Synergizing Trust and Autonomy: Gaia-X Enabled Multi-Agent Ecosystems for Advanced Freight Fleet Management

Dennis Maecker[1][0009-0005-8932-0477], Felix Harenbrock[2][0009-0004-8510-1130], Henning Gösling[1][0000-0003-4522-0464], Timon Sachweh[3] and Oliver Thomas[1]

[1] German Research Institute for Artificial Intelligence, Osnabrück, Germany
{dennis.maecker, henning.gösling, oliver.thomas}@dfki.de
[2] embeteco GmbH & Co. KG, Rastede, Germany
fh@embeteco.de
[3] TU Dortmund University, Dortmund, Germany
timon.sachweh@tu-dortmund.de

Abstract. This paper explores the integration of the Gaia-X framework into a Multi-Agent System (MAS) for managing a smart freight fleet, emphasizing identity and trust management. Focusing on a subsystem of delivery agents and autonomous robots, this study exemplarily illustrates how Gaia-X can be integrated in existing ecosystems consisting of software agents and appertaining services and assets. By utilizing Organizational Credential Managers (OCMs), mediator services and wallets, the paper addresses the challenges of credential management and connectivity for mobile edge devices like delivery robots. This integration showcases the potential of Gaia-X to improve the security and interoperability of smart freight systems, contributing to the advancement of trusted digital ecosystems in the logistics sector.

Keywords: Multi-Agent System, Autonomous Parcel Delivery, Data Ecosystems, Gaia-X, Smart Managed Freight Fleet.

1 Introduction

The increasing demands on logistics due to the rise of e-commerce highlight the need for innovative solutions in last-mile delivery. Multi-Agent Systems (MASs) emerge as a viable solution, leveraging decentralized networks of autonomous delivery robots and other logistics assets to enhance delivery efficiency and adaptability in dynamic environments. These systems facilitate real-time decision-making and optimize delivery routes, addressing the complexities of urban logistics.

However, the decentralized nature of MASs, coupled with the diversity of stakeholders in the logistics ecosystem, presents challenges in data exchange, identity management, and trust. The introduction of the Gaia-X framework [3, 10] into MASs addresses these challenges by establishing a secure, interoperable, and transparent data infrastructure, ensuring data sovereignty and fostering trust among participants. Gaia-X's alignment with European values on data privacy and security further enhances the framework's suitability for complex logistics operations, providing a robust foundation for data exchange and collaboration within the MAS.

This paper specifically focuses on a subsystem involving delivery agents and autonomous robots. By delving into the technical aspects of integrating Organizational Credential Managers (OCMs), mediator services, and digital wallets, the study elucidates the mechanisms through which Gaia-X facilitates interaction between agents and freight assets, ensuring secure credential management and reliable connectivity for mobile edge devices.

The paper begins with an introduction to a concept of a Multi-Agent System (MAS) for smart freight management, focusing on the subsystem involving delivery robots (Section 2). It proceeds to discuss the Gaia-X framework, emphasizing its significance in enhancing trust and identity within the system. The Hyperledger Aries protocol is examined for its role in secure communications. Following this foundation, the paper details the proposed solution (Section 3), incorporating Organizational Credential Managers (OCMs), digital wallets, and mediator services to address the subsystem's challenges. The discussion (Section 4) assesses the implication of this work and outlines potential future developments, suggesting directions for advancing the integration of Gaia-X in MASs for logistics.

2 Background

This section first outlines the specific MAS that has been developed within the research project and which serves as an example case for elaborating the introduction of the Gaia-X framework. Subsequently, the Gaia-X framework is introduced, focusing on the topics of digital identities and the required technologies.

2.1 The MAS Applied to Freight Fleet Management

The MAS that is used as an application case in this work was conceptualized within the Gaia-X 4 ROMS project, a consortium research endeavor dedicated to the application-oriented establishment of a connected and automated fleet management concept based on fleet assets along intermodal transport chains for parcel deliveries [12, 16]. Therein, a MAS enables the decomposition of complex problems and efficient distribution of both data and control across physical boundaries. The agents in the MAS are envisaged to be deployed on a decentralized server infrastructure. This innovative concept developed in the consortium research project is currently being realized through active collaboration with practitioners and software companies in the transportation sector, ensuring practical applicability and industrial relevance. In a business-focused point of view, the MAS under development can be regarded as a Software-as-a-Service (SaaS) solution, offering the smart management of freight assets not only to carriers of vehicle fleets (e.g., parcel delivery robots, telematics-enabled trailers, and swap-bodies), but also to operators of logistics infrastructure (e.g., workshops and depots). Within the system, agents coordinate tasks, such as parcel delivery orders, using the contract net protocol [20, 29]. Furthermore, the MAS is dependent on auxiliary services, such as Estimated-Time-of-Arrival (ETA) services, routing services as well as platforms for stakeholder interaction, such as operator cockpits or booking platforms for clients. The workshop agent further interfaces with the workshop staff by so-called Freight-Fleet-Glasses, an augmented-reality solution [11]. The corresponding MAS is depicted below in Figure 1 together with its interfacing assets and service that are embedded with the MAS into a Gaia-X ecosystem. Hence, each interaction between agents of the MAS and external services and assets has to adhere to Gaia-X standards. In the further course of this work, elaborating the integration of Gaia-X services in this system, we will focus on the subsystem consisting of the parcel delivery robot (PDR) and its corresponding PDR agent to propose an exemplary solution to the Gaia-X requirements regarding identity and trust.

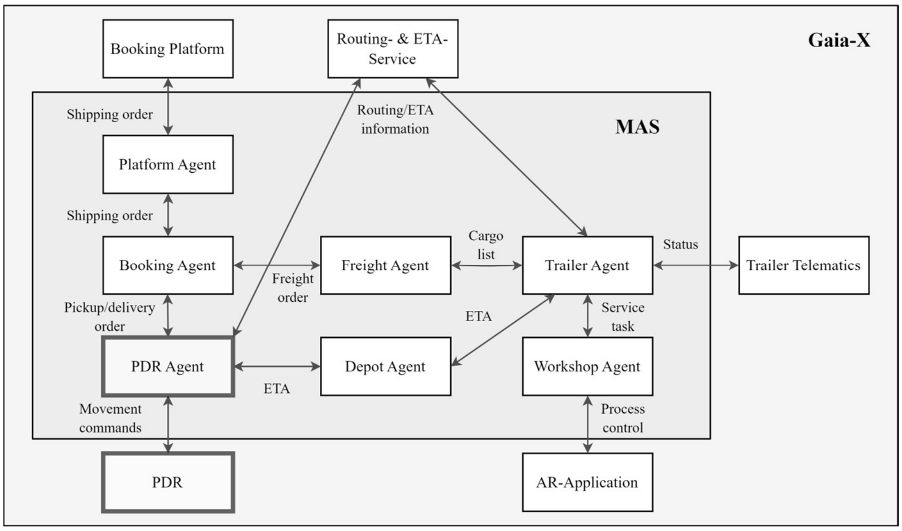

Fig. 1. The different types of software agents comprising the MAS developed in the consortium research project. Further depicted are the external services and platforms that are embedded into a Gaia-X ecosystem with the MAS. Highlighted is further the subsystem considered in this work, consisting of PDR and PDR agent.

2.2 Trust and Identity within the Gaia-X Framework

Gaia-X is a European initiative aimed at fostering innovation through data sharing, emphasizing data sovereignty, privacy, security, and interoperability [13, 25]. The project seeks to build trust within decentralized ecosystems through a trust framework that sets minimum participation requirements, ensuring shared governance and interoperability while giving users full control over their decisions. Cross Federation Service Components (XFSC) serve as the technical backbone, providing essential services and standards to facilitate secure collaboration among federations [7, 8].

Gaia-X aims to establish a secure and trustworthy digitalization framework by embracing the Self-Sovereign Identity (SSI) model [15], which allows individuals, organizations, or machines to manage their digital identities and credentials autonomously, without relying on centralized identity management systems. At the core of Gaia-X's SSI framework is the concept of Decentralized Identifiers (DIDs) [21], which are globally unique identifiers for entities within the ecosystem. These DIDs, along with Verifiable Credentials (VCs) [22], enable entities to maintain control over their identifiers and associated key materials, thereby enhancing privacy and security.

The Organizational Credential Manager (OCM) is a technology designed to establish trust among various participants in the decentralized ecosystem by managing the digital identities of participants [2]. It encompasses all trust-related functions necessary for managing and offering Gaia-X self-descriptions in the W3C Verifiable Credential format, covering tasks such as creating verifiable credentials with digital signatures, issuing verifiable presentations, and validating connection requests.

Wallets in general, which also encompass the OCM, serve as secure storage for digital credentials, empowering individuals, and autonomous devices to independently manage their identities [24]. This autonomy is crucial, as it enables entities to share only the necessary credential information with relevant applications, ensuring privacy and minimizing data exposure. The flexibility of wallet solutions, ranging from mobile apps to cloud-hosted options [17], facilitates tailored and secure interactions within digital environments, without the need for centralized identity providers.

In decentralized networks, mediators enhance the robustness of communication by addressing dynamic addressability challenges [4, 9]. They facilitate reliable message delivery across devices or agents with variable network endpoints, ensuring consistent connectivity within the Gaia-X framework. This function is especially critical for edge devices, enabling their effective participation in the ecosystem without being hindered by fluctuating network conditions.

As one option for implementing the services, the Hyperledger technology is a viable option as it represents an open-source framework based on the SSI concept. Hyperledger Aries offers the protocols and tools for secure peer-to-peer communication and credential exchange [5], while Hyperledger Indy provides the blockchain infrastructure for decentralized identity management [1]. As a recent development, the Aries Askar implementation was introduced, representing a more performant and stable solution as compared to Indy [23, 26].

3 Integration of Gaia-X Services into the MAS

This chapter details the integration of Gaia-X services into the outlined MAS for parcel delivery, focusing on the fundamental workflow in digital identity management. It covers the identification of essential technologies and services, the establishment of secure connections, the issuing and managing of digital credentials, and the verification process to ensure the integrity and validity of these credentials within the network.

3.1 Identification of Services and Technologies

Regarding the subsystem that is considered in this work, consisting of a PDR and a PDR agent, it is first required to identify the necessary Gaia-X services that need to be deployed. As both the MAS and the fleet carrier for delivery robots represent different organizations, it is necessary to employ an OCM for each participant. This OCM then manages the credentials for each entity of the respective organization. Being developed within the Gaia-X project and building on the Hyperledger Aries framework, the OCM-engine implementation by the company Vereign was used [28]. This implementation is publicly available and comes preconfigured for connecting with the Hyperledger Indy test ledger BCovrin[1], developed by the Government of British Columbia. Further, the OCM provides an extensive REST interface for interactions with the instance, such as for example the creation of credentials.

As the PDRs represent autonomously acting entities, each of them needs to be equipped with its own wallet to store its respective VCs. As a useful wallet technology, the Hyperledger Aries Cloud Agent Python (ACA-py) was determined, a Python wrapper for a light-weight Aries wallet agent [14]. ACA-py was initially developed by the same institution as the distributed test ledger and provides a similar API as compared to the OCM-engine, facilitating the interaction and data exchange.

As stated before, the physical PDR units act in a dynamic network environment, hence necessitating a solution for reliable connectivity and addressability. To address this, a mediator service needs to be deployed, that relays all messages between the OCM of the PDR fleet carrier to the respective wallets integrated on the PDR units. Here, the implementation of the mediator by Vereign is being further considered [27].

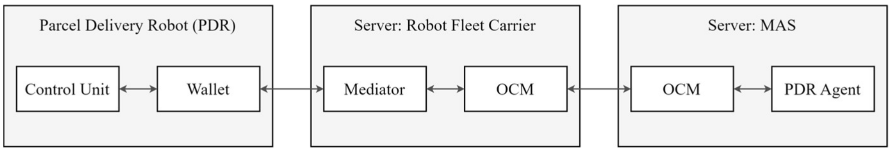

Fig. 2. Architectural overview of the Gaia-X compatible services to be integrated in the considered subsystem consisting of several environments, i.e., different servers and the PDR.

The overall architecture is depicted in Figure 2. On the server that runs the MAS, the PDR agent interfaces with the appropriate OCM for credential management tasks. The OCM instance running on the server of the robot fleet carrier needs to be able to connect to the mediator instance for interfacing the robot's wallet as well as to the OCM instance on the MAS server in order to enable for instance the exchange of credentials in a later step. The wallet deployed on the PDR hardware is controlled by the control unit, managing its credentials, and initiating the connection to further resources, such as the mediator. A detailed description of the connection and credential-related mechanisms are provided in the next section.

[1] http://test.bcovrin.vonx.io/. Accessed: 2024-02-17.

3.2 Establishing Connections Between all Services

In order to obtain a public DID for the wallet that is deployed on the PDR, a new DID can be registered with the ledger from a seed. This DID is used for one wallet instance and is utilized for example in the provisioning process, i.e., the establishment of a wallet instance on the PDR unit.

To establish a system that is capable of exchanging VCs for the identification of participants and entities, it is necessary to establish connections in between all services, i.e., both the OCMs as well as the PDR's wallet and the corresponding mediator. This process is shown in Figure 3 exemplarily for the connection between the two OCM instances. Using the REST API, a new connection request can be made at one of the OCMs. Accordingly, the respective OCM responds with an invitation URL. This invitation URL can then be passed on to the API of the second OCM, where the invitation can be accepted. If this process was executed successfully, the second OCM responds with a connection id that further identifies the connection that was established between the two instances. Similarly, this process can be repeated for the connections between the wallet and the mediator as well as between the mediator and the PDR fleet carrier's OCM.

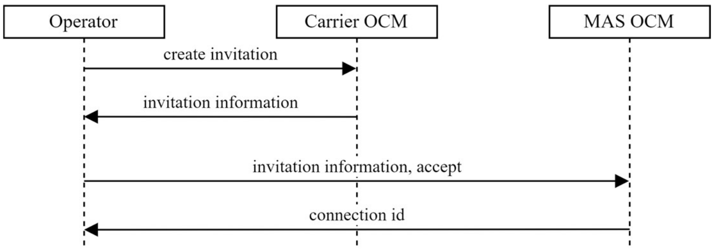

Fig. 3. Sequence diagram for connecting two instances, here as an example the robot fleet carrier's OCM and the MAS OCM.

3.3 Issuing of Credentials

After each instance of wallet and OCM are provisioned with a DID and all connections have been established as described before, verifiable credentials can now be issued. This process, depicted in Figure 4, follows the proceedings of de Jong [6] and Nikita [18]. This is exemplarily described for the credentials to be held by the PDR, issued by the carrier's OCM.

Assuming the OCM is controlled by an operator, first a credential schema and a credential definition have to be created. These are subsequently stored on the ledger. In a second step, the operator can initiate the issuing of credentials, resulting in a credential offer being sent to the holder (here the PDR wallet). The offer needs to be accepted by the PDR wallet, which then sends a credential request back to the carrier OCM. Following this step, the carrier OCM concludes the process by issuing credentials that can be stored on the PDR wallet. According to de Jong [6], the process of issuing a credential can also be initiated by the holder, i.e., the PDR wallet, by sending a credential proposal to the OCM which then answers with the credential offer.

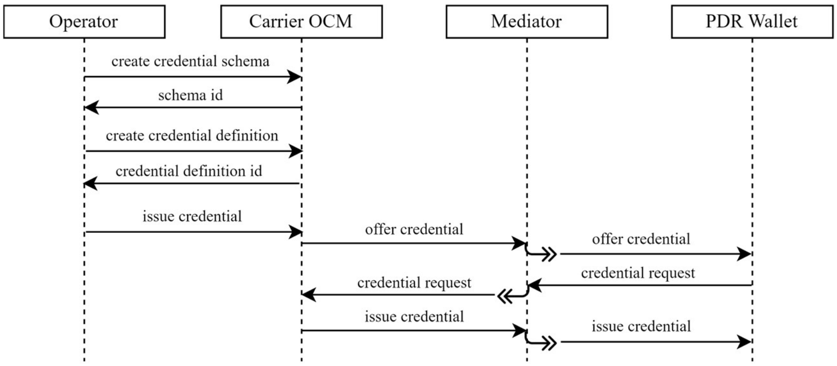

Fig. 4. Sequence diagram for the handling of credentials between two instances, here the carrier OCM and the PDR wallet. The process is instantiated by an operator. Messages between the OCM and the wallet are relayed by the mediator.

3.4 Verification of Credentials

After an entity receives its digital credentials, the next step involves proving these credentials to relevant parties within the network. This process entails presenting cryptographic proof of the credentials, which are then verified against the public keys stored on the ledger. This verification ensures the credentials are valid and have been issued by a trusted authority.

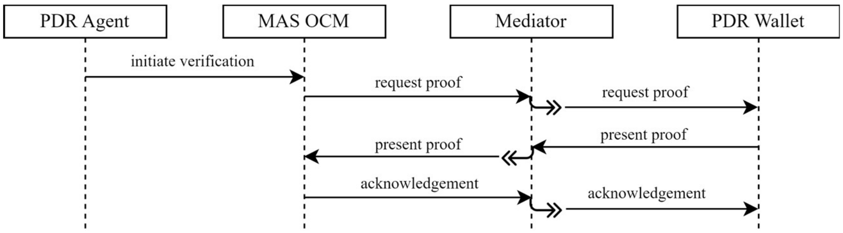

Fig. 5. Sequence diagram for the prove process of credentials, between the MAS OCM (verifier) and the PDR wallet (prover).

In the application case, the verification of credentials between the PDR and the PDR agent is of relevance. The protocol for credential verification [19] is adapted to the situation in this work and depicted as a sequence diagram below in Figure 5. First, a request from the verifier (MAS OCM) to the prover (PDR wallet) describes the format and content that needs to be fulfilled by the prover. In a response to the request, the PDR's wallet presents the required proofs to the OCM, which subsequently verifies the proof using information on the distributed ledger and finally sends an acknowledgement back to the prover. Hence, the credentials of the PDR wallet have been verified. According to [19], the process above can also be initiated by the prover by sending an initial proposal to the verifier, which then answers with a request proof to the prover.

4 Discussion

Within this work, an application-oriented MAS, dedicated to freight fleet management is regarded with the aim to integrate it with auxiliary services and resources adhering to Gaia-X standards. A subsystem of a parcel delivery robot (PDR) and its respective agent representation, the PDR agent, are considered as an example case. The Gaia-X domain of trust and identity is considered as it represents an entry point for the realization of a decentralized, self-sovereign identity management system. After the crucial services, consisting of OCM, wallet and mediator were identified along with the corresponding implemented technologies, a workflow was presented in order to connect all employed Gaia-X services. Based on this, the process of issuing and verifying credentials in between the participants of the ecosystem was elaborated.

This study's value extends beyond theoretical implications, offering tangible benefits for industries employing physical entities as agents within MAS. The incorporation of the Gaia-X framework not only broadens the ecosystem to include a variety of stakeholders but also strengthens data sovereignty and collaborative efforts. Such advancements are pivotal for the practical application of MAS, ensuring robust and efficient operations across a spectrum of sectors, not limited to logistics.

After integrating the core components of the Gaia-X's trust and identity framework, further services are envisaged to be employed in the project. Notably, the Trusted Services API (TSA), pivotal for managing usage policies and digital signature validation, will augment the trust and identity infrastructure [2]. Concurrently, the inclusion of the Eclipse Dataspace Connector (EDC) is envisioned to facilitate secure inter-organizational data exchange, reinforcing the system's alignment with Gaia-X principles. The integration will also extend to other Gaia-X components, including the federated catalogue, sovereign data exchange, and compliance services [10], enhancing ecosystem interoperability. Specifically, the federated catalogue will enable the listing of MAS agents as bookable services, thereby allowing engagement from external entities such as delivery robot fleet operators with the data ecosystem.

Acknowledgments. This paper was written as part of the project Gaia-X 4 ROMS - Support and Remote Operation of Automated and Networked Mobility Services (FKZ: 19S21005C). The joint project is funded by the German Federal Ministry of Economics and Climate Protection (BMWK). The authors are responsible for the content of this article.

References

1. Bhattacharya, M.P., P. Zavarsky, and S. Butakov. Enhancing the Security and Privacy of Self-Sovereign Identities on Hyperledger Indy Blockchain. in 2020 International Symposium on Networks, Computers and Communications (ISNCC). 2020.
2. Binzer, M., et al. GXFS - IDM & Trust. Architecture Overview. 2021; Available from: https://www.gxfs.eu/idm-trust-architecture/. Accessed: 2024-02-17.
3. Braud, A., et al., The Road to European Digital Sovereignty with Gaia-X and IDSA. IEEE Network, 2021. **35**(2): p. 4-5.
4. Capela, F., Self-Sovereign Identity for the Internet of Things: A Case Study on Verifiable Electric Vehicle Charging. 2021: Rijksuniversiteit Groningen.
5. Chicano Valenzuela, D., Identifying and tracking physical objects with hyperledger decentralized applications. 2022: Universitat Politècnica de Catalunya.
6. de Jong, L. Becoming a Hyperledger Aries Developer: Issue Credentials V2. 2021; Available from: https://ldej.nl/post/becoming-a-hyperledger-aries-developer-issue-credentials-v2/. Accessed: 2024-02-17.
7. Eclipse Foundation. Eclipse XFSC Creation Review. n.d.; Available from: https://projects.eclipse.org/projects/technology.xfsc/reviews/creation-review. Accessed: 2024-02-17.
8. eco – Verband der Internetwirtschaft. GXFS and the XFSC Toolbox. n.d.; Available from: https://www.gxfs.eu/set-of-services/. Accessed: 2024-02-17.
9. Ferdous, M.S., A. Ionita, and W. Prinz. SSI4Web: A Self-sovereign Identity (SSI) Framework for the Web. in Blockchain and Applications, 4th International Congress. 2023. Cham: Springer International Publishing.
10. Gaia-X, Gaia-X Architecture document, release 22.04. 2021, European Association for Data and Cloud, AISBL: Brussels.
11. Heinbach, C., T. Dreesbach, and O. Thomas, Freight Fleet Glasses – Augmented Reality Einsatz zur Unterstützung eines automatisierten und vernetzten Flottenmanagements. HMD Praxis der Wirtschaftsinformatik, 2023. **60**(1): p. 89-109.
12. Heinbach, C., et al., Smart Managed Freight Fleet: Ein automatisiertes und vernetztes Flottenmanagement in einem föderierten Datenökosystem. HMD Praxis der Wirtschaftsinformatik, 2023. **60**(1): p. 193-213.
13. Hoffmann, F., et al., Developing GAIA-X Business Models for Production. Proceedings of the Conference on Production Systems and Logistics: CPSL 2022, 2022: p. 583-594.
14. Hyperledger. Hyperledger Aries Cloud Agent Python (ACA-Py). 2023; Available from: https://github.com/hyperledger/aries-cloudagent-python. Accessed: 2024-02-17.
15. Lange, C., J. Langkau, and S. Bader, The IDS Information Model: A Semantic Vocabulary for Sovereign Data Exchange, in Designing Data Spaces : The Ecosystem Approach to Competitive Advantage, B. Otto, M. ten Hompel, and S. Wrobel, Editors. 2022, Springer International Publishing: Cham. p. 111-127.
16. Maecker, D., et al., Exploring Multi-Agent Systems for Intermodal Freight Fleets: Literature-based Justification of a New Concept. Wirtschaftsinformatik 2023 Proceedings. 97, 2023.
17. Maier, B. and N. Pohlmann, Gaia-X Secure and Trustworthy Ecosystems with Self Sovereign Identity, in Developing a Decentralised, User-Centric, and Secure Cloud Ecosystem. 2021, eco – Verband der Internetwirtschaft.

18. Nikita, K. Aries RFC 0036: Issue Credential Protocol 1.0. 2019 2024-02-17]; Available from: https://github.com/hyperledger/aries-rfcs/blob/main/features/0036-issue-credential/README.md.
19. Nikita, K. and S. Curran. Aries RFC 0454: Present Proof Protocol 2.0. 2021; Available from: https://github.com/hyperledger/aries-rfcs/tree/main/features/0454-present-proof-v2. Accessed: 2024-02-17.
20. Smith, R.G., The Contract Net Protocol: High-Level Communication and Control in a Distributed Problem Solver, in Readings in Distributed Artificial Intelligence, A.H. Bond and L. Gasser, Editors. 1988, Morgan Kaufmann. p. 357-366.
21. Sporny, M., et al. Decentralized Identifiers (DIDs) v1.0 – Core architecture, data model, and representations. W3C Recommendation 2022; Available from: https://www.w3.org/TR/2022/REC-did-core-20220719/. Accessed: 2024-02-17.
22. Sporny, M., et al. Verifiable Credentials Data Model 1.1. W3C Recommendation 2022; Available from: https://www.w3.org/TR/2022/REC-vc-data-model-20220303/. Accessed: 2024-02-17.
23. Stephen, C. and H. Grace. 2022 Q2 Hyperledger Indy Project Update. 2022; Available from: https://wiki.hyperledger.org/display/TSC/2022+Q2+Hyperledger+Indy. Accessed: 2024-02-17.
24. Stodt, F. and C. Reich, A Review on Digital Wallets and Federated Service for Future of Cloud Services Identity Management, in Service Computation 2023: The Fifteenth International Conference on Advanced Service Computing. 2023: France.
25. Tardieu, H., Role of Gaia-X in the European Data Space Ecosystem, in Designing Data Spaces : The Ecosystem Approach to Competitive Advantage, B. Otto, M. ten Hompel, and S. Wrobel, Editors. 2022, Springer International Publishing: Cham. p. 41-59.
26. Utku, S. and A. Bahce, A Case Study for Mobile Wallet Implementation in Self-Sovereign Identity Infrastructure. Journal of Artificial Intelligence and Data Science, 2023. **3**(1): p. 1-16.
27. Vereign. AFJ-Mediator. 2024; Available from: https://code.vereign.com/gaiax/ocm/ocm-engine. Accessed: 2024-02-17.
28. Vereign. Organization Credential Manager Engine. 2024; Available from: https://code.vereign.com/gaiax/ocm/ocm-engine. Accessed: 2024-02-17.
29. Wooldridge, M., An Introduction to Multiagent Systems. 2 ed. 2009, Chichester, UK: Wiley.