A shared responsibility model to support cross border and cross organizational federation on top of decentralized and self-sovereign identity: Architecture and first PoC

Michael Kubach[1], Isaac Henderson[2], Bithin Alangot[3], Theo Dimitrakos[3], Juan Vargas[2], Matthias Winterstetter[2], and Ioannis Krontiris[3]

Abstract: This paper discusses the challenges of transitioning from legacy federated identity systems to emerging decentralized identity technologies based on self-sovereign identities (SSI) and verifiable credentials, which are being used in initiatives such as Gaia-X and Catena-X for secure and sovereign data sharing. The adoption of SSI and decentralized identity technologies requires a standardized reference model that addresses challenges around trust in cross-border and cross-organizational federations based on decentralized identities. To facilitate this transition, the paper proposes a new Fed2SSI architecture that introduces a middle layer of abstraction for the policy-based transformation of credentials, enabling interoperability between legacy federated identity solutions and SSI/decentralized identity environments. The architecture is implemented in a prototype and an exemplary use case is presented to illustrate the added value of this approach.

Keywords: self-sovereign identity, ssi, decentralized identity, data spaces, gaia-x, verifiable credentials, trust infrastructure, trust policy, federated identity.

1 Introduction

Identity and access management solutions currently widely in productive use are based on federated protocols like OpenID Connect, SAML 2.0 and LDAP. Major identity management (solution) providers have invested in such identity solutions. Small and medium-sized enterprises (SMEs) and large enterprises alike use those solutions in their productive environments and are hesitant to switch to emerging decentralized identity technologies based on decentralized identifiers [W322a] and verifiable credentials [W322b] (also known as Self-sovereign Identities - SSI). These technologies are rather new, could bear risks and a switch would require significant investments. Moreover, SSI and decentralized identity have yet to overcome some challenges, for example with regards to automated authorization and trust management, even though solutions for these challenges are being developed, such as [JCK22].

Still, SSI and decentralized identity are promoted by the European Commission as part of

[1] Fraunhofer IAO, Nobelstr. 12, Stuttgart, 70569, firstname.lastname@iao.fraunhofer.de

[2] University of Stuttgart, Institute of Human Factors and Technology Management (IAT), Nobelstr. 12, Stuttgart, 70569, firstname.lastname@iat.uni-stuttgart.de

[3] Huawei Technologies Düsseldorf GmbH, German Research Center, Munich, Germany, firstname.lastname@huawei.com

cbe doi: 10.18420/OID2023_08

their digital strategy for Europe through initiatives like EBSI ESSIF [Es00] and the EU Digital Identity Wallet (EUDI) [Eu22]. Cloud and data spaces initiatives like Gaia-X [Ga00], GXFS [Gx00] and Catena-X [Ca00] use to a large extent SSI/decentralized identity and Verifiable Credentials for their identity and access management. Data spaces[4] are ecosystems for secure and sovereign data sharing and exchange with the goal of value creation via standardized connections across organizational boundaries. This requires a high level of security, control, and trust – but also easy adoption in order to reach a critical mass of participating entities. A standardized reference model is supposed to facilitates this. The core of the underlying concept is the linkage of data and usage conditions and their organizational and technical processing and enforcement. Data spaces follow a partly federated, partly decentralized architecture - trusted entities act as intermediaries, e.g. as metadata broker or clearing house, while data is exchanged directly between the participants without the need for a third party or a central data store [PSB22].

Hence, for the broad adoption and success of these initiatives, but also to make their potential available to SMEs as well as large enterprises, the transition from legacy federated identity systems to SSI and decentralized identity has to be facilitated. For this, an innovative architecture has to be specified that addresses the novel challenges around trust in cross border and cross organizational federations based on decentralized identities.[5] This architecture forms a credentials bridge that transforms credentials between different domains of trust and/or credential formats. For evaluation purposes, a proof of concept demonstrating the viability of this solution has to be developed.

Our approach is as follows. The newly developed Fed2SSI architecture introduces a middle layer of abstraction for the policy-based transformation of credentials. This layer, called the credentials bridge, enables interoperability between legacy federated identity solutions and verifiable credential-based SSI/decentralized identity environments. The policy-based approach in the credentials bridge enables to build a shared responsibility model [Ba21] to manage credentials across different stakeholders and makes the transformation of the credentials dynamic in nature to satisfy different use-case as well as trust domain requirements. In addition, the credentials bridge can be easily adopted to new use-cases with ease due to the configurable nature of its architecture and policy-based approach [Ba21]. Moreover, it leverages the TRAIN approach to establish and manage trust [JCK22]. This architecture is implemented in a proof-of-concept prototype (supporting Open ID Connect) and will be evaluated for different use cases in a federated data cloud context. The evaluation of the developed technology ensures its maturity and the actual applicability in different areas. Developed software components will be published under an Open-Source license.

The remainder of this paper is structured as follows. In section two we present related work and approaches. After that, section three presents the Fed2SSI architecture. Section

[4] A uniform notation for data spaces or dataspaces has not yet emerged. In this document we will use the notation that used in the respective reference or component. We use “data spaces” for our own thoughts.

[5] The challenge to establish trust across different domains or boundaries in electronic transactions has of course been identified well before and goes beyond decentralized identities [Unec18].

four describes an exemplary use case and the proof of concept that is currently being developed in an ongoing project. Section 5 closes the paper with a conclusion.

2 Background and related work

Particularly in the context of the International Data Spaces (IDS) [In00] as well as Gaia-X and Catena-X there have been related initiatives. As Fed2SSI aims to complement them, we will mention the most important ones for our concept in the following section. Moreover, Fed2SSI builds on other already existing elements in the context of trust management such as UCON+ with ALFA Policies and the TRAIN trust management infrastructure. Hence, these building blocks will also be briefly described.

2.1 International Dataspace Connectors

The Eclipse Dataspace Components (EDC) contain a connector component to provide a generic way to connect to a dataspace and exchange data. It is stated that the EDC will implement the International Data Spaces standard as well relevant protocols and requirements associated with Gaia-X. The EDC is supposed to provide capabilities for discovering, connecting, automated contract negotiation, policy enforcement, and auditing processes. The EDC allows organizations to exchange data compliant to rules and policies of Gaia-X while Catena-X uses it to build a data space between participants. Identity management can be either centralized or decentralized via Dynamic Attribute Provisioning Service (DAPS, see below) or WEB-DID [Ec21]. The EDC and other Dataspace Connectors are based on the Dataspace Connector (also IDS Connector) [Fr00].

The FIWARE TRUE Connector (FTC) is a connector to the International Dataspace ecosystem for the FIWARE ecosystem that claims to be compliant with the latest IDS specifications as well. It interacts with specific identity providers and the DAPS [FI00].

2.2 Identity Hub and DAPS

To deliver DID-based Verifiable Credentials and Verifiable Presentations, dataspace issuers and dataspace participants can use an Identity Hub (sometimes also written IdentityHub). It acts as decentralized credential storage and message relay system that is run by a part of a dataspace [Ec22]. As it builds on verifiable credentials and DIDs only, additional integration work is required for legacy systems that do not yet support this approach.

The Dynamic Attribute Provider Service (DAPS) is the central component of the International Dataspaces Identity Provider. The DAPS delivers a JSON web token (JWT) for authentication ad a IDS connector (the DAT Token) [Id21]. It allows for the dynamic enrichment of identity with additional attributes. In contrast to Identity Hubs it is a centralized identity management system based on certificates. Using DAT Tokens, dynamic permissioning for services is possible. For integration into legacy systems, additional work is required, as no bridge-like transformation of credentials is offered.

2.3 UCON+ with ALFA policies

UCON+ (from UCON for Usage Control), as presented by [Di20], is a new model, policy language and architecture for trust aware continuous authorization. While conventional UCON supports only contextualization and authorization sessions, UCON+ aims to fulfil the need for continuous multi-sensor authentication, trust level evaluation and authorization in an IoT environment and to be flexible and modular. The policy language of UCON+ is ALFA (Abbreviated Language For Authorization), a pseudocode domain-specific policy language, mapping into XACML but more human readably, which comprises both access control and usage control rules [Oa15]. It can be used to define credential mapping as well as usage control policies. UCON+ together with ALFA policies furthermore allow for the creation of administrative and delegation policies. These policies can administer and delegate the right and responsibility for creating further policies to other employees of an organization, thus sharing responsibility. This also allows the recreation of business logic through policies and provides a high degree of configurability and adaptivity in the identity mapping and administrating process which would otherwise require additional manual or coding effort. All this makes UCON+ well-suited for industrial dataspace application scenarios that require for example a dynamic mapping of credentials to permissions.

2.4 TRAIN

TRAIN for “TRust mAnagement Infrastructure” was developed in the EU NGI eSSIF-Lab project [Es22]. It makes use of the global, well-established, and trusted infrastructure of the Internet Domain Name System DNS as its root of trust (with DNSSEC). The basic technology used by TRAIN had already been developed and validated in several pilots of the EU LIGHTest project (which developed the general context for trust in digital transactions). TRAIN addresses the issue of establishing trust in certain institutions in the SSI ecosystem beyond the trust achieved mainly through cryptographic means. An example would be the verification of the credibility of credential issuers, e.g., to find out whether the credential issuers really are who they claim to be through publication and query of list of trustable issuers. Using TRAIN, the entity has the possibility of subscribing to one or several trust frameworks that can be defined by trustworthy institutions (the roots of trust), thereby giving the entity the opportunity to verify the credibility of other entities. This approach is decentralized and not limited to a certain identity concept – so it is compatible with the decentralized VC/ DID-approach as well as with legacy IdM systems.

2.5 Related initiatives combining FDC with Verifiable Credentials

The OIDC Bridge [Oi00] developed by MATTR seeks to solve a similar challenge as the credentials bridge that is proposed in this paper. Its goal is to bridge the worlds of federated OIDC environments to the decentralized digital trust environment of SSI. To achieve this, the OIDC Bridge connects OIDC to the emerging decentralized web standards using the MATTR VII and the MATTR Wallet app. While the OIDC Bridge and the credentials bridge are aligned with their goals to a certain degree. The credentials bridge seeks to go beyond OIDC to SSI, supporting more credential/protocol formats and providing additional value in the dynamic transformation and flexible configuration area by using ALFA policies as well as supporting the integration of different trust frameworks though the TRAIN concept.

The Authentication Authorization Services (AAS) component of Gaia-X [Ga23] has also recognized the importance to bridge between SSI-based authentication and the established OpenID Connect specification for authentication and request of claims including related proofs using SSI OIDC and SSI SIOP [Op22] brokers. Moreover, the Open ID Connect specification OIDC4VP [Te00] extends OpenID Connect with the support for the presentation of claims via W3C Verifiable Credentials.

3 Fed2SSI credentials bridge architecture

With the Fed2SSI architecture we present a credentials bridge that integrates UCON+ with ALFA policies and TRAIN to complement the aforementioned IDS connectors and Identity Hub and DAPS approaches. The goal is to transform the credentials of an entity with a legacy federated identity management system to verifiable credentials / presentations in order to interact with a such a consumer, e.g., from a dataspace context, who follows a verifiable credential-based identity management. For a high-level architecture of the Fed2SSI bridge in a dataspace context for an exemplary use case scenario please refer to figure 2 (section 4.3).

The credentials bridge helps to bridge credentials, that can be of different formats, across different trust domains or ecosystems based on the rules set by a common Trust Framework. An example could be the Gaia-X Trust Framework and the necessary integration of the Gaia-X Federation Services with the Trust Framework as elaborated in the GXFS IDM & Trust Architecture [Gx21] that could be achieved with the credentials bridge. The bridge can be deployed and configured as an Identity Hub (in the cloud) that provides sovereignty at different levels such as individual, organizational, or even on a state level. The credential exchange and transformation are policy based, with UCON+ as policy engine for ALFA policies that can be flexibly used for configuration according to the use case and the respective requirements of a specific dataspace or Gaia-X federation. Federated credentials (for the proof of concept these are OIDC Tokens, due to the modular design other tokens/credential types are possible) are transformed into verifiable credentials (W3C JSON-LD) based on user defined rules and obligations expressed in

ALFA policies. TRAIN is used to establish trust through integrating different decentral trust anchors via lists of trusted entities that are operated under trust frameworks that can be configured according to the requirements of the respective domains.

The credentials bridge facilitates the integration into new trust domains such as new data spaces through easy configurability on several levels and avoids the otherwise necessary implementation of new domain specific features and additional development efforts. ALFA policies can be used to configure the credentials bridge and replicate business logic related to identity transformation. This means that by administrative and delegative policies can for example replicate a hierarchy and connected authorizations in a company. These can then be change dynamically if this is needed – without coding and with minimal efforts for configuration. Moreover, using ALFA Policies, administrators can easily define, based on their trust requirements, which claims are to be extracted from the credentials or tokens that are transformed and which claims are to be included into the credential subject of the verifiable credential and/or the verifiable presentation. Moreover, the bridge can be configured between using an internal verifiable credentials issuer and an external one. Specific metadata to be included into the verifiable presentation can be defined as well. Finally, admins can pre-define policy templates (depending on use case or Data Spaces requirements) and pre-install them for the user to comfortably configure them and update the bridge via the GUI in one click.

Leveraging TRAIN, the credential bridge can be configured to evaluate the inclusion of entities into specific trust frameworks. Through TRAIN, different trust anchors can be integrated, e.g., to verify the inclusion of a verifiable credential issuer into a specific trust framework (e.g., membership in a certain GAIA-X Federation or Data Space).

4 Exemplary use case and proof of concept

A first illustrative use case in a data space environment is behind the following scenario that can be facilitated through Fed2SSI. Other, more complex use cases for Fed2SSI are currently being developed and evaluated but omitted here due to the restricted space that is available.

4.1 Exemplary use case scenario

A hotel guest arrives with his own car at a hotel and the hotel valet takes over the car to drive it to the parking space. The parking space is provided by the municipality and is located outside of the hotel grounds. Before the hotel valet can drive the car over there, he accesses the municipal parking system to locate and reserve a free parking spot. The following figure illustrates the use case.

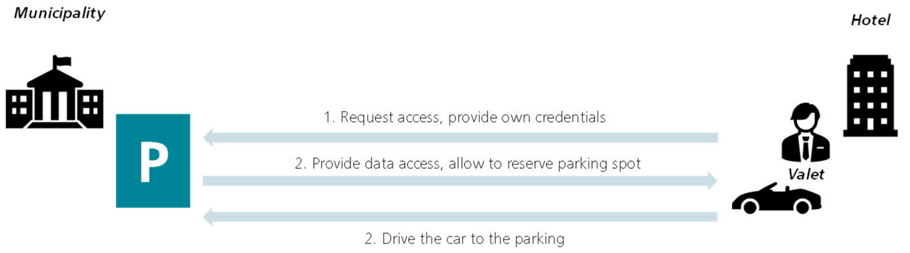

Municipality
Hotel
P
1. Request access, provide own credentials
2. Provide data access, allow to reserve parking spot
Valet
2. Drive the car to the parking

Figure 1: Exemplary use case scenario: Hotel Valet

4.2 Data Spaces setup and challenges

The hotel and the municipality are both part of the Mobility Data Space and are running Connectors (in this case EDC connectors) to exchange credentials. Each entity (hotel and municipality) in the Mobility Data Space has its separate identity management and issues their own credentials (this means they are part of different trust domains). The hotel is a consumer of the data, the municipality provides data, the valet of the hotel is the user. The data exchange happens only after check of trustworthiness of credentials provided by consumer, and via Connectors.

The scenario in this data spaces setup illustrates the following challenges that are encounter without the Fed2SSI bridge. Currently, the provision of a valet credential issued by the hotel proving that the valet is an eligible employee of the hotel according to the trust requirement defined by the municipality is currently not possible. This would require a trust establishment across organizational boundaries so that individual users behind connectors (here: the valet) can use their own credentials to communicate across trust domains (here: to the municipality). The trust frameworks of the different domains are not connected. Hence, the valet would need a new credential from the data provider without the Fed2SSI bridge. This then increases the efforts for identity life cycle management (e.g., in the case of revocation) – which induces higher costs and/or increases the risks of the overall interaction. Further requirements of the setup might be that the valet has to provide additional credentials to be allowed to drive the car over public roads to the parking. If this should be requested and provided in an automated manner, this is not possible in the described setup.

This illustrates that without the Fed2SSI bridge there are significant adoption costs and risks related to limited (trust) interoperability and lack of automation and easy configurability.

4.3 The PoC in the use case

The figure on the next page illustrates the role of our proof of concept implementation in the use case scenario that was presented above. This scenario could take place in a

Mobility Data Space. The connection to the data space could be realized via the EDC. The Fed2SSI credentials bridge is placed between the EDC connectors in order to bridge over the trust frameworks that are behind the respective connectors. It transforms OIDC tokens (traditional federated IdM-approach) to W3C JSON-LD Verifiable Credentials (decentralized IdM-approach) based on user-defined ALFA policies that are executed in UCON+. The bridge used data extracted from the OIDC token to configure the bridge PIP (Policy Information Point).

The configurability of the bridge is facilitated through a Policy Configuration GUI that is shown in the screenshots on the following page. The hotel and the municipality can use the GUI to configure policies. Those ALFA policies can be pre-defined through templates that accommodate the requirements of different trust domains (e.g., different data spaces or use cases). The policy fields change dynamically based on the user input. With the GUI a user without any programming skills can display a policy, change policy attributes, and specify the targeted credentials bridge. With one simple click, the policy is installed on the bridge.

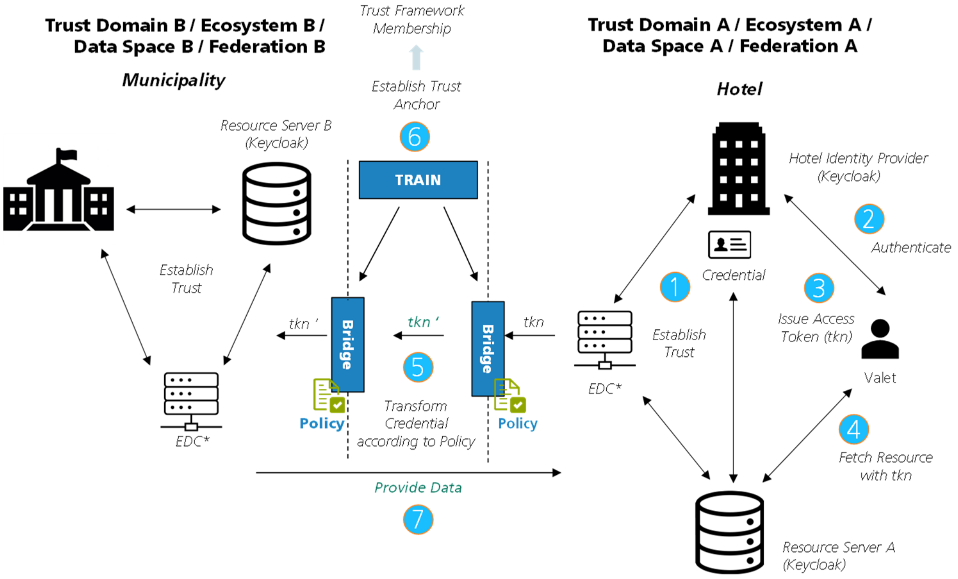
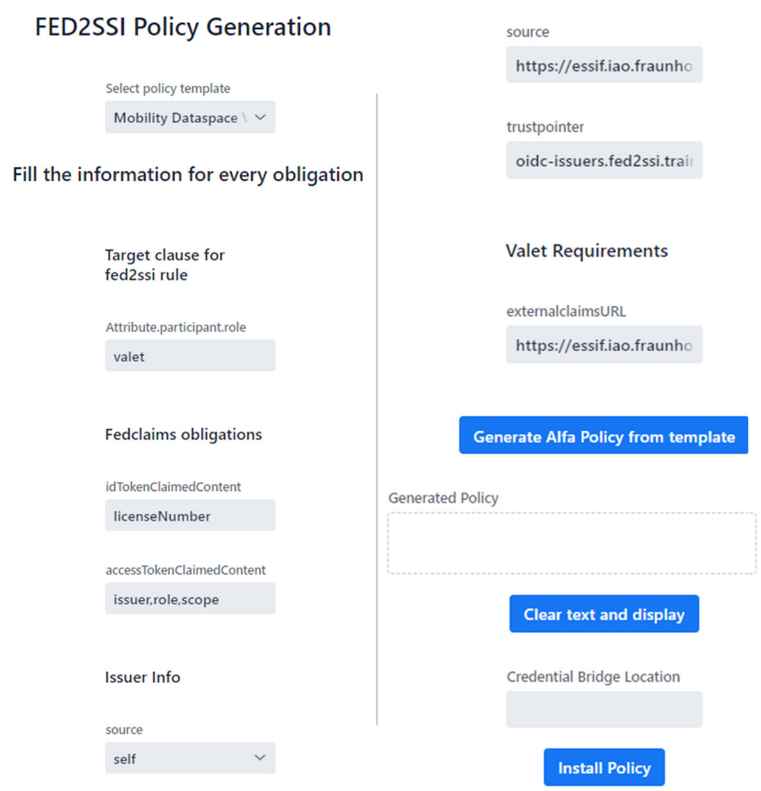

Trust Domain B / Ecosystem B /
Data Space B / Federation B
Municipality
Trust Framework Membership
Establish Trust Anchor
Trust Domain A / Ecosystem A /
Data Space A / Federation A
Hotel
Resource Server B (Keycloak)
6
TRAIN
Hotel Identity Provider (Keycloak)
2
Authenticate
Establish Trust
Credential
1
3
Issue Access Token (tkn)
tkn '
tkn '
tkn
Bridge
Bridge
5
Establish Trust
Valet
EDC*
EDC*
Policy
Policy
Transform Credential according to Policy
4
Fetch Resource with tkn
Provide Data
7
Resource Server A (Keycloak)

Figure 2: The Fed2SSI bridge in an illustrative use case scenario in the Mobility Data Space

The TRAIN component is used to verify the inclusion into a trust framework that can be defined according to the respective requirements. For this, the Terms of Use Attribute according to the W3C definition of Verifiable Credentials [W322b] is used to embed a Trust Scheme/Framework Pointer. This pointer can be pre-configured and fetched from policies. Inclusion into multiple trust frameworks can be considered at the same time and TRAIN is also expandable to consider other formats to manage trust frameworks than the currently used XML trust lists according to ETSI standard via DNSSEC (e.g., to consider

EBSI Ledger Trusted Issuer Lists).



FED2SSI Policy Generation

Select policy template

Mobility Dataspace \

Fill the information for every obligation

Target clause for fed2ssi rule

Attribute.participant.role

valet

Fedclaims obligations

idTokenClaimedContent

licenseNumber

accessTokenClaimedContent

issuer,role,scope

Issuer Info

source

self

source

https://essif.iao.fraunho

trustpointer

oidc-issuers.fed2ssi.trai

Valet Requirements

externalclaimsURL

https://essif.iao.fraunho

Generated Policy

Credential Bridge Location

Figure 3: Screenshots showing the Fed2SSI credentials bridge Policy Configuration GUI

4.4 Added value of the Fed2SSI credentials bridge in the use case

From a merely technical standpoint, the credential bridge helps to bridge credentials of across different trust domains/Ecosystem based on the rules set by common trust frameworks. Moreover, it allows for the real-time transformation of credentials between OIDC ID-Tokens and W3C JSON-LD Verifiable Credentials based on requirements from the provider (current implementations, other identity token / credential formats are foreseen). The transformation of the credentials is based on the usage policies expressed in ALFA.

Focusing on trust, the credentials bridge establishes trust using decentralized trust anchors integrating different trust frameworks via TRAIN. Data consumer and provider can sovereignly decide on their own trust anchors and pre-configure them. The trust automation through UCON+ allows for credential mapping and usage control policies to transform credentials according to the trust requirements of the respective use case and trust domain.

From a business perspective, the increased interoperability increases the flexibility of data provider and data consumer. New use cases and trust domains can be easily added and require minimal integration efforts as the mapping logic can be defined by administrators using policies instead of having to integrate new features and writing code by programmers. Hence, adoption costs are significantly reduced due to lower setup-efforts for complex manual configuration and implementation of identity solutions currently not supported. Furthermore, maintenance costs are reduced as credential lifecycle management is simplified. This is also related to a reduction in risk-induced costs from more consistent lifecycle management – e.g., due to facilitated revocation.

5 Conclusion

The presented solution is a shared responsibility model that supports cross border and cross organizational federation on top of decentralized and self-sovereign identity (SSI). Its major component is a policy-based identity and trust middleware that automates the issuance, verification, and exchange of identity credentials between SSI/decentralized identity and federated identity management solutions. Legal aspects, such as compliance with eIDAS 2.0 and GDPR and statements of the quality level of the credentials (LoA) after the transformations are beyond the scope of this paper. Those aspects are nevertheless highly relevant and are to be demonstrated in future iterations of the proof of concept.

Already in the current version, policies are leveraged to automate authorization as well as trust management, to include administrative requirements and delegation of authority. The Fed2SSI approach demonstrates how the coexistence of legacy centralized identity technologies with emerging decentralized SSI solutions can be made feasible. Weak spots of current SSI/decentralized identity solutions around automated authorization and trust management are addressed. Finally, Fed2SSI lowers the costs and risks of adoption for new data spaces such as Gaia-X that build on SSI and decentralized identity management.

Future work will focus on a further refinement of the use cases for the proof of concept of the credentials bridge that allow for further development and testing. We will concentrate our efforts on data spaces and evaluate the added value of Fed2SSI in this context. The goal is also to offer the solution to the wider data spaces community, to discuss it with them and work towards standardization. The components of the proof of concept will be developed further, for example through additional features of the GUI and potentially the bridging between additional credential/token formats beyond OIDC to SSI. The architecture already allows for this and it can be realized by developing respective modules.

Bibliography

[Ba21] Bandopadhyay, S., Dimitrakos, T., Diaz, Y., Hariri, A., Dilshener, T., La Marra, A., Rosetti, A.: Datapal: data protection and authorization lifecycle framework. In: 2021 6th south-east Europe design automation, computer engineering, computer networks and social media conference, pp. 1-8, 2021.

[Ca00] Catena-X: Catena-X Automotive Network/ Catena-X, https://catena-x.net/, accessed: 08/02/2023.

[Di20] Dimitrakos, T., Dilshener, T. Kravtsov, A., La Marra, A., Martinelli, F., Rizos, A., Rosetti, A., Saracino, A.: Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communication (TrustCom), pp. 1801-1812, 2020.

[Ec21] Ecplipse Foundation, Maria Teresa: Eclipse Dataspace Components, https://projects.eclipse.org/projects/technology.edc, accessed: 10/02/2023.

[Ec22] Eclipse EDC: GitHub, https://github.com/eclipse-edc/IdentityHub/tree/ main/docs/ developer/decision-records/, accessed: 13/02/2023.

[Es00] ESSIF-LAB: Help Shape a Safe and Secure Next Generation Internet, https://essif-lab.eu, accessed: 01/03/2021.

[Es22] ESSIF-LAB: eSSIF-TRAIN by Fraunhofer Gesellschaft. eSSIF-Lab, https://essif-lab.eu/essif-train-by-fraunhofer-gesellschaft/, accessed: 11/02/2022.

[Eu22] European Commission: European Digital Identity Wallet. Shaping Europe´s digital future, https://digital-strategy.ec.europa.eu/en/funding/european-digital-identity wallet, accessed: 19/08/19.

[Fi00] Fiware True Connector: Welcome to Fiware True (Trusted Engineering) Connector, https://fiware-true-connector.readthedocs.io/en/latest/index/html, accessed: 10/02/2023.

[Fr00] Fraunhofer ISST: Dataspace Connector, https://international-data-spaces-association.github.io/DataspaceConnector/, accessed: 10/02/2023.

[Ga00] Gaia-X: Home Gaia-X. A Federated and Secure Data Infrastructure, https://gaia-x.eu/, accessed: 08/02/2023.

[Ga23] Gaia-X: Gaia-X. Data-Infrastructure Federation Services/AuthenticationAuthorization. GitLab, https://gitlab.com/gaia-x/data-infrastructure-federation-services/authentication authorization, accessed: 15/03/2023.

[Gx00] GXFS: Gaia-X Federation Services, https://www.gxfs.eu, accessed: 08/02/2023.

[Gx21] GXFS.eu: GXFS-IDM & Trust: Architecture Overview, https://www.gxfs.eu/download/3397/, accessed: 15/03/2023.

[Id21] IDSA: Identity Provider, https://international-data-spaces-association.github.io/ DataspaceConnector/CommunicationGuide/v6/IdsEcosystem/IdentityProvider, accessed: 13/02/2023.

[In00] International Data Spaces. International Data Spaces Association, https://internationaldataspaces.org/, accessed: 10/02/2023.

[JCK22] Jeyakumar, I.H.J., Chadwick, David W., Kubach, M.: A novel approach to establish trust in verifiable credential issuers in self-sovereign identity ecosystem using TRAIN. In: Roßnagel, H., Schnuck, C.H., Mödersheim, S. (ed.), Open Identity Summit 2022, Gesellschaft für Informatik e.V., pp. 27-38, 2022.

[Oa15] OASIS: Abbreviated Language for Authorization Version 1.0.

[Oi00] OIDC Bridge, https://learn.mattr.global/docs/platform/extensions/oidc-bridge/overview, accessed: 08/02/2023.

[Op22] OpenID Connect: Self-Issued OpenID Provider v2, openid-connect-self-issued-v2-1_0-07, https://openid.net/specs/openid-connect-self-issued-v2-1_0html.

[PSB22] Pettenpohl, H., Spikermann, M., Both, J.R.: International Data Spaces in a Nutshell. In: Otto, B., Ten Hompel, M., Wrobel, S. (ed.): Designing Data Spaces: The Ecosystem Approach to Competitive Advantage, Springer International Publishing, pp. 29-40, 2022.

[Te00] Terbu, O., Lodderstedt, T., Yasuda, K., Lemmon, A., Looker, T.: OpenID Connect for Verifiable Presentations, https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0.html., accessed: 16/05/2022.

[Un18] UNECE Executive Committee: White Paper on Trusted Transboundary Environment: Ensuring Legally Significant Trusted Trans-Boundary Electronic Interaction.

[W322a] W3C: Decentralized Identifiers (DIDs) v1.0, W3C Recommendation, https://www.w3.org/TR/did-core/, accessed: 08/02/2023.

[W322b] W3C: Verifiable Credentials Data Model v1.1., W3C Recommendation, https://www.w3.org/TR/vc-data-model/, accessed: 16/06/2022.