Closing SolidLab Launching Trustflows

2026-01-19

FLANDERS

Vlaamse overheid

DEPARTMENT OF
**ECONOMY
SCIENCE &
INNOVATION**

**Gefinancierd door
de Europese Unie**
NextGenerationEU

SHARCS
imec.icon 2022-2023

Ben De Meester - IDlab, imec – Ghent University
Martin Lagauw – Enhansa
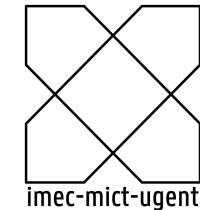
The Challenge

Personal Data for HR

As a candidate, your data is held by:

     Companies, where you directly applied for a job

     Recruiters, sharing your data with companies they present you to

For companies and recruiters

     Privacy issues (who can see what and why)

     Confidentiality issues (information is often more detailed than needed)

SHARCS: Selective Sharing of Accredited Solid Pod Data
Put the Candidate in Control

Secure disclosure

Strict **identity management**

Explicit approval by the candidate

Access control

Selective disclosure

You only share what is strictly needed

End-to-end demonstrator that empowers end-users

Backed by societal, legal and business research

9 Published Publications

De Mildt, M. The business models of Solid-based data sharing, short abstract of a talk at BDSA life long learning session, Brussels, June 20th 2024. https://solidlab.be/wp-content/uploads/2024/07/BDSA-LLL-Session-3-The-business-models-of-Solid-Based-data-sharing.pdf

Theys, T. et al. Enhancing users' attitudes towards webids : exploring the effects of persuasive messaging on user adoption : an experiment exploring the effects of persuasive messaging on the user adoption of WebIDs. Mensch Und Computer 2023. https://doi.org/10.1145/3603555.3608559

OSLO Leerprestatiecredential (applicatieprofiel). Dec 2023. https://data.vlaanderen.be/doc/applicatieprofiel/leerprestatiecredential/

Steinbach, J. et al. Inter-pod credential exchange protocol via linked data notifications. 2nd International Workshop on Semantics in Dataspaces. May 2024. https://ceur-ws.org/Vol-3705/short04.pdf

De Mildt, M. The added value of using Solid data pods in a lifelong learning context, BDSA Day, Brussels, May 27th 2024. https://solidlab.be/wp-content/uploads/2024/06/The-added-value-of-using-Solid-personal-data-pods-in-a-life-long-learning-context.pdf

Theys, T. et al. Solid-enabled personal online data stores : uncovering UX implications for online data management. Human Systems Engineering and Design: Future Trends and Applications. Sep 2024. https://doi.org/10.54941/ahfe1005533

Verbrugge, S. et al., Data Spaces Business Models, International Data Spaces Association, 2024. https://doi.org/10.5281/zenodo.14101303

Verbrugge, S. Data spaces business models, Global Data Spaces connect, Vienna, Austria. Nov 13th 2024.

De Mulder, G., & De Meester, B. (2025). Pseudonymity for personal data stores : pseudonymous webIDs and decentralized identifiers. In B. Coppens, B. Volckaert, V. Naessens, & B. De Sutter (Eds.), AVAILABILITY, RELIABILITY AND SECURITY, ARES 2025, PT IV (pp. 111–129). https://doi.org/10.1007/978-3-032-00639-4_7

Ideal scenario – JobMatch

Lea is looking for a job, and uses a new HR application (JobMatch) to help her find it.

She only shares the minimal information needed to go through the selection process.

Once Hanna (the recruiter) selects suitable matches, Lea is invited to share her full profile to ease the hiring process.

During the entire flow, both Lea and Hanna are strongly authenticated,

each interaction is double-checked with the active policies,

only authentic data is shared, and

minimized where possible.

Demonstrator scenario – JobMatch

Lea is looking for a job, and uses a new HR application (JobMatch) to help her find it.

Scenario validated by Randstad Group

She only shares the minimal information needed to go through the selection process.

Once Hanna (the recruiter) selects suitable matches, Lea is invited to share her full profile to ease the hiring process.

During the entire flow, both Lea and Hanna are strongly authenticated,

Combining TrustBuilder and Itsme

each interaction is double-checked with the active policies,

Enhansa could check all TrustBuilder-authenticated interactions

only authentic data is shared, and

MAGDA data via Athumi pods

minimized where possible.

Via DocByte

Jobmatch
Een job vinden was nog nooit zo eenvoudig.

1. Haal **moeiteloos** jouw professionele gegevens zoals jouw diploma's op.
2. Wij **matchen jou anoniem** met jobs op basis van jouw gegevens.
3. Start je **nieuwe job**!

Login bij Jobmatch

Login als Kandidaat

Login als Recruiter

Conclusions

We built an **end-to-end demonstrator** showcasing an HR use case for secure data sharing, taking identity, authorization, and data minimization into account.

We **better understood user engagement, legal boundaries, and business opportunities**.

The Solid monitor showed that **HR is a very good use case** to create Solid prototypes, hence the will of intention of end-user is deemed very high for the SHARCS use case.

We hit some walls. As expected. **More research is needed** to improve and align the used technologies with other relevant projects such as the EUDI wallet and EBSI.

Like to know more?

Read our white paper at https://solidlab.be/sharcs/!
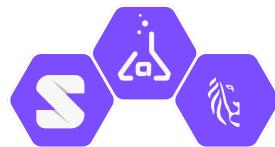
SHARCS – SolidLab Closing Event

Policy Based Authorisation Decisions
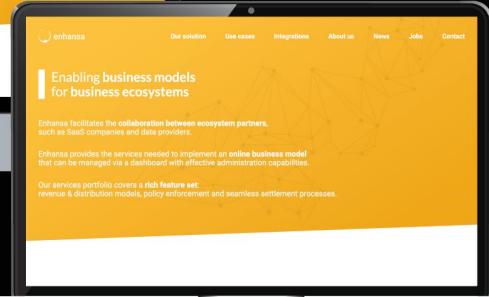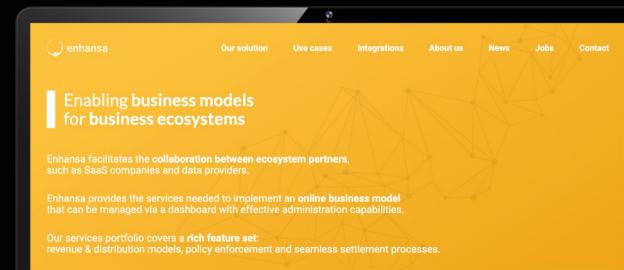
Applicable for "green fields" and/or "central governed"

ecosystems

Enhansa
STATE OF THE ART

Central Identity Realm

Autorisation Flows for

+ Subscriptions

+ Extensions

+ In App Purchases

Complex Transactions

Product Reselling

Partner Dashboards

Confidential
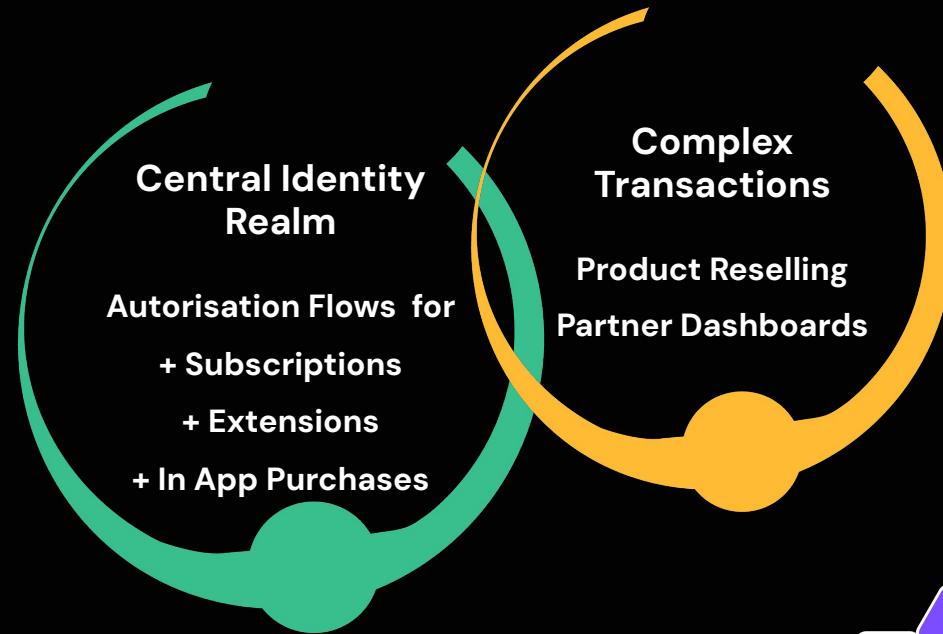
Problem Statement

Our 'state of the art' platforms do not fully leverage the commercial opportunity, due to technical limitations. We can not include third party applications in the ecosystem catalogue due to the lack of cross Identity interoperability.

The concept of Federated Identity solves **cross IDM authentication** to implement a multi-APP SSO environment.

However we did not have a solution for **authorisations in a multi-Identity context**, to enforce the business model and usage policies.

Enhansa

SHARCS R&D

Multi Identity Realms

Policy based Authorisation Engine

Complex Transactions

© Confidential
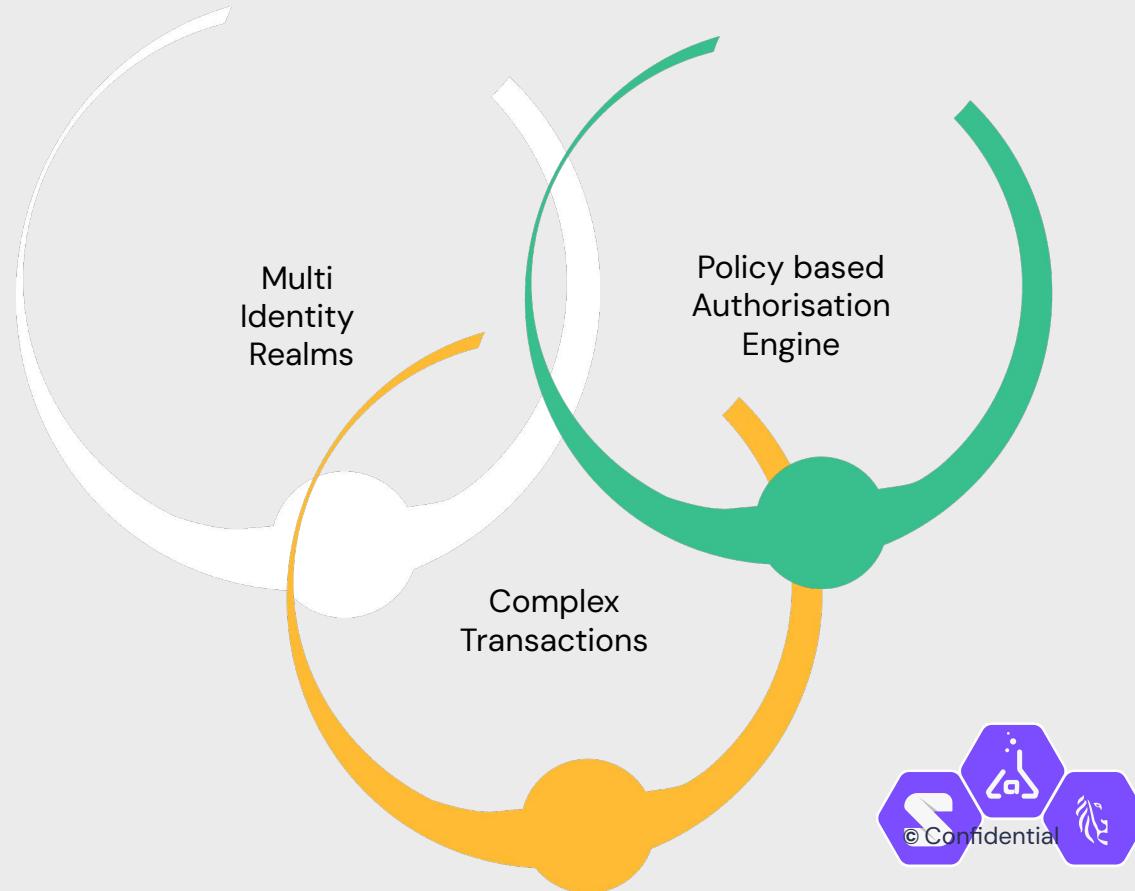
Objectives

A. Validate the IDSA Clearing House architecture as a cross Identity authorisation approach.

B. Validate a Solid POD as a sovereign storage for digital rights on a company level.

© Confidential

Solution Architecture

We chose an architecture based on XACML.

We chose Eye-Reasoner technology for the PDP to ensure the storage of decision proofs and to incorporate its semantic foundation.

- We converted policies in N3 to invoke Eye Reasoner.
- We adopted XACML to interact with Trustbuilder IDM.
- We provided a PDP endpoint for Trustbuilder..
- We implemented a PoC for sovereign storage for digital rights on a company level, but did not yet implement this on a SOLID pod.