Cornerstones of a Future Solid B2B Ecosystem: Authorization App and Delegation Proxy

Abstract

The Solid framework for decentralized and self-sovereign data management proposed by Berners-Lee enables dynamically binding an identity to a Solid application and a user-specific Solid data store, thus enabling interoperability within the Solid ecosystem. We evaluated Solid in the context of a typical B2B use case, the granting of a loan between a bank and a receiving company, and thereby identified two business functionalities that are particularly relevant in the B2B context: The need to provide secure and easy access to internal data between companies and the need for employees to be able to take on different roles in business processes depending on whether they are acting internally or externally (i.e. on behalf of the company). We transferred these business requirements into two separate applications, the "Authorization App" and the "Rights Delegation Proxy", and evaluated them based on our use case.

Keywords

Solid, Web technologies, data-driven ecosystems, B2B, data sovereignty

1. Introduction

Solid[1] (Social Linked Data) intends to change the way web applications work today, aiming for true data ownership and improved privacy, establishing data sovereignty in web-based data-driven ecosystem [1, 2, 3, 4]. It utilizes the idea of a data-providing web service (Solid Pod) that can on demand of a user be integrated into web applications, s.t., a prosperous, but safe ecosystem can be established where the users are in control of their data (data sovereignty).

Figure 1 outlines our motivating example. A small- or medium-sized enterprise (SME) applies for a loan from a bank. The bank, in turn, requests additional internal data from the SME (business assessment reports) in order to prepare a loan offer to the SME. However, credit applications and credit offers are not issued by the companies themselves. Rather, employees act *on behalf* of their companies. Two aspects are of particular relevance in this scenario and need to be solved on a technical level. Secure and simple sharing of information through mutual access to internal data (annual reports and credit offers) and the different roles of the involved employees in this business process, both internally and in relation to external partners. We propose a solution that consists of two independent components. An application for secure and easy data sharing, and an application/service that allows people to perform actions on behalf of others.

The 1st Solid Symposium Poster Session, co-located with the 2nd Solid Symposium, May 02 – 03, 2024, Leuven, Belgium

[1] https://solidproject.org/

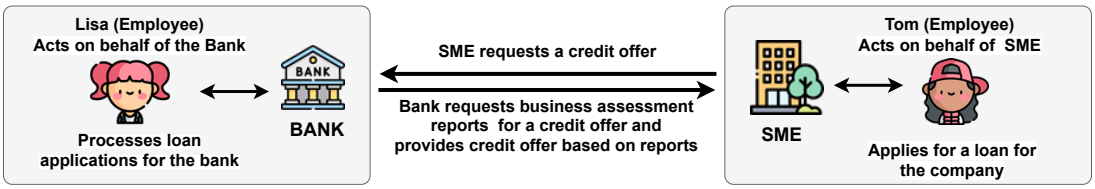

Figure 1: Outline of the use case

2. Related work

Data sovereignty in a web-based ecosystem is the goal of the Solid movement [1, 2, 3, 4]. The *Solid platform*, specifications, and technologies aim for a safe, decentralized web where users are in complete control of their data. This was already applied prototypically in several fields, e.g., for social applications [2], Building Information Modeling (BIM) [5], machine-to-machine transactions [6], processes between public administration and citizens [7], or B2B environments [8].

However, while the latter is in the same context as this work, it and all the mentioned works didn't address the aspects of functionalities of components across different domain-specific applications which should be the focus of a Solid-based application infrastructure as intended by the Solid protocol.

3. Concept

Figure 2 schematically displays the technical concept of integrating Solid Pod, business app, *Authorization App*, and *Rights Delegation Proxy* (RDP) in the context of our motivating example showing the bank and the employee Tom. Additionally, Figure 3 shows the business process of our use case which requires a cross-company workflow where the employees (Lisa, Tom) of the companies act on behalf of the corresponding companies (SME, Bank). Hence, it shows a typical example of modern data-driven B2B ecosystems.

3.1. Authorization Agent

One of the key principles of the Solid concept, the ability to dynamically bind an identity to a Solid application and a Solid pod, means that users must frequently process data access requests on demand and grant or deny them or revoke existing access rights to data. Processing and managing such access requests and access rights in a Solid environment requires a comparatively high number of HTTP requests.

To enable efficient handling of these tasks and to prevent the need to re-implement this functionality for new use cases, we developed a prototype of a reusable web-based user interface to grant access to data in a Solid Pod, the Authorization App, short AuthApp, which will be presented at the ICWE 2024. The application allows both the monitoring and processing of received, existing, rejected, and revoked requests for data sharing.

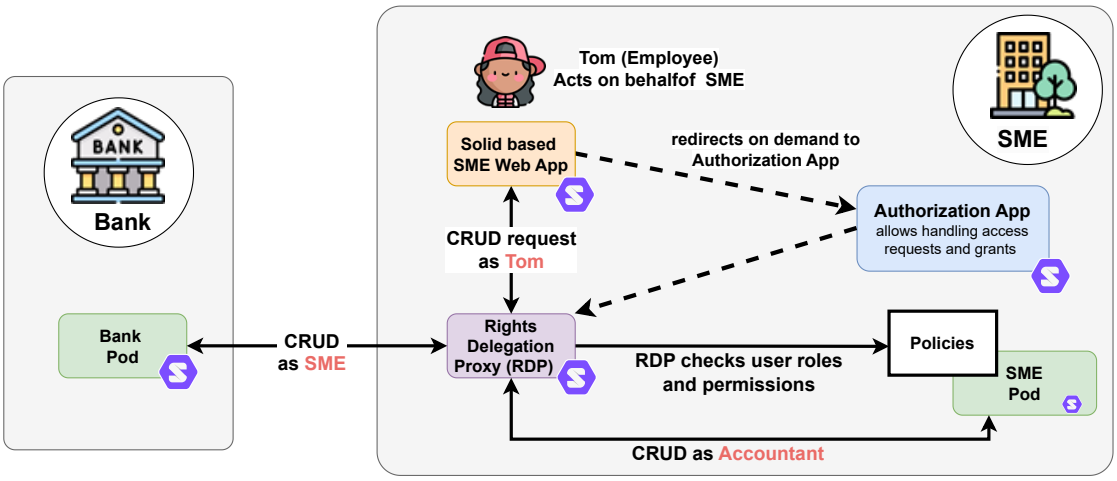

Figure 2: Schematic technical illustration including Authorization App and Rights Delegation Proxy for use case on the example of the SME and Tom, accountant of the SME.

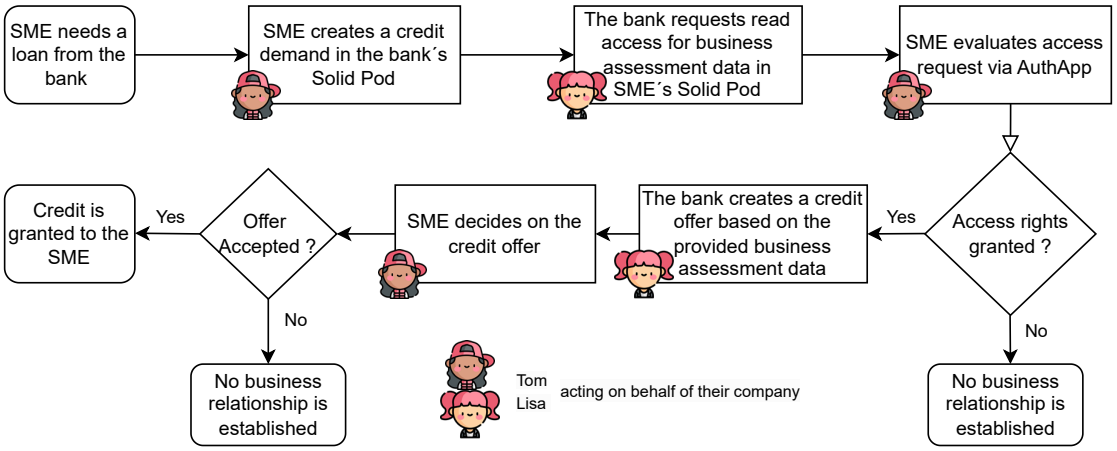

Figure 3: Interaction between Bank and SME

By design, the AuthApp is not integrated directly into the business applications. The Authorization Agent, resp. the application, for a given Social Agent can be discovered by de-referencing the identity of that Social Agent, and extracting the object value of the `interop:hasAuthorizationAgent` statement defined in the W3C Solid Community Group's Application Interoperability Specification [9] from the Social Agent graph in the returned identity profile document. Further, we designed the application to avoid the need to copy or store data outside the personal / company context, meaning all data remains under the user's / company's control. By this, any business app just needs to redirect the web browser to the corresponding IRI to provide the user with the functionality of data sharing.

3.2. Rights Delegation Proxy

In our use case, agents have to act on behalf of others, here especially natural persons on behalf of organizations e.g. an employee signs the loan contract on behalf of their employer. The transfer of rights from one agent to another is a so-called delegation or power of attorney. In a delegation, a delegator defines policies for a delegate that state the rights and transactions that may be exercised in the delegator's name toward an affiliate. We use Solid to realize dataspaces between agents to share data and also delegations to act on data, but for rights delegation, the current process is based, e.g., on Access Control Lists[2] (ACL) or the membership in vCard groups[3]. When considering privacy, issues arise quickly, as the delegate's identity and the delegation are revealed to an affiliate who has to set the corresponding ACLs, despite the delegate's potential interest to stay hidden. Still, a delegator needs to keep control over defined policies. To solve the questions of privacy and business secrets while realizing more complex policies (that go beyond ACLs), we propose the Rights Delegation Proxy (RDP) as an approach for private and legitimate data sharing and delegations. As the delegation of rights among agents occurs frequently and still has far-reaching implications in terms of the power of attorney, e.g., along hierarchies or only between individual citizens [10], and is often similar in terms of basic roles (delegator, delegate, affiliate), we opted for a general, reusable form that may be used across different organizations.

As a component, the RDP receives all requests the delegate makes, checks that the delegate's WebID is authenticated, and extracts the requested web resource. The RDP looks up suiting policies as defined by the delegator depending on the WebID or web resource and evaluates if the delegate's request is valid concerning the policies. Such policies can, e.g., be defined as Shape Expressions (ShEx)[4] or SPARQL[5] ASK queries. If the policy is valid, the RDP logs and forwards the delegate's request to the resource authenticated as a delegator, s.t., a separation between delegate and affiliate is made. From the affiliate's perspective, only the delegator was involved.

4. Conclusion

In this paper, we addressed reusable components in the Solid ecosystem. Our approach is driven by the potential of the Solid technology stack that is enabling web components that can safely interact. Motivated by the demands in the B2B world, we identified two processing steps that have a high potential to be reused in most B2B use cases: Rights Delegation Proxy (RDP) and Authorization App (AuthApp). We designed and implemented these components as pure Solid apps, s.t., they can be reused by design. With our contributions, we follow our long-term agenda of providing the required standard functionality for B2B data-driven ecosystems as Solid apps. Hence, we envision a future environment where Solid apps for business can be implemented rapidly while still meeting the highest demands in relation to GDPR, security, traceability, and protecting business secrets.

[2] https://solidproject.org/TR/wac
[3] https://www.w3.org/2006/vcard/ns#Group
[4] https://shex.io/
[5] https://www.w3.org/TR/sparql11-overview/

References

[1] A. V. Sambra, E. Mansour, S. Hawke, M. Zereba, N. Greco, A. Ghanem, D. Zagidulin, A. Aboulnaga, T. Berners-Lee, Solid: a platform for decentralized social applications based on linked data, MIT CSAIL & Qatar Computing Research Institute, Tech. Rep. (2016).

[2] E. Mansour, A. V. Sambra, S. Hawke, M. Zereba, S. Capadisli, A. Ghanem, A. Aboulnaga, T. Berners-Lee, A demonstration of the Solid platform for social web applications, in: Proceedings of the 25th International Conference Companion on World Wide Web, WWW '16 Companion, 2016, p. 223–226. doi:10.1145/2872518.2890529.

[3] R. Verborgh, Re-decentralizing the Web, For Good This Time, 1 ed., ACM, 2023, p. 215–230. URL: https://doi.org/10.1145/3591366.3591385.

[4] O. Seneviratne, A. van der Hiel, L. Kagal, Tim Berners-Lee's Research at the Decentralized Information Group at MIT, 1 ed., ACM, 2023, p. 201–213.

[5] J. Werbrouck, P. Pauwels, J. Beetz, L. van Berlo, Towards a decentralised common data environment using linked building data and the solid ecosystem, in: 36th CIB W78 Conference, 2019, pp. 113–123.

[6] X. Wang, C. H.-J. Braun, A. Both, T. Käfer, Using schema.org and Solid for linked data-based machine-to-machine sales contract conclusion, in: Companion Proceedings of the Web Conference 2022, WWW '22, Association for Computing Machinery, 2022, p. 269–272. doi:10.1145/3487553.3524268.

[7] B. E. Penteado, J. C. Maldonado, S. Isotani, Methodologies for publishing linked open government data on the web: A systematic mapping and a unified process model, Semantic Web 14 (2023) 585–610. doi:10.3233/SW-222896, 3.

[8] D. Henselmann, K. Kolinsky, S. Schmid, D. Schraudner, A. Both, A. Harth, Solid proof of concept in an enterprise loan request use case (2022). URL: https://publica.fraunhofer.de/handle/publica/445586.

[9] J. Bingham, E. Prud'hommeaux, E. Pavlik, Solid Application Interoperability. W3C Editor's Draft. Nov. 2023, ???? URL: https://solid.github.io/data-interoperability-panel/specification.

[10] M. M. Hughes, Remedying financial abuse by agents under a power of attorney for finances, Marquette Elder's Advisor 2 (2012) 39. URL: https://api.semanticscholar.org/CorpusID:37730572.