imec

Kapeldreef 75

B-3001 Leuven

Technical report

SHARCS Consortium

SHARCS – findings and conclusions

Author(s):	Ben De Meester, Maarten de Mildt, Paul Henon, Martin Lagauw, Peter Mechant, Tim, Raymaekers, Kurt Ryckaert, Carlo Schupp, Tim Theys, Sofie Verbrugge
Date:	20-02-2025
Keywords:	Solid, Personal Data, HR

Selective sharing of accredited solid pod data in an HR context (SHARCS): main findings

Data pods – for example based on Solid technology – securely store personal data and allow n-to-m data sharing between individuals and apps/third parties. However, there are still quite some research challenges remaining. These relate to which data are shared and with whom they are shared, but also to the validity of the data that are shared. The SHARCS project aims to solve a number of these challenges for the case of secure and selective sharing of accredited personal data.

Solid: a user-centric approach to data

Today the users' data have become a major source of income and differentiation for Internet companies. But if these data are tightly linked to the use of specific apps, they are difficult to monitor and share. Therefore, a number of industries are now adopting a more user-centric approach, managing data based on individual users instead of applications. That way, data are more application-agnostic and the user can keep control over which data to disclose to which application. A new technology facilitating such user-centric data storage and sharing is Solid, a collection of protocols for building decentralized apps based on Linked Data principles and for keeping the data available in a Personal Online Datastore or 'pod'.

Challenges for selective data sharing

Although the Solid protocols are based on existing web technologies, their adoption is still in its infancy and there are still many unsolved challenges. In this project, we focus on secure and selective sharing of accredited personal data, using an HR context as demonstrator.

These are some of the challenges: while governmental institutions, universities, or payroll providers… enter certified data (e.g., a pay slip) there is no guarantee that partial information, or information aggregated from several certified sources is in itself also reliable or even certified. On top of that, a receiver may have a legal obligation to receive and store a copy of certain certified information (e.g., a diploma). But as a pod owner always has control over the data in the pod and data access to the pod, how can data be certified and remain certified? In sum: how can we solve the conflict between control and transparency for the user and the legal obligations and needs of the third parties that rely on the data?

Goal and outcomes

With SHARCS we have researched and developed innovative extensions that take a closer look at the entire Solid ecosystem:

- the connection to strong, decentralized authentication mechanisms and the EUDI wallet;
- the decentralized management of data access control through a XACML-based architecture and a semantic reasoning engine to make transparent decisions; and
- data minimization techniques to share only what is needed, while ensuring and maintaining data accreditations, through selective disclosure algorithms applied to the Verifiable Credentials standard.

In the broader context, the research on this extended Solid ecosystem translated into

- A Solid app style guide that clarifies how apps built on a Solid ecosystem can be better accepted by end users;
- A legal and governance framework within which such an ecosystem can exist; and
- A presentation of different viable business models.

This whitepaper summarises the results of the SHARCS project.

For more information, please contact the respective lead authors of the following sections:

- Identity
  - Carlo Schupp, TrustBuilder, cs@trustbuilder.com
- Policy Checking
  - Martin Lagauw, Enhansa, martin@enhansa.com
- Data Minimization
  - Paul Henon, DocByte, paul.henon@docbyte.com
  - Ben De Meester, IDLab – imec, UGent, ben.demeester@ugent.be
- User Empowerment for Personal Data
  - Peter Mechant, peter.mechant@ugent.be
  - Tim Theys, tim.theys@ugent.be
- End-to-end demonstrator
  - Kurt Ryckaert, Athumi, kurt.ryckaert@vlaanderen.be
- Legal Landscape
  - Tim Raymaekers, Randstad Group, tim.raymaekers@randstadgroup.be
- Commercial Opportunities
  - Maarten de Mildt, IDLab-TE, maarten.demildt@ugent.be

- Sofie Verbrugge, IDLab-TE, sofie.verbrugge@ugent.be

Identity

TrustBuilder

Within the SHARCS, we studied the viability of Decentralised Identity for access control and identity information sharing in an enterprise context.

TrustBuilder researched whether the WebID and SOLID Pods technologies are ready for the sharing with privacy model in an enterprise context. In the terminology of SOLID and OpenID, enterprise applications are so-called Relying Parties.

More specifically, TrustBuilder participated in building a Demonstrator to study whether WebIDs and SOLID Pods can effectively be used in an enterprise context with the objectives:

1. to identify a user in a fully self-sovereign way using their WebID. Self-sovereign means that identification means are not steered or constrained by relying parties;
2. to convert raw identity information about a subject obtained from an authoritative source in a minimised way as verifiable credentials in the SOLID Pod;
3. to authenticate subjects and relying parties in a way that they can choose without interference from relying parties using their WebID; and
4. to authorise a relying party to obtain information from the subject's SOLID Pod under a number of conditions that include (1) subject must have given consent relative to the relying party, (2) the relying party must be authenticated, (3) the relying party complies with the ecosystem policy, and (4) the relying party's request is logged independent from the relying party.

The Demonstrator took a specific use case in the recruitment domain, namely vacancy/candidate matching. TrustBuilder showed how access to candidate data is controlled, and when and for what consent is obtained from candidates. It also shows when user interactions happen and what happens behind the scenes. The Demonstrator further shows how the SOLID based model of the SHARCS project can support accountability and compliance of the different actors and service providers.

Research Conclusion

Many people would like to see a SOLID Pod as an Identity Wallet. In fact, the SOLID specifications do not define an Identity Wallet at all; they describe a protocol with set of APIs and a data format using the concepts of Linked Data and RDF namespaces. The SHARCS project demonstrated that while the SOLID specifications handle API security, they do not cover trust, data protection using encryption, authenticity, and practical concerns such as recoverability after loss or theft.

Furthermore and due to the lack of formal standardisation, we found that the SOLID technology concerning decentralised identity has not reached maturity and suffers from

lack of interoperability between SOLID servers, and lacks wide support from vendors, issuers, and governments. Moreover, its current specifications lack support for a true, protected personal wallet and for user-friendly interaction with such wallet regarding consents and selective disclosure. TrustBuilder's use of SOLID in the SHARCS project has confirmed these observations.

The main conclusion of our research in the SHARCS project, is that the EUDI Wallet is much more promising than SOLID Pod for the purposes listed above. Compared to EUDI Wallet, SOLID misses following key enablers:

1. Decentralised Identifiers (DIDs) as identifier, Verifiable Credentials (VCs) as signed claims
2. OAuth/OIDC federation protocol with mandatory MFA
3. Qualified Electronic Signatures with End-to-End Encryption
4. Trust Anchors and Revocation

The EUDI Wallet natively employs a combination of encryption, digital signatures, strong authentication, and user-centric features like selective disclosure and consent management to ensure the security and privacy of its contents. These mechanisms collectively make the EUDI Wallet a reliable and user-friendly tool for managing digital identity while maintaining trust and user sovereignty, much better than SOLID Pods. Moreover, the EUDI Wallet is grounded by the EU Regulation in effect since May 2024 and becoming local law in all EU member states no later than May 2026.

Opportunities for using semantic rules in policy checking

Enhansa

At **Enhansa**, we build the backbone of **multi-vendor platforms**—powering subscriptions, in-app purchases, and seamless digital transactions. With our **Workspace**, **Wallet**, and **Market** components, platforms like **Kolibrx**, **FinoMarker**, **StarFisk** and **ProActor** are shaping the future of digital commerce. But as we expanded, we hit a wall:

How do we bring third-party applications into our ecosystem while ensuring secure, seamless authorization across different identity systems?

We had solved **authentication** with **Federated Identity**, enabling users to log in across multiple apps. But that was just half the battle. The real challenge was **authorization**—who gets access to what, under which conditions? Business models, data policies, and digital rights all hinge on this crucial step. Without it, we couldn't **fully open our marketplace to external applications**.

Our research and development efforts in **SHARCS**, aimed to bridge this gap and unlock the full commercial potential of our platforms.

Navigating the Challenges

Our journey wasn't without hurdles such as alignment on an **IDSA-compliant architecture or affordable Solid infrastructure** to create a sustainable product roadmap. .

But amidst these challenges, we also found unexpected wins. **IDSA released 20 compliant connectors**, saving us time and resources. And an **open-source Solid Server alternative** is emerging, giving us a potential path forward for **storing company-level digital rights**.

The Breakthrough

To crack the cross-identity authorization problem, we went deep:

- **We dissected the IDSA Clearing House architecture**, understanding its potential to enforce business policies across identity domains.
- **We built a Policy Decision Point**—a smart layer that evaluates multiple policies and determines authorization in real-time.
- **We designed a next-gen architecture** that prepares our platforms for **true cross-IDM authorization**.

And to make this work, we made some key technology choices:

- **Eye-Reasoner and N3 policies**—our foundation for **semantic decision-making** and proof storage.

- **XACML-based authorization architecture and interface**—to ensure compatibility with identity management systems.
- **A proof-of-concept Workspace**—showing that cross-IDM authorization is not just an idea, but a reality.

What's Next?

With **SHARCS**, we've proven that the future of digital business is not just **single sign-on**, but **seamless cross-app authorization**. Now, we're taking it further. We're embedding the **Workspace POD** into our core Enhansa components and are exploring **new commercial applications**:

- **Coupons (Kolibrx)**
- **FinoMarker's semantic assessment within the WCO tool**
- **Future integrations with third-party vendors**

The world of **multi-vendor platforms** is evolving. And with SHARCS, we're ensuring that our platforms don't just keep up—they lead the way.

Welcome to the future of digital commerce. Let's build it together.

Delivering Trust through Data Minimization

DocByte

As organizations increasingly prioritize data privacy and security, the SHARCS project has achieved a milestone in data minimization. Our approach empowers individuals and organizations to share only the necessary information—no more, no less—while ensuring that every data exchange remains secure, trusted, and compliant with privacy standards.

At the heart of our solution is a data minimization component integrated into a secure pod. This component achieves a balance between reducing data exposure and maintaining the integrity and trustworthiness of the information being shared. What sets our approach apart is the seamless use of Verifiable Credentials to accredit minimized data, making it both verifiable and reliable.

Key Features and Achievements

- **Accredited Data Sharing**: Users can share only the data that is necessary for a specific purpose, while preserving its accreditation. This guarantees that the data meets the highest standards of trust and security.
- **Streamlined Validation**: Data users can validate the accreditation of the data they receive, including real-time checks on accreditation status and the ability to detect revocations. This transparency builds confidence and fosters trust among all stakeholders.
- **End-to-End Security**: Trusted parties ensure that data placed in the pod is securely processed and accredited. This eliminates ambiguity and creates a robust framework for secure data handling.
- **Commercial Readiness**: With a working proof-of-concept, the minimization component is not just a theoretical advancement; it's a tangible, operational solution ready for real-world applications.

Commercial Impact

Our data minimization solution addresses some of the most pressing challenges in today's digital landscape: data overexposure, compliance with evolving regulations, and the need for secure, scalable systems. By integrating this component into a secure pod ecosystem, we are enabling organizations to meet these challenges head-on, while also unlocking new opportunities for secure and efficient data-driven collaborations.

Looking Ahead

The realisation of our minimization component is a harbinger of new opportunities for secure data exchange. As part of the SHARCS project, this innovation is poised to support industries by empowering businesses to share information selectively and securely, without compromising trust. Whether it's used for personal data sharing, regulatory compliance, or

streamlined operational processes, the SHARCS data minimization process is an important step to achieve true secure data control.

Effective User Empowerment for Personal Data

imec-mict-UGent

The job search process today can be an overwhelming task for applicants. Navigating through countless vacancies across various platforms, each requiring the repetitive entry of information like diplomas and work experience, can lead to frustration and inefficiency. Solid personal data stores offer a promising solution by consolidating relevant data in a single, user-controlled location. This data can then be seamlessly shared across platforms, eliminating the need to fill out forms repeatedly and significantly reducing administrative overload. Additionally, these data stores can feed job-matching algorithms to help users identify relevant opportunities more effectively, saving time and effort.

In this context, we explored the idea of 'meaningful control' and 'intelligible communication and tangibility' in personal data sharing in human resources. Meaningful control refers to how individuals can be provided with control over their data. Here, the challenge lies not only in implementing a user-friendly and intelligible way to provide consent for sharing information but also with developing interfaces that do this in a meaningful way thus circumventing what is known as the 'consent dilemma' , e.g., through consent intermediaries. Intelligible communication and tangibility targets understandable communication about Solid personal data vaults to the public. This refers to ways in which Solid can be made tangible to people (when needed), for instance through education and storytelling. More broadly it entails questions about how to communicate about data management and privacy self-management.

During the outlining phase, we (i) evaluated the (prototype) workflows and onboarding strategies of the HR partners, (ii) explored the effects of different types of persuasive reasoning on their intention to create a WebID, and (iii) assessed the adoption potential of HR-related Solid use cases. The onboarding flow of Karamel was iteratively evaluated based on expert reviews and real-life testing of the Randstad prototype was conducted with 10 people. Then, an online experiment was set-up that presented participants with different persuasive messages and the choice of creating a WebID or using existing accounts (Google, Apple, Facebook) to register on a news website. Finally, we developed – in close collaboration with SolidLab – a HR & Skills use case description that was evaluated using an online questionnaire with +2500 respondents. Next to this, we also conducted expert and end-users interviews in collaboration with partner Karamel in order to evaluate potential user interaction flows. Overall, results showed that specific terminology such as WebID or Solid led to much confusion and misunderstanding by participants; they were not aware of what a personal data vault or a WebID actually entails and wanted more information. Not usability but (lack of) explainability proved to be major impediment for a satisfying quality of experience.

We then evaluated and optimized the user experience and data engagement via a multi-method approach. An initial largescale survey provided preliminary insights into users' behavioural intentions and willingness to share data across different use cases. However, findings from user testing involving a prototype suggested interpreting survey results with caution, as participants demonstrated significantly higher behavioural intentions when

engaging directly with the prototype. This difference was especially pronounced for the HR use case. Further qualitative feedback from potential end-users offered deeper insights into their willingness to share specific data types. Also, 7 design and ‘Solid’ experts were interviewed on 'How To present Solid to end-users?’. The overall consensus among these interviewees was that the primary goal of presenting Solid to end-users should be to clearly communicate its benefits, rather than explaining Solid in complete technical detail. This is reflected in the general agreement that terms like “Solid” and “WebID” should not be user-facing.

Finally, we took the learnings from the previous tasks and translated these into a set of guidelines for designers in order to reduce the difficulties and hurdles designers encounter and in order to bring more consistency into the design of Solid interfaces to optimize the adoption potential. This accumulated in a set of design guidelines for personal data stores in the job application process, organized into three main categories. ‘Guidelines for designing effective data requests’ elaborates on guidelines such as ‘Clearly communicate the purpose of data requests’, 'Offer granular control', 'Leverage brand trust' and 'Request only necessary data'. The second category, ‘Guidelines for the design of the job matching functionality’ encompasses best-practices such as 'Enable customizable settings' and 'Provide transparency in algorithms'. The final category of guidelines addresses the evaluation process and cautions for relying solely on survey data based on descriptions of use cases for design or strategic decisions. It argues for prototyped based research as prototypes make use cases more tangible, helping users form a clearer mental model and providing a basis for more accurate evaluations (Show, don’t tell).

Demonstrating end-to-end compliance

Athumi

The SHARCS project demonstrated a strong interconnected set of components on a pod infrastructure sandbox, which can be leveraged in real world applications. More-over the demonstrated flow combines an applicable user journey for end-user applications in the HR-sector with the underlying components that underpin several challenges involved. The demonstrator proves that the challenge of trust, data minimisation, semantic standardisation and identification are not theoretical challenges but can be tackled and actually combined in in proof-of-concept flow. The demonstrator was set up iteratively with the different partners involved starting from user persona's to a set of requirements combined in a user journey flow and mapped out architecturally.

Key Features and Achievements

- **Suitable for end-user applications**: The SHARCS project started from a set of challenges multiple end-user applications are facing. The set of technical components, data standards and user journey can be re-used for different end users in HR cases or other domains (for multiple datapoints).
- **Gui for sharing minimized data**: A user-friendly interface has been created to help share minimizing diplomas. When a user selects their diploma, the system works with an external service to create a minimized version of the diploma that includes only the essential details. This minimized diploma is then securely stored and can be shared with others, ensuring data privacy while keeping the process smooth and transparent.
- **Semantic data operability**: During the SHARCS project, an OSLO track has been conducted to standardize the latest ELM standard in Flanders. Learning credential data is currently spread across different systems and applications that are not connected to each other. Citizens, companies, and institutions can gain great added value from clear and accessible learning credentials. This supported data model, in the form of an OSLO standard, makes it possible to share and exchange data between different stakeholders.
- **Integration**: The components of the different partners were integrated in an overall architecture and demonstrated working interchange of the different components.
- **Commercial Readiness**: The demonstrator showed a working proof-of-concept of multiple integrated components on the solid pod sandbox infrastructure of Athumi. The integration shows potential towards multiple use cases across multiple industries and multiple production cases can be applied.

Commercial Impact

The delivered user journey and architectural solution addresses several challenges many companies face: balancing the need for authentic data, imposing minimalisation and strong

authentication and trust in the ecosystem. This demonstrator proved that the different components can be integrated across multiple partners, even though challenges. Many real life cases show potential to provide value across multiple sectors involved for datapoints such as diploma, student attestation, flexijob attestation, address changes, …

Looking Ahead

The demonstrator showed clear promise for future integrations but also revealed challenges in the commercial domain, minimisation protocols and identity management. Those lessons provide great value for further optimising the different components in an integrated landscape that can assist companies in easy onboarding, both technical, commercial and legal and pairing this with an optimised workflow for access across multiple datapoints.

Legal landscape

Randstad Group

We conducted legal research in collaboration with Athumi to set out the legal landscape for the data pods. In-depth attention was paid to the legal reasoning applicable to employers that could hinder or aid the use of a data pod when dealing with employment of possible candidates. It does so on the basis of use cases of an employer verifying a student certificate and a diploma.

We made an overview of the most important articles of the law establishing Athumi from a practical perspective, in order to get a clear idea of what the legal boundaries are for Athumi when hosting the data pods. Where relevant, the comments that were provided by the Belgian Data Protection Authority and the Vlaamse Toezichtscommissie are also referred to. We found the advice that has already been provided by these two instances concerning the boundaries on data protection to be sufficient to conclude this overview.

After setting this (legal) scene, we delved deeper into the possibility of Athumi acting as a data intermediary under the new Data Governance Act of the European Union. Although there are some advantages as well as restrictions to this, no decision has been taken yet on the matter, partly because there is no official authority yet in Belgium that can provide such a label.

We then analysed the possibility of the data pods being used to provide a digital identity wallet under the European Digital Identity Regulation, which states that each member state should provide their data subjects with a digital identity wallet that is capable of producing qualified electronic signatures. However, there is currently no indication that Athumi's data pods would take up such a role (possibly only for the Flemish region).

Finally, we focused on the possible issues employers can run into when using the data pods to check documents for their employees. While in most cases it would be sufficient for the employer to look at a document in the datapod without requiring lasting proof, several areas are identified where this would not be the case, namely that of employing students with reduced social security contributions, whereby the social security authorities require sufficient evidence that the student is still studying, as well as evidence issues in case of gross negligence in the hiring of certain profiles. On the point of the social security authorities (Rijksdienst voor Sociale Zekerheid), we note that these authorities have wide discretionary powers to decide which evidence is required. As such, negotiations are ongoing between Athumi and the social security authorities in order to find a solution that satisfies the evidence requirements of the social security authorities. It should then be checked whether such a solution would also suffice for the tax authorities, and the DVZ in case of foreign students. Unfortunately, at the time of writing this paper, no conclusion has been reached.

As a conclusion, we suggest that for both these use cases some form of proof is required that respects both the obligation of evidence on the employer, and the prohibition on copying of the content from the datapod. In order to respect the obligation for the

employer, we identify that the content provided should at least count as evidence in writing according to the new Civil Code. Since this would constitute a 'beginning of proof', it would be up to the other party to refute such proof, which should not be possible.

Legal and Commercial Opportunities

IDLab-TE

What are the legal and commercial opportunities of decentralized, consent-based data sharing?

We tried to uncover what the opportunities are of the technical and UI set-up of SHARCS. Given their technical means to share data in decentralized fashion based on consent and the accompanying authorization and authentication, the question rises if this opens new opportunities. Specifically, how can these opportunities arise, and what are the (current) legal and business challenges or boundaries of such a system.

In essence, the question is how the data sharing system can grow into an ecosystem of multiple and diverse parties. It must present itself as an attractive alternative to more traditional approaches like manual and bilateral data sharing. For example, the system must be able to compete with a student manually retrieving an accredited document from their educational institution to proof that they are a student. One way it can do so is by building a diverse and automated ecosystem of data sharing. However, this requires the data sharing solution to be legally sound, trusted and beneficial for each ecosystem partner. If the data shared would not hold in court or false claims are made by untrusted parties, ecosystem partners might fear hefty fines. Naturally, if the ecosystem cannot provide clear benefits compared to current alternatives, there would be a lack of interest.

We performed a legal and business analysis of an HR use case where an HR bureau recruits employees with specific attributes (e.g. diploma or student status) using the SHARCS data sharing system (which means Athumi is the data and pod provider). These potential employees must then provide accreditation of these attributes, like showing the validity of their student status. We analyzed the law founding Athumi in perspective of other relevant legislation and law in Belgium and the EU, in the context of the HR use case. The Solid specification was examined, to uncover what is considered a trusted data exchange therein. Additionally, to determine how a decentralized trust environment can be set up, we defined the role of the Data Clearinghouse as a data sharing policy engine in the HR use case at hand. Finally, the value and costs for potential data consumers in multiple sectors (HR, mobility and student housing) were determined in the context of this HR use case.

What we uncovered were several remaining challenges for decentralized, consent-based data sharing. First, the three conditions required for a "proof to be in writing" according to Belgian Law, namely that the content must be comprehensible, durable and that the integrity of the content must be protected are not fulfilled. On this point, a balance must be formed between the prohibition on copying content from the data pod and the need

for the employer to have a beginning of proof that they have fulfilled their obligations. Second, the Solid specification lacks maturity on what a trusted exchange is. Therefore, standardizing the concept of a trusted exchange will be required to build a governance strategy that allows each party to communicate on the same terms. As suggested before, competing technologies like the EUDI Wallet might provide answers here. A Data Clearinghouse could provide an essential part therein, as an independent ecosystem partner that allows other parties to define data sharing policies (e.g. who to share with, on what terms…). Third, regarding the benefits for data consumers in the ecosystem, we revealed that benefits are to be found for diverse data consumers. However, the costs of data sharing impact the inclusion of a consumer (here: whether the case is viable for a data consumer), and these vary greatly between diverse consumers. There appears to be no one-size-fits-all pricing model for decentralized ecosystems. Different pricing models of Athumi as a data provider majorly impact this cost and can make or break the inclusion of a certain data consumer. In an early bootstrapping phase of the ecosystem, we showed that this more centralized approach of Athumi can work for multiple data consumers. However, given it does not work for all of them, the question remains how this can evolve into a more decentralized approach. If the goal is to share more data among various parties by means of decentralization, then such costs and the impact of pricing, legal challenges and the notion of trust need to be considered and transparently communicated to create a viable decentralized ecosystem.