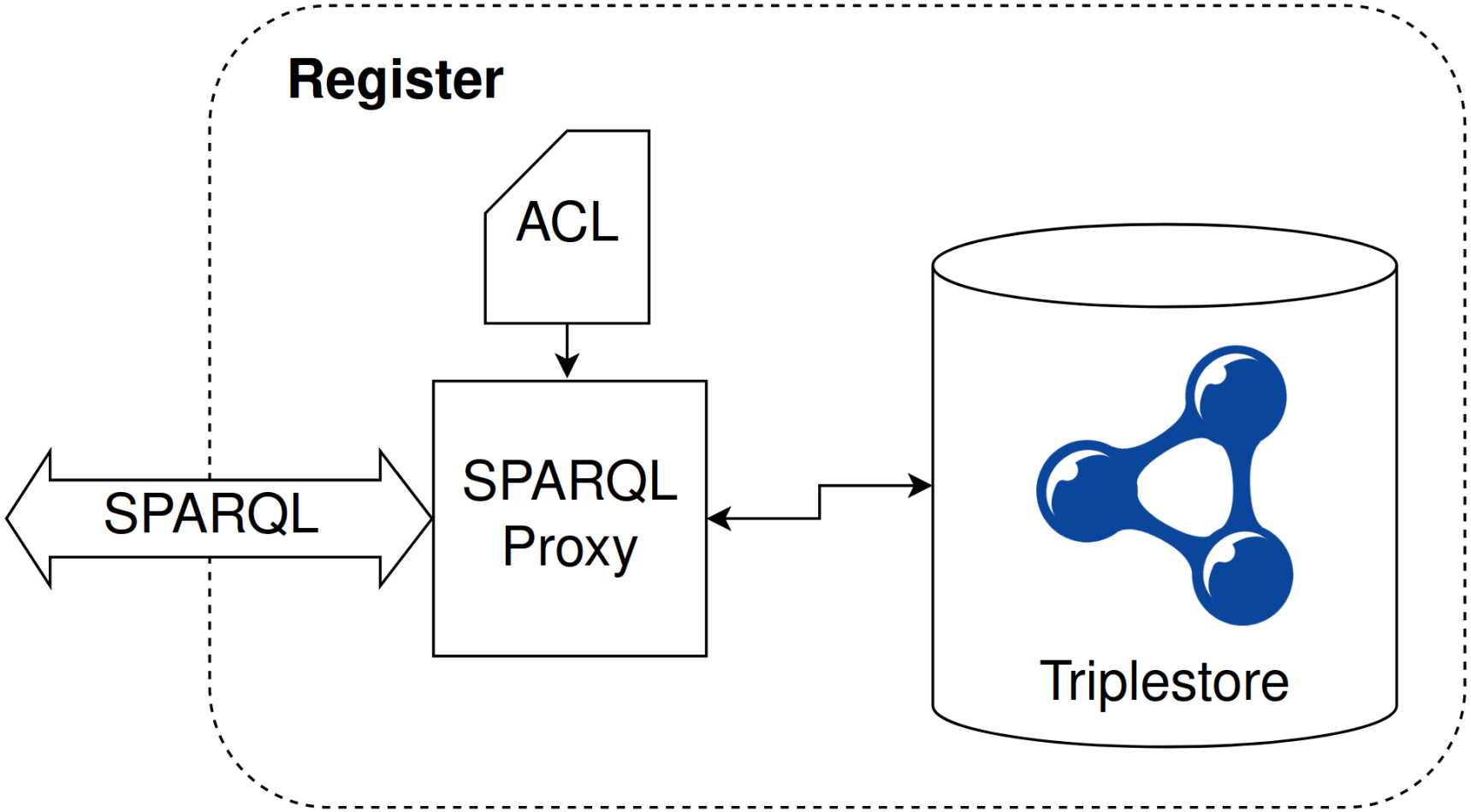

Frage zu verteilten Daten und Verantwortung
Use Case zur Konkretisierung
Variantenbildung, Lösungsmuster und Technik
Semantik
Testdaten
Proxy und Instanziierung der Lösung
Fachliche Implikationen
Prototyp
Gelerntes

# Resultate

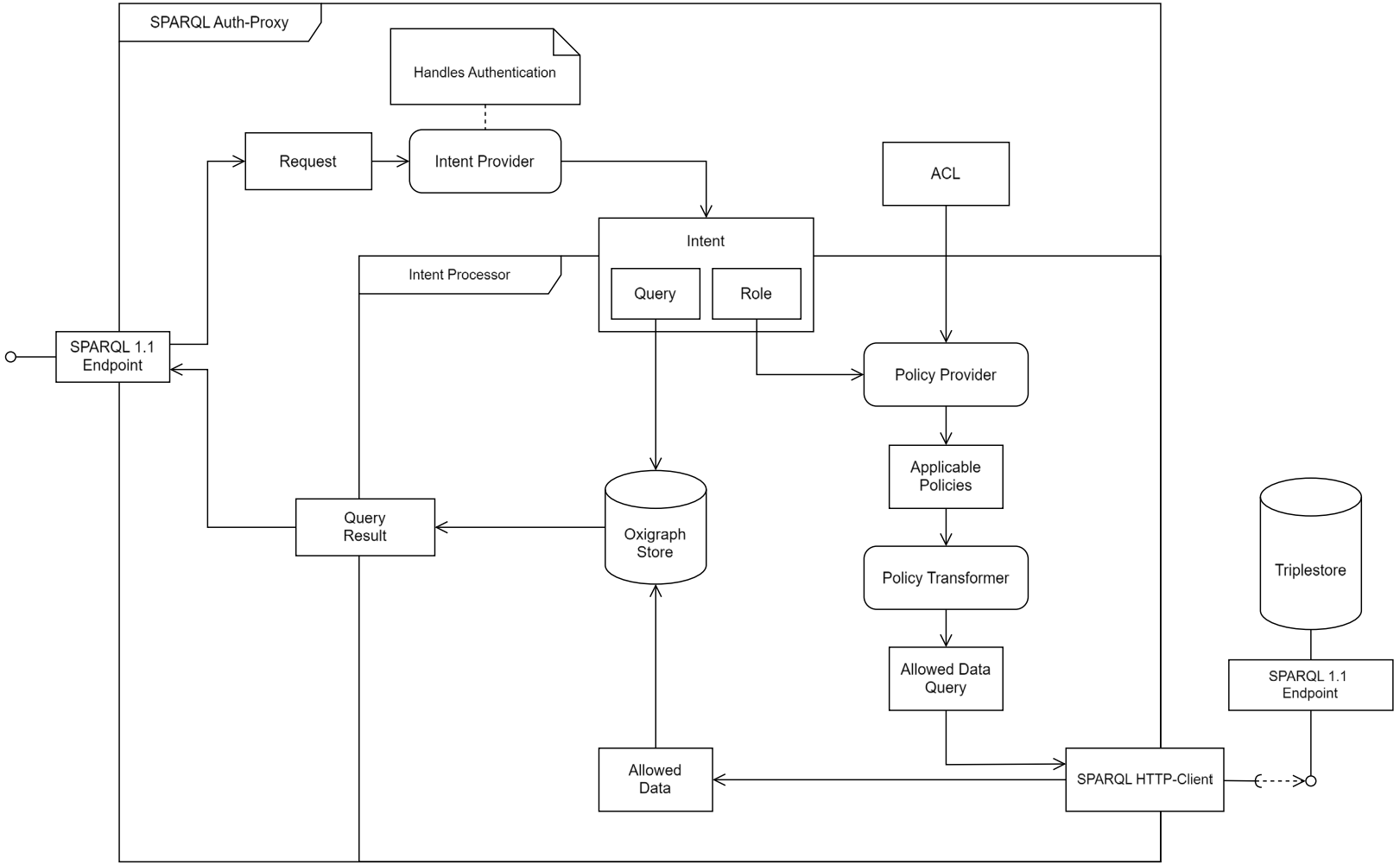
# Technische Umsetzung Prototyp (Konzept)

- **Idee**
  - *"Authorization Proxy for SPARQL Endpoints"*, R. Stojanov + M. Jovanovik, 2017
  - *"Linked Data Authorization Platform"*, R. Stojanov, S. Gramatikov, I. Mishkovski + D. Trajanov, 2017 / 2018
  - Implementation vorhanden, jedoch veraltet (bspw. Java 8)
  - Kann evtl. als Vergleichsvariante für Tests in Betrieb genommen werden
- **ld-prototype-proxy (BFH)**
  - Implementation in JavaScript
  - Im Wesentlichen SPARQL-Endpoint + SPARQL-Client
    + ACL-Engine
    + In-memory Triplestore
  - Umsetzung der ACLs durch Modifizierung der originalen Client-Queries an den Backend-Triplestore
  - Original Client-Query (zum Proxy) auf reduzierten Antwort-Graph im internen Triplestore
  - Siehe: https://github.com/swiss/ld-prototype-proxy/

# Lösungsarchitektur



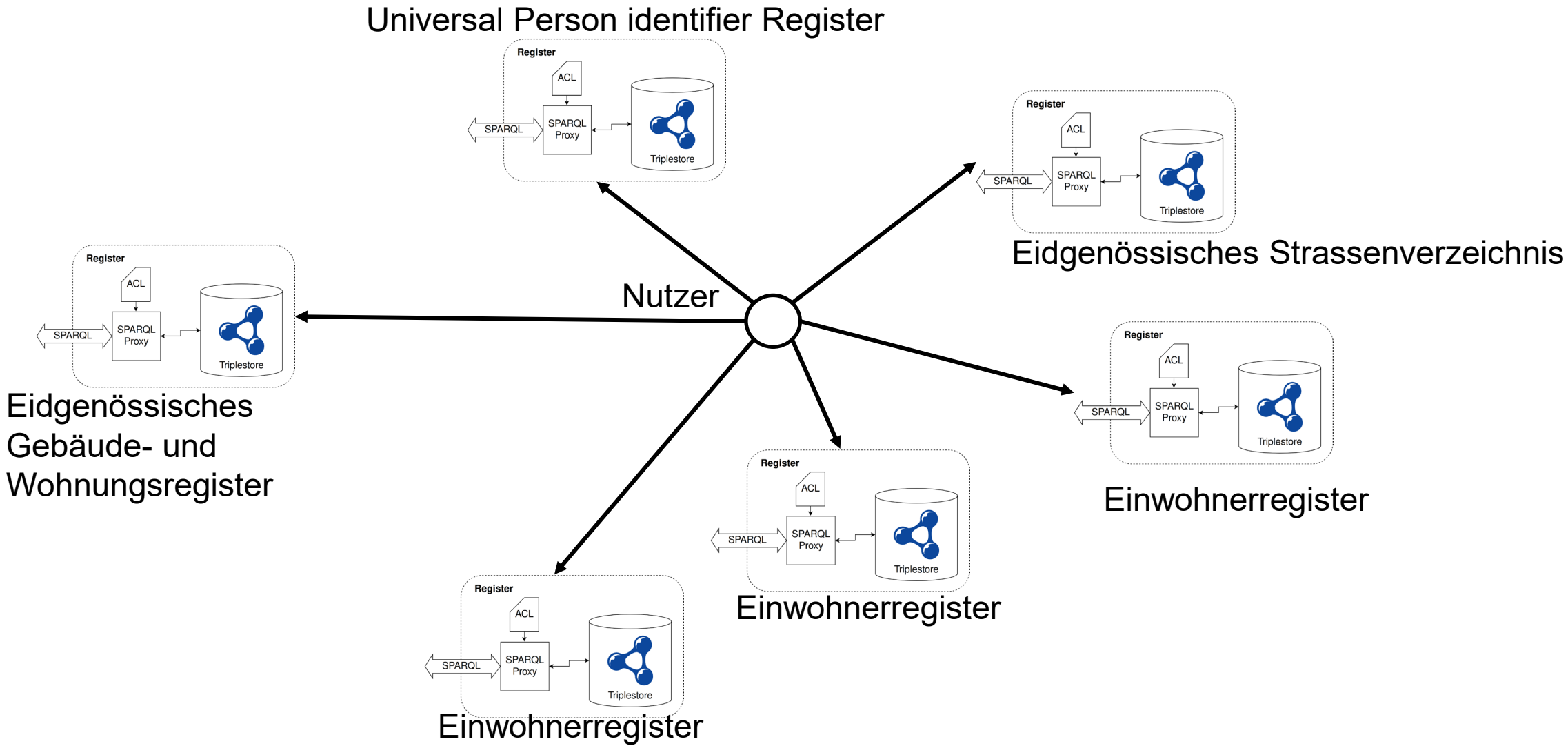
# Architekturübersicht Proxy



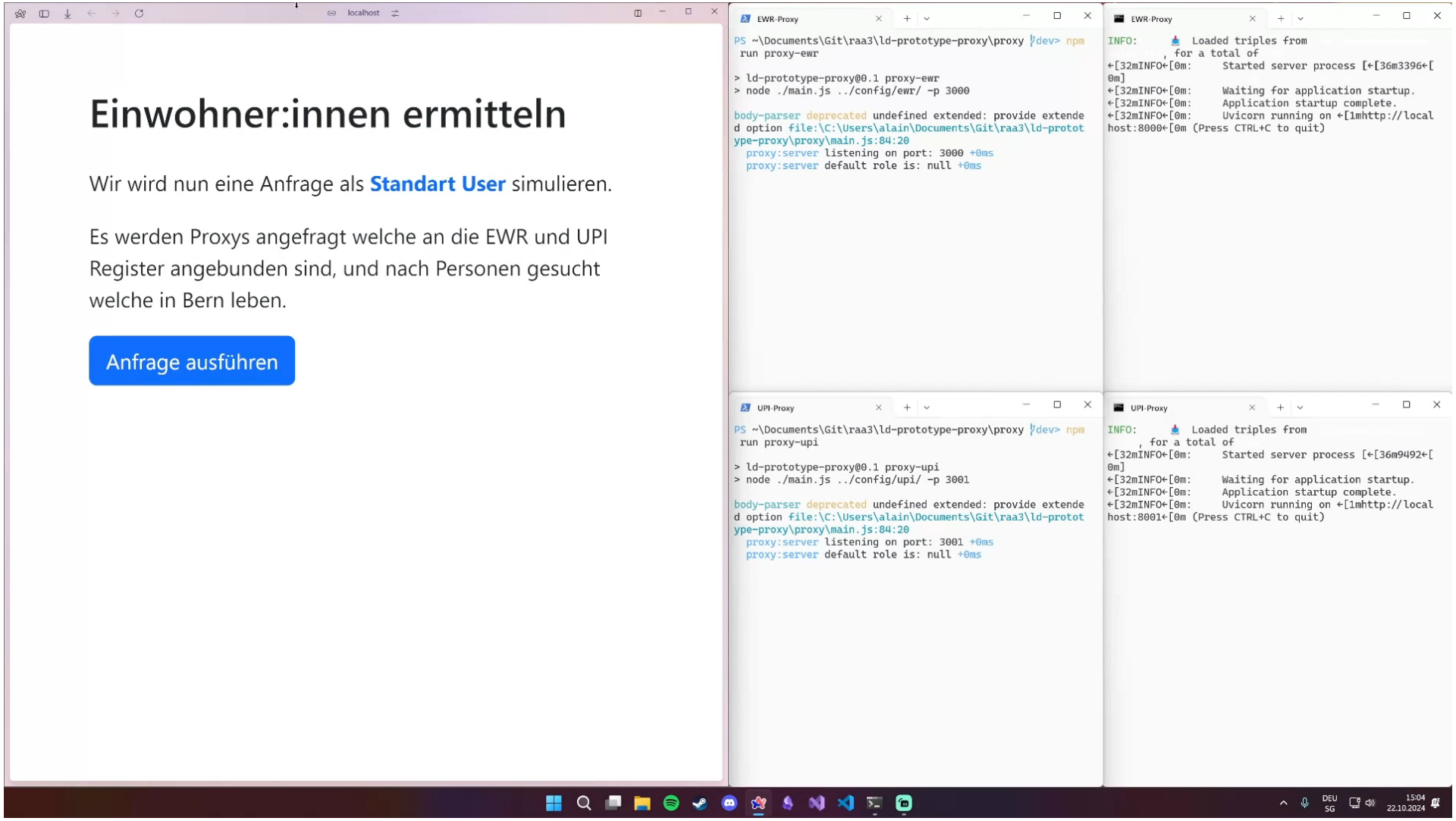
# Beispiel für eine ACL mit zwei Policies

```
{
    "role": null,
    "permission": "allow",
    "subject": [ "wd:Q556", "wd:Q560" ],
    "predicate": "*",
    "object": "*",
    "priority": 1
},
{
    "role": "alice",
    "permission": "deny",
    "subject": "*",
    "predicate": "rdfs:label",
    "object": "*",
    "priority": 2
}
```

# Umsetzung


Universal Person identifier Register
Register
ACL
SPARQL
SPARQL Proxy
Triplestore
Nutzer
Eidgenössisches Strassenverzeichnis
Eidgenössisches Gebäude- und Wohnungsregister
Einwohnerregister
Einwohnerregister
Einwohnerregister

# Prototyp – Demo



# Herausforderungen und Erkenntisse

- Keine standardisierte Lösung für die Beschreibung und Durchsetzung von Berechtigungen in gängigen Tools – jeder macht sein eigenes Ding.
- Das Umsetzen eines einheitlichen Berechtigungskonzepts über verschiedene Verantwortungsbereiche hinweg erfordert zusätzliche Lösung. Ansätze werden auf akademischer Ebene diskutiert, im produktiven Einsatz haben wir nichts gefunden. Es blieb uns nur die Lösung, es selbst zu tun.

# Offene Fragen und mögliche nächste Schritte

- Auswirkungen auf nichtfunktionale Anforderungen untersuchen
  - Performance
  - Verfügbarkeit
- Konzeption IAM zur Zuweisung von Berechtigung bei Nutzer-Organisation und Durchsetzen der Rechte bei Datenowner
- Proxy mit weiteren Funktionalitäten erweitern
  - fachliches Logging, Accounting
  - Proxy für nicht SPARQL-Abfragen (Dereferenzierung)
  - Anbindung IAM & ACL Ontologie auswählen und implementieren
- Weitere Kommunikationsmuster
  - Push
  - Ereignis-Orientiert


# Veröffentlichte Informationen

Webseite zum Prototyp mit Folien der letzten Sounding Boards

- deutsch, français, italiano

Webseite Datenökosystem

- deutsch, français, italiano

Zwei GIT-Repositories wurden erstellt, worin die Arbeiten direkt geteilt werden.

- Repository Data für die Daten, Transformation & einfache Schnittstelle
- Repository Proxy für die Entwicklung des Security-Layer mit dem Proxy & Gesamtintegration

Projekt-Webseite BFH Bern

# Fazit

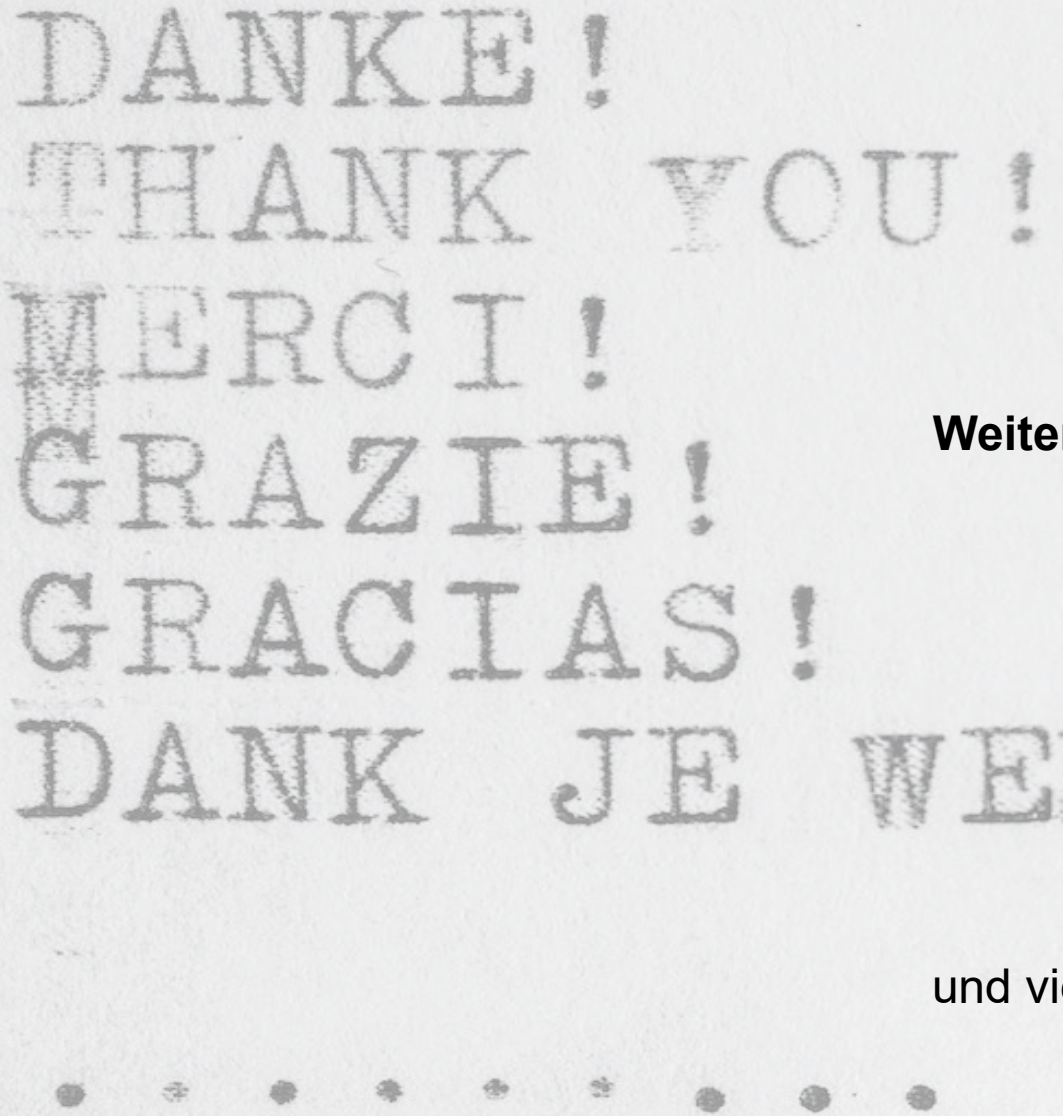
Linked Data lässt sich in einem föderalen Netz auch schützen.

Fachlich braucht es gemeinsame Regeln um dem Nutzer ein konsistentes Erlebnis zu bieten.

Der Einsatz eines lokalen Proxy’s macht in unserem Szenario Sinn. Weitere Funktionalitäten können potentiell ebenfalls an der Stelle implementiert werden.

Es eignet sich besonders gut um Rechte zu beschreiben!

# Fragen



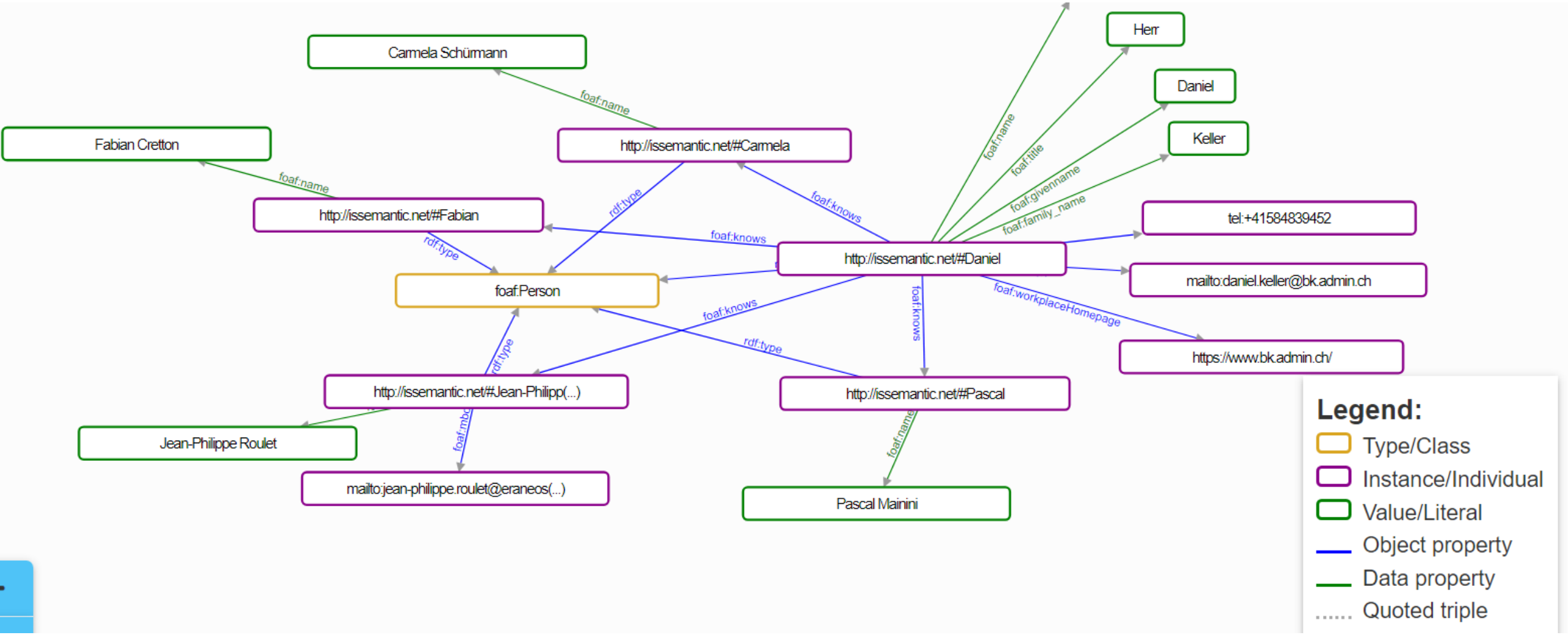

**Kernteam**

Alain Rohrbach
Carmela Schürmann
Fabian Cretton
Jean-Philippe Roulet
Pascal Mainini

**Weitere im Hintergrund**

Andreas Spichiger
Andreas Burren
Diego Fischer
Hanspeter Näf
Jürg Wüst
Michael Luggen
Stefanie Hänsli
und viele weitere mehr…

# Kontakt




Made by: FOAF-a-matic -- Sich selbst beschreiben mit RDF (ldodds.com) & Online RDF graph visualizer: Turtle, JSON-LD, TriG, RDF-star (issemantic.net)