Fraunhofer
IIS

Fraunhofer Institute for Integrated Circuits IIS

Marco Hauff – Solid Symposium 2023 Nürnberg – 31.03.2023

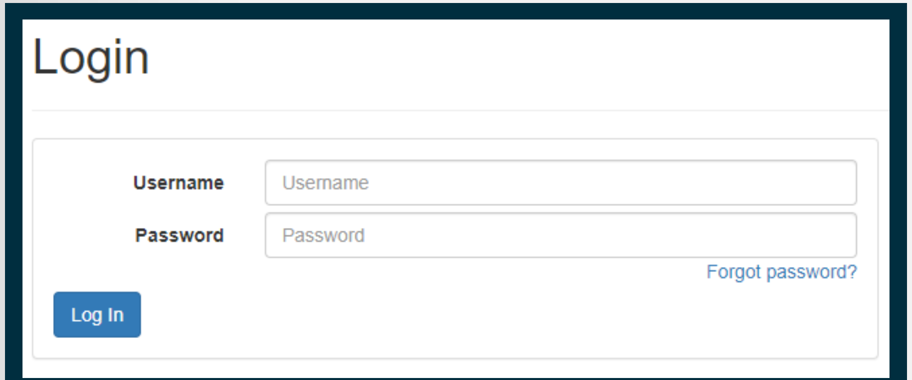
Towards a Framework for Trustworthy Access Control in Decentralized Data Storage with Solid

Discussion Topics from the Solid Taskforce (Fraunhofer IIS & FAU TI)

SOLID-SE: a search engine for Solid Pods

The essential requirements

1


Login

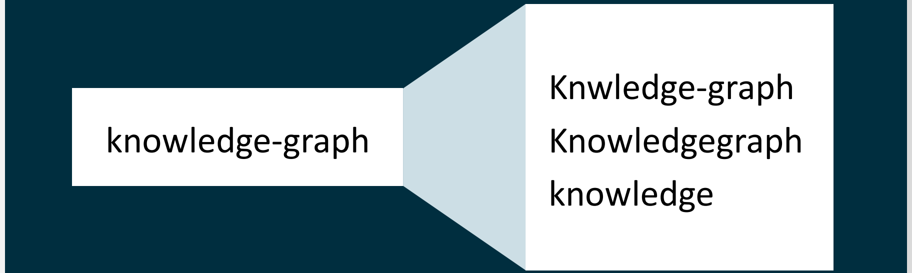
Username: Username

Password: Password

Forgot password?

Log In

Authentificated users only

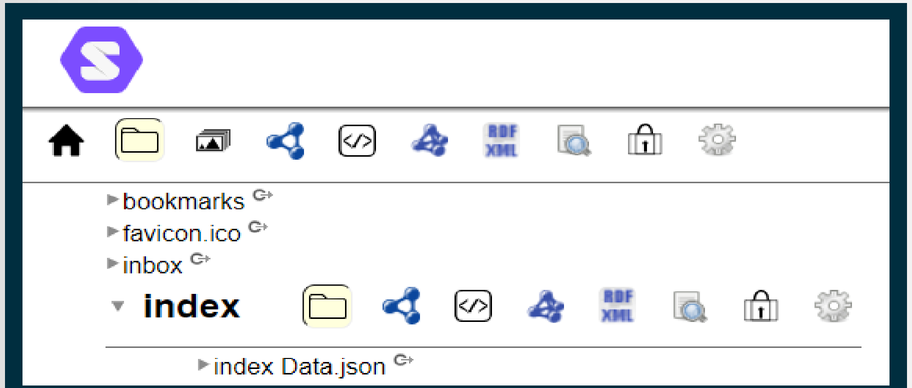

knowledge-graph

Knwledge-graph
Knowledgegraph
knowledge

Smart search with fuzzy-matching

3

2


▸ bookmarks
▸ favicon.ico
▸ inbox
▾ index
  ▸ index Data.json

Functional user interface

- highlighting functionality
  → mark matching terms
- reusable index
  → save the crawled text content in one file
- cross-container support
  → access external ressources/containers

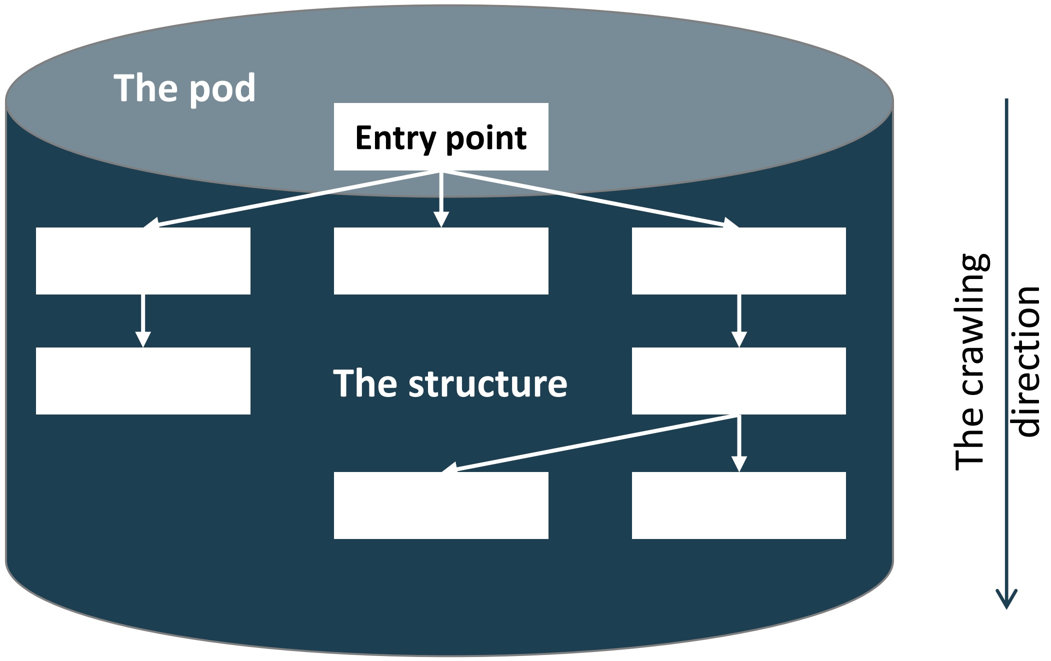
Helpful features

4

SOLID-SE

The working principle

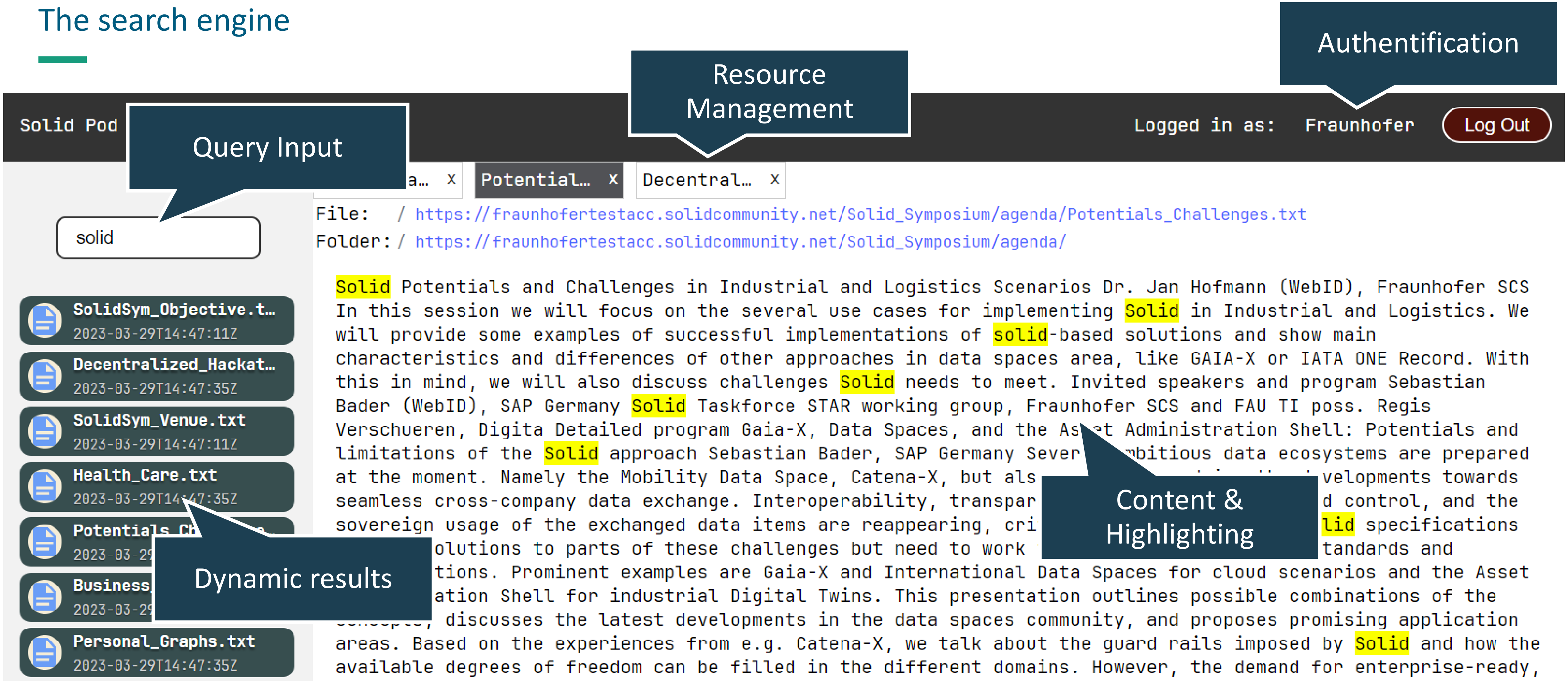
SOLID POD structure



1. User logs into his/her account
2. Identify all containers below a given entry point
3. Extraction of related RDF
4. Retrieval of all files with valid data-types
5. Storage of the retrieved data in an “.json“ index
6. Search of terms that match the user input
7. Provide manageable results

Solid-SE

The search engine



Solid Pod

Logged in as: Fraunhofer

Log Out

solid

SolidSym_Objective.t… 2023-03-29T14:47:11Z

Decentralized_Hackat… 2023-03-29T14:47:35Z

SolidSym_Venue.txt 2023-03-29T14:47:11Z

Health_Care.txt 2023-03-29T14:47:35Z

Potentials_Ch… 2023-03-29

Business… 2023-03-29

Personal_Graphs.txt 2023-03-29T14:47:35Z

a… x | Potential… x | Decentral… x

File: / https://fraunhofertestacc.solidcommunity.net/Solid_Symposium/agenda/Potentials_Challenges.txt

Folder: / https://fraunhofertestacc.solidcommunity.net/Solid_Symposium/agenda/

Solid Potentials and Challenges in Industrial and Logistics Scenarios Dr. Jan Hofmann (WebID), Fraunhofer SCS
In this session we will focus on the several use cases for implementing Solid in Industrial and Logistics. We
will provide some examples of successful implementations of solid-based solutions and show main
characteristics and differences of other approaches in data spaces area, like GAIA-X or IATA ONE Record. With
this in mind, we will also discuss challenges Solid needs to meet. Invited speakers and program Sebastian
Bader (WebID), SAP Germany Solid Taskforce STAR working group, Fraunhofer SCS and FAU TI poss. Regis
Verschueren, Digita Detailed program Gaia-X, Data Spaces, and the As et Administration Shell: Potentials and
limitations of the Solid approach Sebastian Bader, SAP Germany Sever mbitious data ecosystems are prepared
at the moment. Namely the Mobility Data Space, Catena-X, but als velopments towards
seamless cross-company data exchange. Interoperability, transpar d control, and the
sovereign usage of the exchanged data items are reappearing, cri lid specifications
olutions to parts of these challenges but need to work tandards and
tions. Prominent examples are Gaia-X and International Data Spaces for cloud scenarios and the Asset
ation Shell for industrial Digital Twins. This presentation outlines possible combinations of the
discusses the latest developments in the data spaces community, and proposes promising application
areas. Based on the experiences from e.g. Catena-X, we talk about the guard rails imposed by Solid and how the
available degrees of freedom can be filled in the different domains. However, the demand for enterprise-ready,

SOLID-SE

Current fields of activity

Increase crawling and indexing speed

Fuzzy Highlighting

Control features for the user

- Datatype limitations
- Index storing
- Search parameters/statistics

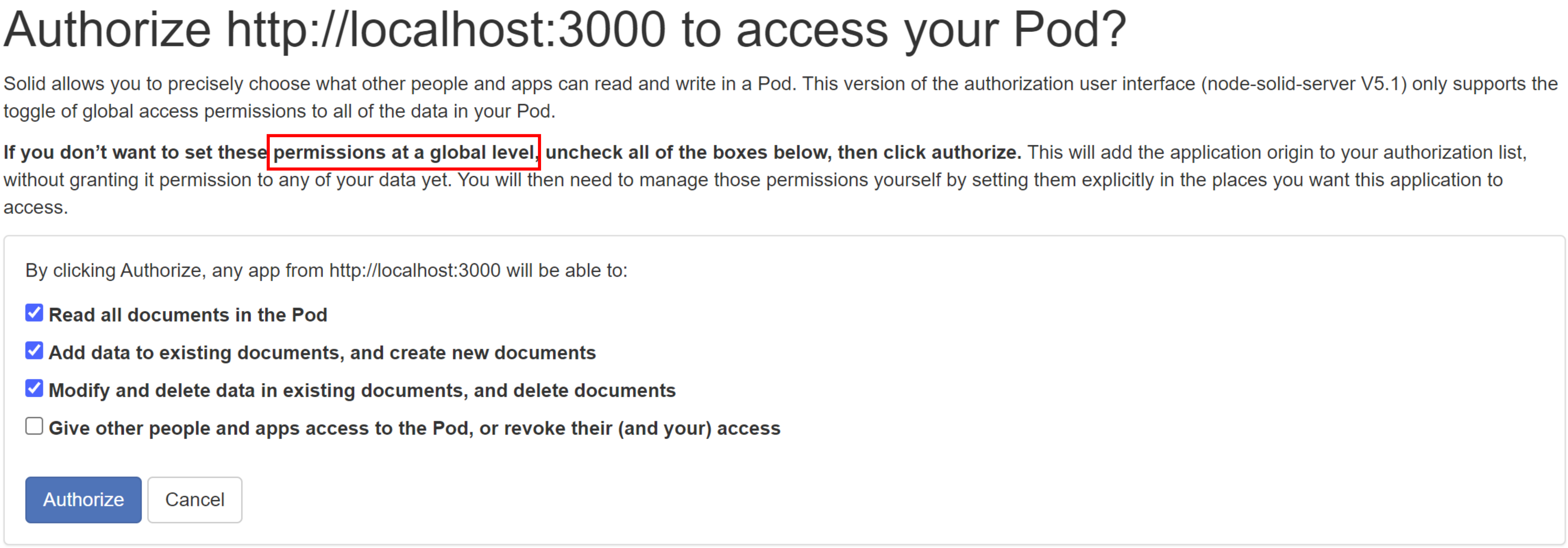
Enhance search capability

- Formatting of displayed contents
- Additional file formats / Include files without typical file-ending

Better UI (Obsidian-like)
Enable the search on mobile devices

Data access

Application authorization



Authorize http://localhost:3000 to access your Pod?

Solid allows you to precisely choose what other people and apps can read and write in a Pod. This version of the authorization user interface (node-solid-server V5.1) only supports the toggle of global access permissions to all of the data in your Pod.

If you don’t want to set these permissions at a global level, uncheck all of the boxes below, then click authorize. This will add the application origin to your authorization list, without granting it permission to any of your data yet. You will then need to manage those permissions yourself by setting them explicitly in the places you want this application to access.

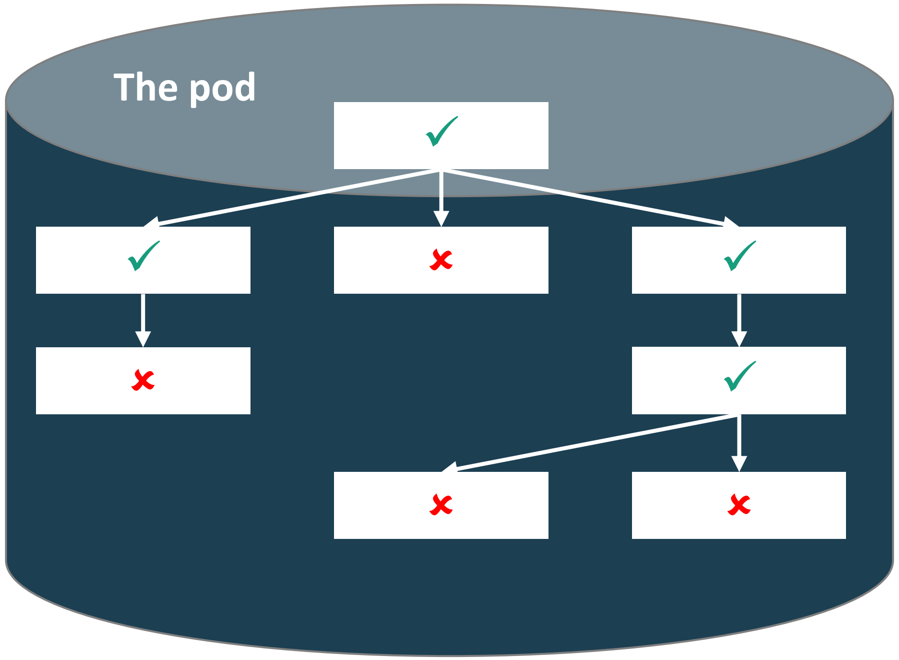
By clicking Authorize, any app from http://localhost:3000 will be able to:

- ☑ **Read all documents in the Pod**
- ☑ **Add data to existing documents, and create new documents**
- ☑ **Modify and delete data in existing documents, and delete documents**
- □ **Give other people and apps access to the Pod, or revoke their (and your) access**

Data access

Current access options and limitations

Targeted access structure



✓= access
✗ = no access

- More in-depth management by using access control lists (ACLs)
  - Determination which agent can access specific resources
  - *Read, Append, Write* and *Control* Rights
  - Rights can be inherited from the top-level container
  - Changes require another ".acl" file
- Maintaining access rights is a major effort
  - Demand for automation tools
  - Easier access options
- Deeper control logic yet to be implemented
  - E.g., legal agreements and sharing duration
  - Elaborate control flow through multiple ACL files

Data access

Current developments

- Refinement of access control lists (ACL) towards access control policies (ACP)
  - ACPs allow for implementation of (request-grant) access, e.g.,
    - limited in time
    - location-based
    - device-dependent
    - …
  - Establishment of control flows e.g., through combination with digital right management (ODRL)
- Technical measures to prevent data from being copied and processed after sharing
  - Current workaround: e.g., prove data violations through server logs

Data access

Use cases for party interactions

Party 1	Party 2	Conflicts	Exemplary use case
a	r	-	Undeletable logs
w	r	-	Deletable logs
r+a	r	-	Government data
r+w	r	-	unilateral data exchange
r+a	a	-	Bank account transactions
r+w	a	w ⚡ a	File access logs
r+a	w	a ⚡ w	
r+w	w	w ⚡ w	? Shipment announcement
r+a	r+a	-	Chat
r+w	r+a	w ⚡ a	Aggregation bot
r+w	r+w	w ⚡ w	Cooperative working

r = read, a = append, d = delete, w = write

- Theoretically there are 55 possible combinations of rights
- For party interactions, the 11 combinations shown in the table are currently considered

Data access

Summary

- The current system works but needs to be improved!
- Continuous work on
  - Finer granulation through access control policies
  - Combination with digital rights management
- To fully comply with standards such as the General Data Protection Regulation, Solid still lacks features and capabilities as well as a certain degree of user friendliness.

Fraunhofer IIS

Fraunhofer Institute for Integrated Circuits IIS

This work was funded by the German Federal Ministry for Economiic Affairs and Climate Action (BMWK) through the ”Antrieb 4.0“ project (Grant No. 13IK015B)

Fraunhofer IIS

Fraunhofer Institute for Integrated Circuits IIS

Thank you for your time and input

Fraunhofer
IIS

Fraunhofer Institute for Integrated Circuits IIS

Contact

Marco Hauff
marco.hauff@iis.fraunhofer.de

Center for Applied Research on Supply Chain Services
at Fraunhofer Institute for Integrated Circuits IIS
Nordostpark 93
90411 Nürnberg
Germany