Journal of Network and Systems Management (2026) 34:61
https://doi.org/10.1007/s10922-026-10037-6

Promoting Interoperability and Data Sovereignty in Telecommunications: Integration of IDS Data Spaces with TM Forum Open APIs

Johnny Choque[1] · **Luis Sánchez**[1] · **Jorge Lanza**[1] · **Pablo Sotres**[1] · **Luis Muñoz**[1]

Received: 8 April 2025 / Accepted: 12 February 2026 / Published online: 3 March 2026
© The Author(s) 2026

Abstract

Communication Service Providers (CSPs) are continuously looking forward for new business opportunities and provision of new services to their customers. The TM Forum Open APIs have been providing an open ecosystem for CSPs to standardize operations and promote interoperability. However, in complex multi-stakeholder scenarios like providing Business-to-Business (B2B) multi-site services, inter-Autonomous System cooperation, and roaming, different telecom stakeholders must collaborate and share resources to deliver services to their customers. The integration of TM Forum Open APIs with International Data Spaces (IDS) represents a critical advancement in telecommunications service management as information exchange is crucial for maintaining end-to-end service assurance and there is currently no solution that allows such cooperation in these contexts. This paper presents a novel integration approach that combines IDS data spaces with TM Forum Open APIs, leveraging the FIWARE Business API Ecosystem (BAE) and Eclipse Dataspace Components (EDC) as reference implementations. This work contributes to the telecommunications service management by presenting a practical framework that bridges interoperability and data sovereignty, addressing critical industry challenges related to secure data exchange and regulatory compliance, with potential applications across various digital service scenarios. The validation approach is comprehensive, evaluating the integrated solution across multiple dimensions. Key assessment criteria include maintaining interoperability, enforcing data sovereignty, preserving business ecosystem functionalities, and implementing precise access control mechanisms.

Keywords Data spaces · Integration · Interoperability · Data sovereignty · Telecom

Extended author information available on the last page of the article

1 Introduction

The increasing complexity in network and service management faced by operators in the 1980 s, driven by the liberalization of the telecommunications sector, revealed several critical challenges: the prevalence of proprietary systems, lack of interoperability between solutions from different vendors, and the absence of common standards for operations management. The TM Forum was established in this context with fundamental objectives aimed at addressing these industry-wide problems. The TM Forum's most significant impact on the telecommunications industry has been realized through its Open APIs, which have fundamentally transformed how Communication Service Providers (CSPs) and providers develop and integrate their systems. These standardized APIs have enabled system interoperability, substantially reduced integration costs, and accelerated the deployment of new digital services. The widespread adoption of TM Forum Open APIs has enabled operators to modernize their legacy systems and embrace more agile and flexible architectures, establishing itself as a de facto standard in the telecommunications industry for digital transformation and service automation.

Furthermore, in today's increasingly digital world, data has become a vital asset, fueling innovation, guiding decision-making, and shaping advanced business strategies. Traditionally, CSPs have focused on using data from customer management systems to optimize internal operations, including price adjustments, network optimization, and predictive churn analysis. However, the real value lies in leveraging this data for collaboration, uncovering insights that would be impossible to generate on their own. By participating in collaborative data ecosystems, CSPs can transform this data into a valuable asset that drives the creation of innovative products and services. Collaborative data ecosystems are reshaping how businesses interact and operate, enabling organizations to share data to enhance customer satisfaction, mitigate supply chain risks, and introduce new offerings. As CSPs embrace this collaborative approach, they can transition from seeing data management as a cost to integrating it into their business model, making it a key driver of their business.

1.1 Industry Context and Current Solutions

In the telecommunications sector, the ability to exchange and advantage data across multiple stakeholders has become a strategic requirement. Existing data-sharing solutions—ranging from hyperscaler cloud ecosystems (e.g., AWS Data Exchange, Google Cloud Analytics Hub), to industry-specific marketplaces (e.g., Snowflake Data Marketplace, Databricks Delta Sharing), and even standardized API frameworks such as the TM Forum Open APIs—have enabled Communication Service Providers (CSPs) to interoperate more effectively and accelerate digital service delivery. These solutions have reduced integration costs, provided more agile service orchestration, and facilitated collaboration with third-party developers.

However, their limitations are increasingly evident in complex multi-stakeholder scenarios such as inter-operator roaming, cross-domain service assurance, and Business-to-Business (B2B) multi-site service provisioning. Most current approaches remain centralized or platform-dependent, raising concerns about vendor lock-in,

lack of transparency in data governance, and the absence of fine-grained control once data is shared. In particular, while the TM Forum Open APIs have emerged as a de facto standard for interoperability in telecommunications, they lack mechanisms for enforcing data sovereignty—that is, ensuring that data providers retain control over the conditions of access and use once data leaves their domain. These shortcomings highlight the need for new paradigms that go beyond interoperability to include governance, trust, and sovereignty.

1.2 Dataspace Paradigms: IDS and GAIA-X

In response to these challenges, the concept of data spaces has gained prominence, particularly in Europe, as a foundation for federated, secure, and sovereign data exchange ecosystems. Among the most influential initiatives are the International Data Spaces (IDS) and GAIA-X frameworks.

IDS provides a reference architecture model that emphasizes usage control, data sovereignty, and trust between participants. Its connector-based architecture allows organizations to exchange data while retaining fine-grained control over how their data is accessed, processed, and redistributed. IDS has been piloted across domains such as manufacturing, health, and energy, but remains largely unexplored in telecommunications.

GAIA-X, on the other hand, extends the dataspace paradigm beyond data exchange by incorporating federated cloud and edge infrastructures, governance frameworks, and service portability requirements. Its scope is broader, encompassing not only data sharing but also cloud infrastructure, artificial intelligence services, and compliance with European regulatory frameworks.

Both initiatives play pivotal roles in shaping the future of trustworthy digital ecosystems. However, given its narrower focus on sovereign data exchange and its maturity in defining technical building blocks for data usage enforcement, IDS aligns more closely with the objectives of this work, which seeks to integrate data sovereignty into telecommunications service management.

1.3 Problem Statement and Motivation

Despite the widespread adoption of TM Forum Open APIs and the maturity of IDS in enabling sovereign data spaces, there is no practical integration framework that combines the two. Current solutions face significant shortcomings:

- Traditional API ecosystems (including TM Forum Open APIs) provide interoperability but lack mechanisms for secure, sovereign control over shared data.
- Dataspace initiatives such as GAIA-X offer strong governance and federated service models, but do not address the specific requirements of telecommunications service orchestration.
- IDS adoption in telecom remains minimal, with most deployments limited to other industrial domains.

This absence of integration results in a clear research gap: the telecommunications sector lacks a framework that simultaneously ensures interoperability, sovereignty, scalability, and regulatory compliance in multi-stakeholder environments. Bridging this gap is essential for enabling next-generation digital services, where operators and partners must cooperate without compromising security or business autonomy.

1.4 Research Objectives and Contributions

This paper addresses the identified gap by proposing and validating an integration framework that combines IDS data spaces with TM Forum Open APIs. The specific objectives of this study are:

- To analyze the complementarities and limitations of IDS and TM Forum Open APIs in the context of telecommunications.
- To design a structured methodology for integrating IDS sovereignty principles with the interoperability capabilities of TM Forum Open APIs.
- To implement and validate this integration using reference technologies, namely the FIWARE Business API Ecosystem (BAE) and the Eclipse Dataspace Components (EDC).
- To provide a critical comparison with alternative approaches, situating the proposed work within the broader landscape of data-sharing initiatives.

The contributions of this paper are threefold:

- A novel integration model that bridges interoperability and sovereignty in telecommunications service management. TM Forum Open APIs contribute their widespread industry adoption and proven capability to standardize telecommunications operations. Complementing this foundation, IDS data spaces provide a robust framework for data sovereignty and secure exchange of data. This synergy would enable telecommunications operators not only to maintain current operational efficiency but also to ensure secure and controlled data exchange in an increasingly complex and regulated digital ecosystem. The combination of both technologies would facilitate the creation of new business models based on secure data exchange while keeping control and sovereignty over sensitive business and customer information and leveraging solutions that create value from data to develop product offerings, manage asset catalogs, and handle product ordering through well-established Open APIs.
- A reference implementation that demonstrates the feasibility of the proposed approach using open-source technologies. This implementation is grounded in a structured three-phase methodology: (1) functional integration of TM Forum Open APIs with IDS data spaces principles, (2) analysis of the reference implementation and case study of both technologies, and (3) software integration based on theoretical insights and case studies. Furthermore, the validation approach comprehensively evaluates the integrated solution across multiple assessment criteria, including interoperability, data sovereignty enforcement, catalog and marketplace management, and precise access control mechanisms implementa-

tion. Notably, the source code of the application implemented to demonstrate the integration is archived in Zenodo[1].

- A critical comparative analysis that situates the proposed IDS–TM Forum Open API integration within the broader landscape of data-sharing initiatives. Unlike previous Industry 4.0-oriented integrations, the proposed solution demonstrates distinct advantages in terms of (1) seamless business process integration; (2) monetization capabilities; (3) dual compliance with TM Forum and IDS standards; (4) implementation flexibility; and (5) extensibility. This analysis highlights how the solution complements existing business ecosystems while incorporating sovereignty features, thereby addressing both technical and commercial requirements.

Paper Organization: The remainder of this paper is structured as follows. Section 2 provides the related work and background, combining both the technological foundations and the critical review of existing approaches, while identifying the research gap. Section 3 details the methodology, describing the structured approach used to integrate both frameworks. Section 4 analyzes the technological foundations of IDS data spaces and TM Forum Open APIs, leading to the proposed functional integration. Section 5 presents a technical study of reference implementations, evaluating their capabilities and interoperability. Section 6 describes the integration process, demonstrating how IDS data spaces enhance data sovereignty within the FIWARE Business API Ecosystem. Section 7 provides a comparative analysis of the proposed approach, highlighting its advantages over existing solutions. Finally, Sect. 8 concludes the study and discusses future research directions.

2 Related Work and Background

The integration of IDS data spaces and TM Forum Open APIs represents a promising yet underexplored avenue for enhancing data exchange, governance, and interoperability in the telecommunications sector. While significant advancements have been made in both domains independently, and their mutual synergies have been identified, existing literature does not yet provide a comprehensive framework for their integration. This section reviews the state of the art and background of data-sharing solutions and dataspace initiatives, with particular attention to their applicability in telecommunications. It begins by analyzing traditional approaches, including hyperscaler ecosystems, data marketplaces, and standardized API frameworks such as TM Forum Open APIs, highlighting their strengths and inherent limitations. The section then examines the most relevant dataspace paradigms, namely IDS and GAIA-X, outlining their architectural principles, governance models, and sectoral adoption. A comparative perspective is provided through two systematic analyses: the first contrasts traditional solutions with IDS and GAIA-X, while the second focuses on the complementarities and weaknesses of IDS and TM Forum Open APIs. This critical

[1] https://doi.org/10.5281/zenodo.14796958.

review not only clarifies the advantages and shortcomings of existing approaches but also identifies the research gap that motivates the proposed integration.

2.1 Data-Sharing Solutions in Telecommunications

The telecommunications sector has long relied on diverse mechanisms for data exchange, ranging from bilateral APIs to centralized data platforms. Traditional solutions include hyperscaler ecosystems (e.g., AWS Data Exchange, Google Cloud Analytics Hub, Microsoft Azure Data Share), which enable large-scale data marketplaces but often imply risks of vendor lock-in and limited sovereignty. Similarly, industry data marketplaces (e.g., Snowflake Data Marketplace, Databricks Delta Sharing, Oracle Data Marketplace) provide structured access to datasets but follow centralized governance models that do not guarantee fine-grained control over data usage.

In parallel, telecommunication-specific API frameworks—notably the TM Forum Open APIs—have become a de facto standard for interoperability. They enable system integration, support service orchestration, and reduce operational complexity [1–3]. However, despite their adoption, such APIs lack mechanisms to enforce data sovereignty once data is shared, creating trust and governance challenges in multi-stakeholder environments.

To contextualize these limitations, Table 1 contrasts traditional solutions (APIs, marketplaces, hyperscalers) with emerging dataspace paradigms (IDS and GAIA-X).

2.2 Dataspace Initiatives: IDS and GAIA-X

International Data Spaces (IDS) emerged as one of the earliest and most comprehensive specifications of the dataspace paradigm. The IDS Reference Architecture

Table 1 Comparative analysis of traditional data-sharing solutions, IDS, and GAIA-X

Criterion	Traditional solutions	IDS	GAIA-X
Architecture	Centralized, often platform-dependent	Federated, decentralized via IDS connectors [4, 5]	Federated services and infrastructure ecosystem [6]
Data sovereignty	Absent; data providers have to fully rely on the control enforced by the platform but they lose control once shared	Strong: usage policies, enforcement, and traceability [4, 7]	Broader scope: includes sovereignty of data, cloud, and services [6]
Interoperability	Limited, sector-specific	High, based on open standards and semantic interoperability [8, 9]	Cross-sector interoperability via standardized service descriptions and federated catalogues [10]
Governance	Defined unilaterally by platform owners	Federated governance model with trust anchors [4, 5]	European governance with compliance to GDPR, Data Act [10]
Scalability & adoption	Mature, widely deployed (TM Forum, hyperscalers)	Growing adoption in Industry 4.0, energy, health, but limited in telecom [11–13]	Early-stage adoption, with pilots in mobility, energy, and cloud services [10]
Main weakness	Vendor lock-in, lack of trust and sovereignty	Complexity of adoption, limited sector-specific implementations	Immaturity, dependency on broad political/industrial alignment

Model (IDS-RAM) defines a federated infrastructure enabling participants to retain control over their data through usage policies, identity management, and trust frameworks [4, 5, 14]. Its applications span domains such as health, energy, and manufacturing [8, 9, 11]. Despite its maturity, telecommunications remain underrepresented in current IDS deployments [11]. Studies such as [7] and [12] emphasize the potential of IDS for enabling sovereignty in digital ecosystems, while [13] demonstrates scalability challenges in industrial contexts.

GAIA-X, in contrast, extends the concept of data spaces to encompass cloud federation, service portability, and regulatory compliance [6, 10]. Its ambition is to establish a pan-European framework that ensures sovereignty not only of data but also of the infrastructures and services operating on top of it. While GAIA-X aligns with European regulatory priorities (GDPR, Data Act), its broad scope dilutes its immediate applicability to the specific operational needs of the telecommunications sector.

Overall, IDS provides a more targeted foundation for sovereign data-sharing solutions, while GAIA-X complements it at the infrastructure and governance layers. However, given the scope and objectives of this work, the subsequent analysis and integration process will concentrate exclusively on IDS. The rationale for this decision is twofold. First, GAIA-X addresses a broad spectrum of concerns—including federated cloud services, infrastructure portability, and regulatory compliance—that, while essential at the European policy level, extend beyond the specific problem of enabling sovereign and interoperable data exchange in telecommunications. Second, IDS focuses directly on the data layer, providing well-defined architectural components such as connectors, identity management, and usage control mechanisms that are directly applicable to the integration of data sovereignty into telecom service management. By narrowing the scope to IDS, this study ensures methodological precision and practical relevance, aligning the integration framework with the technical requirements of the telecommunications sector while avoiding the added complexity of infrastructure-level federation that GAIA-X entails.

2.3 TM Forum Open APIs and Telecommunications Interoperability

The TM Forum Open APIs have become the backbone of interoperability in telecommunications, with adoption by major CSPs and vendors worldwide [1–3]. These APIs facilitate catalog management, product ordering, billing, and cross-operator integration, forming a robust ecosystem for digital service management. TM Forum's Catalyst projects [15, 16] have even explored the creation of trusted Telco Data Spaces, combining APIs with data sovereignty requirements. However, these remain at the conceptual stage, with no large-scale deployments integrating IDS principles.

Despite their maturity, TM Forum Open APIs are primarily focused on technical interoperability and process standardization, lacking mechanisms to guarantee traceability, non-repudiation, and automated enforcement of data usage policies—core elements in IDS [4, 14]. This limitation underscores the need for complementary approaches that embed sovereignty and trust.

2.4 Comparative Analysis: IDS vs. TM Forum Open APIs

The integration of IDS and TM Forum Open APIs is motivated by their complementary strengths and weaknesses. While TM Forum Open APIs provide a well-established industry standard for interoperability and operational agility, IDS ensures sovereignty, trust, and secure governance of shared data. A direct comparison is presented in Table 2.

In summary, IDS and TM Forum Open APIs present complementary strengths and weaknesses. IDS offers a robust framework for ensuring data sovereignty, fine-grained usage control, and trusted exchange across domains, but lacks widespread adoption in telecommunications. Conversely, TM Forum Open APIs are widely adopted and highly effective in achieving interoperability and business process integration, yet they do not provide mechanisms to guarantee sovereignty or enforce usage policies. This complementarity underscores the potential value of combining both approaches, setting the stage for the identification of a research gap where no existing framework fully integrates IDS sovereignty principles with TM Forum Open APIs' interoperability capabilities.

2.5 Identified Research Gap

The comparative review presented in the previous sections highlights that while IDS and TM Forum Open APIs address critical but distinct dimensions of data exchange, no existing framework effectively integrates their capabilities. Current research has demonstrated the maturity of IDS in enabling sovereignty across domains such as manufacturing and health [11–13], while TM Forum Open APIs have proven indispensable for interoperability in telecommunications [1–3]. Yet, their evolution has remained largely parallel, with limited cross-fertilization. Existing initiatives, such as TM Forum Catalyst projects [15, 16], explore the potential of telco data spaces but remain at the conceptual stage and lack concrete implementation. As a result, the telecommunications sector continues to face a structural gap: it has access to interoperable API frameworks without sovereignty, and to sovereignty-focused data space architectures without sector-specific adoption. Bridging this divide is therefore

Table 2 Comparative analysis of IDS and TM forum open APIs

Criterion	IDS	TM forum open APIs
Primary focus	Data sovereignty, usage control, and trust frameworks [4, 14]	Interoperability and process standardization in telecommunications [1–3]
Architecture	Federated, connector-based, decentralized [4, 5]	Centralized API-driven integrations
Data control	Fine-grained usage policies, automated enforcement, traceability [7, 9]	No native usage control; once accessed, data can be reused freely
Interoperability	Cross-sector, semantically rich [8, 9]	Sector-specific, widely adopted in telco [1, 2]
Adoption	Growing in manufacturing, health, energy; limited in telecom [11, 12]	Very high in telecommunications, global adoption by CSPs [3]
Weaknesses	Complexity, lower maturity in telecom sector	Lack of sovereignty, trust, and usage control mechanisms

essential for enabling sovereign, interoperable, and business-oriented data exchange in telecommunications.

Summarizing, the review highlights three critical insights:

(1) Traditional data-sharing solutions (including TM Forum Open APIs) are mainly focused on the provision of interoperability but they are typically secured with mechanisms such as OpenID and OAuth2.0, which are good at providing the authentication and authorization baseline, but fail to ensure advanced sovereignty, trustworthiness, and fine-grained control over data usage, even more when considering in a fully de-centralized and many-to-many scenarios.
(2) Dataspace initiatives (IDS and GAIA-X) offer sovereignty and governance, but their adoption in telecommunications remains minimal, with GAIA-X being too broad and IDS lacking sector-specific implementations.
(3) No existing framework provides a practical integration of IDS sovereignty mechanisms with TM Forum Open APIs' interoperability, leaving a gap in enabling sovereign, scalable, and interoperable Telco Data Spaces.

This gap provides the foundation for the present work, which proposes and validates the integration of IDS with TM Forum Open APIs as a novel contribution to telecommunications service management.

3 Integration Methodology

This research follows a systematic approach to integrate TM Forum Open APIs with IDS data spaces technologies, focusing on enabling data sovereignty and trusted data exchange while maintaining standardized interoperability and process automation capabilities. The methodology comprises three sequential phases: (1) defining the functional integration framework, (2) analyzing reference implementation and case studies, and (3) integrating these cases to validate the proposed approach.

This methodology provides a structured framework for integrating data spaces technologies with business ecosystems, balancing theoretical rigor with practical applicability. The approach can serve as a reference for integration in the field of trusted and sovereign data exchange applied to the management of telecommunication services.

3.1 Phase 1: Theoretical Framework Development

The first phase involves a comprehensive analysis of both technological frameworks to establish functional integration. For TM Forum Open APIs, the analysis focuses on understanding the standardized interfaces that manage the complete service lifecycle, from offering creation to billing and revenue sharing. For IDS data spaces, the analysis examines the core processes defined in the IDS-RAM, particularly those related to data sovereignty and trusted data exchange. Based on this analysis, a functional integration approach is proposed that combines both technologies, identifying key integration points and defining the necessary interactions between their components.

This phase's main outcome is the development of a conceptual model that sketches the interactions between TM Forum components and IDS data spaces, serving as a fundamental reference for the integration process.

3.2 Phase 2: Reference Implementation and Case Study Analysis

The second phase focuses on the practical analysis of reference implementations for both TM Forum Open APIs and IDS data spaces. FIWARE Business API Ecosystem (BAE) is used as a reference implementation for TM Forum Open APIs, particularly in the context of catalog and marketplace management (i.e. service monetization and digital business automation). Correspondingly, Eclipse Dataspace Components (EDC) Connector is employed as a reference implementation for IDS data spaces, enabling policy-driven data transactions. Alternative implementations of these technologies also exist—for example, ONAP [17] for the TM Forum Open APIs, and the Fraunhofer ISST Dataspace Connector [18] or the Engineering True Connector [19] for dataspace solutions. Nevertheless, we selected BAE and EDC because both projects are backed by active communities, ensuring long-term support. Indeed, most of the first implementations of IDS Connectors, like the two mentioned above (i.e. Fraunhofer ISST or Engineering True Connector) have been explicitly or implicitly discontinued in favor of EDC. Furthermore, in the case of EDC, its software architecture is specifically designed to facilitate seamless integration with other developments, which constitutes the key feature underpinning the contribution we present in this work.

To assess their effectiveness, this phase also includes a detailed analysis of a representative case study for each technology. The first case study evaluates EDC's capabilities in secure data transfers and contract-driven access control, while the second case study investigates how FIWARE BAE's plugin architecture can incorporate IDS governance mechanisms to ensure controlled service commercialization. These case studies provide critical insights into the practical applicability of both frameworks within real-world scenarios.

3.3 Phase 3: Integration and Validation

In the third phase, the insights gained from the previous two phases are employed to integrate the aforementioned case studies and validate the proposed approach. This involves integrating the functionalities of BAE and EDC Connector, enabling contract negotiation, dynamic policy enforcement, and controlled data exchange. The integration process ensures that sovereign data-sharing principles are maintained while preserving TM Forum's interoperability standards. The validation process assesses key metrics such as interoperability, compliance with IDS policy enforcement, scalability across digital service ecosystems, and the ability to enhance security and governance within business operations.

4 Analysis of Technological Frameworks

This section provides a comprehensive analysis of the two technological frameworks at the core of this study: TM Forum Open APIs and IDS data spaces. It examines their key characteristics, capabilities, and limitations, establishing a foundation for their integration. By identifying complementarities and gaps, this analysis allows deriving the functional integration approach proposed.

4.1 TM Forum Open APIs

In the third phase, the insights gained from the previous two phases are employed to integrate the aforementioned case studies and validate the proposed approach. This involves integrating the functionalities of BAE and EDC Connector, enabling contract negotiation, dynamic policy enforcement, and controlled data exchange. The integration process ensures that sovereign data-sharing principles are maintained while preserving TM Forum's interoperability standards. The validation process assesses key metrics such as interoperability, compliance with IDS policy enforcement, scalability across digital service ecosystems, and the ability to enhance security and governance within business operations.

TM Forum Open APIs are technology-agnostic and can be applied across various digital service scenarios. This high level of abstraction enables TM Forum Open APIs to be utilized in diverse digital service scenarios beyond telecommunications, including B2B, Internet of Things (IoT), smart health, smart grids, big data, Network Function Virtualization (NFV), and more.

The technology-agnostic nature and extensive set of Open APIs presents a significant challenge in demonstrating viable integration with IDS data spaces. Therefore, it is strategic to select a specific application such as FIWARE BAE [20], which implements a relevant subset of TM Forum Open APIs focused on the catalog and marketplace management (that implicitly supports monetization and commercialization) for digital services. In this context, FIWARE BAE provides a concrete and bounded use case that demonstrates the feasibility of integration with IDS data spaces. This approach not only reduces the complexity of the integration process but also offers a practical and replicable example that can serve as a reference for future implementations in other digital service contexts utilizing TM Forum Open APIs.

FIWARE BAE implements the following TM Forum APIs to manage processes from offer creation through billing, accounting, and revenue sharing, providing a comprehensive solution for digital product and service management:

- The Product Catalog Management API (TMF620) manages Product Catalogs, Product Specifications, and Product Offerings. Product Specifications provide the technical definition of products, including all characteristics, functionalities, and configurable parameters. Product Offerings represent different commercial ways to offer products to the market, encompassing prices, promotional packages, and terms and conditions. Product Catalogs facilitate the organization and publication of these offerings.
- The Product Ordering Management API (TMF622) handles customer-initiated

Product Orders, which are created from Product Offerings defined in a catalog. When creating orders, customers can select values for various configurable characteristics and specify the applicable pricing. This API facilitates the creation, modification, tracking, and cancellation of product orders.

- The Product Inventory Management API (TMF637) enables customers to retrieve information about their purchased products, including specific characteristics and selected pricing models. This API manages product inventory operations, such as creating, updating, and retrieving product representations in the inventory.
- The Party Management API (TMF632) manages parties, which can be individuals or organizations having any kind of relationship with the enterprise. This API handles information about involved parties, including customers and organizations, centralizing relevant data for business interactions.
- The Customer Management API (TMF629) handles customer private information that cannot be included within party resources. It maintains different shipping contact mediums, including email, phone, and address, attached to different billing accounts.
- The Billing Management API (TMF636) controls billing processes, generating customer invoice structures and managing customer payments for specific products acquired in the system.
- The Usage Management API (TMF635) monitors and records service usage, providing essential data for billing and performance analysis.

By integrating these APIs the FIWARE BAE exposes its complete functionality through industry-recognized standards, facilitating interoperability and integration with other systems and platforms. This feature is key in achieving software integration tasks that are pursued as part of the work described in the paper.

Based on a comprehensive analysis of TM Forum Open API portfolio [21], Fig. 1 has been developed to illustrate the functional relationships between the APIs implemented within the FIWARE BAE. This architectural diagram serves as a crucial foundation for understanding the complex interactions between different API components and their respective roles in the system's operation. Figure 1 does not only summarize the technical specifications outlined in TM Forum's documentation but also demonstrates how these standardized interfaces work together to support the complete digital service lifecycle, from product catalog management through billing and usage tracking. This systematic representation has been taken as a fundamental reference point for achieving the integration objectives of this work, particularly in establishing a coherent functional integration framework between FIWARE BAE and IDS data spaces.

4.2 IDS Data Spaces Ecosystem

A data space is a decentralized and open infrastructure that implements additional layers to ensure sovereignty, interoperability, and trust during data exchange. Data spaces do not replace existing data transfer technologies but rather integrate them into a broader framework, enabling more secure and controlled data exchange across various sectors and applications. Data sovereignty allows companies and organi-

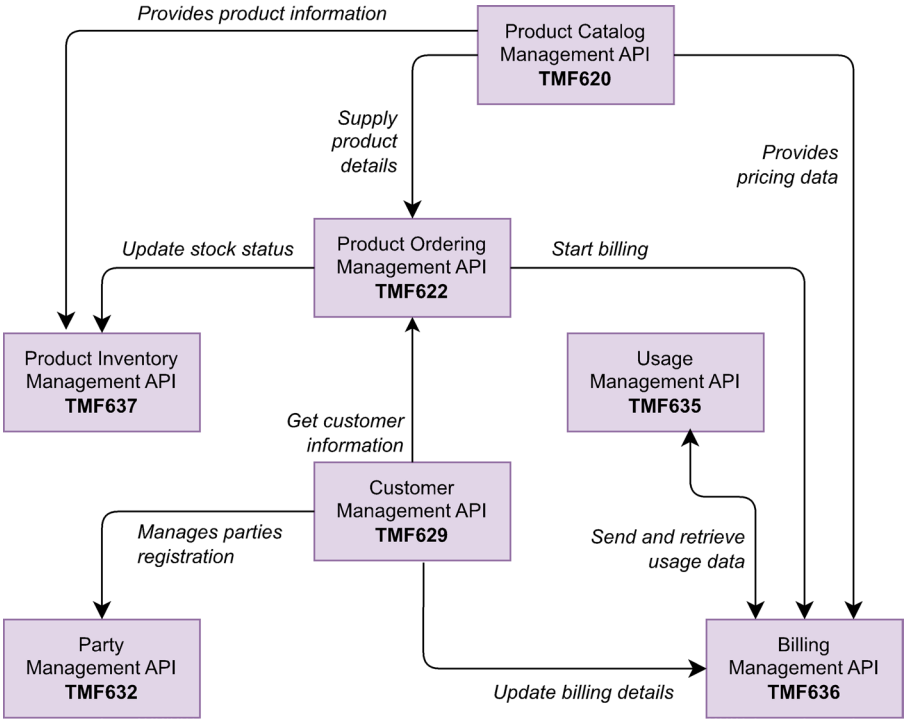

Fig. 1 Key functional relationships between the TM Forum's Open APIs

zations to maintain complete control over their data. This means that data owners decide who can access their data and under what conditions. Data spaces implement interoperability through a combination of standards, open architectures, and specific technical components that facilitate data exchange between different systems and organizations. Finally, trust is implemented through a certification framework and standards that ensure all participants and ecosystem components meet security criteria and operate reliably.

The IDS-RAM provides a high abstraction level focusing on the generalization of concepts, functionality, and overall processes involved in the creation of an IDS data space. The IDS-RAM uses a five-layer structure whose baseline is the System Layer. The IDS-RAM System Layer consists of several technical components designed to facilitate secure and efficient data exchange between participating organizations. These components include the IDS Connector, Identity Provider, App Store, Metadata Broker, Clearing House, and Vocabulary Hub.

Apart from specifying the decomposition of the logical software components at its System Layer, the IDS-RAM also specifies, as part of its Process Layer, the interactions taking place between the different components of an IDS data space. As it can be seen in Fig. 2, the IDS-RAM Process Layer defines a series of key steps that facilitate secure and efficient data exchange between participating organizations:

- Onboarding: This process involves incorporating an organization into the IDS

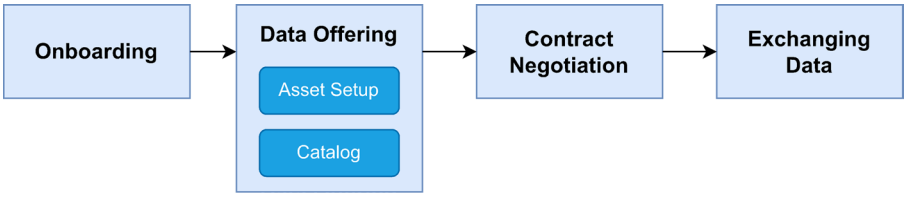

Fig. 2 IDS-RAM process layer

data space ecosystem. It includes credential verification, IDS Connector configuration, and alignment with established security and governance policies. The goal is to ensure that each participant meets the required standards to maintain trust and interoperability within the data space.

- Data Offering: Once an organization is onboarded, it can offer its data products to the ecosystem. This process is where assets and catalogs are created and managed within the IDS ecosystem. Data providers define and create their data assets, which are representations of the data products they wish to share (IDS Asset Setup), and organize them into structured catalogs to facilitate discovery (IDS Catalog). As part of this definition, metadata associated with each asset is specified, including descriptions, formats, schemas, and conditions of use. Simultaneously, access and usage policies are established for each asset, as well as pricing models or commercial terms if applicable.
- Contract Negotiation: This process focuses on negotiating the terms and conditions under which a data product (i.e. a dataset or data stream) will be shared and used. It involves creating and reviewing contract offers that specify data usage policies, restrictions, and obligations for both provider and consumer. The negotiation can be automated or semi-automated and seeks to reach an agreement that satisfies both parties.

A key function of the Onboarding process is to address the security and validation requirements of participants. To achieve this, several security models have been proposed. They have been designed to align with both the fundamental requirements established in IDS-RAM and the specific characteristics of the environment in which they are implemented.

However, when considering integration with TM Forum Open APIs, addressing all these components and steps may prove unfeasible due to the diversity of use cases and the complexity associated with each one. Therefore, in terms of components, only the IDS Connector, as the cornerstone for the creation of a data space, is chosen to demonstrate the integration. Technically, the IDS Connector processes and transforms data according to specific needs while managing its storage and access. Its design ensures interoperability through the implementation of common protocols and standards, facilitating communication between different systems and domains. Additionally, it aids regulatory compliance by implementing privacy controls and maintaining detailed audit logs.

As it has been already said, the IDS Connector is a fundamental component within the IDS architecture that acts as a control and access point for secure data exchange

between participants. Its importance lies in implementing IDS core principles, especially data sovereignty and trusted exchange. The relevance of the IDS Connector is present in multiple dimensions. In terms of sovereignty, it allows organizations to maintain complete control over their data even after sharing it, implementing and enforcing specific usage policies. From a security perspective, it provides robust authentication mechanisms and establishes secure communication channels between participants. However, although some of the functionalities related to product lifecycle management and business operations, which are key when considering the complete business process, are partially addressed within the Data Offering process, they fall outside the main scope of the IDS Connector. Hence, they are not comprehensively covered.

The integration proposed in this work will primarily focus on processes directly related to data transfer, including Data Offering — whose associated functionalities will lie on the TM Forum Open APIs — Contract Negotiation, and Data Exchange, which will be supported through the IDS Connector. In this context, the Onboarding process will adopt a basic security model that adheres to IDS standards while it also aligns with the specific characteristics of the technological solutions involved in the integration. This approach maintains the integrity of IDS-RAM security requirements while optimizing resources dedicated to integrating the most relevant components involved in the actual data exchange management and control.

This approach simplifies the process but does not reduce its generality and applicability as it also provides an exemplary model that can be adapted for other use cases associated with the remaining components. This strategy effectively demonstrates integration with TM Forum Open APIs, focusing on the critical aspects of data sovereignty and trusted data exchange, without incurring the additional complexity that would involve the complete implementation of all IDS-RAM system layer components.

4.3 Functional Integration

Based on the previous analysis of IDS data spaces and TM Forum Open APIs, this section proposes a functional integration approach that combines both technologies. As it has been already introduced the objective is to exploit the synergies among TM Forum Open APIs and IDS Connector by incorporating to the inherent features of the IDS Connector to support the creation of IDS data spaces, those brought forward by the TM Forum Open APIs recommendations related to catalog and marketplace management, which are supportive for the Data Offering process. Figure 3 shows the IDS-RAM processes that have been included within the scope of the work presented in this paper, and how they can be supported through the corresponding TM Forum Open APIs, resulting on a functional integration supporting secure data exchange while maintaining control and sovereignty over sensitive business and customer information.

Firstly, as the specification and offering of products are managed through the Product Catalog Management API (TMF620), this API is identified as an appropriate starting point for integration due to its relationship with the functionalities required on the *IDS Asset Setup* process. The creation of an asset at IDS level is based on the

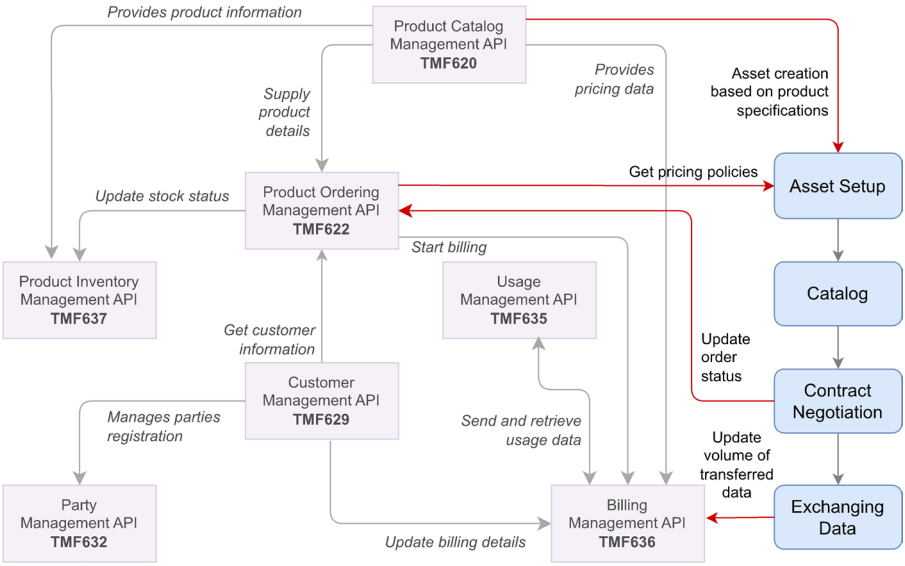

Fig. 3 Key functional integration of IDS data spaces and TM Forum Open APIs

product specifications previously defined in TMF620, along with the pricing policies established in the Product Ordering Management API (TMF622), thereby establishing a connection between both technologies.

Concerning the *IDS Catalog* process, it serves as a facilitating step, triggering the negotiation process within the data spaces. While this process is essential within IDS, it is embedded within TMF620 so it does not require any additional binding with TM Forum Open APIs to run it.

Regarding *IDS Contract Negotiation*, there is a possibility that the negotiation may not be successfully completed. In such cases, it is necessary to notify the Product Ordering Management API to proceed with the cancellation of the previously generated order. In this sense, it is important to note that TMF622 handles the order lifecycle, which also supports orders' cancelation. Creating the order upon the negotiation is triggered and not only after it has been successfully finalized, obeys the need for the provider application to know in advance the order and consumer ids, as it will be detailed in Sect. 6.3.

Finally, in certain scenarios, data exchange may occur on a recurring basis following an initial successful negotiation. In these cases, *IDS Exchanging Data* must communicate the volume of data transferred to the Billing Management API (TMF636) to facilitate the corresponding billing process.

The interactions between IDS processes and Open APIs have implications for other TM Forum APIs. For instance, canceling an order in TMF622 requires updating records in the Product Inventory Management API. Likewise, notifying TMF636 about an increase in the volume of consumed data entails updating records in the Usage Management API. In general, the integration focuses on the most relevant Open APIs, allowing the pre-established functional relationships with other Open APIs to operate autonomously.

5 Technical Study of Reference Implementation

This section examines the technical foundations and practical deployment considerations regarding reference implementations supporting the integration of IDS data spaces with TM Forum Open APIs. By analyzing key technologies—specifically the Eclipse Dataspace Components (EDC) for IDS and the FIWARE Business API Ecosystem (BAE) for TM Forum Open APIs— this study evaluates their interoperability, security features, and role in facilitating trusted data exchange.

The technical insights provided here serve as the basis for the integration framework proposed in later sections, ensuring both theoretical rigor and real-world applicability. In this sense, it is important to highlight that the analysis described in the following sections results from a twofold approach combining both study of the underlying open specifications and assessment of the practical deployments that have been carried out for realizing a real integration among the two frameworks under analysis. Through this overview, the section highlights the critical role of reference implementations in validating the feasibility and effectiveness of the proposed integration approach.

5.1 EDC Connector

The IDS-RAM architecture defines several core components, one of which is the IDS Connector. This component is essential for IDS data space's participants willing to exchange data, as it implements the mechanisms required for secure and efficient communication and data exchange within data spaces. There are multiple implementations of the IDS Connector, both open-source and proprietary [14]. Despite being developed by different solution providers, all implementations must meet the fundamental requirement of technical interoperability. One of the most notable open-source initiatives is the Eclipse Foundation, which has developed the Eclipse Dataspace Components (EDC) project [22], a comprehensive set of components for data spaces that comply with IDS requirements. The connector included in EDC offers one of the highest levels of technological maturity, a design that facilitates the integration of data spaces into other systems, and extensive technical documentation —key reasons for selecting it in this study.

5.1.1 EDC Connector Architecture

The implementation of the EDC Connector is divided into two logical subsystems: the control plane and the data plane. This separation allows the control plane to integrate seamlessly with existing infrastructures and technologies responsible for data transfer. The control plane is designed to be highly available and scalable, which is why it operates independently of the tasks performed by the data plane. The control plane performs various functions, such as verifying that the consumer meets the requirements to access the assets, overseeing policy enforcement, managing contract negotiation, and carrying out any necessary configuration or preprocessing before initiating data transfer, among others.

On the other hand, the data plane is responsible for the actual transfer of data over the network, leveraging existing technologies such as HTTP or FTP, for example. The behavior of the data plane must be configured according to the type of data to be transferred (e.g. big data, streaming, events). In this context, multiple data planes can be configured and tailored to specific use cases.

At the control plane level, message exchange between connectors is carried out following the *IDS Dataspace Protocol* (DSP Protocol) [5], a comprehensive set of specifications that facilitates secure, reliable, and interoperable data exchange among entities within a Data Space. The DSP Protocol includes three groups of protocols that define the processes involved in the various phases of the data exchange lifecycle. First, the *Catalog Protocol* enables the consumer to obtain a catalog of contract offers related to the data provided by the provider. Based on the received catalog, the *Contract Negotiation Protocol* allows the consumer to negotiate a potential agreement with the provider regarding the use of the offered datasets. If both parties reach an agreement, the *Transfer Process Protocol* is used to control the data transfer process between the provider and the consumer. While this protocol manages the initialization and termination of transfer channels, the actual data transfer and the handling of technical exceptions depend on the transport protocol employed in each case (e.g. HTTP, FTP, MQTT). During the negotiation process, it is essential to agree on the properties of the datasets to be transferred, such as the transport protocol, structure, syntax, and semantics of the data.

Third-party applications, being outside the trusted environment of the data spaces, cannot use the DSP protocol. For this reason, the *EDC Management API* [23] allows third-party applications to interact with various functionalities of a running EDC Connector. In some cases, the EDC Management API can trigger message exchanges between Connectors via the DSP Protocol, such as during contract negotiation or data transfer processes.

5.1.2 EDC Case Study

The GitHub repository for the EDC project[2] contains several examples demonstrating how its components can be used, including detailed technical information that enables the developer community to integrate them into other systems[3]. Given that the primary scenario of the proposed integration in this paper focuses on data transfer, it is essential to utilize examples from the EDC project that address this topic. Therefore, as a case study, examples related to data transfer between provider and consumer connectors have been selected (so-called EDC Transfer Samples) [24].

Figure 4 illustrates the entities involved and the messages exchanged during the execution of the EDC case study. The interaction between third-party applications (Provider App, Consumer App) and their respective connectors employs the EDC Management API, while the interaction between connectors is performed as specified by the DSP protocol. It is important to highlight that the DSP protocol specification defines an equivalent state machine ruling the interactions between Connectors and

[2] https://github.com/eclipse-edc.

[3] https://eclipse-edc.github.io/.

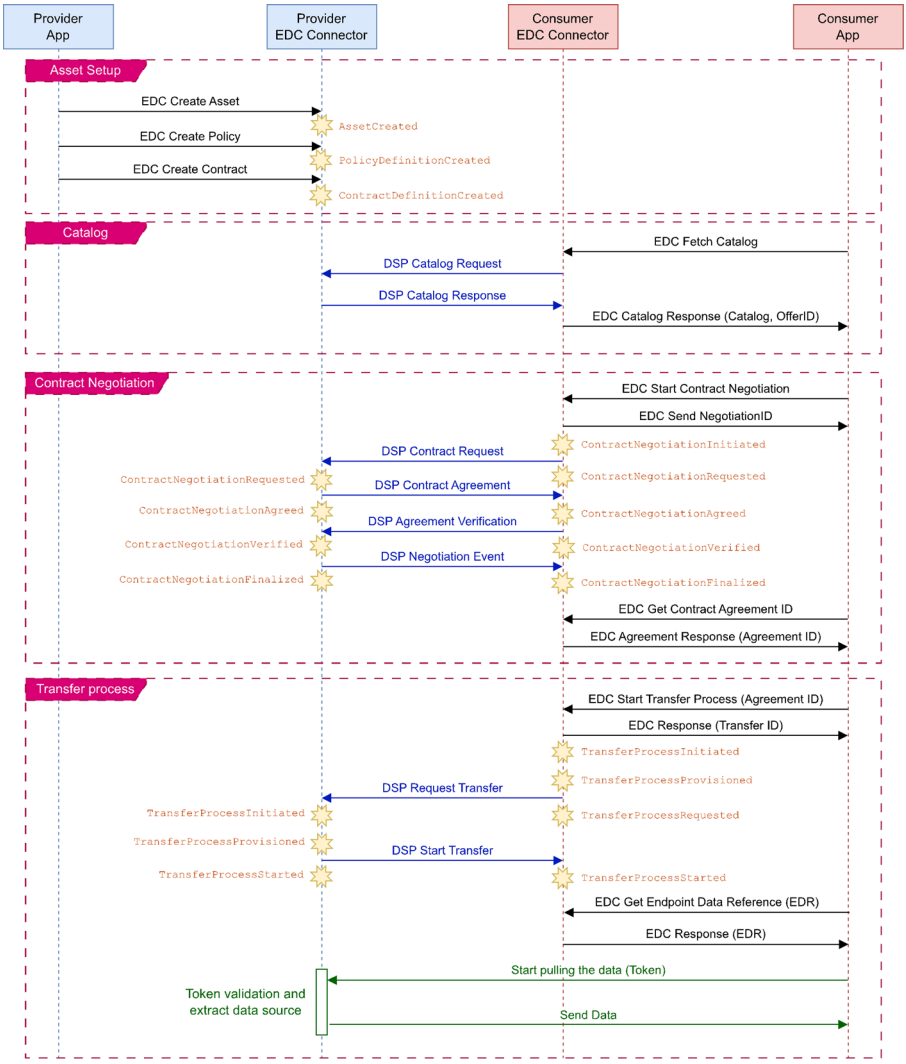

Fig. 4 Protocol messages and events in EDC case study

identifying the states on which a Connector involved in any of the phases of the contract negotiation or data transfer can be, as well as the transitions among such states.

During the *Asset Setup* phase, the data asset that the provider intends to offer is created, along with the definition of the policies and contract conditions associated with that particular asset. Using EDC Create Asset API, the primary configuration involves specifying the URL of the provider's internal endpoint where the datasets to be offered are stored. EDC Create Policy API allows for the definition of a set of rules that specify how a data asset can be accessed and used. These rules essentially define the actions that are permitted, prohibited, or mandatory for a given data asset. EDC Create Contract API enables the provider to link the previously created policies

to a set of assets based on their preferences. This way, the contract created through this API establishes the conditions under which a consumer can access the assets during the negotiation phase, as well as the policy governing the use of the assets once access is granted.

Subsequently, the consumer needs to discover which assets are available for potential use or acquisition within the data space. The catalog facilitates the discovery and identification of assets relevant to the consumer without requiring direct access to the actual data at this stage. The catalog includes key metadata about the data assets, such as dataset descriptions, associated usage policies, and access conditions. EDC Fetch Catalog API enables the consumer to request the provider's data catalog.

Based on the information received from the catalog, the consumer can propose a new contract offer with terms of interest. The negotiation process begins when the consumer sends a contract offer to the provider (EDC Start Contract Negotiation API). The provider validates the received offer by comparing it against its own terms. It then responds with either an agreement or a rejection, depending on the validation outcome. If the validation is successful, both the provider and the consumer store the agreement for future reference. This process is executed asynchronously in the background using a state machine implemented in both the provider's and the consumer's connectors. The outcome of a successful negotiation is a Contract Agreement ID, which is required for the subsequent data transfer phase.

By means of the identifier of the previously negotiated agreement, the consumer can request the provider to initiate the data transfer (EDC Start Transfer Process API). Similar to the negotiation process, data transfer is managed asynchronously by the state machine in each connector. To monitor the current state of the transfer, another identifier, the Transfer ID, is generated. Upon receiving the *DSP Request Transfer* request, the provider sends the consumer an object called Data Address through the *DSP Start Transfer* message.

The *Data Address* object contains the endpoint where the datasets can be requested, the storage type (e.g., Amazon S3, HTTP endpoint), the necessary credentials or access tokens, and any additional parameters required to retrieve the data. Since the EDC Connectors use the Data Address internally, part of its information is exposed to third-party applications through an object called Endpoint Data Reference (EDR). The most relevant information in the EDR is, precisely, the endpoint where the consumer can send requests to query data and the authorization token for validating these requests. Each time the provider receives a request at the endpoint indicated in the EDR associated to that *Transfer ID*, it validates the token, retrieves the requested dataset from its internal data source, and finally replies to the request by sending that dataset to the consumer.

Figure 4 also illustrates the events generated within the EDC Connectors during the execution of the EDC case study, e.g. AssetCreated, PolicyDefinitionCreated, etc. These events are internal notifications that indicate state changes or milestones reached within the DSP equivalent state machine, particularly during the negotiation and data transfer processes. These events are part of the state machine mechanism employed by the EDC Connector. Developers can leverage these events to implement custom logic or extensions that respond to specific stages of the negotiation and transfer processes. Events are fundamental to the internal functioning of the EDC,

enabling the implementation of a flexible and extensible architecture that can adapt to various integration requirements and use cases within IDS data spaces.

For the integration of the case studies conducted in this work, the events *ContractNegotiationVerified*, *ContractNegotiationFinalized*, *TransferProcessInitiated*, and *TransferProcessStarted* have been utilized, as it will be described in Sect. 6.3.

5.2 Business API Ecosystem

The Business API Ecosystem (BAE) is the result of a collaboration between FIWARE and the TM Forum. It is a joint component created by integrating the FIWARE Business Framework with a set of the standard Open APIs provided by the TM Forum [21]. This ecosystem enables the monetization of various types of products throughout the entire service lifecycle, from offering creation to charging, accounting, revenue settlement, and sharing.

5.2.1 BAE Architecture

As it can be seen in Fig. 5 the BAE commonly integrates with other FIWARE ecosystem components to implement comprehensive monetization services. For identity and access management (IdM), FIWARE provides Keyrock [25], a software solution based on OAuth 2.0 that allows applications and services, such as BAE, to delegate authentication and authorization processes. To further secure services, FIWARE offers the PEP Proxy component, which validates the OAuth 2.0 token's identity and the user's assigned policies before forwarding the user's request to the endpoint hosting the dataset of interest. For context data access, this endpoint is typically deployed as an NGSI-LD Context Broker, an HTTP Publish/Subscribe implementation based on

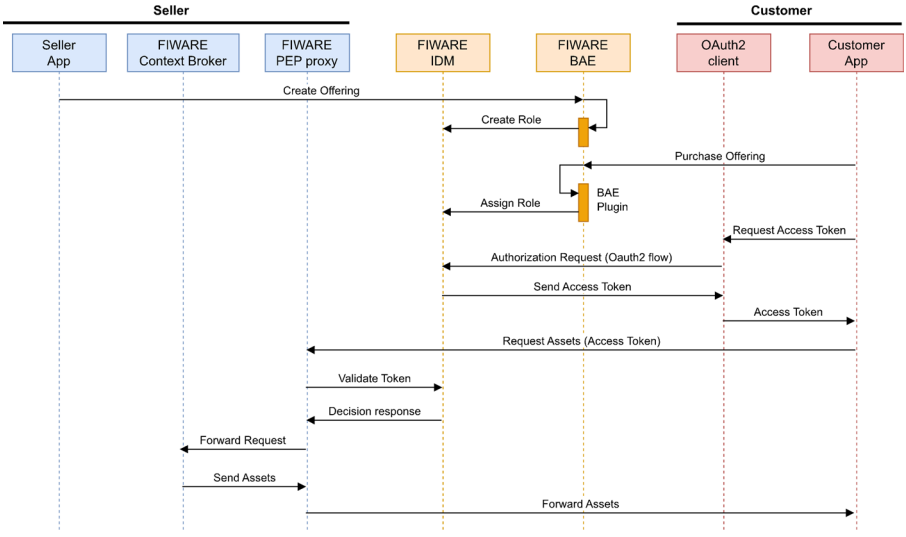

Fig. 5 Business API Ecosystem and FIWARE components relationship

the ETSI NGSI-LD standard [26]. The Context Broker manages the entire lifecycle of context information, including updates, queries, registrations, and subscriptions.

Given the wide range of functionalities offered by BAE, a well-defined model is in place for controlling user privileges and interactions between BAE components. The component responsible for managing these roles and privileges is not the BAE itself but the FIWARE IdM, which provides Role Based Access Control (RBAC) mechanisms. The two basic roles that are typically defined to establish access privileges for FIWARE BAE users are seller and customer. The seller role enables users to publish offerings for others to acquire, while the customer role allows users to acquire those offerings.

FIWARE BAE provides various mechanisms to facilitate the creation of customized solutions and integration with third-party applications. One such mechanism is the so-called BAE Plugins, a software component that allows the ecosystem's functionalities to be extended and tailored to handle specific types of assets and business models. The plugins serve several important purposes:

- Implementing specific features and validations for different asset types that are not included in the core software.
- Facilitating the monetization of various assets, both digital and physical, throughout their lifecycle.
- Performing specific validations, managing resource access, or obtaining relevant accounting information.
- Simplifying the integration of third-party applications with the FIWARE ecosystem.
- Supporting specific pricing models, such as pay-per-use for services or APIs.

Plugins act as extension points for the Business API Ecosystem, enabling developers to adapt the system to particular needs without modifying the software core. This approach simplifies the creation of customized solutions and the monetization of diverse asset types within the FIWARE ecosystem. So, it is the mechanism chosen for implementing the integration of FIWARE BAE (and implicitly the TM Forum Open APIs suite) with IDS data spaces.

The BAE Plugin implements its functionalities through event handlers. These handlers provide methods that allow developers to include code that executes at various points in a product's lifecycle (e.g., product creation, updates, or purchases). Figure 6 shows how these methods are grouped into several categories based on their functionality. The categories relevant to the work presented in this paper are:

- Create Product: Methods in this category manage the creation of new digital products. They include pre- and post-creation validations, as well as the handling of asset information and its inclusion in the product catalog.
- Create Offering: These methods handle the creation of new product offerings. They include pricing model validations before and after creation, ensuring that the pricing model is compatible with the asset and meets the plugin's specific requirements.
- Purchase Product: This method is triggered when a customer acquires a product.

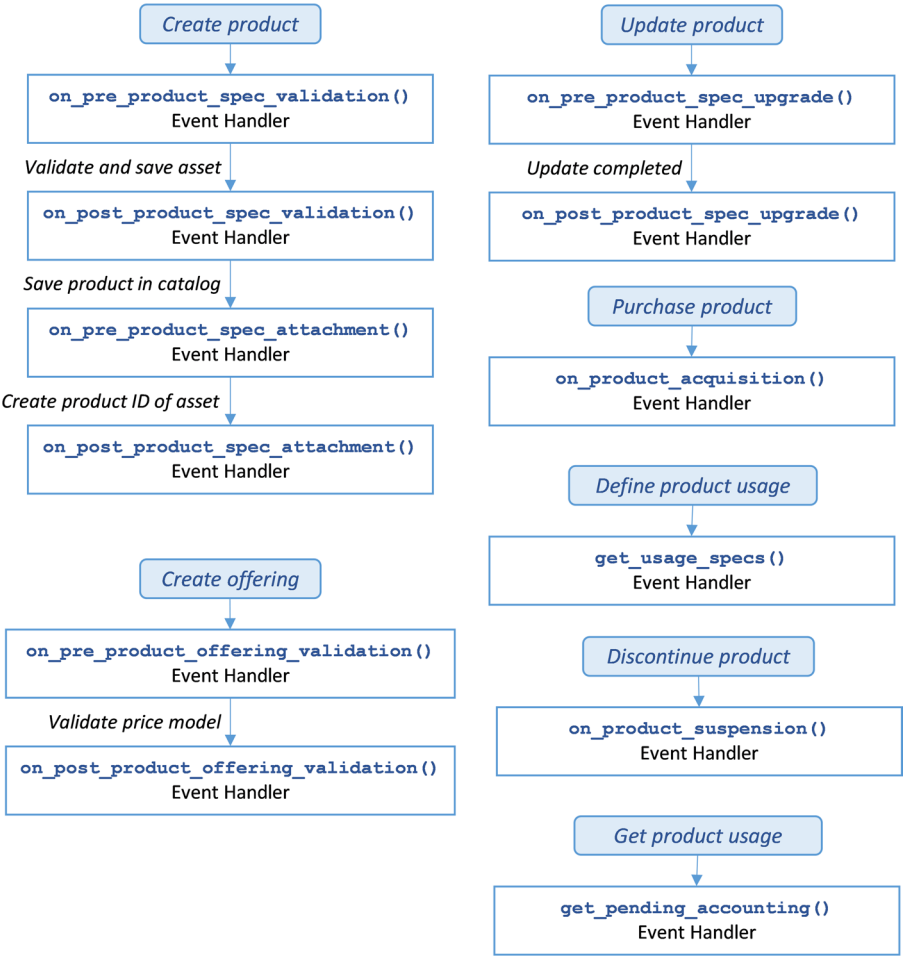

Fig. 6 BAE Plugin event handlers

It is used to trigger the corresponding service and grant access rights to the customer, so the product is available and accessible to the end user.

5.2.2 BAE Case Study

Figure 5 presents the interaction between the seller and customer for a regular situation involving the purchase of products listed in the FIWARE BAE Marketplace, as well as subsequent access to the purchased datasets. FIWARE BAE has its own frontend Graphical User Interface for both seller and consumer to perform their respective actions but, in this case study, the Seller App and Customer App components have been implemented to use the underlying FIWARE BAE API [27] and FIWARE IdM API [28].

It is important to note that the seller is responsible for the installation and configuration of the BAE Plugin and, as a result, is the only entity with the permissions to

modify its settings or functionality. The customer, on the other hand, can utilize the preconfigured features but is not authorized to make changes.

First, the seller creates a product representing the datasets they wish to place in their catalog and an offering that specifies the price for that product. The offered datasets are stored in the Context Broker. To secure them, the seller restricts external access to the Broker's endpoint by placing it within their internal network, allowing access only through the FIWARE PEP Proxy. As the proxy has to channel all the requests, the seller specifies in the product description the URL of the FIWARE PEP Proxy as the endpoint where the customer has to request the datasets. Upon completing the product creation, the *on_post_product_spec_validation* event handler of the BAE Plugin is executed. This handler creates a specific role in FIWARE IdM, defined by the seller, which groups a set of permissions granting access to the purchased datasets.

The customer initiates the purchase process by sending requests to the FIWARE BAE API. First, to retrieve available offerings, and once selected the desired offering, to create a purchase order, and finalize the payment. Upon completion of all these steps of the purchase process, the *on_product_acquisition* event handler of the BAE Plugin is executed. This handler assigns to the customer the role previously associated by the seller in the FIWARE IdM to the purchased product, thereby granting the necessary permissions to access the corresponding datasets.

Before accessing the datasets, the customer must pass through the verification process of the FIWARE PEP Proxy. The customer authenticates through FIWARE IdM using the OAuth2 client module. Hence, the customer receives an access token that authorizes access to the protected resources. The customer then sends a request to retrieve the purchased datasets, which includes the access token. The FIWARE PEP Proxy intercepts this request and verifies with the FIWARE IdM that the customer has been assigned the appropriate role for the purchased product. If the verification is successful, the PEP Proxy forwards the request to the Context Broker, which is the internal endpoint within the seller's infrastructure. Finally, the PEP Proxy only has to forward to the Customer App the requested datasets as they have been produced by the Context Broker.

5.2.3 Limitations of FIWARE BAE in Data Monetization

A notable shortcoming of FIWARE BAE lies in its absence of mechanisms enabling bilateral negotiation of dataset acquisition terms. The product's purchase conditions are unilaterally determined by the seller. Hence, the customer only has the option to accept or reject these pre-established terms. Consequently, the system exhibits a seller-centric structure, granting them substantial control over the commercial relationship while relegating the customer to a primarily passive role as a payer. Furthermore, the purchase conditions predominantly focus on monetary aspects, neglecting the potential inclusion of other salient factors such as defining the scope of permissible dataset utilization or delineating the rights and obligations of both parties. It is also important to highlight that FIWARE BAE's involvement concludes upon payment by the customer, with no subsequent oversight regarding the actual usage of the

acquired datasets. The inherent characteristics of IDS data spaces provides a good complement for addressing these limitations inherent in FIWARE BAE.

6 Integration of Data Spaces into FIWARE BAE

The integration process detailed in this section builds upon the case studies analyzed in the previous sections, demonstrating a practical implementation of data spaces within the FIWARE BAE. Leveraging the interoperability between IDS data spaces and TM Forum Open APIs discussed previously in Sect. 5, this approach leverages the main features of these two ecosystems to ensure both data sovereignty and monetization capabilities.

It is important to bear in mind that the primary participants in data spaces are referred to as provider and consumer, whereas in FIWARE BAE, they are called seller and customer. Since the roles played by both pairs of participants are essentially the same, we will hereafter use the participant names defined by data spaces.

The following subsections present the technical decisions made to achieve this integration, followed by a detailed breakdown of the implementation process.

6.1 Technical Decisions

Several key technical decisions were made to ensure a seamless and effective integration between FIWARE BAE and IDS data spaces.

6.1.1 Implementation of Essential Security Measures

While IDS data spaces are mainly pursuing the use of decentralized security models, such as W3C Verifiable Credentials, FIWARE BAE relies on centralized authentication using OAuth2. Aligning the security mechanisms behind these two views was beyond the scope of this work, as the focus has been put on product lifecycle management and business operations, and data transfer. However, considering that from a functional viewpoint it is possible to reduce it to enabling access rights issuance and verification, in this work we employed an OAuth2-based strategy to ensure interoperability while maintaining compliance with IDS-RAM security standards.

6.1.2 Removal of Overlapping Components

Some FIWARE BAE components have functionalities that overlap with those identified by IDS-RAM System Layer. Since we have considered the IDS data space as the baseline for our work and TM Forum Open APIs as complementary to provide catalog and marketplace management support, the EDC components, specifically the EDC Connector, were prioritized in the integration process. One major component removed from the FIWARE BAE architecture is the FIWARE PEP Proxy, whose functionalities are effectively handled by the EDC Connector, which in turn is mandatory for integrating data spaces. The monetization mechanisms provided by TM

Forum APIs remain unchanged, ensuring product purchases and role assignments continue to serve as a bridge between FIWARE BAE and IDS data spaces.

6.1.3 Implementation of edcUser App

Similar to the BAE case study, the functionalities of the components involved in the integration are accessed through their respective APIs. To facilitate this, a web application (i.e. *edcUser* App) has been developed to act as participants representing fictional companies on both the provider and consumer sides. These applications interact with the APIs (EDC Management API, FIWARE BAE APIs, and FIWARE IdM APIs), triggering the underlying message exchange in each phase of the business process. While neither application dictates the integration process, they must adhere to the business logic to some extent. For instance, despite completing the payment, the consumer cannot access the purchased datasets from the provider until both parties have reached a contractual agreement. The complete source code for the *edcUser* application is available on Zenodo[1].

6.1.4 Customization of EDC Connector

The integration relies on an adapted version of the EDC Connector [29]. The original EDC Connector code was modified to detect specific events and facilitate interactions with other components during contract negotiation and data transfer. The complete source code of the adapted EDC Connector is archived on Zenodo[4].

6.2 Relationship with Functional Integration

The functional integration approach described in Sect. 4.3 laid the foundation for aligning TM Forum Open APIs with IDS data spaces, ensuring interoperability between commercial and data governance processes. The implementation outlined in this section builds upon the conceptual framework established in Sect. 4.3 by applying its principles to a concrete software architecture.

Key aspects of the functional integration that directly influence this implementation include:

- Mapping of API interactions: Sect. 4.3 identified critical points where TM Forum Open APIs interface with IDS data spaces. This implementation extends those mappings by defining concrete API calls and event-driven mechanisms.
- Contract-based data exchange: The integration process formalizes the functional interactions by embedding contract negotiation into the workflow of FIWARE BAE, enabling enforceable data-sharing agreements.
- Role and access control synchronization: Sect. 4.3 discussed the need for aligning role management between FIWARE IdM and IDS data spaces. This section implements that alignment by defining explicit role assignments within the FIWARE IdM framework.

[4] https://doi.org/10.5281/zenodo.14796991.

By linking the theoretical model described in Sect. 4.3 to this implementation, the integration ensures that FIWARE BAE remains fully interoperable with IDS data spaces while keeping its compliance with TM Forum Open API standards.

6.3 Component Interaction and Data Flow

Figure 7 illustrates the architecture of the proposed integration, highlighting the interactions between FIWARE BAE, EDC Connectors, and the FIWARE IdM.

The use of the prefixes 'BAE,' 'IdM,' or 'EDC' in the interaction nomenclature in Fig. 7 denotes the utilization of corresponding APIs: FIWARE BAE API, FIWARE IdM API, and EDC Management API, respectively. Interactions devoid of these designated prefixes serve the purpose of exhibiting demonstration process information within the context of the *edcUser* application. In addition, the grey interactions correspond to the DSP protocols, which work asynchronously in the background.

The workflow can be divided into three main phases: (1) asset creation and commercialization, (2) contract negotiation, and (3) secure data exchange. The steps within each of these phases are described in detail below.

6.3.1 Phase 1: Asset Creation and Commercialization

1. Defining the digital asset in FIWARE BAE:

- A plugin is installed in FIWARE BAE to define a new asset type. In our case, this asset type allows to define a URL as an endpoint. The provider retrieves it using the BAE Get Asset Types API.
- Based on the asset type selected, the provider creates a new digital asset (BAE Asset) using the BAE Create Asset API. The asset defines a public endpoint where the consumer will request the datasets of interest. This endpoint will not respond to consumer requests until access rights are granted.

2. Product and offering definition:

- The provider generates a BAE product linked to the previously defined BAE asset, incorporating additional commercial information (*BAE Create Product*).
- A BAE offering is then created (*BAE Create Offering*), defining the pricing model and payment terms.
- The *on_post_product_spec_validation* event handler in the BAE Plugin is triggered automatically and creates a specific role (*ASSET_BUYER*) in FIWARE IdM. This role will later be assigned to consumers upon successful contract negotiation.

3. Asset registration in EDC:

- The provider generates a new asset (EDC Asset) using the most relevant properties of the previously created BAE asset, BAE offering, and BAE product, enabling the linkage of assets across both technologies. Additionally, the internal

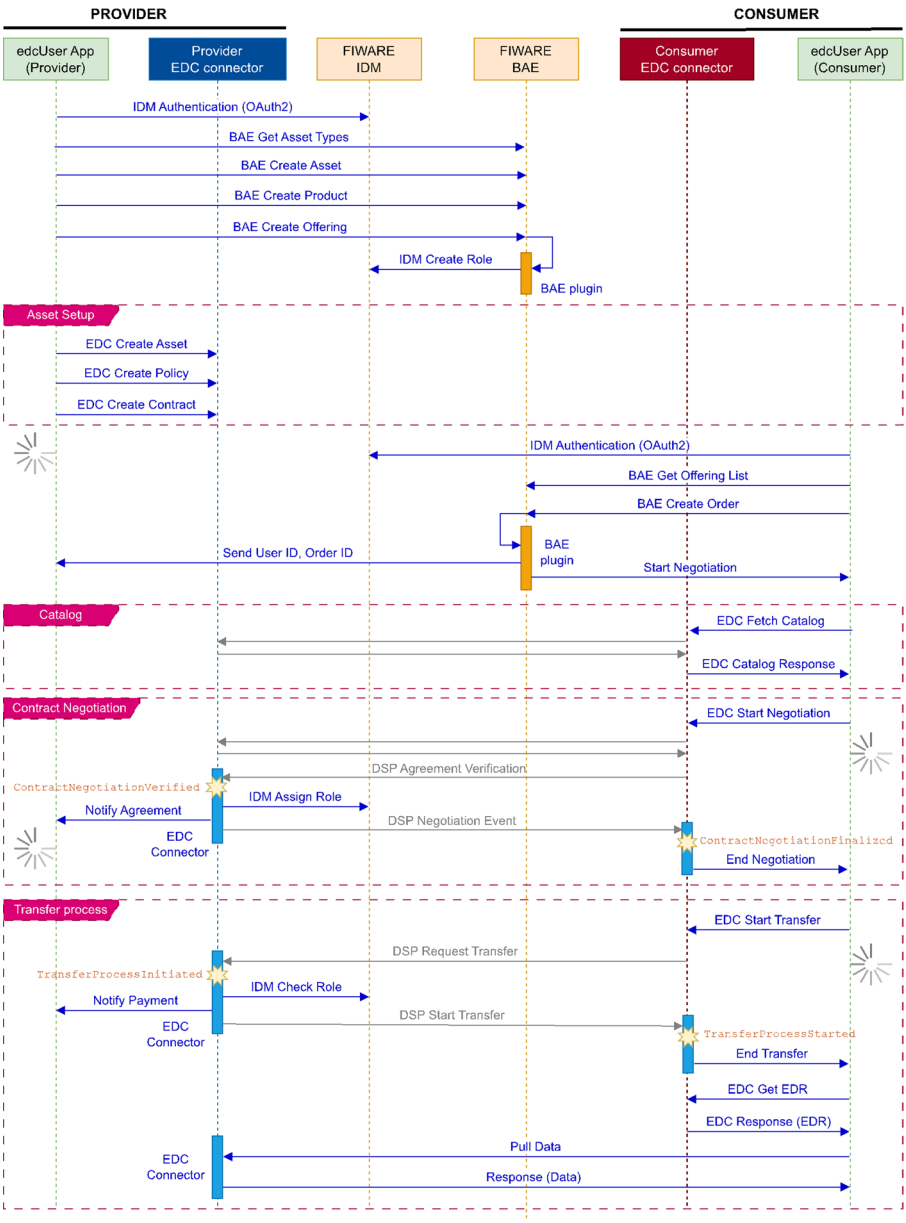

Fig. 7 Integration of data spaces in FIWARE BAE

endpoint of the provider, where the actual datasets intended for sale are stored, is included (*EDC Create Asset*).

- The terms governing the sharing and access of datasets are established through the EDC Create Policy, while the agreements defining the policies to be enforced upon the datasets after their sale are specified in the EDC Create Contract. All

created policies are automatically stored in the EDC catalog.

4. Consumer requests available BAE assets:

- The consumer queries FIWARE BAE for available offerings (*BAE Get Offering List*).
- Once an offering is selected, a purchase order is created (*BAE Create Order*), triggering the standard BAE payment process.
- The *on_product_acquisition* event is triggered in the BAE Plugin, notifying the provider of the information that identifies the consumer and the order acquired. The provider will subsequently use these IDs, during the negotiation process, to assign the ASSET_BUYER role to the consumer.

At this stage of the integration, the customer has already completed the payment for the desired datasets but has not yet been granted access. They already know the URL of the public endpoint to request the datasets. However, they lack the necessary authorization to retrieve them. To obtain access, the negotiation process must be finalized.

6.3.2 Phase 2: Contract Negotiation in the Data Spaces

1. Negotiation process in EDC:

- The consumer retrieves the catalog of available data assets from the provider's EDC Connector (*EDC Fetch Catalog*).
- The consumer selects an asset and initiates contract negotiation (*EDC Start Negotiation*), potentially proposing modifications to the default contract terms.
- The negotiation process occurs asynchronously, with the EDC Connector managing state transitions until both parties reach an agreement.

2. Assignment of access rights:

- When both participants successfully validate the contract, the *ContractNegotiationVerified* event is triggered within the provider's EDC Connector.
- The provider uses FIWARE IdM APIs to assign the ASSET_BUYER role to the consumer, authorizing access to the purchased dataset.
- The negotiation process concludes with the *ContractNegotiationFinalized* event, signaling to the consumer that access to the datasets is now enabled.

If the participants fail to reach an agreement during the negotiation process, the consumer is not assigned the *ASSET_BUYER* role, and a notification is sent to the Product Ordering Management API of the TM Forum APIs embedded within FIWARE BAE to cancel the order for the acquired product. The IDS Dataspace Protocol enables the manual implementation of intelligent retry mechanisms based on the states and error codes generated by failed negotiations.

6.3.3 Phase 3: Secure Data Exchange

1. Initiating the data transfer:

- The consumer starts the data transfer process by sending an *EDC Start Transfer* request.
- When the *TransferProcessInitiated* event is triggered in the provider's EDC connector, it is verified that the consumer holds the required *ASSET_BUYER* role in FIWARE IdM before proceeding.

2. Providing the consumer with access credentials:

- Upon successful verification, the provider's EDC Connector generates an *Endpoint Data Reference* (EDR), containing: (a) the public endpoint for dataset retrieval, and (b) the required authentication token.
- The consumer retrieves the dataset using the EDR, ensuring that data exchange complies with the negotiated contract terms.

The verification phase is crucial, as it ensures that the consumer has successfully completed the negotiation process. If the consumer fails to pass this phase, the dataset transfer is not executed, and a notification is sent to the Billing Management API of the TM Forum APIs embedded within FIWARE BAE to cancel the billing and purchase order.

7 Discussion on Comparative Analysis and Advantages

Recent approaches to integrating data spaces with existing systems have primarily focused on Industry 4.0 scenarios, where the emphasis is on manufacturing processes and industrial data exchange. Stojanovic et al. [30] propose a layered architecture that aligns Industrial Data Space components with Industry 4.0 elements, thereby facilitating industrial automation. Similarly, prior research has explored the integration of Industry 4.0-compliant Digital Twins with International Data Spaces, leveraging the ISO DIS 23,247 architectural framework to ensure data sovereignty [12]. Furthermore, the use of the IDS reference model for scalable Digital Twin implementations has been demonstrated in the manufacturing sector, addressing key concerns related to data protection and sovereignty [13]. While these approaches provide robust solutions for industrial automation and data exchange, they do not comprehensively address the challenges of integrating data sovereignty with broader business ecosystem processes.

Our proposed solution offers several distinct advantages over existing approaches:

1. Business process integration.

- While previous solutions focus mainly on technical interoperability, our approach seamlessly integrates data sovereignty mechanisms with established business

processes through the TM Forum Open APIs framework.
- The integration leverages existing business ecosystem components (BAE Plugin architecture) rather than requiring new intermediate layers, reducing implementation complexity.

2. Monetization capabilities.

- Unlike industrial integration approaches, which primarily address data exchange, our solution maintains full monetization capabilities through the FIWARE BAE.
- The integration enables flexible pricing models and revenue sharing while ensuring data sovereignty, a combination not previously addressed in existing solutions.

3. Standards compliance.

- Our approach maintains compliance with both TM Forum standards and IDS-RAM specifications, ensuring interoperability at both the business level and data spaces level. In fact, the design that has been proposed looks for the synergies that exists between the two ecosystems.
- The solution allows organizations to leverage their existing investments in TM Forum-compliant systems while adopting capabilities of IDS data spaces.

4. Implementation flexibility.

- The modular design, based on the BAE Plugin architecture and EDC Connector events, enables gradual adoption of IDS data spaces features without disrupting existing services.
- Organizations can selectively implement specific aspects pertaining to data sovereignty, identity, authentication and authorization management or access and usage policies, while maintaining their current business operations and the same integration structure.

5. Extensibility.

- The integration framework can be extended to support additional data spaces features or business processes through the plugin mechanism or connector functionalities.
- The event-based architecture facilitates the incorporation of new functionalities without modifying the core integration components.

This combination of features positions our solution as particularly suitable for organizations seeking to enhance their existing business ecosystems with data sovereignty capabilities, especially in contexts where commercial aspects are as critical as technical data exchange requirements.

The integration of IDS data spaces into FIWARE BAE enhances traditional asset monetization by introducing contract negotiation and granular access control. Table 3

Table 3 IDS and FIWARE BAE integration improvements

Aspect	Standard FIWARE BAE workflow	Proposed integration
Negotiation flexibility	Consumers must accept predefined conditions	Consumers can negotiate custom contract terms
Data sovereignty	No control over data usage post-purchase	Data sharing governed by enforceable contracts.
Access control	Role assignment based solely on payment	Role assignment contingent on contract validation. Role assignment depends on the parties reaching an agreement.
Traceability	No tracking of data usage after purchase	EDC Connector enforces data access policies.

summarizes the key improvements that are achieved through the complementarity of both ecosystems that have been leveraged by the solution that we have proposed in this paper.

8 Conclusions and Future Work

The work described in this paper has demonstrated the feasibility and benefits of integrating TM Forum Open APIs with IDS data spaces technologies, addressing critical gaps in current telecommunications service management systems while preserving their established strengths. The implementation, validated through comprehensive case studies, proves that data sovereignty and trusted exchange can be effectively incorporated into existing business ecosystems without compromising their core functionalities.

Key findings include:

- The thorough analysis of the functional characteristics of both frameworks has led to a functional integration, which serves as the foundation for the software integration implementation.
- The successful mapping between BAE Plugin handlers and EDC Connector events enables seamless integration of commercial and data governance processes.
- The proposed architecture maintains separation of concerns while ensuring coordinated operation of both frameworks.
- The integration solution effectively addresses the limitations of TM Forum Open APIs regarding data sovereignty and usage control.

The practical implications of this work are significant for the telecommunications industry. Organizations can now implement robust data governance mechanisms while maintaining standardized business processes, enabling new business models based on controlled data exchange. The solution's modular design, based on plugins architecture and asynchronous events, allows for gradual adoption, reducing implementation risks and costs. Moreover, the modularity also enables for the adoption of different solutions supporting the included functionalities, mainly in terms of how

identities and authorization are managed so that Self Sovereign Identities frameworks (preferred on the IDS data spaces ecosystems) could be used.

However, several limitations should be acknowledged. The current implementation focuses on specific components of both frameworks, and further work is needed to extend the integration to other elements. Additionally, the security model requires further development to fully align with production requirements.

Future research directions include:

- Extending the integration to include additional IDS-RAM components.
- Developing comprehensive security models that address both frameworks' requirements.
- Investigating scalability aspects for large-scale deployments.
- Exploring integration with other data spaces implementations.
- Evaluating performance impacts in production environments.

As data spaces continue to evolve and gain adoption across industries, this integration framework provides a foundation for future developments in trusted data exchange within business ecosystems.

Acknowledgements This work has been supported by the Spanish State Research Agency (AEI) through the projects THROTTLE (TrustwortHy uRban mObility daTa markeTpLacE, Grant Agreement No. TED2021-131988B-I00) and SITED (Semantically-enabled Interoperable Trustworthy Enriched Dataspaces, Grant Agreement No. PID2021-125725OB-I00). It has also been supported by the Spanish Ministry of Science, Innovation and Universities (MICIU) by means of a José Castillejo International Mobility Grant (ref. CAS23/00453).

Author Contributions Conceptualization, J.C. and L.S.; methodology, J.C. and L.S.; software, J.C. and P.S.; investigation, J.C. and P.S.; writing—original draft preparation, J.C. and L.S.; writing—review and editing, L.M., J.L. and P.S.; supervision, L.S.; funding acquisition, L.S. and J.L. All authors have read and agreed to the published version of the manuscript.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Competing Interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. ITP.NET: e& adopts TM forum and Camara-based Open APIs, June 2024. Accessed: January 17, 2025. Available: https://www.itp.net/industry/e-adopts-tm-forum-and-camara-based-open-apis
2. Ericsson: Breaking legacy silos in OSS/BSS: A recipe for CSP success, October 2023. Accessed: January 17, 2025. Available: https://www.ericsson.com/en/blog/2023/10/breaking-legacy-silos-in-ossbss-a-recipe-for-csp-success
3. Forum, T.M.: Open API adoption assessment report, 2021. Accessed: January 17, 2025. Available: https://www.tmforum.org/open-apis/adoption-assessment-report/
4. Otto, B., Steinbuss, S., Teuscher, A., Lohmann, S.: IDS reference architecture model. Zenodo (2019). https://doi.org/10.5281/ZENODO.5105528
5. IDS Dataspace Protocol: Accessed: March 10, 2025. Available: https://docs.internationaldataspaces.org/dataspace-protocol/
6. Otto, B., Hompel, M., Wrobel, S. (eds.): Designing Data Spaces. Springer International Publishing, (2022). https://doi.org/10.1007/978-3-030-93975-5
7. Zrenner, J., Möller, F.O., Jung, C., Eitel, A., Otto, B.: Usage control architecture options for data sovereignty in business ecosystems. J. Enterprise Informat. Manag. **32**(3), 477–495 (2019). https://doi.org/10.1108/jeim-03-2018-0058
8. Otto, B.: The evolution of data spaces. In: Designing Data Spaces, pp. 3–15. Springer International Publishing (2022). https://doi.org/10.1007/978-3-030-93975-5_1
9. Solmaz, G., et al.: Enabling data spaces, Proceedings of the 1st International Workshop on Data Economy. ACM, pp. 42–48, (2022). https://doi.org/10.1145/3565011.3569058
10. Gaia-X European Association for Data and Cloud: Gaia-X Architecture Document-25.05 Release, [Online]. Accessed: September 24, 2025. Available: https://docs.gaia-x.eu/technical-committee/architecture-document/25.05/
11. The Data Spaces Radar: (Version 4), March 2024. Accessed: January 17, 2025. Available: https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/The-Data-Spaces-Radar-Version-4.pdf
12. Jacoby, M., Volz, F., Weißenbacher, C., Stojanovic, L., Usländer, T.: An approach for Industrie 4.0-compliant and data-sovereign Digital Twins. at - Automatisierungstechnik **69**(12), 1051–1061 (2021). https://doi.org/10.1515/auto-2021-0074
13. Moreno, T., Almeida, A., Toscano, C., Ferreira, F., Azevedo, A.: Scalable Digital Twins for industry 4.0 digital services: a dataspaces approach. Product. Manuf. Res. (2023). https://doi.org/10.1080/21693277.2023.2173680
14. Giussani, G., Steinbuss, S., Gras, N., Prasse, T.: Data connector report. Zenodo (2024). https://doi.org/10.5281/ZENODO.7405406
15. Forum, T.M.: Promoting a trusted telco data space to drive new opportunities, October 2021. Accessed: March 03, 2025. Available: https://inform.tmforum.org/research-and-analysis/proofs-of-concept/promoting-a-trusted-telco-data-space-to-drive-new-opportunities
16. TM Forum Catalyst Project: Telco data space. Accessed: February 26, 2025. Available: https://myaccount.tmforum.org/networks/21-0-223/index.html
17. Open Network Automation Platform (ONAP): Offered APIs, Accessed: Septembre 28, 2025. Available: https://docs.onap.org/projects/onap-externalapi-nbi/en/latest/offeredapis/offeredapis.html
18. Fraunhofer ISST Connector: Accessed: September 28, 2025. Available: https://international-data-spaces-association.github.io/DataspaceConnector/
19. Engineering True Connector: Accessed: September 28, 2025. Available: https://github.com/Engineering-Research-and-Development/true-connector
20. FIWARE Business API Ecosystem: Accessed March 10, 2025. Available: https://business-api-ecosystem.readthedocs.io/en/latest/
21. Forum, T.M.: Open API Directory, Accessed: January 17, 2025. Available: https://www.tmforum.org/oda/open-apis/directory
22. Foundation, E.: Eclipse Dataspace Components, Accessed: March 10, 2025. Available: https://projects.eclipse.org/projects/technology.edc
23. EDC Management API: Accessed March 10, 2025. Available: https://eclipse-edc.github.io/Connector/openapi/management-api/
24. EDC transfer samples: Accessed March 10, (2025). Available: https://github.com/eclipse-edc/Samples/tree/main/transfer

25. Identity Manager (IdM:) GE API specifications, Accessed: March 10, 2025. Available: https://keyrock.docs.apiary.io/
26. Context Information Management (CIM) ETSI Industry Specification Group (ISG): NGSI-LD API, March 2024. Accessed: February 26, 2025. Available: https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.08.01_60/gs_cim009v010801p.pdf
27. de la Vega, F.: FIWARE TMF Business API Ecosystem, Accessed: March 10, 2025. Available: https://FIWAREtmfbizecosystem.docs.apiary.io/
28. FIWARE Foundation.: FIWARE Identity Manager API, Accessed: March 10, 2025. Available: https://keyrock.docs.apiary.io/
29. Eclipse Foundation: Eclipse Dataspace Components Connector, Accessed: January 17, 2025. Available: https://github.com/eclipse-edc/Connector
30. Alexopoulos, K., et al.: Bridging the gap between IDS and Industry 4.0 - Lessons learned and recommendations for the future. Zenodo (2024). https://doi.org/10.5281/ZENODO.10730337

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Johnny Choque[1] · Luis Sánchez[1] · Jorge Lanza[1] · Pablo Sotres[1] · Luis Muñoz[1]

✉ Johnny Choque
jchoque@tlmat.unican.es

✉ Luis Sánchez
lsanchez@tlmat.unican.es

[1] Network Planning and Mobile Communications Lab, Universidad de Cantabria, Santander 39005, Spain