www.ECLIPSE DIGITAL-digital.eu

30 November 2025

D3.1 CERF architecture specification and ECLIPSE DIGITAL interoperability profiles

Funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. DIGITAL EUROPE Grant agreement N° 101158494.

Deliverable details

Title	WP	Version
D3.1 CERF architecture specification and ECLIPSE DIGITAL interoperability profiles – preliminary version	WP3	V1.0

Contractual delivery date	Actual delivery date	Delivery type*	Dissemination**
30/11/2025	30/11/2025	R	PU

* Delivery type: R: Document, report; DEM: Demonstrator, pilot, prototype; DEC: Websites, patent fillings, videos, etc; DMP: Data management plan.
** Dissemination Level: PU - Public; SEN – Sensitive, limited under the conditions of the Grant Agreement.

Author(s)	Organization
Dune Sebilleau, Diana Jimenez, Tareq Chy	Trialog

Version	Date	Person	Action	Status***
V0.1	30/04/2025	Dune Sebilleau	Creation of the structure	Draft
V0.2	30/06/2025	Diana Jimenez, Tareq Chy	Integration of contents	Preliminary version

V0.3	22/09/2025	Dune Sebilleau, Diana Jimenez, Tareq Chy	Integration of interoperability profiles	Draft
V0.4	20/10/2025	Dune Sebilleau, Diana Jimenez, Tareq Chy	First version ready for review	Draft
V0.5	10/11/2025	Lola Alacreu, Diego García-Casarrubios Gálvez, Alejandro Vicent, Sonam Parashar, Kamalanathan Ganesan, Kashyap Shievam	Reviews	Draft
V1.0	30/11/2025	Dune Sebilleau, Diana Jimenez, Tareq Chy	Integration of reviews	Final

***Status: Draft, Final, Approved, Submitted (to European Commission).

KEYWORDS

CERF, Interoperability, Architecture, Data exchange, Reference model, SGAM, DERA, interface, standard.

EXECUTIVE SUMMARY

Deliverable D3.1 aims to define the interoperability foundations of the CERF and the ECLIPSE DIGITAL project. It consolidates the architecture, data exchanges, and standards relevant to the CERF, building on inputs from the ECLIPSE DIGITAL pilots and on analyses of previous initiatives. These architectural elements, together with their associated data flows and standards, are mapped to the High-Level Use Cases described in Deliverable 2.2 (Energy services analysis, use cases, and CERF requirements). Once the key components of the CERF architecture and their interactions were identified, the resulting consolidated architecture was formalised as shown below.

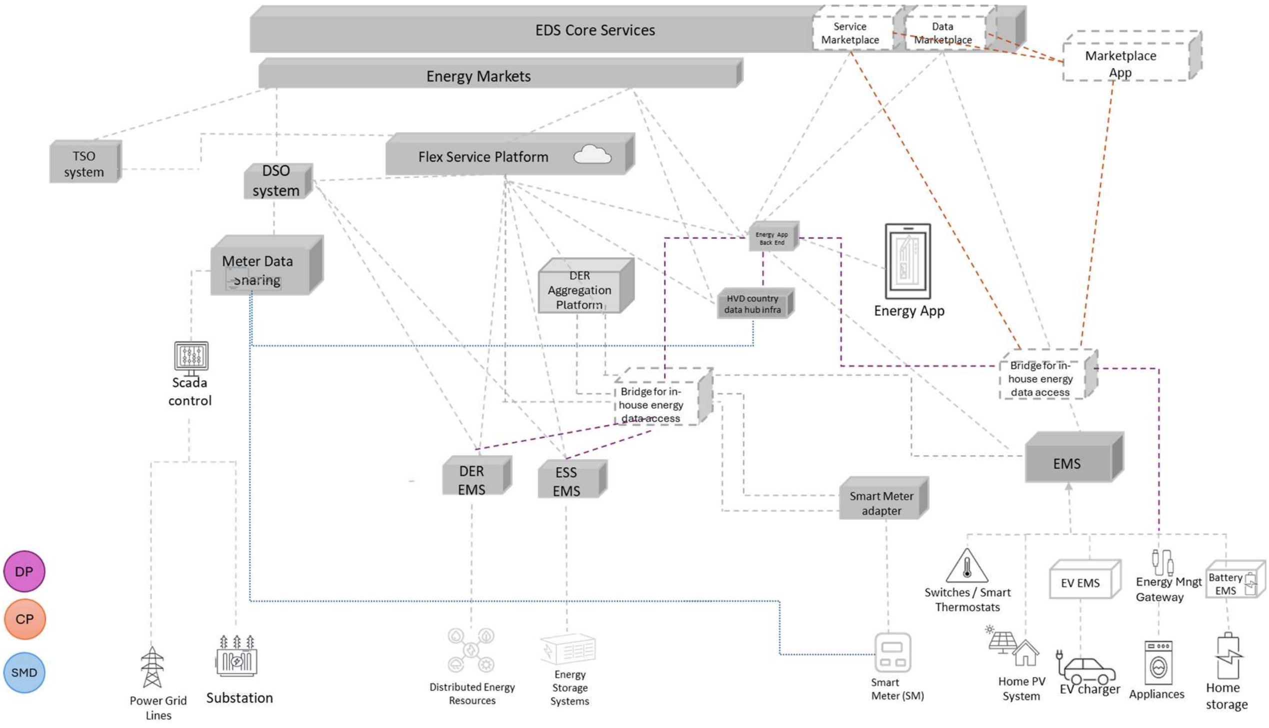


Figure 1: ECLIPSE DIGITAL CERF Architecture

This architecture is further detailed through the application of the SGAM layers, the Hourglass model, and the DERA framework, providing both structural and data-exchange perspectives. In addition, HLUC-specific architectures were developed to guide the implementation of the CERF across the diverse pilot scenarios. A future-proofing exercise complements this work by examining how Data Spaces can be incorporated into the CERF, following the CEEDS framework and principles.

To support implementation, three interoperability profiles were defined for the project's three main interfaces, providing targeted guidance to ensure consistent and interoperable solutions. Building on this architecture, the corresponding data exchanges for each interface were specified, including the labelling, classification, and characterisation of all datasets relevant to ECLIPSE DIGITAL. A dedicated study assessed available data catalogue technologies, leading to the recommendation of using CKAN configured with a DCAT-AP–compliant metadata model and a core FAIR catalogue profile for the ECLIPSE DIGITAL project. Three interoperability profiles were then defined, covering the three main interface types of the project:

- The Energy App Interface profile
- The Data Sources Interface profile
- The DSO Interface profile

Each profile covered five interoperability layers, defining for each of them the context of application, the relevant standards, and recommendations for the implementation:

- Transport interoperability
- Syntactic interoperability
- Semantic interoperability
- Behavioural interoperability
- Policy interoperability

Finally, the governance of the CERF was defined in the last section.

The specifications of this deliverable are to be detailed through the development and deployment phases of the ECLIPSE DIGITAL pilots in WP4 “Design and development of CERF and APIs” and WP5 “Preparation, coordination and monitoring of deployment and demonstration activities”.

COPYRIGHT STATEMENT

The work described in this document has been conducted within the ECLIPSE DIGITAL project. This document reflects only the ECLIPSE DIGITAL Consortium view, and the European Union is not responsible for any use that may be made of the information it contains.

This document and its content are the property of the ECLIPSE DIGITAL Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the ECLIPSE DIGITAL Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the ECLIPSE DIGITAL Partners.

Each ECLIPSE DIGITAL Partner may use this document in conformity with the ECLIPSE DIGITAL Consortium Grant Agreement provisions.

INDEX

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1. PURPOSE OF THE DOCUMENT

This document gathers the findings of the tasks T3.1 (Specifications of suitable data sets and digital environment), T3.2 (Definition of the architecture of a scalable and interoperable European open-source CERF) and T3.3 (Definition of standard interfaces and protocols of the CERF) of the ECLIPSE DIGITAL project. It aims to provide a functional and replicable blueprint for the Common European Reference Framework (CERF) for energy-saving apps. This blueprint should facilitate the implementation of future energy-saving apps and ensure their interoperability with their environment.

1.2. STRUCTURE OF THE DOCUMENT

This document includes the specification of the CERF, focussing on interoperability aspects, its purpose is explained in Section 1.

Section 2 defines the CERF architecture, beginning with the applied methodology, including relevant standards, modelling frameworks, levels of detail, and the relation with the CERF, before presenting the generic architecture through key component identification, the flexibility reference model, consent-driven marketplace considerations, and the generic functional components. It then introduces the use-case-specific architectures for each HLUC, followed by the future-proofing section, which addresses data spaces, component and connector identification, the Energy Data Space concepts applied to ECLIPSE DIGITAL, its SGAM mapping, technical aspects for integration, and the overall future outlook for the CERF architecture.

Section 3 describes the data exchanges within the CERF, defining how the energy apps interact with their environment. It includes the definition of the different interfaces, derived from the architecture, as well as the specification and classification of the data used and exchanged in each interface. It moreover describes the data catalogue developed for the CERF.

Section 4 presents the standard interfaces and protocols relevant to the CERF. It begins with a survey of previous projects, followed by an overview of the protocols and standards most applicable to CERF implementations. This includes recommendations for interface profiles, covering the Energy App Interface Profile, the Data Sources Interface Profile, and the DSO Interface Profile. The section then introduces a set of open-source reusable connectors, providing an overview of potential connector options such as the Generic Adapter (GA) from InterConnect, the EDDIE [1] Connector, and the ECLIPSE DIGITAL Semantic Modelling Framework (ESMF). A comparative analysis of these connectors is provided, together with a mapping of their applicability to the CERF High-Level Use Cases and pilots.

Section 5 describes the construction of interoperability profiles within the CERF. It begins with the methodology used, then outlines the interoperability profiles defined for the CERF architecture. The section proceeds with detailed profiles for the Energy App Interface, starting from the interoperability scenario and point, followed by the interoperability case and the corresponding profile. This profile is broken down across the four layers of interoperability: transport, syntactic, semantic, behavioural, and policy. Next, the section addresses the Data Sources Interface, focusing on flexibility and aggregation use cases. It follows the same structure: scenario, interoperability point, case, and layered profile. Ensuring a consistent approach. A similar breakdown is applied to the

DSO Interface, providing full traceability across each interoperability dimension. This part concludes with an integrated view that consolidates the interoperability findings across all interfaces, followed by a refinement and validation phase to ensure coherence, completeness, and alignment of the constructed profiles.

Finally, Section 6 focusses on the definition of a governance scheme for the CERF.

2. ECLIPSE DIGITAL CERF ARCHITECTURE

2.1. METHODOLOGICAL FOUNDATIONS

The methodological foundations of the ECLIPSE DIGITAL CERF architecture combine established reference models, architectural frameworks, and prior project outputs to ensure a structured, interoperable, and future-ready design. SGAM provides the baseline modelling framework across domains, zones, and interoperability layers; DERA contributes a harmonised view; and the Hourglass model introduces an analysis for Stakeholders and Capabilities. These frameworks are complemented by the initial CERF blueprint developed in the InterConnect project, which ECLIPSE DIGITAL extends toward user-centric energy applications and European-scale demonstrability. Together, these methodological elements guide the systematic development, alignment, and evolution of the ECLIPSE DIGITAL CERF architecture.

2.1.1. SGAM: SMART ENERGY GRID ARCHITECTURE MODEL

The architecture of the system developed and implemented in the ECLIPSE DIGITAL project was designed using the SGAM. It is a unified standard allowing for the representation of a smart grid architecture, described in [2]. It consists of five interoperability layers mapped to electrical domains and information management zones.

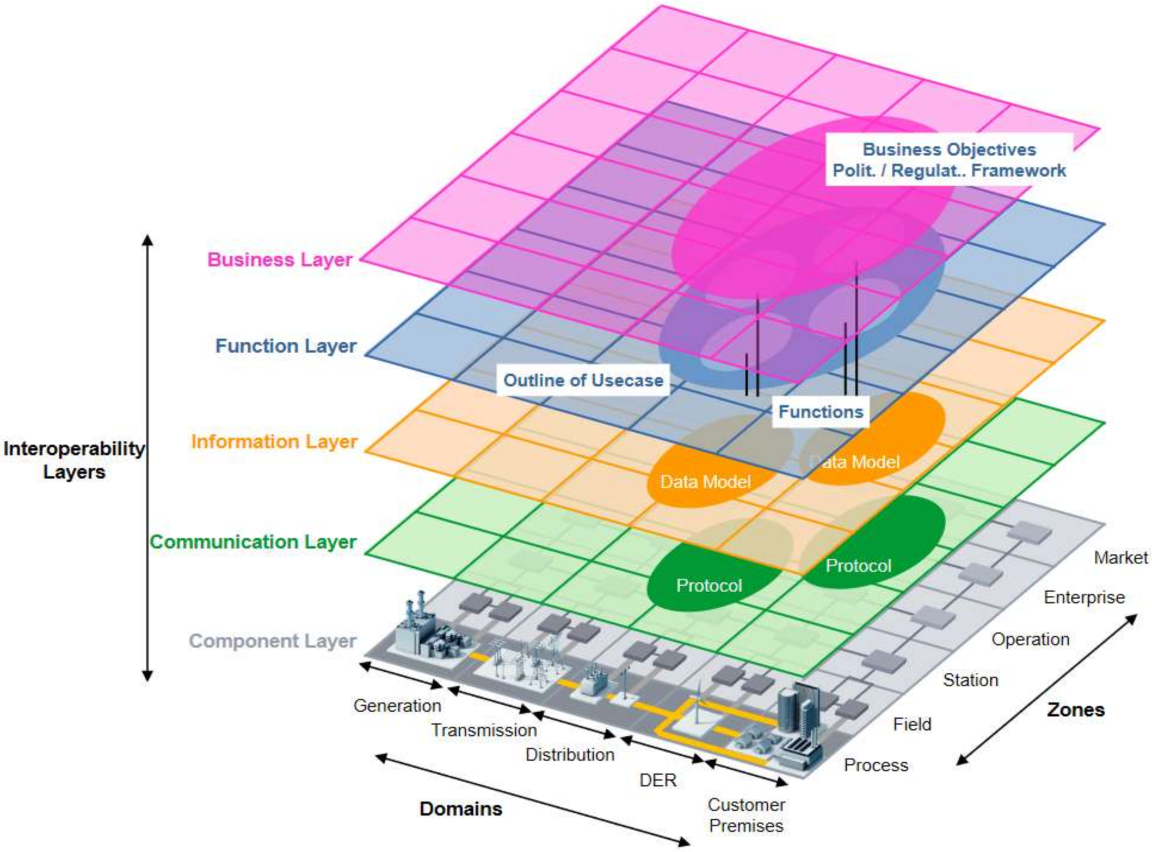


Figure 2: SGAM framework

Each layer focuses on a different level of abstraction:

- The **business layer** is used to map regulatory and economic structures as well as policies, business models, business portfolios (products & services) of market parties involved.
- The **function layer** describes functions performed by the system as well as their relationship to one another.
- The **information layer** describes the information that is being exchanged between functions, services and components. It contains information objects and can specify the underlying canonical data models.

- The **communication layer** describes protocols and mechanisms for the interoperable exchange of information between components in the context of the underlying use case, function or service and related information objects or data models.

- The **component layer** describes the physical distribution of all participating components in the smart grid context. This includes system actors, applications, power system equipment (typically located at process and field level), protection and tele-control devices, network infrastructure (wired / wireless communication connections, routers, switches, servers) and any kind of computers.

Each layer covers the Smart Grid Plane, which is spanned by electrical domains and information management zones. This Plane distinguishes between electrical process and information management viewpoints. These viewpoints can be partitioned into the physical *domains* of the electrical energy conversion chain and the hierarchical *zones* for the management of the electrical process.

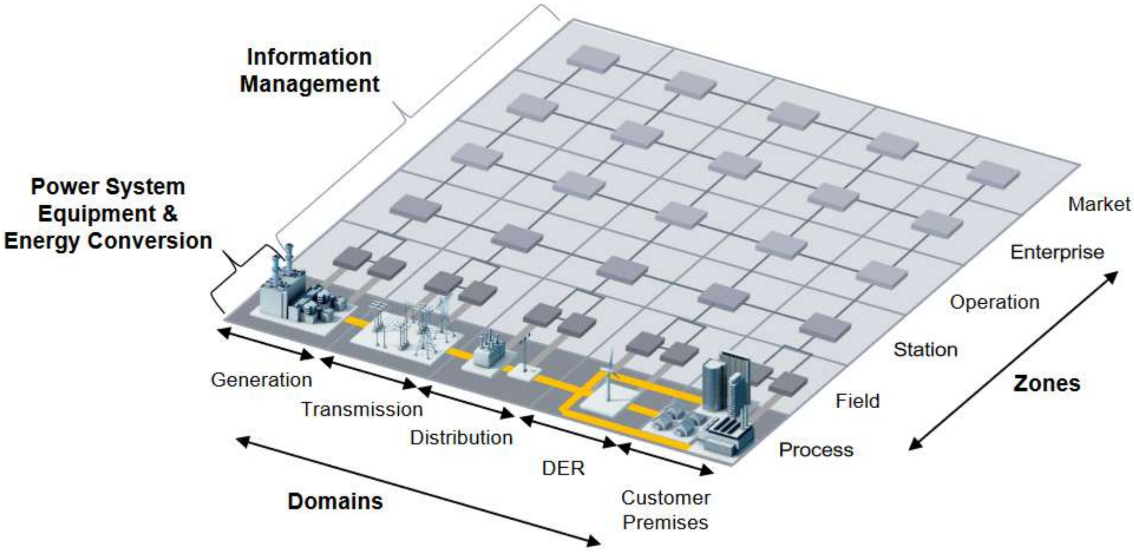


Figure 3: Smart Grid Plane – Domains and hierarchical zones

These domains are arranged according to the electrical energy conversion chain. They are defined as follows:

- **Bulk Generation**: Representing generation of electrical energy in bulk quantities, such as by fossil, nuclear and hydro power plants, offshore wind farms, large scale solar power plant (i.e., PV, CSP)– typically connected to the transmission system.
- **Transmission**: Representing the infrastructure and organization which transports electricity over long distances.
- **Distribution**: Representing the infrastructure and organization which distributes electricity to customers.
- **Distributed Electrical Resources (DER)**: Representing distributed electrical resources directly connected to the public distribution grid, applying small-scale power generation technologies (typically in the range of 3 kW to 10.000 kW). These distributed electrical resources may be directly controlled by the DSO.
- **Customer Premises**: Hosting both end users of electricity and producers of electricity. The premises include industrial, commercial, and home facilities (e.g. chemical plants, airports, harbours, shopping centres, homes). Also, generation in the form of e.g. photovoltaic generation, electric vehicles storage, batteries, micro turbines, etc. are hosted.

The SGAM zones represent the hierarchical levels of power system management and operation. They structure the system according to where functions act within the energy value chain. The zones are defined as follows:

- **Process**: Capturing the physical, chemical, or spatial transformation of energy (electricity, heat, solar, wind, water, etc.) and the equipment directly involved in these transformations. This includes primary assets such as generators, transformers, circuit breakers, overhead lines, cables, electrical loads, as well as sensors and actuators that are part of, or directly connected to, the physical process.

- **Field**: Including equipment to protect, control and monitor the process of the power system, e.g., protection relays, bay controllers, any kind of intelligent electronic devices which acquire and use to process data from the power system.

- **Station**: Representing the areal aggregation level for the field level, e.g., for data concentration, functional aggregation, substation automation, local SCADA systems, and plant supervision.

- **Operation**: Hosting power system control operation in the respective domain, e.g., distribution management systems (DMS), energy management systems (EMS) in generation and transmission systems, microgrid management systems, virtual power plant management systems (aggregating several DER), electric vehicle (EV) fleet charging management systems.

- **Enterprise**: Includes commercial and organizational processes, services and infrastructures for enterprises (utilities, service providers, energy traders …), e.g., asset management, logistics, work force management, staff training, customer relation management, billing and procurement.

- **Market**: Reflecting the market operations possible along the energy conversion chain, e.g., energy trading, mass market, retail market.

2.1.2. DERA: DATA EXCHANGE REFERENCE ARCHITECTURE

The Data Exchange Reference Architecture (DERA) [3] is used to detail the interoperability elements of the architecture, to ensure the interoperable exchange of data.

The DERA 3.1 is described in the Figure 2Figure 4. It is based on the SGAM layers and details the component types that can be used to enable data exchanges, both on local and federated levels.

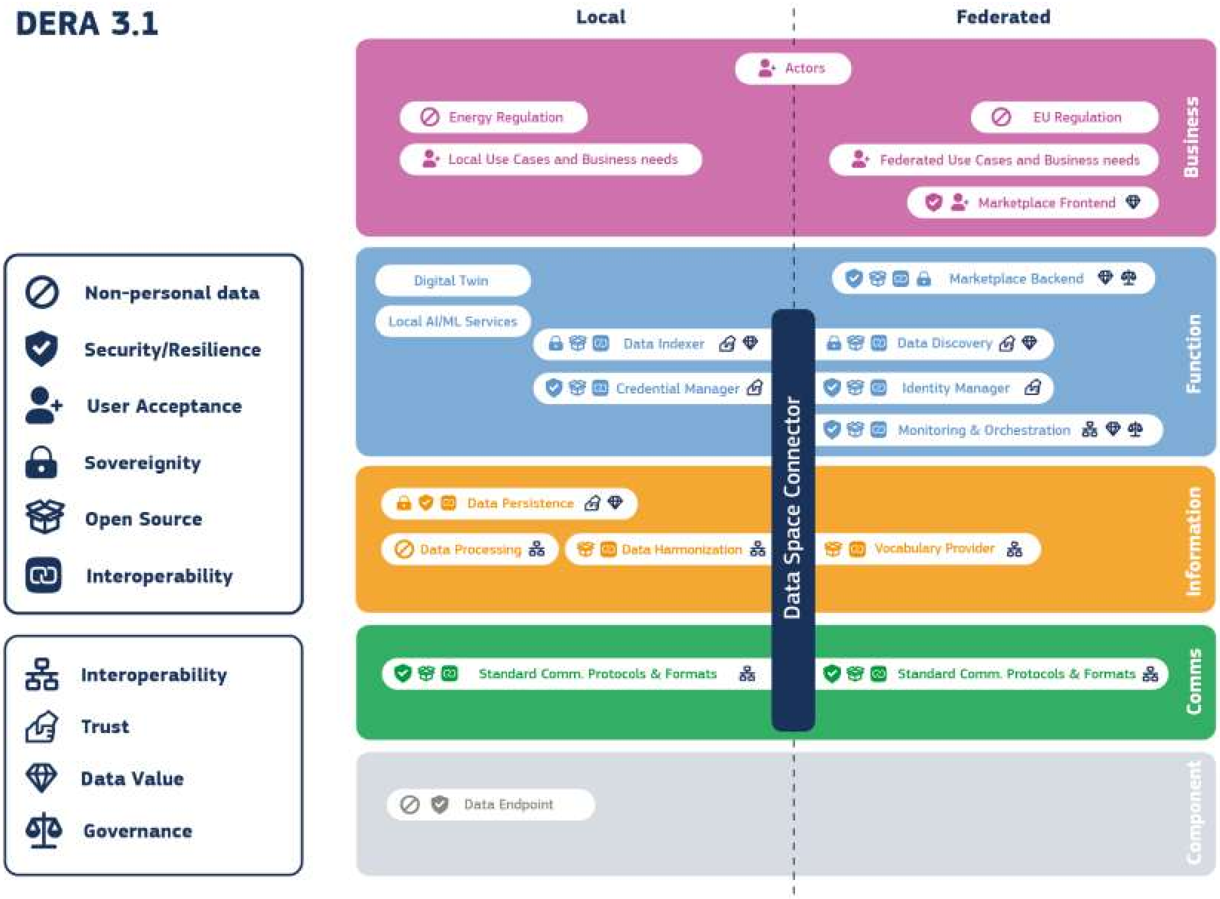


Figure 4: DERA 3.1

As described in DERA 3.1 [4], the main layers are:

- **Component Layer**

  Logical view of system components/subsystems to structure the architecture, understand relationships, and support modular, scalable design. *Elements*: Data Endpoint
- **Communication Layer**

  Enables communication between components so the system can act as a cohesive whole, protocol-agnostic for both local platforms and federated data spaces. *Elements*: Standard communication protocols and formats.
- **Information Layer**

  Handles and stores data, supports local data processing/persistence and semantic harmonisation for efficient, correct data use. *Elements*: Data harmonisation (local) / vocabulary provider (federated), Data processing module, Data persistence module.
- **Function Layer**

  Hosts the concrete functions needed to meet system objectives and support data-space use cases (identification, indexing, monitoring, marketplace). *Elements*: Credential manager (local) / identity manager (federated), Data indexer (local) / data discovery (federated), Monitoring and orchestration module, Marketplace backend module, Digital twins and local AI/ML services.
- **Business Layer**

  Business interoperability across units and systems, aligning roles, processes and regulations, and supporting integration of new systems and regulatory changes. *Elements*: Marketplace frontend module, Local/federated use cases and business needs, Energy and EU regulation, Actors.

2.1.3. HOURGLASS MODEL

The Hourglass Model [5] is a conceptual framework for interoperability that structures digital ecosystems around a narrow waist of common, standardised interfaces and data models. This central layer connects diverse domain-specific applications (the upper part of the hourglass) with heterogeneous technologies and infrastructures (the lower part), ensuring coherence across complex systems.

The hourglass model provides a clear framework for understanding ecosystems, architectures, and systems, emphasizing the role of Minimum Interoperability Mechanisms (MIMs) [6] by enabling a minimal level of interoperability that will enable future solutions using the CERF architecture to be interoperable, resulting in a faster and more efficient roll out of technologies. The MIM is described in the ITU Y.4505 standard [6], previously known as Y.MIM. It follows the structure described in the Figure 5. where it can be seemed that it includes the relevance to public policy, procurement guidelines and implementation guidelines.

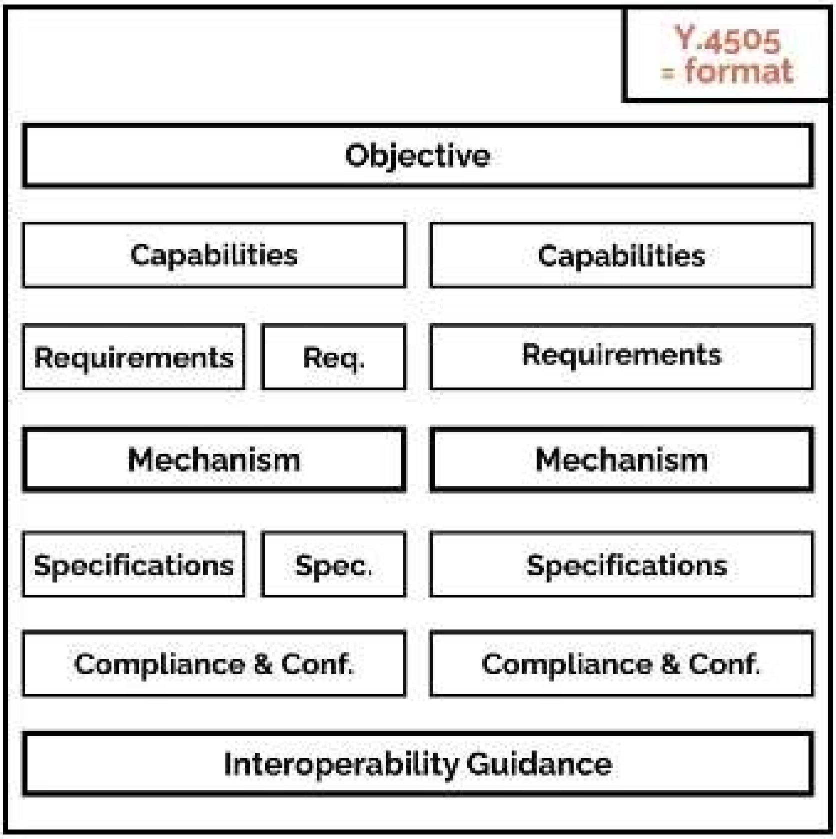


Figure 5: ITU Y.4505 MIM Structure [6]

This approach highlights how diverse infrastructure provisions are funnelled through centralised integrators and platforms, which support a dynamic ecosystem of applications and solution developers. By establishing key interoperability mechanisms, MIMs promote both competition and flexibility while ensuring seamless connectivity across different systems. Consequently, by defining a shared interoperability core, expressed through interoperability profiles, ontologies, and standards, the Hourglass Model promotes seamless cross-domain communication, scalability, and innovation, while maintaining competition, flexibility, and connectivity across different systems.

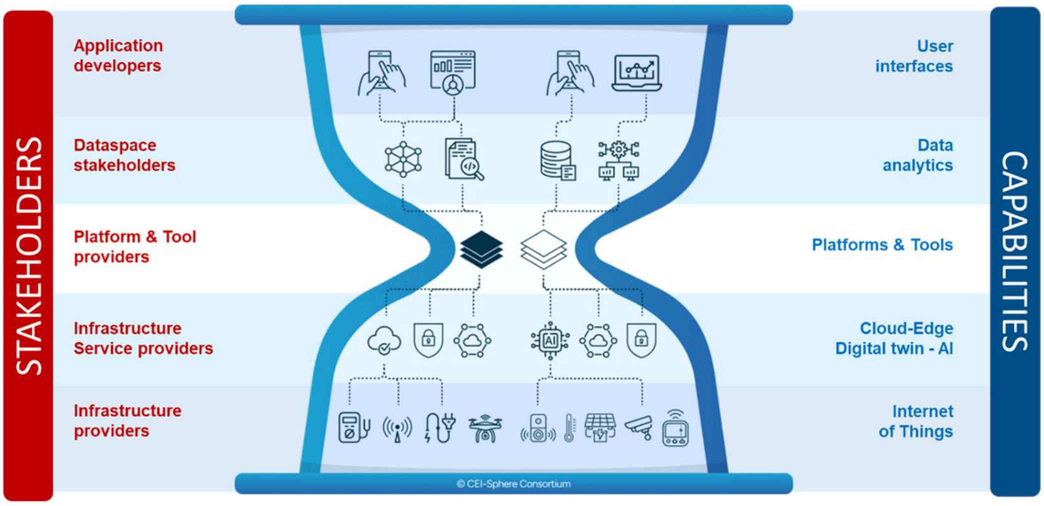


Figure 6: Hourglass Model in ECLIPSE DIGITAL context [5]

2.1.4. REFERENCE ARCHITECTURE STANDARD

In order to review the ECLIPSE DIGITAL CERF architecture and create a Reference Architecture of it, the ISO/IEC 42010 standard (Systems and software engineering, Architecture description) has been employed. Not for depicting the architecture itself, but for defining the design methodology through a structured sequence of distinct and traceable activities. Rather than focusing on graphical representation, its purpose within the ECLIPSE DIGITAL Project is to establish a systematic architectural description process that ensures coherence, transparency, and alignment across all design stages.

Following ISO/IEC 42010 [7], the Reference Architecture (RA) is described through well-defined viewpoints and stakeholder concerns, supporting consistent decision-making and traceability throughout the design. This approach enables the architecture to remain adaptable while maintaining alignment with the overall system goals and interoperability requirements.

The development of the RA follows an iterative process consistent with ISO/IEC 42010 principles, allowing continuous refinement as stakeholder feedback, functional requirements, and integration needs evolve.

2.1.5. ECLIPSE DIGITAL BACKGROUND: INTERCONNECT INITIAL CERF ARCHITECTURE

Building upon the foundational work of the InterConnect project [8], which developed the initial blueprint for the CERF, ECLIPSE DIGITAL seeks to establish guidelines for creating new energy consumer applications and improving existing ones [9].

These applications are designed to provide users with accessible and practical information about energy savings and associated benefits, such as reduced carbon emissions and financial incentives. By encouraging flexible consumption behaviours—like smart electric vehicle charging and load shifting—the project aims to bolster grid resilience and improve overall energy efficiency, all while focusing on consumer engagement and voluntary participation. Building upon the foundation laid by InterConnect, the ECLIPSE DIGITAL project seeks to implement and demonstrate the CERF for energy applications throughout Europe. ECLIPSE DIGITAL focuses on defining requirements and conditions for developing user-friendly applications that provide consumers with actionable information on achieving energy savings and cost reductions. Additionally, these applications aim to enhance the resilience and stability of European electricity grids by leveraging consumer flexibility [10].

Figure 7 shows the initial CERF architecture coming from Interconnect project and considered in the ECLIPSE DIGITAL project.

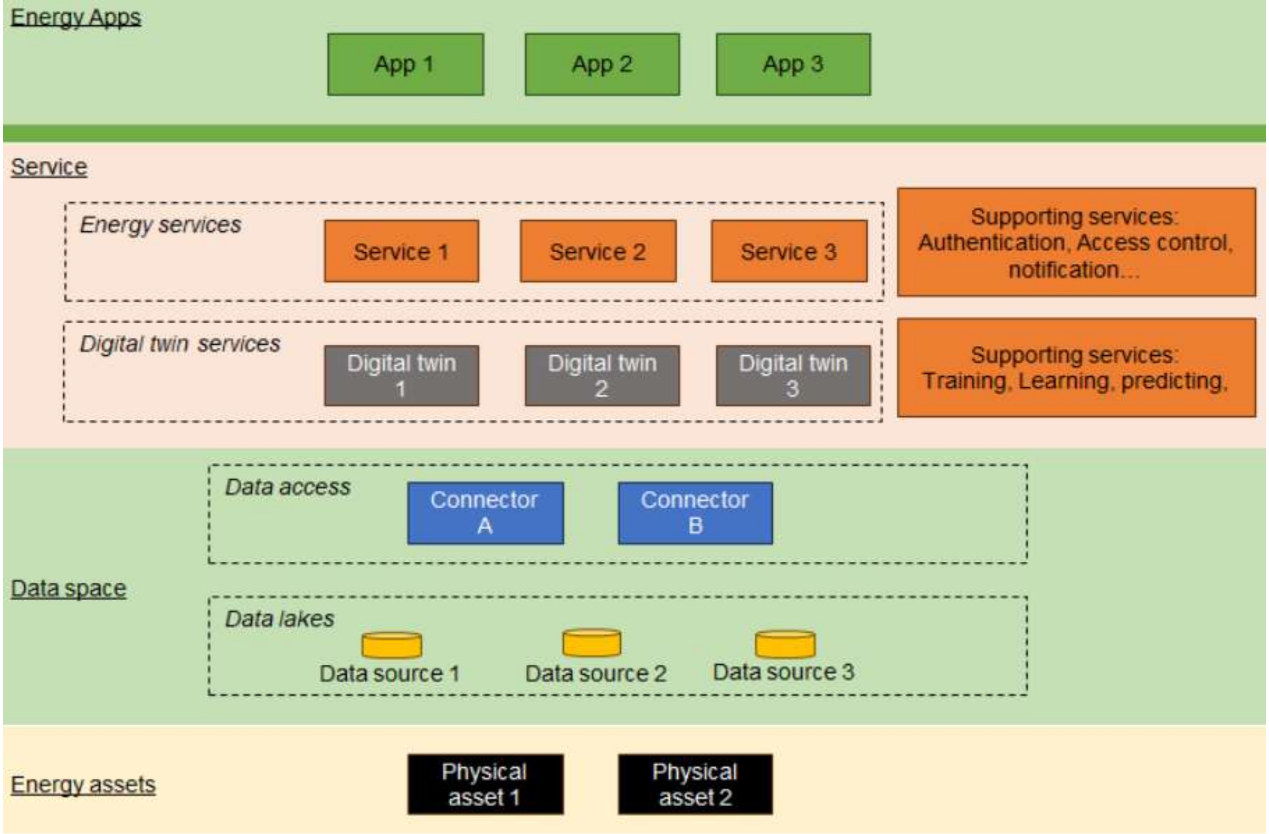


Figure 7: Initial CERF Architecture [11]

The Common European Reference Framework (CERF) architecture, developed under the InterConnect project, is structured into four primary layers:

1. Energy Applications (Apps) Layer: This topmost layer comprises applications designed to assist consumers in managing and reducing their energy consumption. These applications leverage services provided by the underlying layers to deliver functionalities such as consumption monitoring, personalized energy-saving recommendations, and cost reduction strategies.

2. Service Layer: Positioned beneath the Energy Apps layer, the Service Layer offers essential services that support the applications:

- **Energy Services:** These include functionalities directly related to energy management, such as providing consumption advice, facilitating demand response mechanisms, and enabling energy trading. They are accessible to the Energy Apps through a dedicated interface, ensuring seamless integration and functionality.
- **Supporting Services:** These encompass auxiliary features like user authentication, access control, consent management, and push notifications, which are crucial for the secure and efficient operation of energy services.
- **Digital Twin Services:** These services involve the creation and management of digital replicas of physical energy assets, allowing for real-time monitoring, simulation, and optimization. They enable energy services to observe and control specific energy assets effectively. Supporting functionalities within digital twin services include training, learning, and predictive analytics.

3. Data Space Layer: The foundational layer of the architecture, the Data Space Layer, is responsible for storing and managing data related to energy assets. It ensures that data is organised and accessible for analysis and decision-making:

- **Data Access Sublayer:** This sublayer facilitates the retrieval of data through connectors and adapters, ensuring interoperability between different data sources and systems. It also maintains a Data Catalogue, registering available data sources to streamline data discovery and utilization.

- **Data Lakes:** These centralized repositories store vast amounts of raw data, including information on grid status, market conditions, individual consumer contexts, and available consumer offerings. This data is crucial for informed decision-making and the development of responsive energy services.

4. Energy Assets Layer: At the base of the architecture lies the Energy Assets Layer, which encompasses the physical assets involved in energy production, distribution, and consumption. These tangible components are integral to the overall energy ecosystem, serving as the foundation upon which digital services and applications operate.

Role of Digital Twins: A pivotal aspect of the CERF architecture is the integration of digital twin technology, which serves several key functions:

- **Ownership and Responsibility:** By associating digital twins with their corresponding physical energy assets, stakeholders develop a heightened sense of ownership and responsibility, leading to more attentive management and maintenance practices.

- **Simplified Connectivity:** Digital twins offer a streamlined connectivity model, facilitating efficient communication and interaction between physical assets and digital systems. This simplification enhances interoperability and reduces the complexity of integrating diverse components within the energy infrastructure.

- **Observation and Control:** Through digital twins, operators can observe and learn about various elements of the grid in real-time, enabling proactive monitoring and analysis. Additionally, digital twins provide a framework for controlling these elements, allowing for responsive adjustments and optimizations to maintain grid stability and efficiency.

In summary, the ECLIPSE DIGITAL project acts as a concrete implementation and large-scale demonstration of the CERF, showcasing how standardised, user-centric energy applications can reshape Europe’s energy ecosystem. By enabling consumer empowerment and strengthening grid resilience, ECLIPSE DIGITAL illustrates the CERF’s potential to drive a more flexible, interoperable, and future-proof energy landscape. [9]In summary, the ECLIPSE DIGITAL project serves as a practical implementation and demonstration of the CERF, aiming to transform Europe's energy landscape by empowering consumers and enhancing the resilience of power grids through standardized, user-centric energy applications.

2.2. ECLIPSE DIGITAL CERF GENERIC ACHITECTURE

To develop the CERF architecture, the initial step involved consulting project pilots at the project's Kick-off to gather insights on potential building blocks and functional elements. Based on this input, a preliminary architectural concept was drafted and presented to stakeholders for review and refinement.

2.2.1. KEY COMPONENTS IDENTIFICATION

Through iterative discussions, the key components were progressively identified, analysed, and mapped to their respective functions within the overall system. Following multiple rounds of consultation among project partners, three overarching groups emerged, forming the basis for structuring the foundational functional components of the CERF architecture as outlined below:

1. **Customer Domain**: Smart Meters, Smart Meter Adapters, home PV systems, energy storage, appliances, EV chargers, and other behind the meter assets or in-home assets, along with the Energy App that could deliver insights, behavioural nudges, and reward mechanisms.
2. **Aggregation Domain**: The aggregator, envisioned as an edge intelligence component, would optimise and control distributed flexibility (batteries, EVs, HVAC, PV systems). It would enforce local policies, manage flexibility portfolios, and interact with EMS, Retailers, DSOs/TSOs, and the Flexibility Platform to offer validated flexibility services.

3. **Market and Governance Domain**: Energy markets are expected to provide market interfaces, customer-contract management, and incentive mechanisms bridging energy supply with demand-response programs.

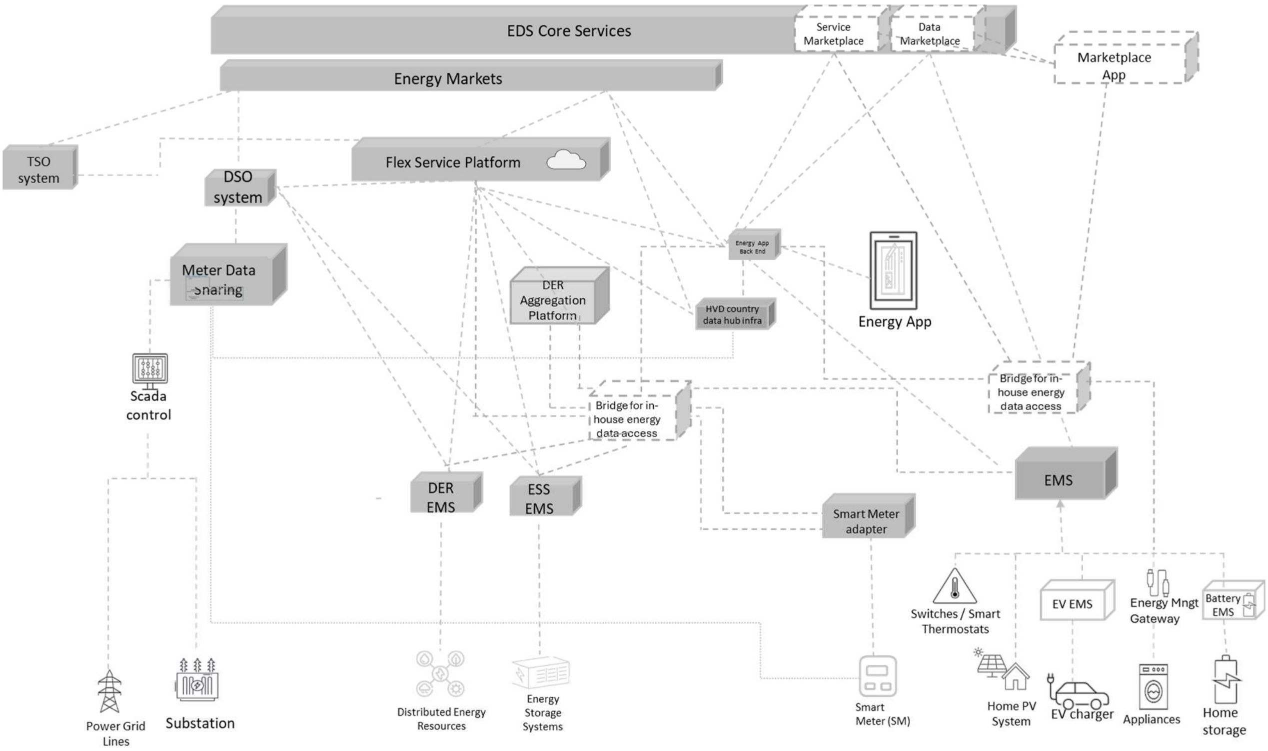


Figure 8: Initial ECLIPSE DIGITAL CERF architecture components

Within the Meter Data Sharing component, the architecture explicitly incorporates the full metering data-exchange infrastructure as shown in the figure below, including the Meter Data Collector (MDC), Meter Data Responsible (MDR), Meter Data Administrator (MDA), Data Access Provider (DAP), and the Permission Administrator [12]. Together, these components form the underlying data-sharing infrastructure through which raw smart-meter readings are collected, validated, securely stored, and made available to authorised actors based on consumer consent, ensuring a trusted and interoperable foundation for energy-service applications and flexibility-related use cases.

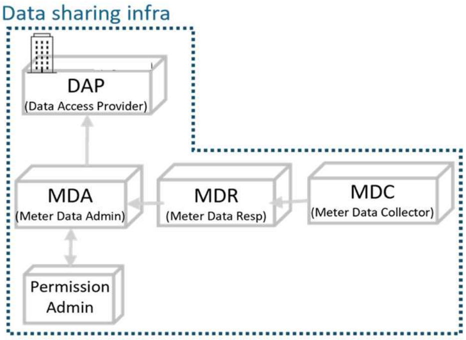


Figure 9: Meter Data Sharing Infrastructure

- **Meter Data Collector (MDC)**: Responsible for obtaining the primary meter readings and ensuring their basic quality and plausibility before further processing.

- **Meter Data Responsible (MDR)**: Validates, estimates or substitutes readings, producing the official validated meter data.

- **Meter Data Administrator (MDA)**: Stores, manages and maintains the validated meter datasets in a secure environment.

- **Data Access Provider (DAP)**: Publishes validated meter data to authorised actors through a standardised interface.

- **Permission Administrator**: Manages customer consent and authorisation rules for data access.

2.2.2. REFERENCE MODEL FOR FLEXIBILITY CONSIDERATION

The above representation of the architecture, intended to be focused on systems and functions (DER aggregation platform, flexibility service platform, DSO system, TSO system, markets, meter data sharing, etc.), considers the work in progress of the D4E ”Reference Model for flexibility” from the transversal sub-group ‘Standardisation of data exchange’ of the Data for Energy (D4E) sub-group of the Smart Energy Expert Group (SEEG).

The below figure intends to describe actors and responsibilities, it illustrates how energy flexibility depends on coordinated information exchange among residential devices, local energy management systems, service providers, and grid actors such as DSOs and TSOs. It highlights the roles, interactions, and data flows required to ensure interoperability across the flexibility ecosystem. The model reflects the minimum data-exchange needs, gaps in existing standards, and the recommended standards framework, all focused on residential flexibility. It shows how common information structures enable consistent communication across the flexibility process, from device registration to market participation and activation.

At the core of the data exchange are the two principal market-based flexibility use cases: implicit flexibility and explicit flexibility. Implicit flexibility refers to situations where consumers adjust their consumption in response to price signals (e.g., time-of-use tariffs or dynamic pricing), while explicit flexibility involves users or assets providing a direct, measurable demand-side management (DSM) action that can be activated, verified, and remunerated. These two use-case types define the operational data flows required for flexibility aggregation and activation, including baseline nomination, bidding, intraday activation, and settlement.

Surrounding elements represent key regulatory and technical drivers such as the Demand Response Network Code, the Electricity Balancing Guideline, and Data Act requirements for connected DERs. Together, the components depicted in the image form a coherent architectural view of how distributed energy resources participate in wholesale, balancing, and redispatch markets through standardised, interoperable information exchange.

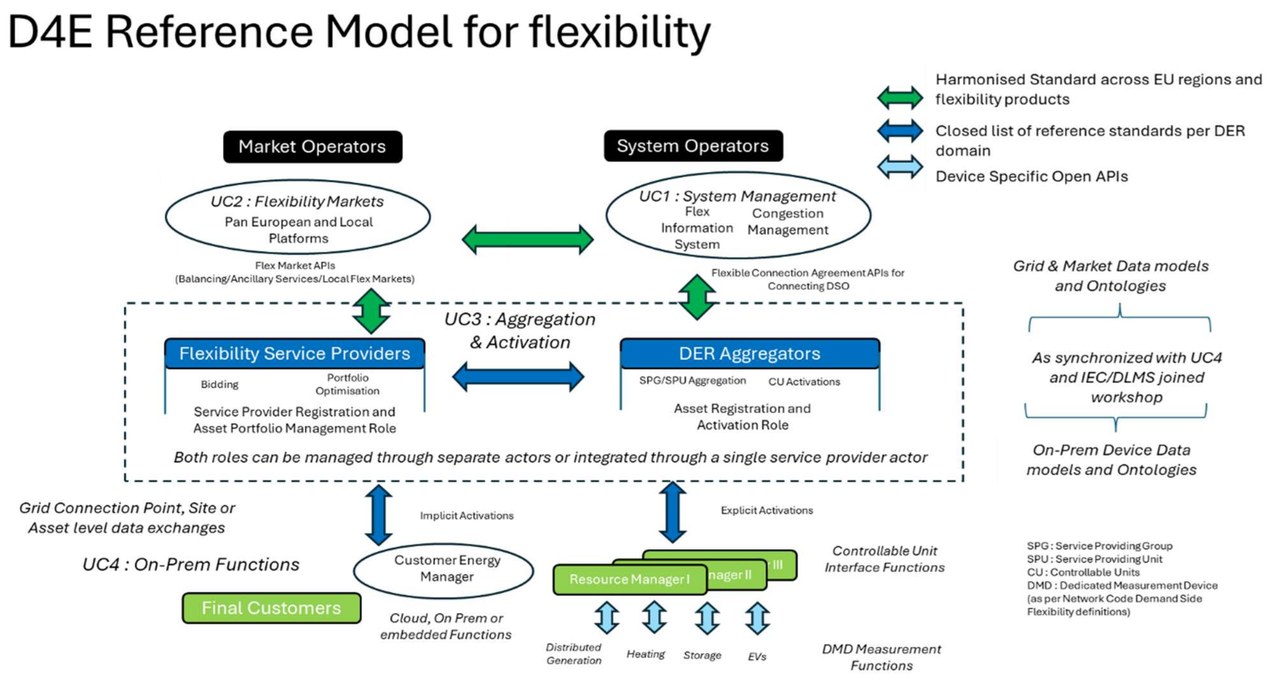


Figure 10: Roles in data exchange in Flexibility aggregation and activation [11]

It also defines a market-edge architecture, describing system-to-system data exchanges, depicted in the figure below, which builds on the technical models developed in the TC13/SC23K JAG4 context, incorporating contributions from the relevant standardisation groups: IEC TC57 WG21 (purple elements), TC13 WG14 (blue elements), and SC23K WG3 (red elements), alongside the discussions within this subgroup. The architecture is defined in terms of roles and functions rather than specific deployment configurations. This logical perspective is meant to accommodate national differences in system setups and business models, allowing regulated entities and market actors to assume multiple roles, and enabling devices to support several functions where appropriate. In order words, it is intentionally deployment-agnostic so that actors can fulfil multiple roles and devices can host multiple functions depending on each Member State's arrangements.

This market-edge architecture supports both direct activation of a single controllable device and coordinated management of multiple devices through a Customer Energy Management (CEM) function, which orchestrates the consumption and production of one or more behind-the-meter assets, while acknowledging that not all functions are required everywhere. Central to this model is the Resource Manager (RM), which ensures exclusive and prioritised control of each Controllable Unit and can expose flexibility for legacy devices. Deployment locations remain flexible, as CEM and RM functions may run locally or in the cloud depending on manufacturer choices.

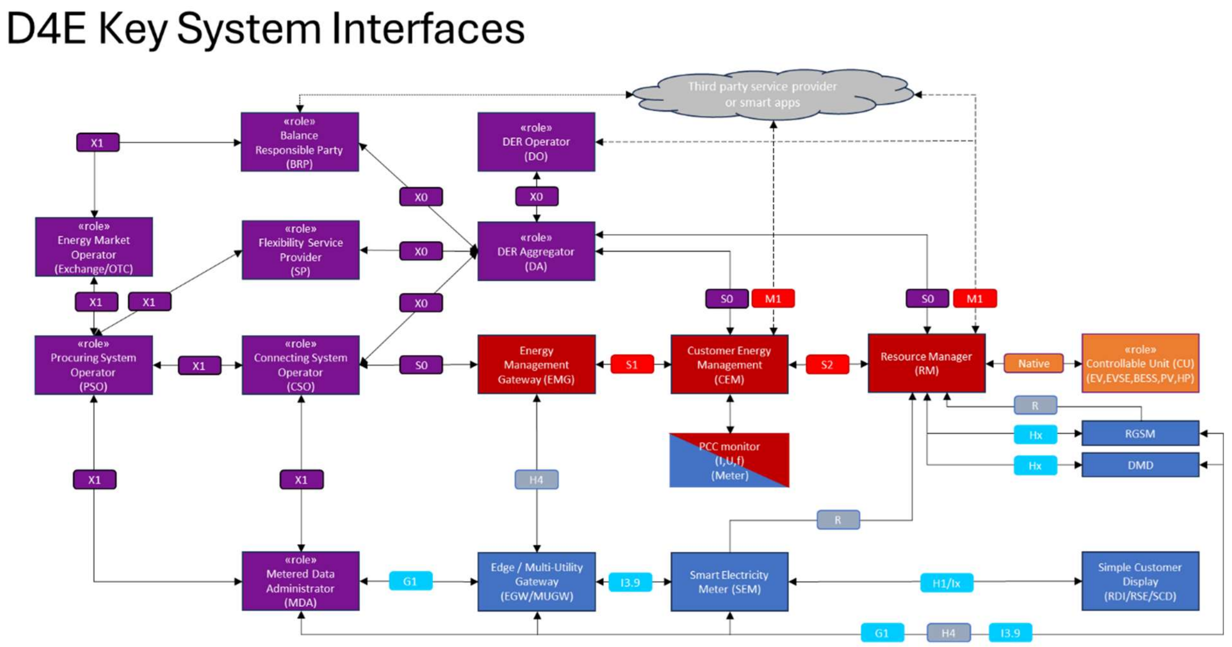


Figure 11: Roles and associated logical functions in a market-edge architectural model. [13]

2.2.3. CONSENT DRIVEN MARKETPLACE CONSIDERATION

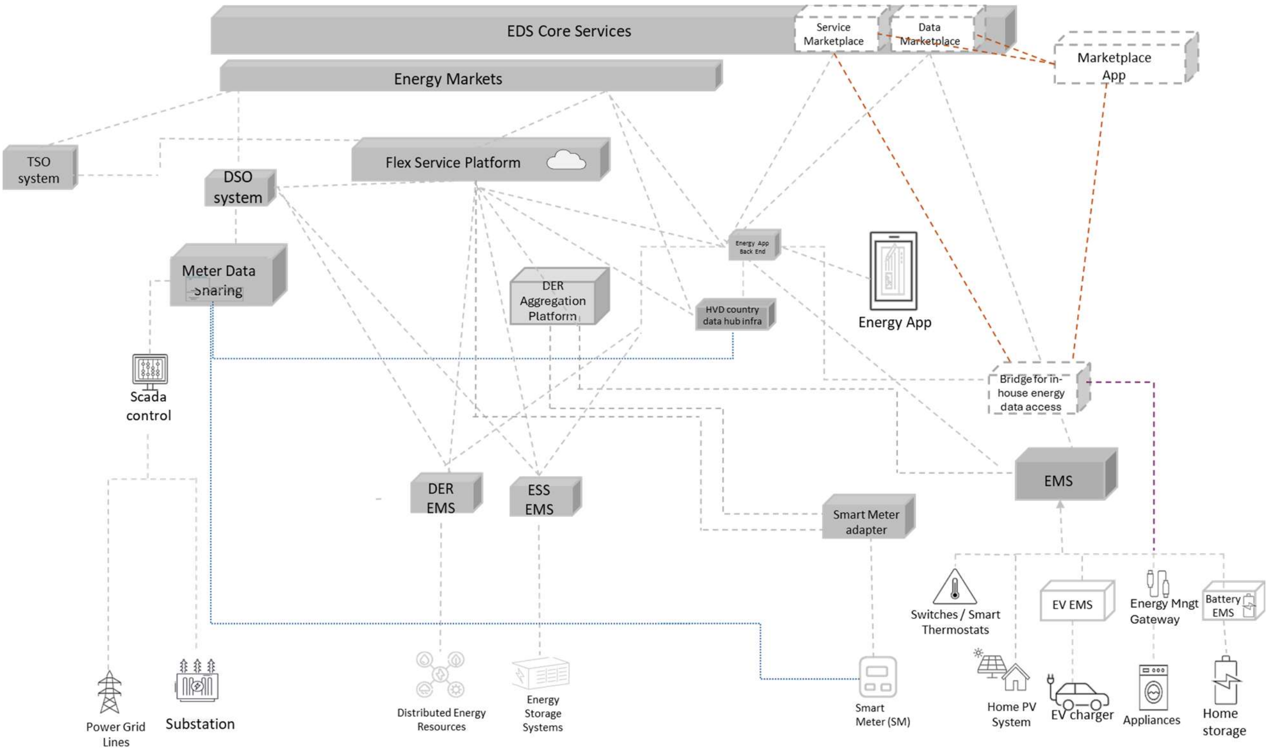


Figure 12: ECLIPSE DIGITAL CERF Architecture Marketplace consideration

As seen in the above figure, an optional but highly valuable component serving as a “Bridge for in-house energy data access” has been added to the architecture. The component represents what in the Austrian pilot, which holds a Data Space enabled architecture, is named as AIIDA.

The consent-driven component functions as an intermediary that can run either as an edge device in the home or as a cloud-based service. Its core purpose is to receive, persist, process and forward data, including performing local calculations when needed. Crucially, all data exchange through this component is strictly consent-based: no data is transmitted unless the data owner explicitly grants permission. This allows the component to interconnect with the EMS, fetch the relevant in-house data, and link it to the wider energy ecosystem while ensuring that access remains fully controlled by the user.

Beyond basic data exchange, the component can operate hierarchically, supporting multi-level aggregation where data flows from households to higher aggregation nodes, only when consent is granted. This is particularly relevant in contexts where smart meters can measure many parameters, but privacy rules prevent their direct use. The component enables access to such data only after explicit customer approval, and the same principle applies when aggregated data or newly generated parameters are of interest to other actors. It also integrates mechanisms for monitoring service-level objectives (SLOs) and service level agreements (SLAs), such as data availability and quality, to ensure reliable operation in environments where connectivity at the residential level may be unstable.

The component is tightly connected to the marketplace concept, both for data and services. Third-party services can be offered through a marketplace and downloaded to the device, like an app-store model, but with a fundamental difference: every service installation and every data flow still require explicit consent. This establishes a trust framework in which the user controls how their in-house data is used, whether for external services, flexibility aggregation, or other applications. By abstracting residential-level data handling and ensuring that data is accessible only under transparent, user-driven policies, the component becomes a key enabler for privacy-compliant participation in data marketplaces and for leveraging in-home energy data in a controlled and trustworthy way.

2.2.3.1. AGGREGATOR CONSIDERATIONS

From the aggregator's perspective, different approaches exist depending on whether the focus is on whole-home data or behind-the-meter data. Aggregators working behind the meter typically connect directly to the EMS, while others may rely on an additional component that handles data access and consent, this optional approach is shown in Figure 13 below, which includes the Data Plane (DP - responsible for actual movement and forwarding of data), Control Plane (CP - makes decisions about how the data flows) and SMD (Smart Meter Data – meter readings) in relation to the Marketplace. This component currently referred as "Bridge for in-house energy data access", can operate either at the "DER Aggregation platform" edge or in the cloud and serves as an add-on that abstracts the residential layer. It provides connectivity when the EMS cannot support certain interfaces or devices, and it can also execute services or manage data handling. Although optional in many pilots, some pilots use it for both whole-home and behind-the-meter scenarios. In functional terms, it can fulfil the role of the aggregator edge node, particularly where DER aggregation depends on consent-driven data exchange.

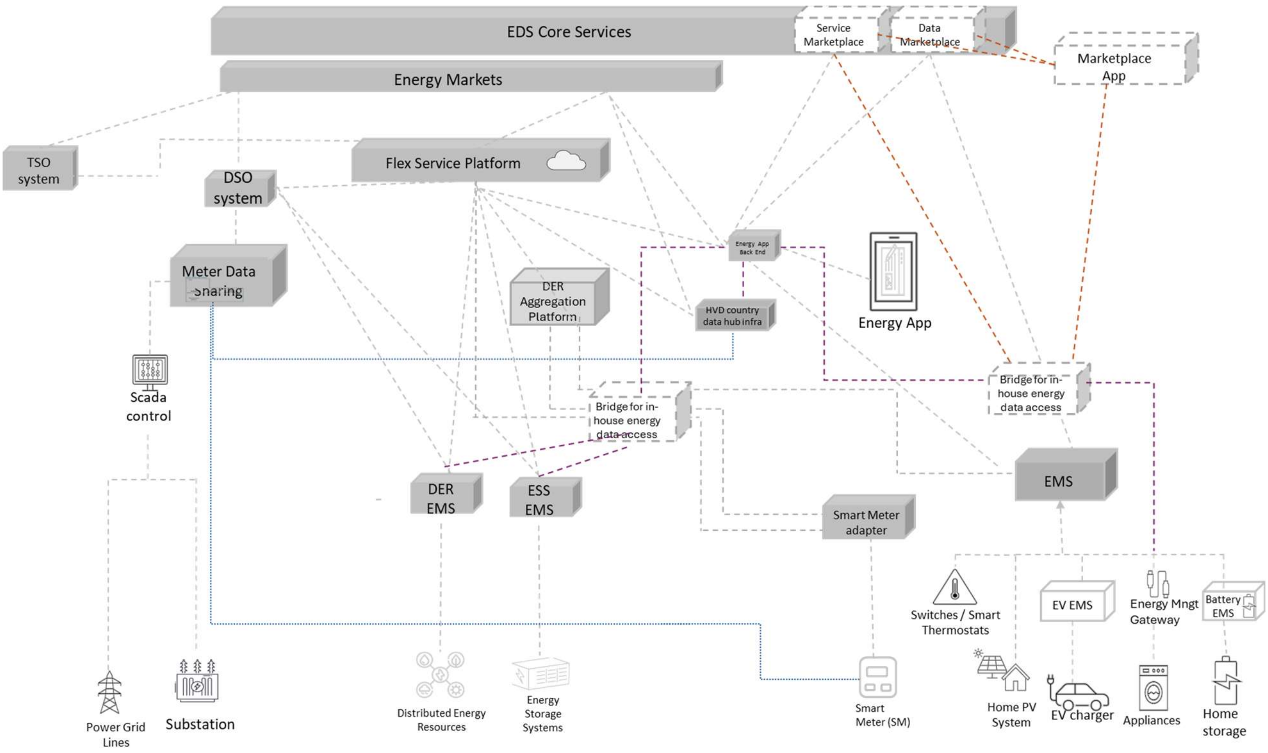


Figure 13: ECLIPSE DIGITAL CERF Marketplace and Aggregator consideration

Aggregation itself can occur across several levels, such as within energy communities. End users may each host an instance of the " Bridge for in-house energy data access", while an energy-community operator hosts another instance to perform the first aggregation step. Data then flows bidirectionally between these actors, always based on explicit consent managed via the marketplace or consent broker. In this way, the component supports DER aggregation not only as a communication mechanism but also as one of its inherent functionalities. It can link the EMS, the aggregation layer, and the marketplace, offering a reusable consent-driven framework that fits naturally within the aggregator's workflow while remaining optional and adaptable to different business models.

2.2.4. GENERIC FUNCTIONAL COMPONENTS

The above components were then related to a list of generic functions to be used throughout the project. In the ECLIPSE DIGITAL project context, a *component refers to a functional building block or system within the energy ecosystem that contributes to the execution of specific tasks, services, or roles*.

They can range from data-processing tools and operational systems to physical energy assets.

The set of ECLIPSE DIGITAL CERF architecture components presented in the Table 1 is aligned with the Harmonised Electricity Market Role Model defined by ENTSO-E [14], in the sense that each component corresponds to recognised market roles and responsibilities within the European electricity sector. Consumer-facing applications, device management tools, forecasting and real-time data systems, market data exchange services, and compliance or balancing tools reflect the functional domains associated with established actor roles such as consumers, suppliers, flexibility service providers, data providers, metering actors, and system operators.

Table 1: CERF Architecture components placement

CERF Architecture Components		
Component	**Description**	**Examples**
Consumer-Facing Applications	Applications designed for end-users (consumers or prosumers) to monitor, manage, and optimise their energy	• Mobile Apps for tracking energy usage. • Tariff Benchmarking tools for cost comparison.

	consumption and generation.	- Alerts and Tips for energy-saving recommendations.
Consumer Device Management & Digital Twin	Tools that manage customer interactions and use digital twins to simulate and optimise energy behaviours.	- Prosumer Digital Twin: Simulates energy behaviour for optimization. - Home Energy Management: Manages in-home devices for efficiency.
Energy Management Tools	Applications providing insights and control over energy usage and emissions, often integrating AI	- CO_2 Footprint Calculators for environmental tracking. - AI-based Load Shifting Recommendations for peak shaving.
Forecasting and Monitoring	Systems predicting energy generation, consumption, and grid reliability.	- Performance Monitoring for distributed energy resources (DER). - Solar and EV Usage Forecast tools.
Real-Time & Near-Real-Time Streaming	Systems delivering high-frequency data to enable fast decision-making in energy markets.	- Near Real-Time Measurement Streaming: Provides live insights into grid and market operations. - Market Data Streaming: Real-time exchange of market-related information.

Data Catalogues & Models	Repositories and structures for storing and organizing energy-related data based on industry standards.	• CIM-Based Data Catalogues for power grid data. • Grid Models (IEC standards) for network planning.
Market Data and Exchange	Platforms for sharing and distributing market and operational data.	• Market Nomination Tools: Facilitate scheduling in markets. • Transparency Platforms for market visibility.
Home and Grid Devices	Hardware supporting energy generation, consumption, or management	• Smart Thermostats for energy-efficient heating/cooling. • Bidirectional EV Chargers for vehicle-to-grid integration.
Renewable Energy and Storage	Components managing renewable energy generation and storage	• Generators (PV, wind turbines, hydro plants…) for generation • Batteries and Inverters for energy storage. • Home Energy Storage systems for backup and optimization.
Privacy & Compliance	Tools ensuring privacy related data	• GDPR Compliance systems for data privacy.

	management and regulatory adherence	• Authentication and Access Control mechanisms.
Data Exchange and Connectivity	Systems ensuring seamless integration between various data sources and platforms	• Connectors for ETL (Extract, Transform, Load) processes. • Message Routing for data flow optimization.
Analytics and AI-Based Support	Advanced tools for processing large datasets and providing actionable insights using AI	• Neural Flexibility Platforms for demand-side response. • Background Data Analysis for operational insights.
Market Interaction and Compliance	Tools facilitating participation in energy markets and ensuring compliance with regulations	• Revenue Calculation systems for market players. • Activation and Prequalification tools.
Congestion and Balancing Management	Systems managing grid congestion and balancing supply-demand mismatches.	• TSO Communication Apps for system balancing. • Balancing Market Participation tools.
Energy Communities	Tools supporting collective energy usage and generation by local communities.	• Community Monitoring Platforms for collaborative energy management. • Load Shifting Tools for distributed optimization.

2.2.1. SGAM MODEL MAPPED IN ECLIPSE DIGITAL CERF ARCHITECTURE

SGAM generic layers for the ECLIPSE DIGITAL Architecture project are shown below. Figures below include representation of Data Plane (DP), Control Plane (CP) and SMD (Smart Meter Data) flow in relation to the Marketplace. Interfaces, type of data, and complementary details about data represented in these diagrams are found in section 3 and section 4.

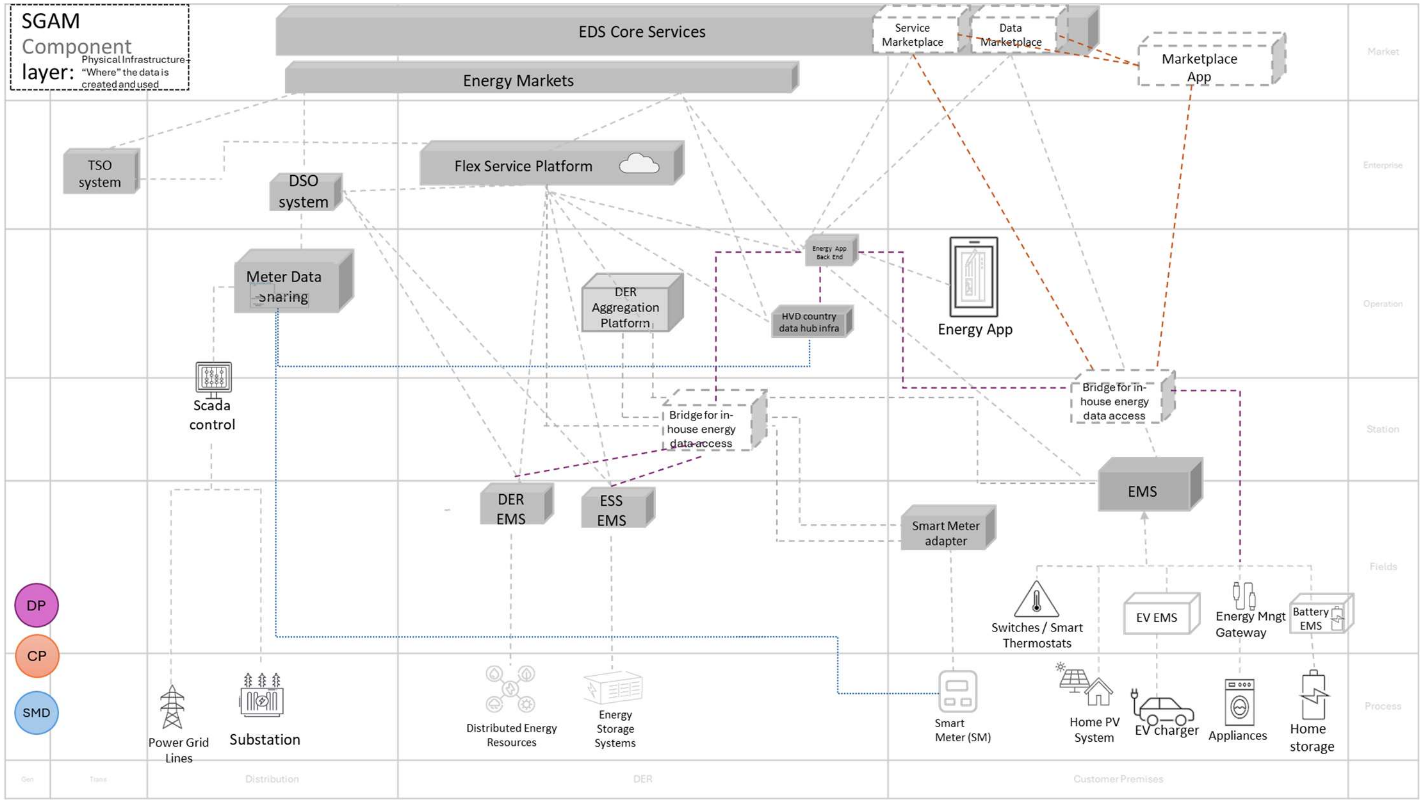


Figure 14: Generic SGAM architecture for ECLIPSE DIGITAL – Component Layer

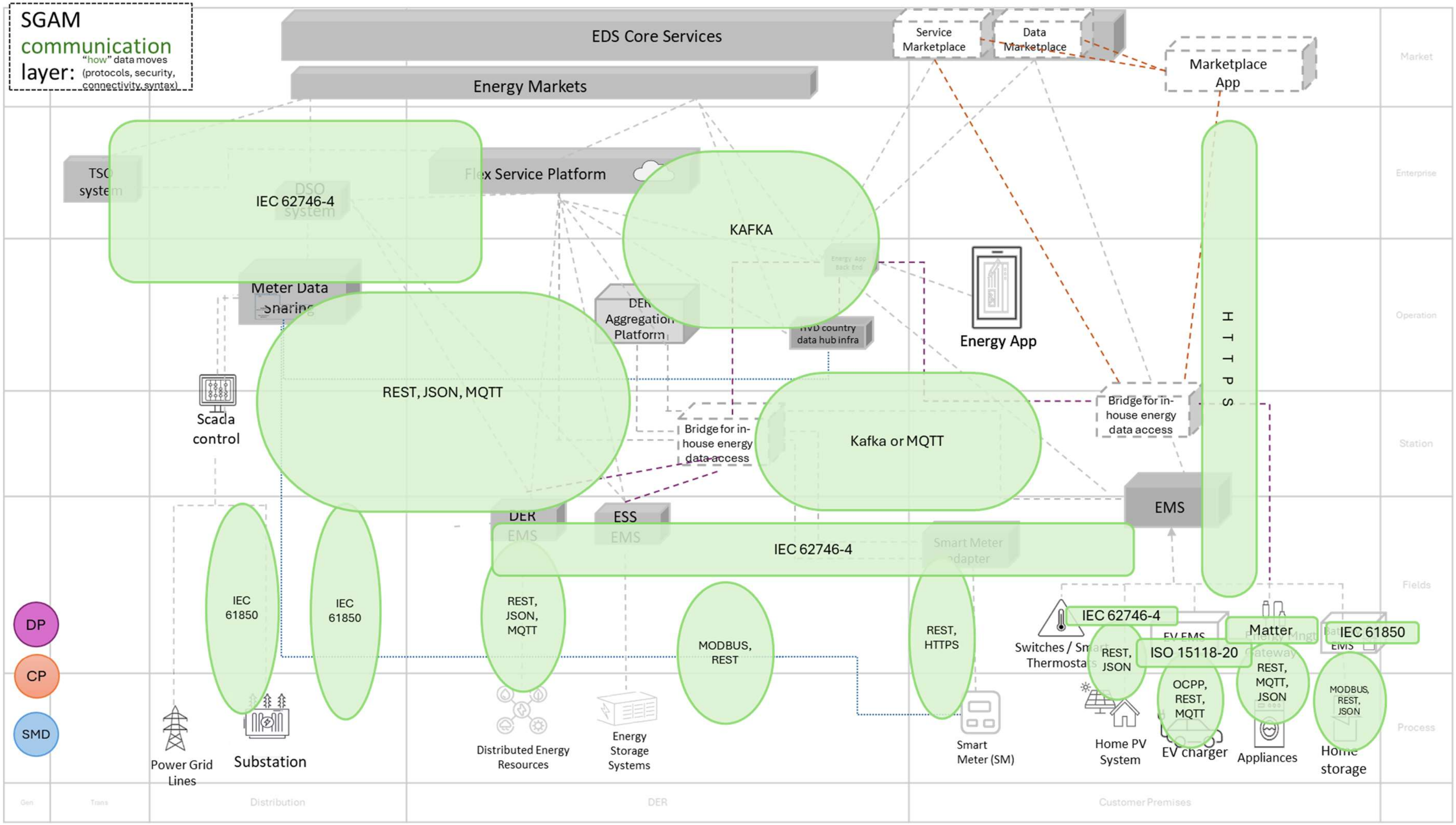


Figure 15: Generic SGAM architecture for ECLIPSE DIGITAL – Communication Layer

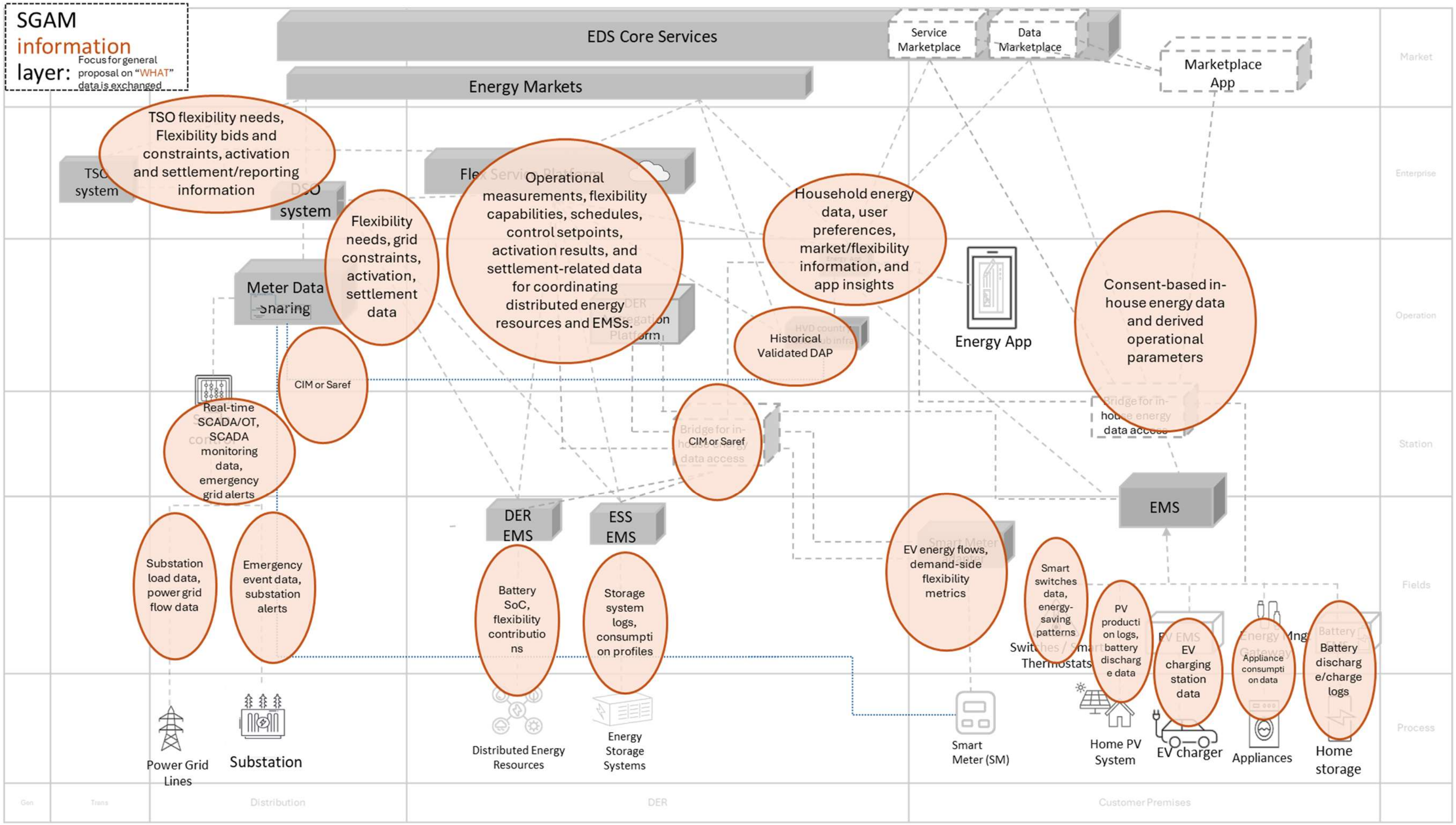


Figure 16: Generic SGAM architecture for ECLIPSE DIGITAL – Information Layer

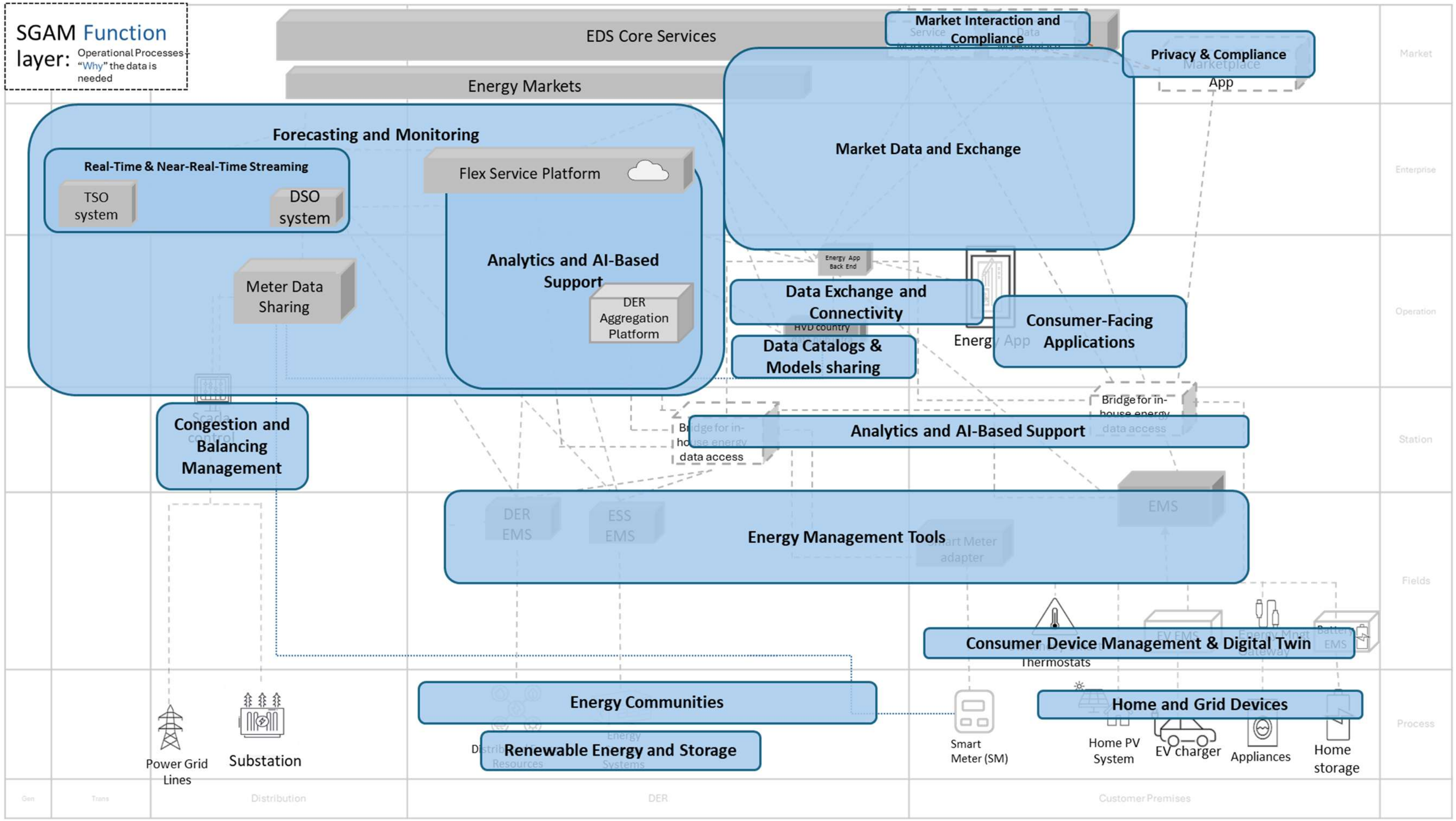


Figure 17: Generic SGAM architecture for ECLIPSE DIGITAL – Function Layer

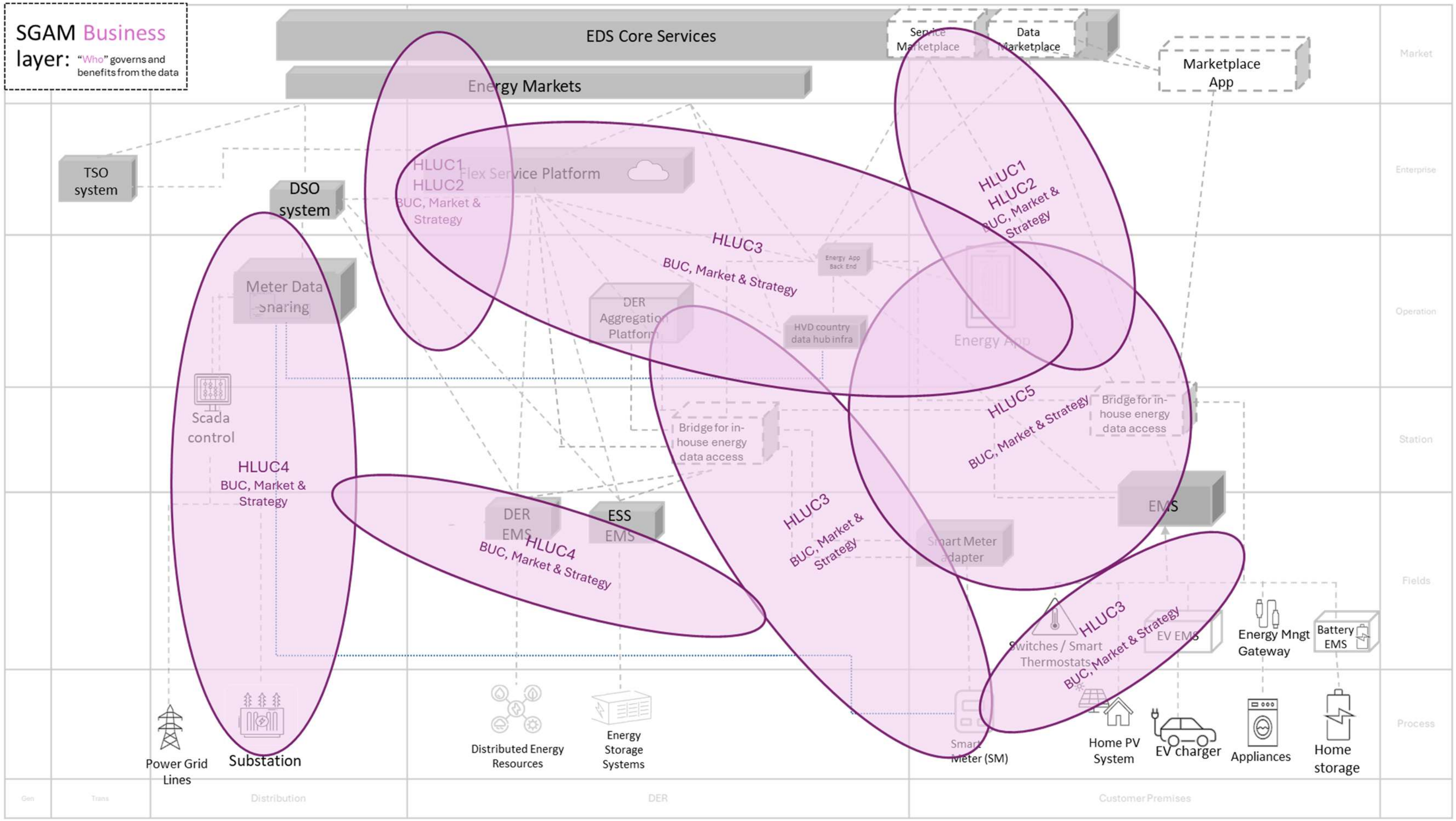


Figure 18: Generic SGAM architecture for ECLIPSE DIGITAL – Business Layer

2.2.2. USE-CASE SPECIFIC ARCHITECTURE

The five High-Level Use Cases (HLUCs) outlined in this project, and describe in Deliverable 2.2 “Energy services analysis, use cases, and CERF requirements”, represent key areas of focus for enhancing energy management through digital solutions, consumer engagement, and grid stability. Each HLUC addresses a distinct aspect of the energy ecosystem, from personalised energy efficiency guidance to real-time alerts and emergency response, sustainability awareness, demand-response participation, and data-driven consumption monitoring.

In addition, the current version of D3.1 establishes a roadmap for the integration of Data Space principles into the CERF architecture. By outlining how data sovereignty, trust frameworks, and standardised exchange mechanisms can be embedded into existing components, the document sets out the foundation for adopting interoperable Data Space models within the project’s ecosystem. This roadmap is complemented by the extension of HLUC components into Smart Grid Architecture Model (SGAM) diagrams, ensuring that data-sharing roles, interfaces, and governance aspects are coherently represented across all SGAM described layers and domains. Together, these elements provide a comprehensive and future-aligned approach to large-scale energy data interoperability, without requiring additional iterations of the deliverable.

2.2.2.1. HLUC 1 - PERSONALISED MESSAGES FOR CONSUMER FLEXIBILITY BASED ON ECONOMIC BENEFITS

It focuses on integrating smart devices and consumer participation into energy systems, leveraging real-time data, dynamic pricing, and flexibility mechanisms to optimise energy consumption, prevent grid congestion, and provide financial incentives for contributing to grid stability.

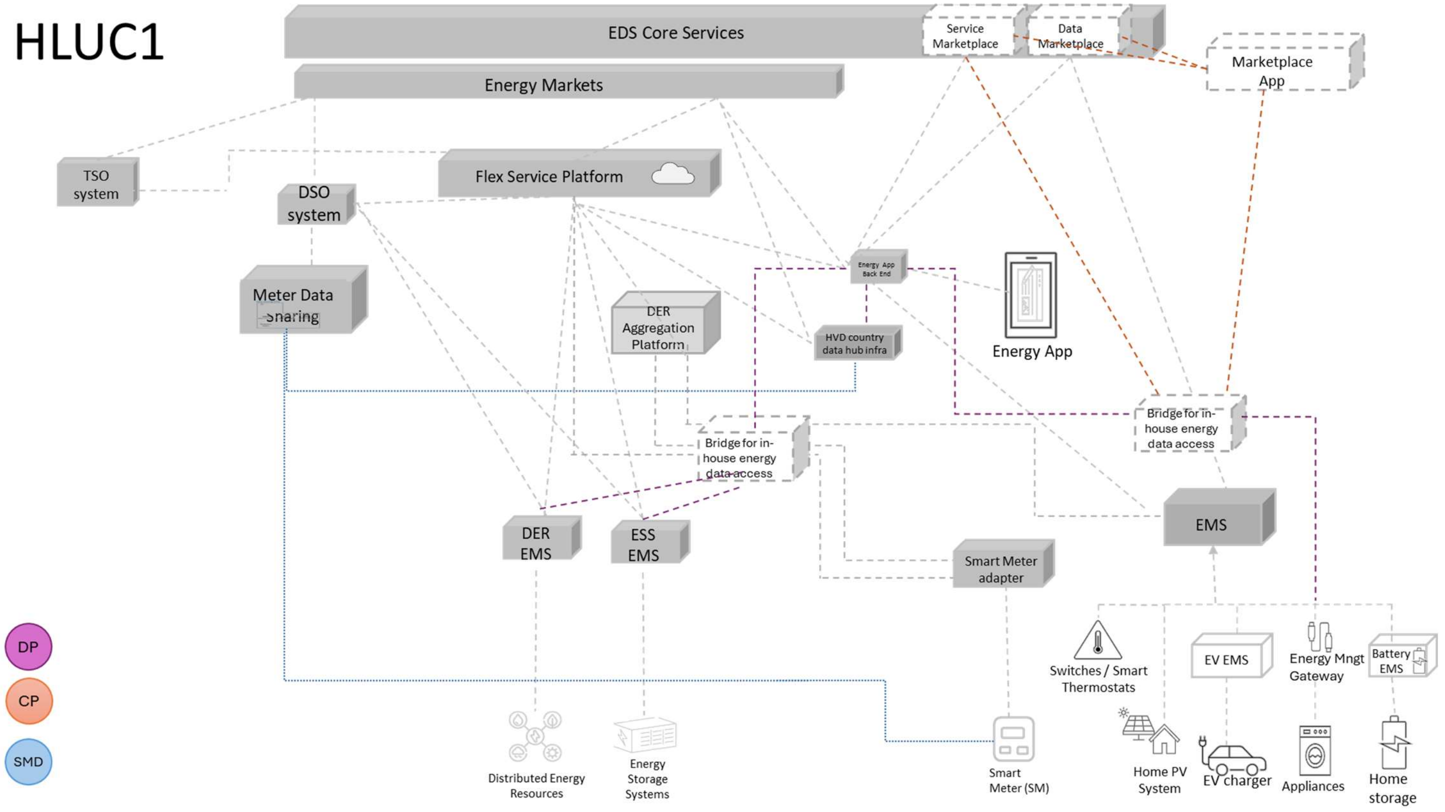


Figure 19: HLUC1 Generic ECLIPSE DIGITAL CERF architecture

2.2.2.2. HLUC 2 - PERSONALISED MESSAGES FOR CONSUMER FLEXIBILITY BASED ON NON-ECONOMIC INCENTIVES

It focuses on leveraging real-time data, smart devices, and personalised or general information to optimise energy consumption, promote sustainability, and reduce carbon footprints by engaging users with actionable insights.

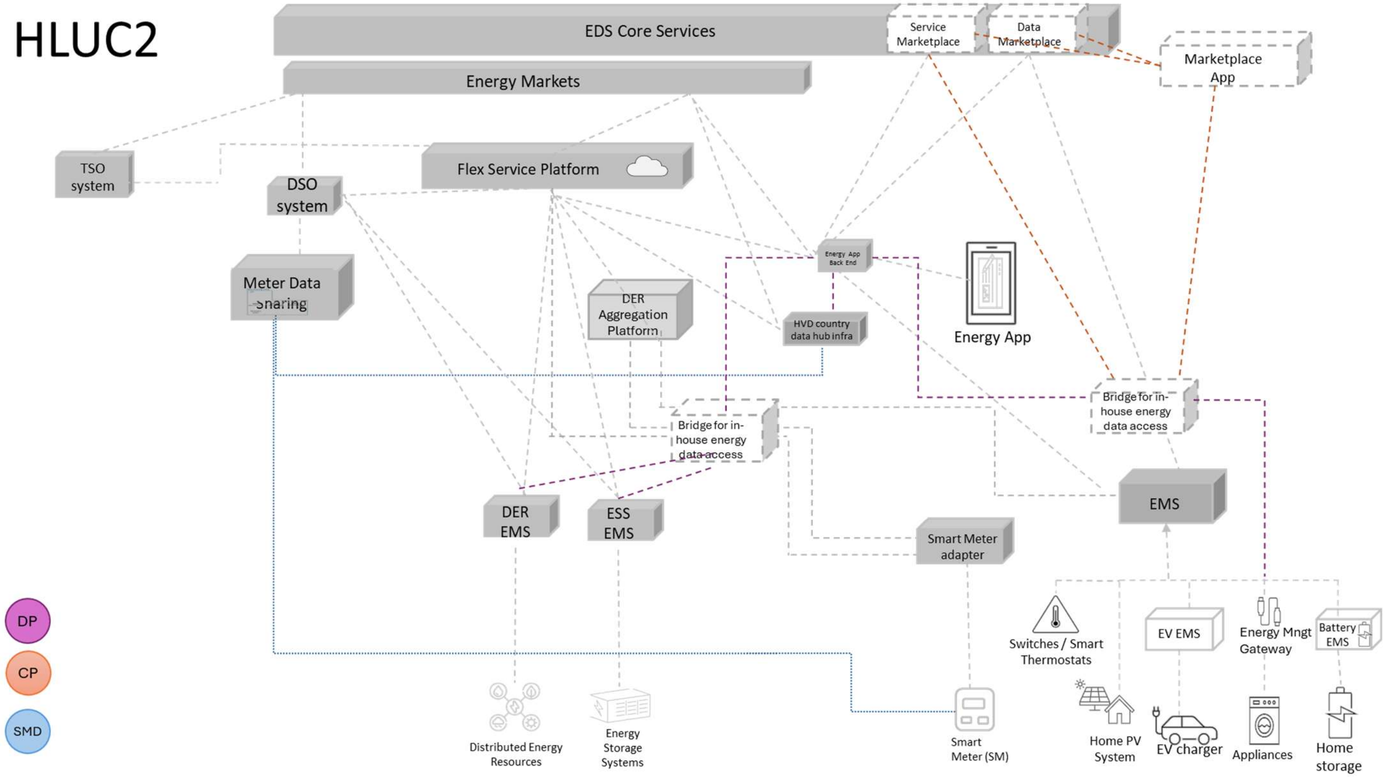


Figure 20: HLUC2 Generic ECLIPSE DIGITAL CERF architecture

2.2.2.3. HLUC 3 - PERSONALISED MESSAGES TO CONSUMERS ABOUT ENERGY EFFICIENCY POTENTIAL

The system integrates real-time and historical data from diverse energy sources to provide personalised recommendations, notifications, and advisory services, enabling users to optimise their energy consumption, reduce costs, and align their energy use with sustainability goals.

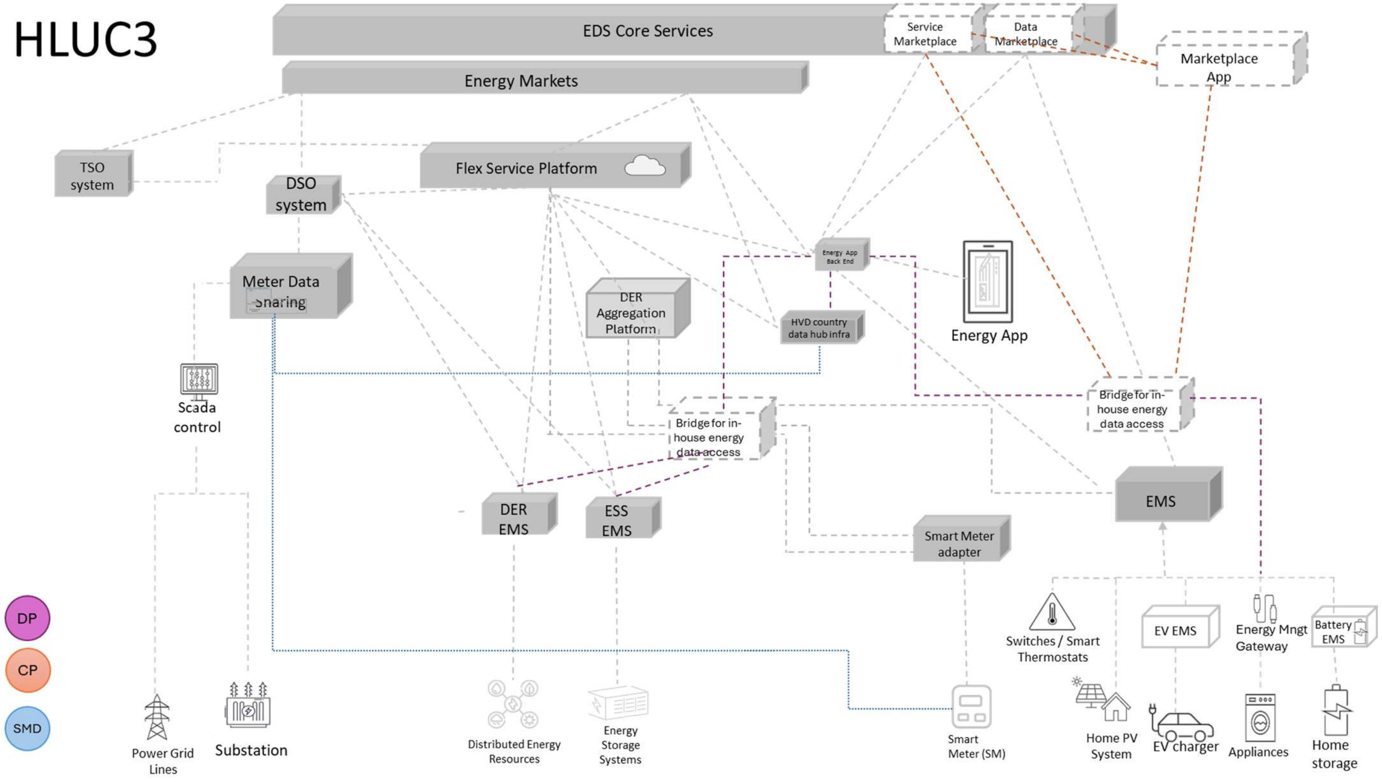


Figure 21: HLUC3 Generic ECLIPSE DIGITAL CERF architecture

2.2.2.4. HLUC 4 - GENERAL MESSAGES/ALERTS DUE EXTREME SITUATIONS IN THE GRIDS

The system integrates real-time grid data from TSO and DSO to provide immediate alerts, personalised recommendations, and participation mechanisms for consumers. Grid status information may also be sourced from SCADA systems, enabling more accurate real-time awareness of grid conditions for operator-triggered alerts and flexibility requests. The HLUC aims to enhance grid stability by encouraging energy-saving actions during critical events, leveraging demand response programs, standardised messaging, and simulations of extreme grid conditions.

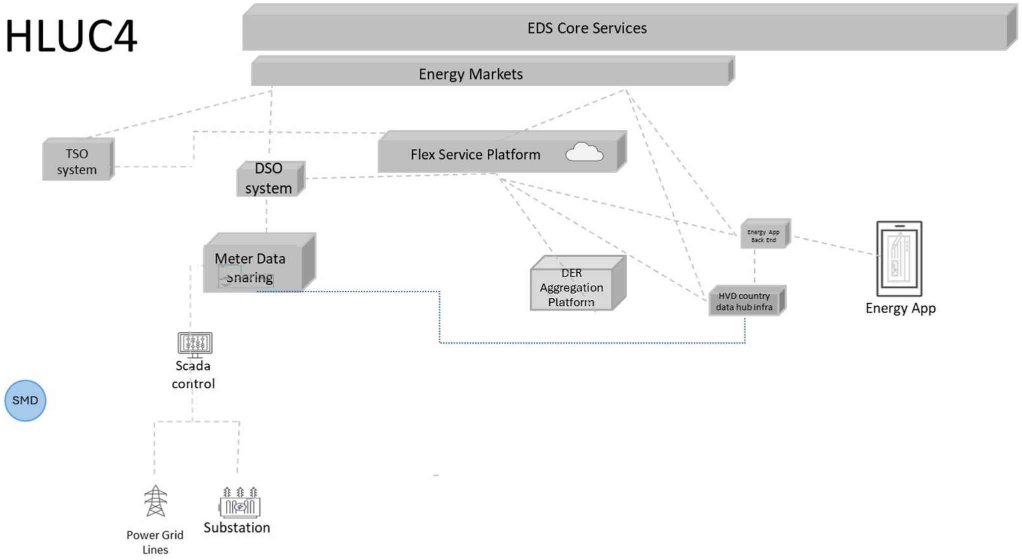


Figure 22: HLUC4 Generic ECLIPSE DIGITAL CERF architecture

2.2.2.5. HLUC 5 - GENERAL TIPS AND GUIDANCE TO CONSUMERS ABOUT ENERGY EFFICIENCY POTENTIAL

The system combines real-time data and historical insights. the app provides personalized recommendations, general tips, and educational content, promoting energy-efficient behaviours. It engages users through mobile apps, web pages, and gamification, catering to diverse audiences, from individual users to student residences and technical consumers.

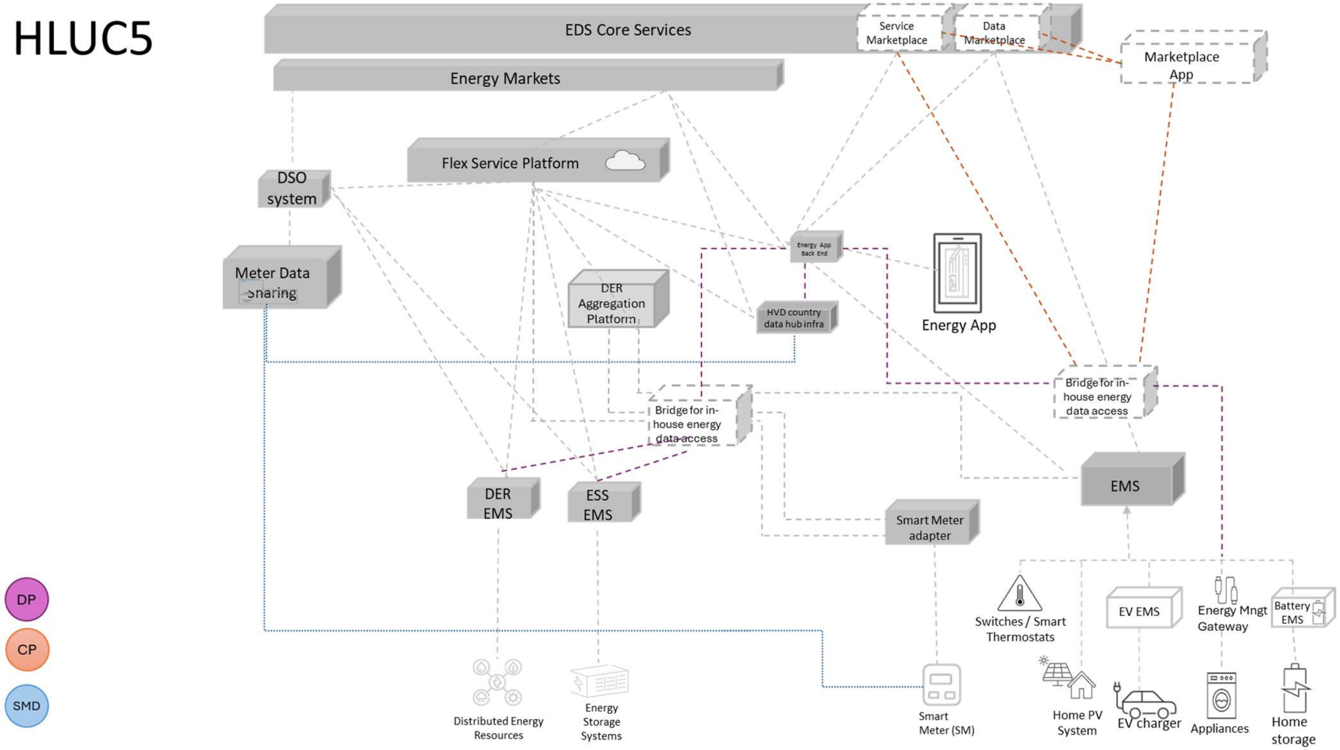


Figure 23: HLUC5 Generic ECLIPSE DIGITAL CERF architecture

2.3. ENSURING ARCHITECTURAL EVOLUTION AND INTEROPERABILITY

2.3.1. ALIGNMENT WITH DATA SPACE FRAMEWORKS

Building upon the SGAM-based system design, this section provides recommendations on how the CERF architecture could evolve toward compliance with Data Spaces (such as Gaia-X and IDSA) principles through the future integration of Energy Data Spaces (EDS).

These integrations would ensure interoperability, sovereignty, and trust across all stakeholders, preparing the CERF architecture for potential real-world deployment.

While a full Data Space is not implemented uniformly across all pilots, some, such as the Austrian pilot, already make use of Data-Space-related components. The CERF therefore the CERF architecture is intentionally designed to accommodate both the integration of a Data Space where available and alternative data-exchange mechanisms where appropriate. Across the architectural figures, this flexibility is reflected in the way the system conceptually brings together three foundational pillars:

1. A governed smart-meter data infrastructure envisioned to provide inclusive and trustworthy ground-truth measurements;
2. Aggregators that would convert distributed flexibility into market-ready products;
3. Planned EDS connectors intended to enable identity management, consent, policy enforcement, and semantic interoperability across domains.

2.3.1.1. ADDITIONAL COMPONENT IDENTIFICATION

The Energy Data Space continuous integration would provide governance, catalogue discovery, identity, and sovereignty services, while Market Actors (DSO, TSO, and Market Operators) would coordinate balancing, settlement, and pricing signals. Along with components defined earlier in section 2.2, they define the intended operational and governance perimeter of a potential Energy Data Space integration.

2.3.1.2. DATA SPACE CONNECTORS

Interoperability and sovereignty could be achieved in future through standardised connectors forming the EDS layer, as shown in Figure 24

- Southbound connectors will link Technical Aggregators to local EMS and Smart Meter devices via industrial/IoT protocols (OCPP, Modbus, EEBUS, IEC 61850, etc).

- Lateral connectors will interlink Technical Aggregators, FSPs, and Retailers using secure APIs or IDS/GAIA-X-compliant connectors, each embedding usage-control policy.

- Northbound connectors will connect FSPs and Retailers to Market Operators and EDS Core services, allowing catalogue discovery, authentication, and trusted data exchange.

Each data exchange is foreseen to carry machine-readable contractual metadata defining ownership, permitted use, retention, and pricing, ensuring that flexibility data remain sovereign and auditable throughout their lifecycle.

Together, these connectors would enforce the Data Space principles of identity, sovereignty, and interoperability, once adopted by project participants.

A data space connector has been identified as important to support sovereign data sharing (including smart meter and behind-the-meter data) between systems such as DR aggregation platforms, flexibility service platforms, DSO systems, and external domains. As mentioned in section 2.2, consent management is complex and may involve different actors (e.g. DR operators as first to enrol devices, and flexibility platforms like Voltalis), with everyone needing consent when sharing personal data. As first step, this could be arranged by distinguishing clearly between energy markets (capacity, balancing, local flexibility, etc., where TSOs/DSOs operate) and data marketplaces, which is described in 2.2.3.

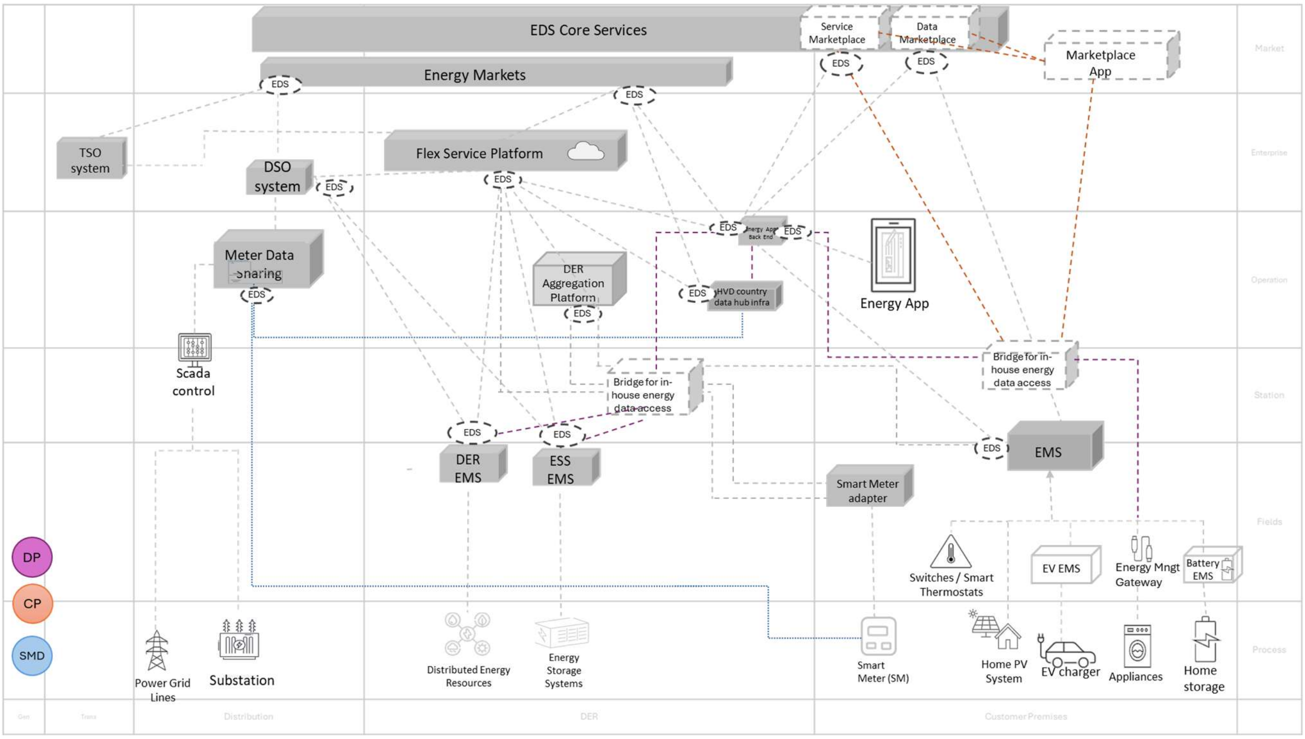


Figure 24: ECLIPSE DIGITAL Project Architecture Connector Placement

2.3.1.3. CREATION OF THE ENERGY DATA SPACE FABRIC

Once such connectors are deployed, the Energy Data Space fabric could emerge as a trusted digital backbone linking all energy actors.

Each future Data Space established between two connectors, as shown in Figure 25, would support sovereign, secure, and policy-controlled data exchange, each ellipse has its governance and instantiation.

The following components come into play, each responsible for a particular facet of how the Data Space operates and is integrated within the architecture:

- Energy Data Space Core Services: Provides governance (rules reinforcement), catalogue (discovery), identity (trustworthiness), and sovereignty services (trustworthiness).
- Connectors: Enable secure, standardised data exchange between all participants (households, aggregators, DSOs, energy service providers).
- Market Actors: Distribution System Operators (DSOs), Transmission System Operators (TSOs), and energy markets coordinate balancing, settlement, and pricing signals.

Same components along with the connector could be mapped in the different SGAM layers as:

- **Component & Communication Layers**: Distributed sovereign connectors and trust anchors could be deployed to implement secure communication.

- **Information Layer**: Harmonised semantics (CIM, SAREF [15], OpenADR) could be adopted to describe consumption, flexibility, and pricing data.
- **Function Layer**: Shared services such as identity, catalogues, access control, consent, and usage monitoring, that could be developed to enable cross-domain collaboration.
- **Business Layer**: Governance frameworks and legal agreements should coordinate Retailers, FSPs, and DSOs, ensuring transparency and accountability.

Through this proposed structure, the aggregation, flexibility, and energy marketplaces could become integrated participants in a federated, sovereign Energy Data Space. The resulting fabric would enable real-time, standards-based interoperability between technical operations, market transactions, and customer engagement, forming a potential digital foundation for next-generation flexibility and energy services.

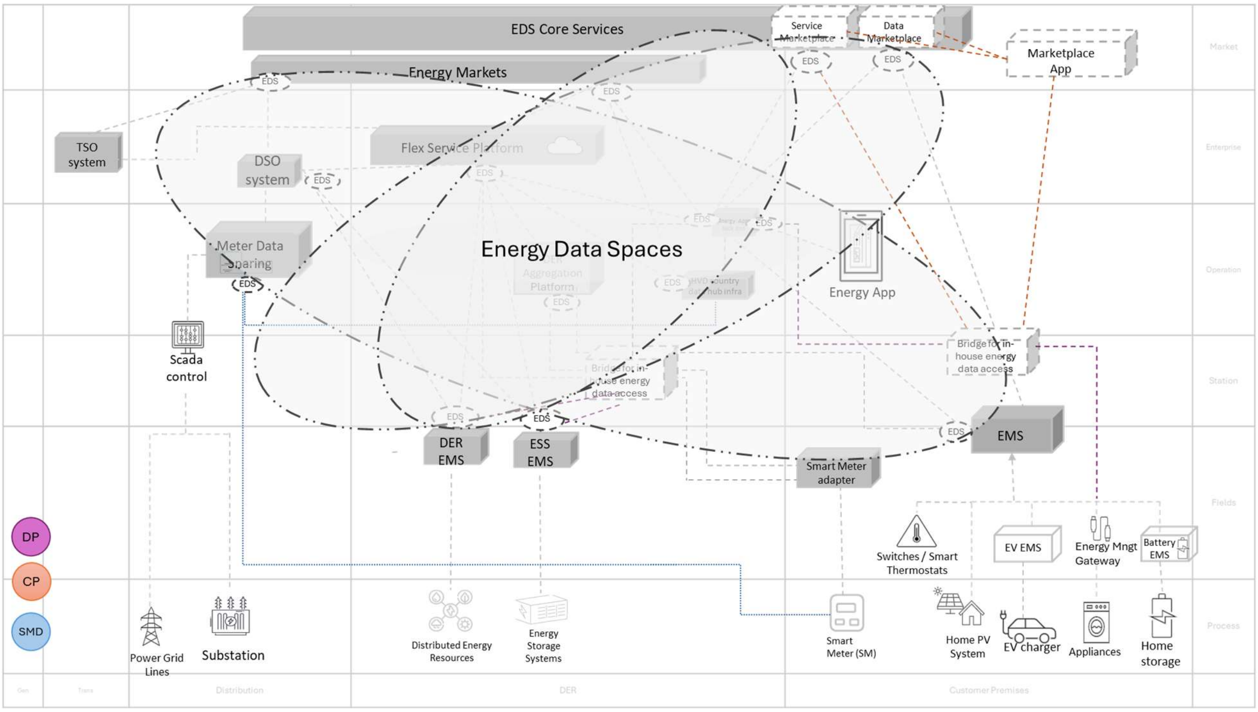


Figure 25: Emerging Energy Data Spaces in the ECLIPSE DIGITAL Project Architecture

2.3.2. FORWARD-LOOKING ARCHITECTURAL ALIGNMENT

Reflecting what was described as **¡Error! No se encuentra el origen de la referencia.**, the ECLIPSE DIGITAL CERF architecture is designed to remain adaptable to emerging European initiatives and technological developments, this section outlines several forward-looking considerations that extend beyond the current project scope. These perspectives highlight areas where CERF-based architectures may evolve to maintain long-term relevance and interoperability in the European energy ecosystem.

Key domains of alignment include the ongoing development of the following:

- **European Energy Data Space (CEEDs)** [16]: Incorporation of outcomes from the int:net project's first-generation blueprints for the energy data spaces, ensuring the architecture is in step with the latest EU digital strategy. Consequently, the CERF architecture aligns with the Data Space Support Centre (DSSC) framework established under the European Commission’s Digital Europe Programme. The DSSC provides the common building blocks, interoperability guidelines, and governance patterns used across all European Data Spaces. By following these reference blueprints, ECLIPSE DIGITAL ensures that its proposed Energy Data Space is fully compatible with cross-sector initiatives, bridging energy, mobility, and manufacturing, and remains compliant with Gaia-X and IDSA principles.

- **Aggregator and Flexibility Market Maturity**: Operational pilots demonstrate coordination between aggregator platforms and distributed energy assets.

- **Integration of an Energy App–to–EDS Connector**: Enabling trusted energy data exchange by market platforms. It will allow the consumption of data through an Energy Data Space, particularly by Marketplaces, intake of HDV data, Flex aggregation and recommendations personalisation based on users’ energy consumption.

- **Integration of High-Value Datasets (HVDs):** Placeholder for connection with national HVD hubs (e.g., weather, mobility) to enrich energy forecasting and enhance aggregator services.

- **Embedding data provenance metadata:** It could be integrated as a foundational mechanism to ensure trust, transparency, and sovereignty across all data exchanges within the Energy Data Spaces. Every data asset, whether originating from smart meters, aggregators, flexibility platforms, or market services, should carry provenance metadata describing its source, transformation history, ownership, and applicable usage policies. By embedding provenance into the information and governance layers of the SGAM framework, the ECLIPSE DIGITAL project ecosystem would ensure that all actors, DSOs, TSOs, retailers, and service providers can verify where data comes from, how it has been processed, and under what rights it can be reused. This not only strengthens interoperability and regulatory compliance (e.g., GDPR, AI Act) but also establishes a trusted fabric for energy data exchange, supporting accountability, certification, and automated trust scoring within the federated environment.

This future integration path creates a foundation for accountable, certified, and automated trust across federated Energy Data Spaces.

2.3.2.1. DERA MAPPING

When instantiating DERA (described in Section 2.1.2) in ECLIPSE DIGITAL project, we move from a system-centric SGAM view to a data-exchange-centric view. SGAM is primarily used to model smart grid use cases across domains, zones and the five interoperability layers (Business, Function, Information, Communication, Component), focusing on system functions and information flows in the grid [17]. DERA, by contrast, reuses these interoperability layers but organises them around local data platforms and federated data-space components, such as data connectors, harmonisation and vocabulary services, identity and access management, cataloguing/discovery and marketplace modules [3]. For ECLIPSE DIGITAL, mapping into DERA therefore highlights how each component participates in European energy-data spaces, rather than only where it sits in the smart-grid system. It makes explicit the roles of local vs. federated building blocks, data sovereignty and governance, and aligns the architecture with BRIDGE's Data Management work and emerging Common European Energy Data Space and data-space blueprints. Mapping the ECLIPSE DIGITAL architecture to the DERA is shown in Figure 26 below figure.

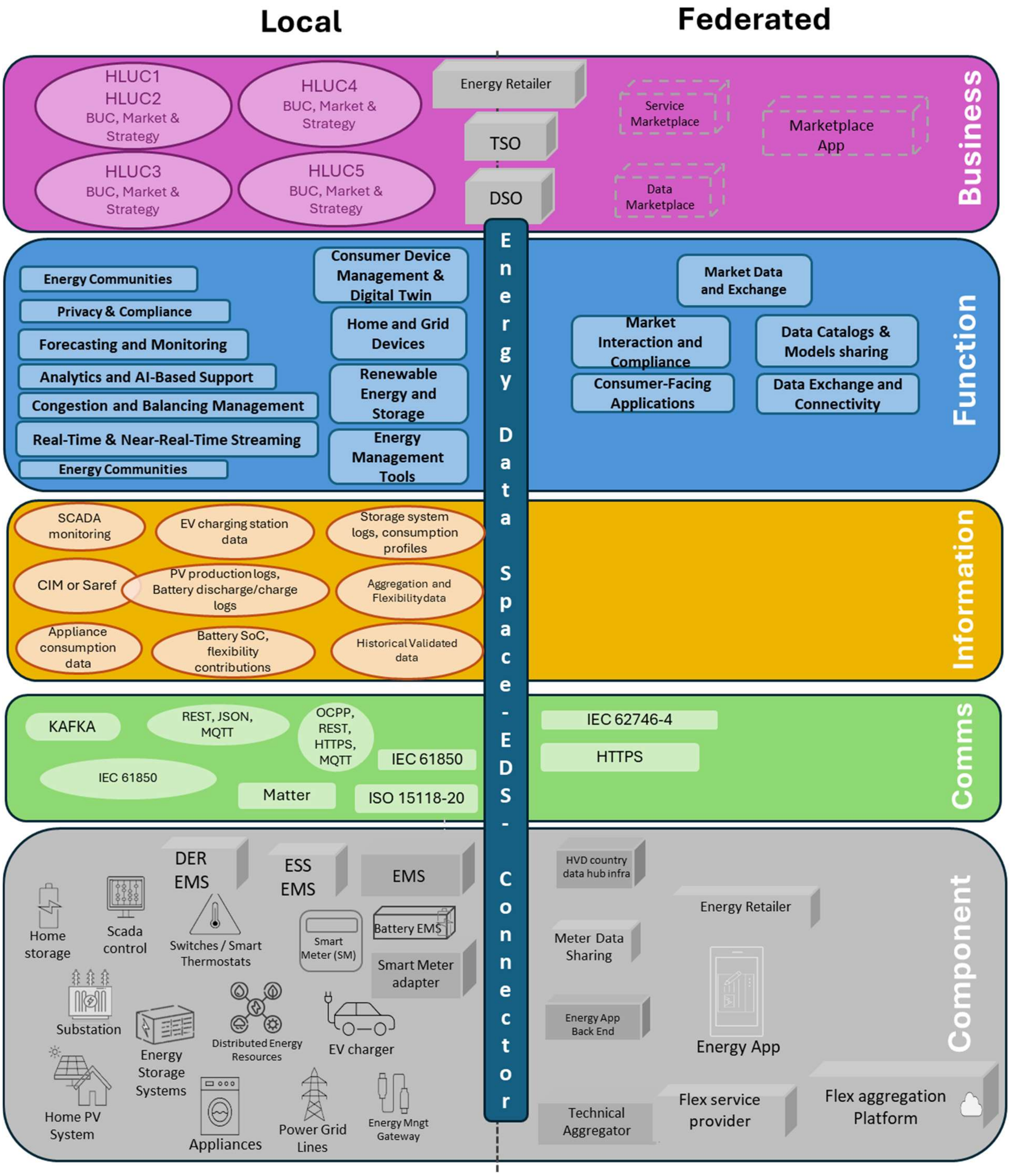


Figure 26: ECLIPSE DIGITAL project DERA mapping

2.3.2.2. HOURGLASS MODEL

Mapping of the Hourglass Model [18] to the ECLIPSE DIGITAL project is shown in Figure 27.

As described in Section 2.1.3, the hourglass model provides a structured way to map the ECLIPSE DIGITAL stakeholders (grouped across the upper, middle, and lower layers) to their corresponding capabilities (represented by the previously identified functional components). By aligning stakeholders with these components through the narrow "waist" of the model, we can clearly identify the minimal, interoperable set of interfaces that anchor the system. This mapping process was instrumental in determining where a Data Space and its connector could be positioned within the overall architecture, particularly with respect to applicable data-sharing standards and protocols. The implications of this placement, and the resulting architectural options for implementing open, standards-based data exchange, are further elaborated in Section 4.3 Open-Source Reusable Connectors.

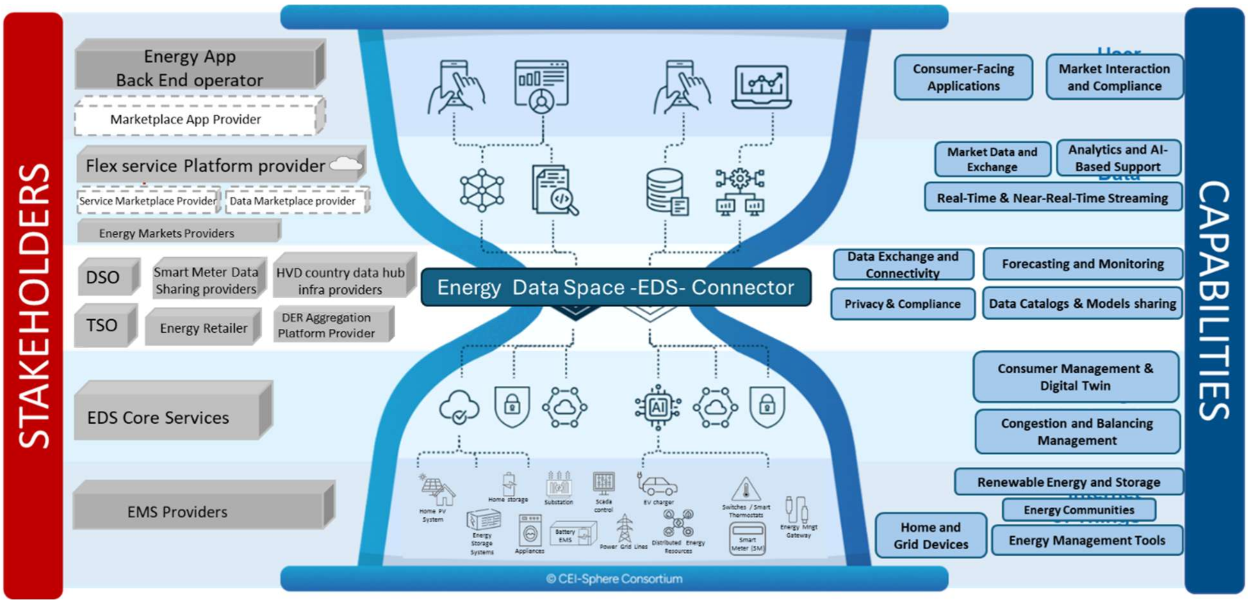


Figure 27: CERF Architecture mapping to Hourglass model

2.3.2.3. REFERENCE ARCHITECTURE STANDARD ITERATION OF CERF

Considering the described methodology in section 2 to comply with ISO/IEC 42010, the ECLIPSE DIGITAL Reference Architecture must identify the key stakeholders involved in the architectural iterations shown in Figure 28, the concerns that drive their requirements, and the viewpoints used to organise and address those concerns. In the context of ECLIPSE DIGITAL, stakeholders span the full system-of-systems landscape of the project, including consumer-facing actors, market and aggregation actors, grid-operation actors, and Data Space governance bodies. Their concerns include interoperability across heterogeneous systems, data sovereignty and consent management, operational coordination for flexibility activation, and adherence to emerging Common European Energy Data Space (CEEDS) principles.

The architectural specialisations depicted in Figure 28, ranging from SGAM-based modelling to CERF alignment, CEEDS integration, and Data Space–ready extensions, represent a sequence of architecture decisions taken to respond to these concerns through appropriate viewpoints. These iterative transitions reflect the progressive adoption of SGAM as the baseline modelling framework, the incorporation of CERF components, the alignment with CEEDS guidance, and the evolution of the CERF architecture toward patterns that natively support Data Space participation.

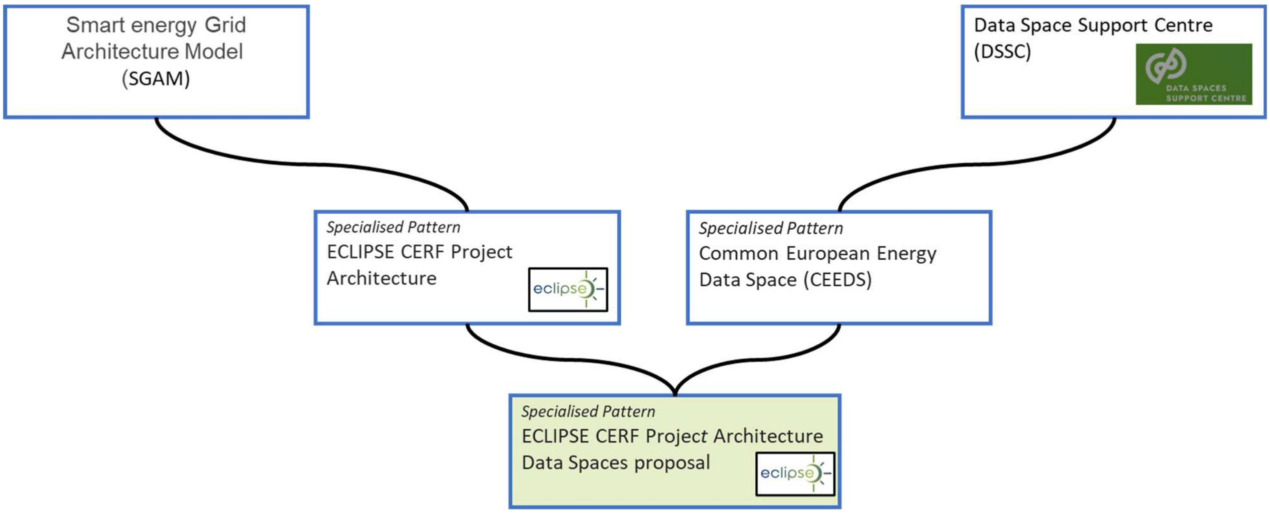


Figure 28: ECLIPSE DIGITAL Reference Architecture in ISO/IEC 42010 iterative process Data Space Proposal

2.3.2.3.1. ECLIPSE DIGITAL CERF PROJECT DATA SPACE ENHANCED CERF

Since the CERF architecture builds upon the Common European Reference Framework (CERF) established in the InterConnect project [8], as explained in section 2, which defines a modular and interoperable architecture for energy applications, it is here referenced as “Initial CERF Architecture” and while it provides the foundational layers of interoperability, covering data models, communication interfaces, and application logic, ECLIPSE DIGITAL project provides wider architectural capabilities guidance by proposing the integration of Data Space principles (as defined by Gaia-X and IDSA), which will be referenced as “ECLIPSE DIGITAL CERF Architecture”. This enhancement introduces sovereign data exchange, usage-control enforcement, and provenance tracking, enabling CERF-based architectures to evolve toward federated, trusted, and compliant ecosystems. In this way, ECLIPSE DIGITAL project does not replace InterConnect’s initial CERF but extends it to align with the next generation of European digital infrastructures, ensuring readiness for integration within the Common European Energy Data Space (CEEDs).

The Reference Architecture iteration integrating the Initial CERF Architecture is shown below in Figure 30. It maps all current identified components (section 2.2.1) to the initial CERF Architecture (Section 2.1.5).

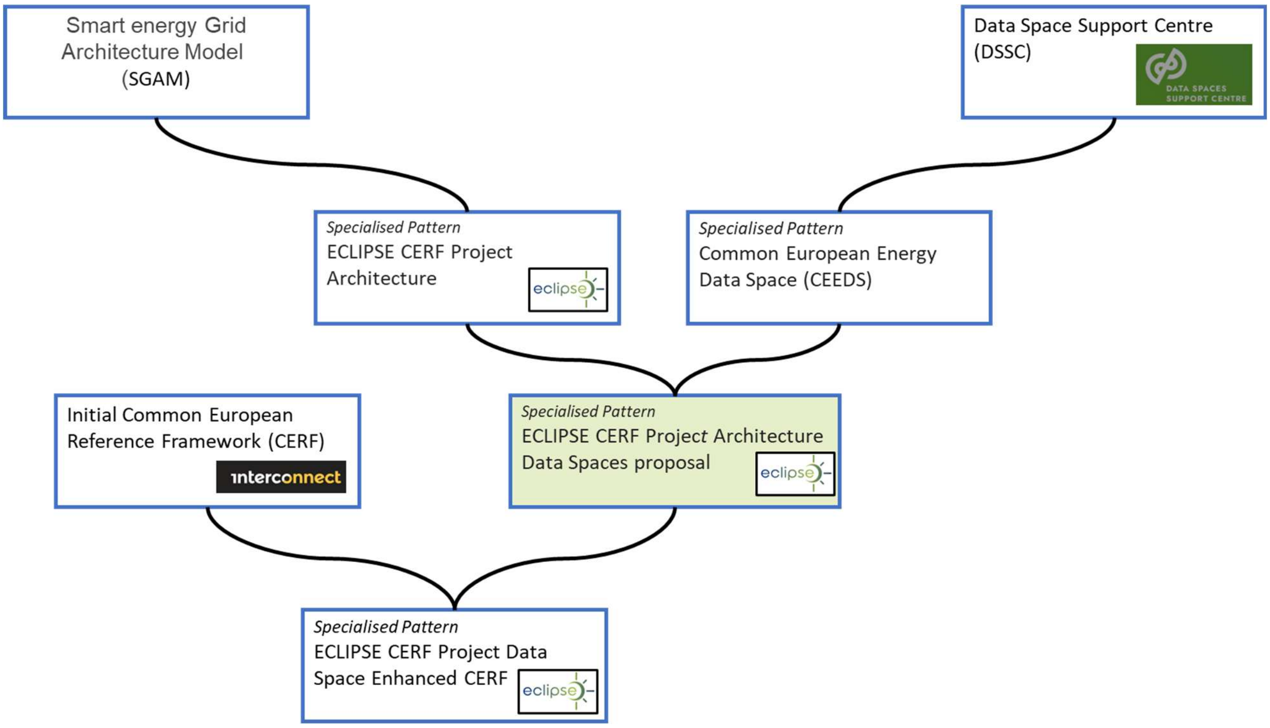


Figure 29: ECLIPSE DIGITAL Reference Architecture in ISO/IEC 42010 iterative process integrating Interconnect's initial CERF

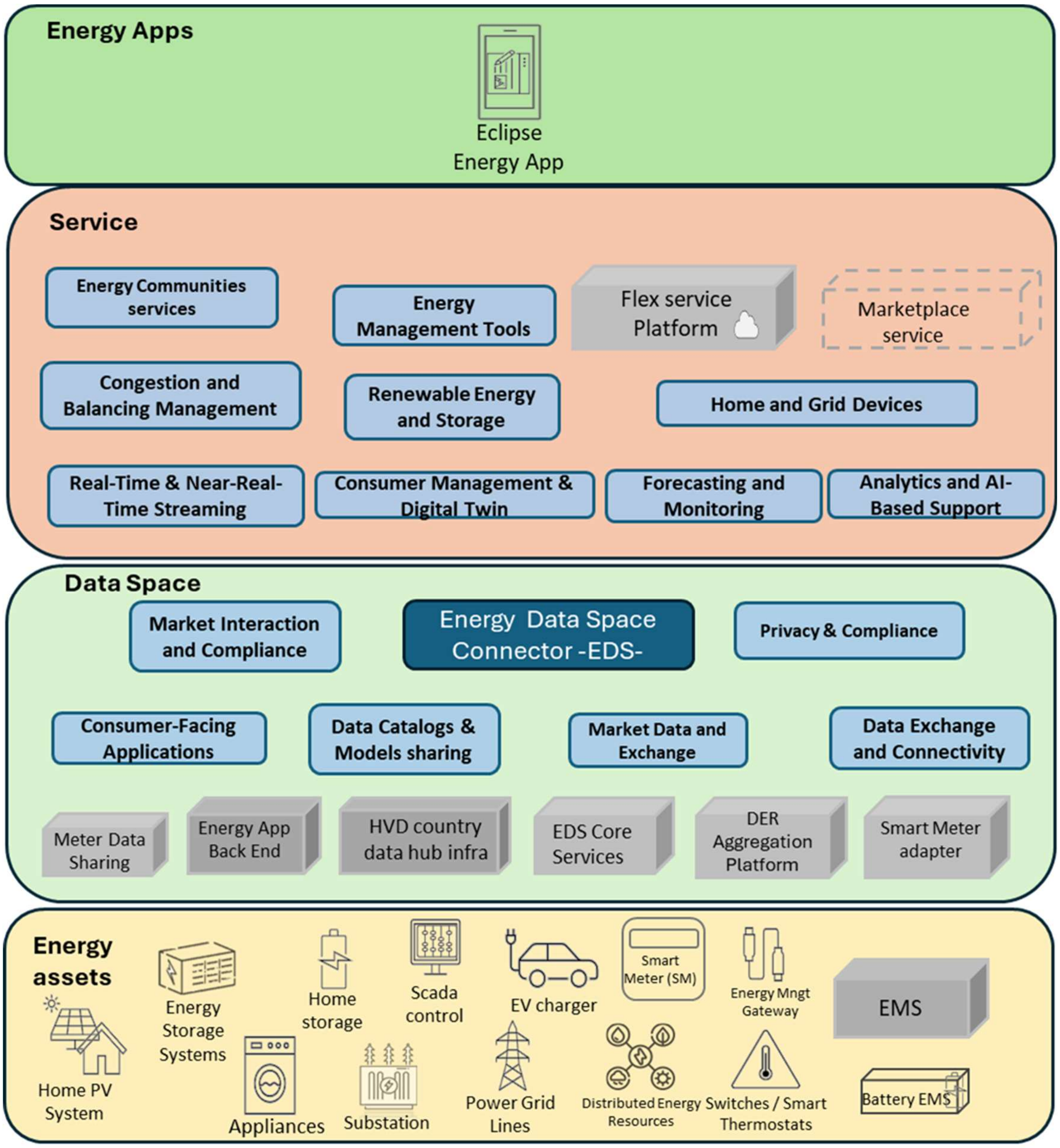


Figure 30: Mapping from initial CERF Architecture baseline to ECLIPSE DIGITAL project Data Space–enabled architecture

2.4. TECHNICAL ASPECTS FOR FUTURE INTEGRATION

Given that CERF already supports principles such as interoperability, secure data exchange, and role-based data governance, but does not implement an Energy Data Space or the associated mechanisms in full in all pilots. The following illustrate how the CERF could be extended in future initiatives to align with emerging Gaia-X and IDSA practices.

Potential future features (outside the current CERF scope)

These items are presented as recommendations for long-term technical alignment, not as requirements or deliverables of the project:

- **Interoperability**: Adoption of standardized EDS connectors aligned with Gaia-X and IDSA principles, enabling seamless smart-meter and flexibility data exchange across domains.
- **Data Sovereignty**: Implementation of consent-based data-usage policies ensuring that prosumers retain control over household and device data.
- **Data Provenance**: Integration of provenance mechanisms to verify data origin, transformation history, ownership, and usage rights, ensuring traceability, accountability, and compliance (GDPR, AI Act).
- **Advanced Smart Meter Infrastructure**: Harmonization of data models and interfaces to support near-real-time analytics for consumer apps and aggregator platforms.

These elements outline a forward-looking roadmap for how CERF-based architectures may evolve in subsequent projects or operational deployments, without implying that they are part of the current project's implementation.

This integration of Data Spaces into the CERF Architecture, can lead the way to new specialised pattern along with results of INSIEME project, the iterative process and how it could look is shown in Figure 31.

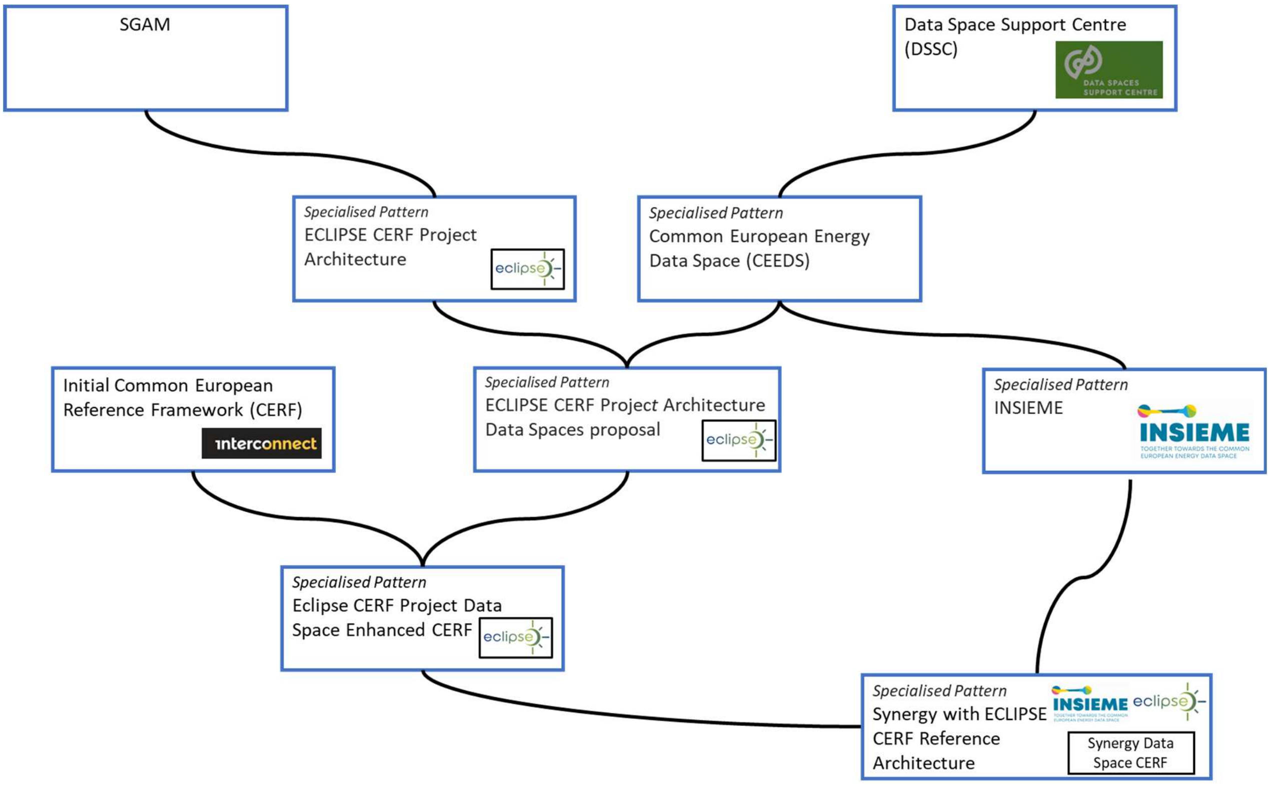


Figure 31: Data Spaces iterative architecture approach from ECLIPSE DIGITAL and INSIEME results

3. DATA EXCHANGES

3.1. METHODOLOGY

The section presents the analysis and mapping of data exchanges and interfaces for the ECLIPSE DIGITAL project. The focus is on identifying the key interfaces between systems, mapping them to High-Level Use Cases (HLUCs), and detailing the relevant data information associated with these interfaces. This work is aligned with Task 3.1 (Specifications of suitable data sets and digital environment) of the project and aims to ensure seamless system integration and data interoperability. The analysis was based on detailed reviews of ECLIPSE DIGITAL project documents, in particular the ECLIPSE DIGITAL Data Management Plan (DMP), the ECLIPSE DIGITAL Generic Architecture description, and the ECLIPSE DIGITAL Grant Agreement (GA), in order to establish a reliable and consistent foundation. Following this, project partners and ECLIPSE DIGITAL pilot sites were engaged with targeted questions to clarify aspects of the data exchanges and interfaces. Virtual meetings were then held with representatives from ECLIPSE DIGITAL pilot sites, such as Slovenia and Portugal, to discuss any unclear points and reach a common understanding of the requirements. The initial draft was distributed among the pilot sites for validation, and the feedback received was carefully analysed and incorporated, resulting in an updated version of the document. Finally, a second round of validation was conducted to confirm the accuracy and completeness of the information.

3.2. INTERFACES

3.2.1. DATA EXCHANGES PER INTERFACE

The main objectives of this section are:

i. Identifying Interfaces and HLUC Relevance: Provide a comprehensive list of interfaces, showing the interacting systems and identifying their relevance to specific HLUCs.

ii. Identifying Relevant Data: For each interface, use the DMP, input from project partners, and pilot feedback to document the relevant data being exchanged.

iii. Data Characterization: Collaborate with pilots to characterise the data for each interface, including Identification Data, Technical Data, Operational Data, and Training Data, ensuring alignment with project goals and interoperability requirements.

3.2.2. INTERFACE LABELLING AND FAMILY CLASSIFICATION.

In the Generic SGAM Architecture (Component Layer), each connection between components is identified with an interface code combining a family letter and a sequential number (for example, A1, B2). These labels group interfaces by their functional domain, making the diagram clearer and easier to interpret. The core seven interface families are defined as follows:

- Family A - Energy Markets & Flexibility Management Services
- Family B - System Operators / Grid Operations
- Family C - Aggregation & Coordination Layer

- Family D - DER / ESS Control
- Family E - Energy App & Backend Services
- Family F - Customer Premises & Device Layer and
- Family G - EDS / Data-Space & Cross-Domain Exchange.

In addition to these core families, some pilots require a dedicated in-home service orchestration and consent layer (for example, the Austrian pilot with AIIDA). For these pilots, an eighth, pilot-specific interface family is introduced:

- Family H - Consent Management & In-Home Service Orchestration

Family H is only used in pilots that implement this specific consent and in-home orchestration pattern. It is not required for all ECLIPSE DIGITAL pilots.

This classification reflects the logical organization of system interactions within the SGAM Component Layer, and the corresponding visual representation is illustrated in the figure presented below.

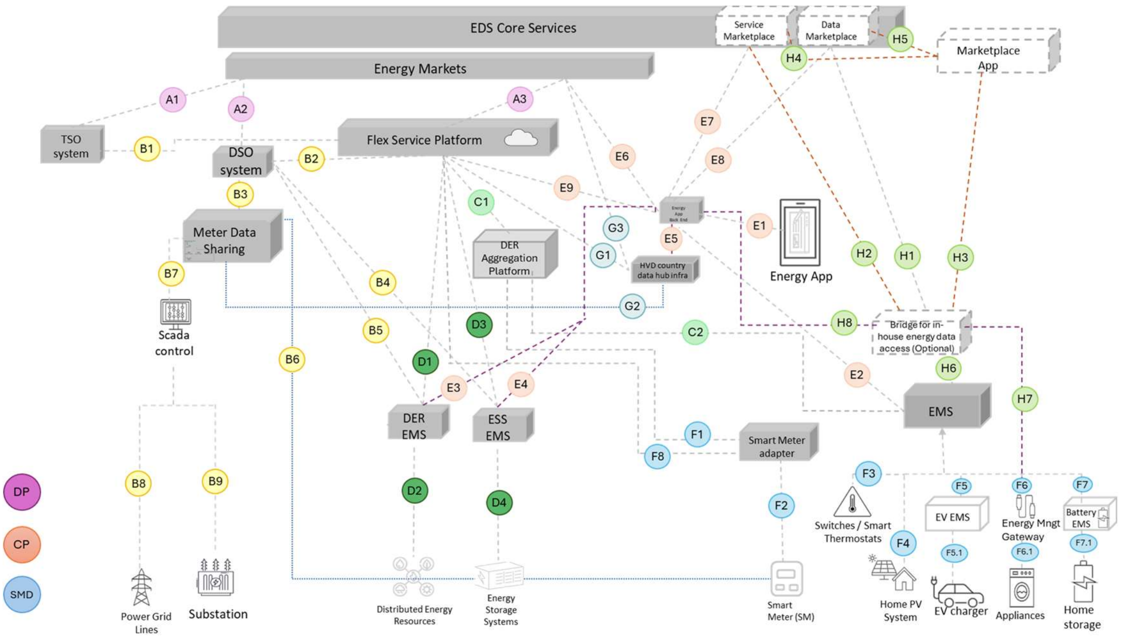


Figure 32: Defined Interfaces with Corresponding Interacting Components

The following table (List of Interfaces with Interacting Systems and Relevant HLUCs) presents the list of identified interfaces within the Generic SGAM Architecture and their linkage to the project's High-Level Use Cases (HLUCs). Each entry specifies the interacting components, the corresponding HLUCs they support, and the pilot sites where these exchanges will be implemented. This overview provides a clear understanding of how data flows are distributed across different domains and how each pilot contributes to validating specific aspects of the architecture.

Table 2: List of Interfaces with Interacting Systems and Relevant HLUCs

Interface Name	Interacting Systems/ components	Relevant HLUC(s)	Relevant Pilot Site Name
Interface A1	Energy Markets & TSO system	HLUC-1, HLUC-4	France, Sweden
Interface A2	Energy Markets & DSO system	HLUC-1, HLUC-4	France, Sweden
Interface A3	Energy Markets & Flex Service Platform	HLUC-1, HLUC-2, HLUC-4	France, Estonia, Finland, Denmark, Belgium, Sweden, Portugal, Austria
Interface B1	Flex Service Platform & TSO system	HLUC-1, HLUC-4	France, Sweden
Interface B2	Flex Service Platform & DSO system	HLUC-1, HLUC-4	France, Sweden
Interface B3	DSO system & Meter Data Sharing	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria, Slovenia, Portugal, Poland, Czech Republic
Interface B4	DSO system & ESS EMS	HLUC-4	Sweden, Portugal
Interface B5	DSO system & DER EMS	HLUC-1 (partial)	France (partial), Spain (partial)
Interface B6	Meter Data Sharing & Smart Meter (SM)	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria, Slovenia, Portugal, Poland, Czech Republic
Interface B7	Meter Data Sharing & Scada control	HLUC-4	Croatia, Romania
Interface B8	Scada control & Power Grid Lines	HLUC-4	Croatia, Romania

Interface B9	Scada control & Substation	HLUC-4	Croatia, Romania
Interface C1	Flex Service Platform & DER Aggregation Platform	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	France, Estonia, Finland, Denmark, Belgium, Sweden
Interface C2	DER Aggregation Platform & EMS	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	France, Estonia, Finland, Denmark, Belgium, Sweden
Interface D1	Flex Service Platform & DER EMS	HLUC-1, HLUC-2, HLUC-4	France, Estonia, Finland, Denmark, Belgium, Sweden, Spain
Interface D2	DER EMS & Distributed Energy Resources	HLUC-1, HLUC-2, HLUC-3	France, Estonia, Finland, Denmark, Belgium, Sweden, Spain, Greece
Interface D3	Flex Service Platform & ESS EMS	HLUC-1, HLUC-4	France, Sweden
Interface D4	ESS EMS & Energy Storage Systems	HLUC-1, HLUC-3	France, Sweden
Interface E1	Energy App Back End & Energy App	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	France, Austria, Spain, Slovenia, Portugal, Sweden, Bulgaria, Cyprus, Greece, Croatia, Poland, Czech Republic, Romania
Interface E2	Energy App Back End & EMS	HLUC-1, HLUC-4	Austria, Greece

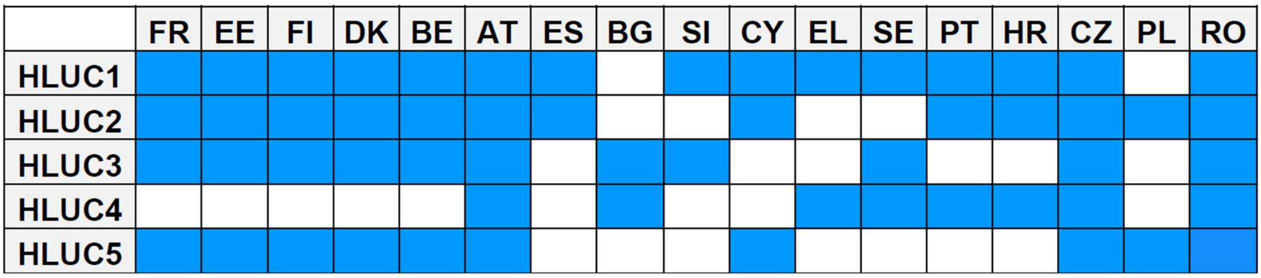
Interface E3	Energy App Back End & DER EMS	HLUC-1, HLUC-2, HLUC-3	France, Spain, Sweden, Greece
Interface E4	Energy App Back End & ESS EMS	HLUC-1	Sweden
Interface E5	HVD country data hub infra & Energy App Back End	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria, Slovenia, Portugal, Czech Republic, Poland, Romania
Interface E6	Energy Markets & Energy App Back End	HLUC-1, HLUC-2, HLUC-4	Poland, Portugal, Spain, Sweden, Austria
Interface E7	Service Marketplace & Energy App Back End	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria
Interface E8	Data Marketplace & Energy App Back End	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria
Interface E9	Flex Service Platform & Energy App Back End	HLUC-1, HLUC-2, HLUC-4	France, Estonia, Finland, Denmark, Belgium, Spain, Sweden, Portugal, Croatia, Greece, Cyprus
Interface F1	DER Aggregation Platform & Smart Meter adapter	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	France, Estonia, Finland, Denmark, Belgium, Sweden, Slovenia, Portugal, Austria, Czech Republic, Poland, Croatia, Romania

Interface F2	Smart Meter adapter & Smart Meter (SM)	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	France, Estonia, Finland, Denmark, Belgium, Sweden, Slovenia, Portugal, Austria, Czech Republic, Poland, Croatia, Romania
Interface F3	EMS & Switches / Smart Thermostats	HLUC-1, HLUC-2, HLUC-3	France, Estonia, Finland, Denmark, Belgium, Greece, Austria
Interface F4	EMS & Home PV System	HLUC-1, HLUC-3	France, Estonia, Finland, Denmark, Belgium, Greece, Sweden, Austria
Interface F5	EMS & EV EMS	HLUC-1, HLUC-4	France, Estonia, Finland, Denmark, Belgium, Spain, Greece, Austria
Interface F5.1	EV EMS & EV charger	HLUC-1, HLUC-4	France, Estonia, Finland, Denmark, Belgium, Spain, Greece, Austria
Interface F6	EMS & Energy Mngt Gateway	HLUC-1, HLUC-2, HLUC-3	France, Greece, Austria
Interface F6.1	Energy Mngt Gateway & Appliances	HLUC-1, HLUC-2, HLUC-3	France, Greece, Austria
Interface F7	EMS & Battery EMS	HLUC-1, HLUC-3	France, Estonia, Finland, Denmark,

			Belgium, Sweden, Greece
Interface F7.1	Battery EMS & Home storage	HLUC-1, HLUC-3	France, Estonia, Finland, Denmark, Belgium, Sweden, Greece
Interface F8	Flex Service Platform & Smart Meter adapter	HLUC-1, HLUC-2, HLUC-4	France, Sweden, Spain, Portugal, Croatia, Austria, Czech Republic, Poland
Interface G1	Flex Service Platform & HVD country data hub infra	HLUC-1, HLUC-2, HLUC-3, HLUC-5	France, Estonia, Finland, Denmark, Belgium, Austria, Slovenia, Portugal, Czech Republic, Poland, Romania
Interface G2	HVD country data hub infra & Meter Data Sharing	HLUC-1, HLUC-2, HLUC-3, HLUC-5	Austria, Slovenia, Portugal, Czech Republic, Poland, Romania, France, Estonia
Interface G3	Energy Markets & HVD country data hub infra	HLUC-1, HLUC-2, HLUC-3	France, Estonia, Finland, Denmark, Belgium, Austria
Interface H1	Data Marketplace & Bridge for in-house energy data access	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria
Interface H2	Service Marketplace & Bridge for in-house energy data access	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria

Interface H3	Marketplace App & Bridge for in-house energy data access	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria
Interface H4	Marketplace App & Service Marketplace	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria
Interface H5	Marketplace App & Data Marketplace	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria
Interface H6	Bridge for in-house energy data access & EMS	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria
Interface H7	Bridge for in-house energy data access & Energy Mngt Gateway (in-home assets)	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria
Interface H8	Energy App Back End & Bridge for in-house energy data access	HLUC-1, HLUC-2, HLUC-3, HLUC-4, HLUC-5	Austria

It is important to note that, as shown in Table 2: List of Interfaces with Interacting Systems and Relevant HLUCs, not every pilot site will implement every High-Level Use Case (HLUC), reflecting the unique operational priorities and contextual requirements of each demonstration location. Some pilots may adopt multiple HLUCs to capture a wide range of functionalities, while others focus on a select few that align more closely with their regional needs. To provide a clear visual summary of these variations, the figure below illustrates which HLUCs apply to each pilot site. This figure helps to clarify which pilot site will implement which HLUC.



	FR	EE	FI	DK	BE	AT	ES	BG	SI	CY	EL	SE	PT	HR	CZ	PL	RO
HLUC1	🟦	🟦	🟦	🟦	🟦	🟦	🟦		🟦	🟦	🟦	🟦	🟦	🟦	🟦		🟦
HLUC2	🟦	🟦	🟦	🟦	🟦	🟦	🟦			🟦			🟦	🟦	🟦	🟦	🟦
HLUC3	🟦	🟦	🟦	🟦	🟦	🟦		🟦	🟦			🟦			🟦		🟦
HLUC4						🟦		🟦			🟦	🟦	🟦	🟦	🟦		🟦
HLUC5	🟦	🟦	🟦	🟦	🟦	🟦				🟦					🟦	🟦	🟦

Figure 33: ECLIPSE DIGITAL Demonstration site and related HLUCs

Table 3 (Relevant Data for Each Interface) summarises the main data elements associated with each identified interface. For every interface, it lists the relevant data exchanged within the project, the corresponding data sources, and the partner organisations (linked to specific pilot sites) responsible for their provision or management. This section builds upon the previously defined interface mapping and HLUC relationships, ensuring continuity between the functional and data perspectives.

Table 3: Relevant Data for Each Interface

Interface Name	**Relevant Data**	**Data Source**	**Linking Relevant Partner Company Name (Pilot)**
Interface A1	- TSO balancing and flexibility product definitions (e.g. FCR, FFR). - Flexibility bids and offers (product, volume, price). - TSO activation requests, activation results and opt-out logs.	- TSO market and balancing platforms. - TSO control-centre systems and APIs. - Flex Service Platform (FSP) or VPP portfolio systems.	- VOLTALIS (France, multi-country pilot): Flexibility Service Provider (FSP) portfolio on national TSO balancing markets. - D4G (France): Auto-bidding and portfolio scheduling for residential DER behind Voltalis smartboxes. - CheckWatt (Sweden): VPP bids and activations

	- Delivered energy and settlement / performance KPIs.		toward Swedish TSO products.
Interface A2	- DSO local flexibility product definitions and technical constraints. - Local flexibility needs by feeder or area (kW, voltage, congestion zone). - Activation instructions, time windows and acknowledgements. - Validation and settlement evidence for local services.	DSO operational / flexibility platforms and SCADA planning tools. - DSO MDMS and grid models for constraint checks. - Flex Service Platform portfolio data.	- VOLTALIS (France): residential flexibility used to support DSO constraints. - D4G (France): orchestration of residential DER for DSO use cases. - CheckWatt (Sweden): VPP services to local DSOs for congestion relief.
Interface A3	- Wholesale / retail price signals and time windows. - Market-linked flexibility products and schedules per portfolio. - Aggregated baselines and forecasted flexibility for offers. - Activation and settlement logs shared with the Flex Service Platform.	- Energy market platforms and retailer systems. - TSO / DSO market interfaces where relevant. - Flex Service Platform front-office modules. - Smart-meter histories from hubs where used.	- VOLTALIS + D4G (France): Market signals combined with residential flex offers. - D4G/Voltalis replication (Estonia, Finland, Denmark, Belgium): Same logic via digital twins / replication pilots. - CheckWatt (Sweden): Price-driven schedules for PV/battery VPP. - E-REDES + R&D Nester (Portugal): DSO market-aligned signals into flex platforms. - FHOOE (Austria): Consumer apps and data marketplace integrating market signals via CERF / AIIDA.
Interface B1	- TSO flexibility needs and activation requests per product / time slot.	- TSO market and control-centre APIs.	- VOLTALIS (France): FSP response to national TSO balancing products.

	- FSP bids, availability windows and portfolio constraints. - Activation results, delivered energy and imbalance correction. - Opt-in / opt-out logs for participating assets.	- Flex Service Platform / VPP telemetry and forecasting backends. - Settlement and reporting modules.	- D4G (France): Portfolio bidding and auto-scheduling for residential DER. - CheckWatt (Sweden): VPP interaction with Swedish TSO for flexibility services.
Interface B2	- Local flexibility needs from DSO by feeder, MV/LV area or transformer. - Voltage or loading constraints and curtailment windows. - Activation instructions, acknowledgements and curtailment metrics. - Validation, meter-based verification and settlement KPIs.	- DSO operational or flex platforms. - Flex Service Platform / aggregator cloud job logs. - DSO MDMS and grid analytics tools.	- VOLTALIS (France): Execution of DSO requests on household portfolios. - D4G (France): Orchestration of DER flexibility for DSO constraints. - CheckWatt (Sweden): Aggregation and activation of flexibility toward DSOs.
Interface B3	- Validated smart-meter load curves and events (15/60-minute or better). - Metering point identifiers, consents and tariff attributes. - LV feeder and transformer aggregates for grid analytics. - Historical data used for baselines and billing.	- DSO MDMS and measurement databases. - National or regional data hubs accessed via EDDIE/AIIDA where present. - Corporate billing and customer-care systems.	- FHOOE (Austria): EDDIE/AIIDA connectors to national data access providers and P1 adapters. - Elektro Ljubljana (Slovenia): MDMS feeding Moj Elektro and new 1-minute app. - E-REDES (Portugal): MDMS and DSO interfaces feeding Balcão Digital. - TAURON Dystrybucja (Poland): AMI and eLicznik backends (XML, twice-daily loads).

			- CEZ Distribuce (Czech Republic): MDMS feeding Proud app and DIP / hub exports.
Interface B4	- DSO requests for storage dispatch at feeder or area level. - Battery state of charge, limits and availability windows. - Charge / discharge schedules and verification metering for services. - KPIs for congestion relief and service quality.	- DSO flexibility platforms and planning tools. - ESS EMS or BMS telemetry and configuration. - Aggregator VPP scheduling outputs.	- CheckWatt (Sweden): Household battery dispatch to support DSO constraints. - E-REDES (Portugal): DSO requests toward residential storage. - R&D Nester (Portugal): Forecasts at TSO-DSO interfaces supporting dispatch decisions.
Interface B5	- DSO smart-charging and load-shift requests for EV fleets. - DER EMS capability, location and availability of EV chargers. - Activation logs, constraint violations and compliance metrics.	- DSO control or flexibility platforms (e.g. SIORD context in Spain). - DER EMS or EV EMS / charger controllers. - Aggregator or retailer middleware.	- i-DE Iberdrola (Spain): SIORD-mediated DSO requests towards CPOs / EV EMS. - VOLTALIS (France): Household DER orchestration responding to DSO smart-charging or load-shift signals.
Interface B6	- Raw and validated meter reads and load curves. - Outage and power-quality events (voltage, frequency, interruptions). - 15-minute or near-real-time data for analytics and settlement.	- AMI meters and concentrators. - DSO MDMS and data-hub APIs. - Customer portals and internal analytics platforms.	- Elektro Ljubljana (Slovenia): Smart-meter data to Moj Elektro and analytics (1-minute and 15-minute views). - E-REDES (Portugal): AMI and Balcão Digital feeds. - TAURON Dystrybucja (Poland): AMI and eLicznik application (hourly / 15-minute).

			- CEZ Distribuce (Czech Republic): AMI and Proud app. - FHOOE (Austria): Access via EDDIE/AIIDA P1 adapters to smart-meter data.
Interface B7	- Aggregated demand and energy profiles from MDMS into SCADA / EMS. - Alarm and event correlation datasets. - Historian datasets for situational awareness and post-event analysis.	- MDMS to SCADA or EMS links. - Control-centre historians and data lakes.	- HOPS (Croatia): SCADA and accounting data correlation for operations and forecasting. - UNSTPB / national operator (Romania): SCADA integration with meter data for grid supervision.
Interface B8	- Line flows and voltages, breaker and switch statuses. - Switching plans, outage records and restoration logs.	- TSO or DSO SCADA and RTUs along lines. - Network model databases and topology processors.	- HOPS (Croatia): Line monitoring and control via SCADA. - Romanian pilot TSO/DSO (Romania): Line status and switching operations.
Interface B9	- Substation topology and feeder states. - Transformer tap positions and VAR set-points. - Protection, alarm and event logs.	- Substation automation gateways and IEDs. - SCADA or EMS historians.	- HOPS (Croatia): Substation SCADA operations and logs. - Romanian pilot TSO/DSO (Romania): Substation telemetry and controls.
Interface C1	- Portfolio telemetry and device status per cluster. - Load and state-of-charge forecasts per portfolio / region. - Baselines, availability and consent metadata.	- Flex Service Platform IoT cloud (MQTT, REST). - DER Aggregation Platform orchestration bus.	- D4G (France): IoT cloud to DER aggregation coordination for residential DER. - VOLTALIS (France): FSP portfolio integrated with DER aggregation functions.

	- Dispatch job queues, acknowledgements and compliance KPIs.	- Smart-meter histories via EDDIE / adapters where used.	- CheckWatt (Sweden): VPP layer acting as DER Aggregation Platform.
Interface C2	- EMS capability descriptors and controllable devices per site. - Site schedules and set-points from aggregation platform. - Telemetry, acknowledgements and opt-out logs. - Comfort and safety constraints.	- DER Aggregation Platform southbound API. - Site EMS and local gateways. - IoT telemetry from devices.	- D4G / TRIALOG (France): EMS orchestration for PV, EV, batteries via Home Energy Station. - VOLTALIS (France): Heater and appliance EMS control via smartbox. - CheckWatt (Sweden): EMS integration for batteries and inverters in VPP sites.
Interface D1	- Aggregated schedules and set-points from Flex Service Platform to DER EMS. - Device grouping, priorities and constraint parameters. - Acknowledgements, activation logs and compliance records.	- Flex Service Platform job queue and dispatch APIs. - DER EMS controllers and gateways.	- D4G (France): FSP set-points to DER EMS for PV, EV and storage. - VOLTALIS (France): Explicit DR commands to DER EMS / smartboxes. - CheckWatt (Sweden): FSP dispatch to household DER EMS. - i-DE Iberdrola (Spain): Smart-charging control path from flex platform to EV EMS.
Interface D2	- Device telemetry (power, temperature, state-of-charge, on/off state). - EMS to device commands (on/off, set-points, charging rates). - Comfort and safety constraints.	- DER EMS software. - Device controllers for thermostats, inverters and EVSE. - Home IoT hubs and local gateways.	- VOLTALIS (France): Heater and water-heater control via smartbox. - D4G (France): PV, EV and batteries via EMS interfaces. - CheckWatt (Sweden): EMS control of batteries and inverters. - i-DE / CPO (Spain): EMS commands to EVSE in

	- Usage breakdowns for efficiency feedback.		smart-charging scenarios. - Mytilineos (Greece, Aspra Spitia): EMS/IoT commands to HVAC, DHW, PV and batteries.
Interface D3	- Battery state-of-charge, limits and availability from ESS EMS. - Charge / discharge schedules and service set-points from Flex Service Platform. - Response telemetry for settlement and KPI tracking.	- Flex Service Platform scheduling and VPP optimization engines. - ESS EMS and BMS telemetry.	- D4G (France): Storage control aligned with market / grid activations. - CheckWatt (Sweden): VPP dispatch to household batteries for services.
Interface D4	- Battery inverter commands (power / reactive power). - Real-time power and state-of-charge telemetry. - Thermal and safety constraints and alarms.	- ESS EMS to battery systems. - BMS and inverter APIs.	- D4G (France): Home storage within Home Energy Station orchestration. - CheckWatt (Sweden): Household battery control for arbitrage and flexibility services.
Interface E1	- User profiles and consent tokens. - HLUC message payloads: economic signals, non-economic feedback, efficiency tips, alerts. - App engagement and interaction metrics. - Consumption histories and benchmarks.	- Energy app backend services and notification engines. - Mobile and web energy apps. - Smart-meter histories where available via hubs or MDMS.	- VOLTALIS (France): MyVoltalis app messaging. - D4G (France): Consumer app for flexibility monetisation. - FHOOE (Austria): End-Customer App and Data-Marketplace App. - i-DE Iberdrola (Spain): Customer smart-charging app. - Elektro Ljubljana (Slovenia): Moj Elektro and new 1-minute app.

			- E-REDES (Portugal): Balcão Digital app. - CheckWatt (Sweden): End-user app for PV/battery services. - ESO + EDG West + IEIT (Bulgaria): Consumer digital platform. - TSOC + CINTECH (Cyprus): Consumer energy-saving app. - Mytilineos (Greece): ACCEPT / Citizen app integration in Aspra Spitia. - HOPS (Croatia): Demand-reduction information modules. - TAURON Dystrybucja (Poland): eLicznik app. - CEZ Distribuce (Czech Republic): Proud app. - UNSTPB (Romania): Campus / consumer messaging and tips.
Interface E2	- Control intents from backend to EMS (load reductions, schedules). - Critical grid alerts and automated actions. - Feedback and compliance telemetry from EMS.	- App backend orchestration APIs. - Site EMS and home gateways.	- FHOOE (Austria): App-driven EMS automations in demo homes. - Mytilineos (Greece, Aspra Spitia): Backend-to-EMS control for HVAC and DHW via Citizen App / IoT.
Interface E3	- DER control and optimization requests from backend to DER EMS (non-battery).	- Energy app backend orchestration layer.	- D4G and VOLTALIS (France): App-mediated DER EMS control in residential flex pilots.

	- Schedules and set-points for EV, PV and controllable loads. - Telemetry and acknowledgements for applied controls.	- DER EMS APIs.	- i-DE / retailer or CPO (Spain): Smart-charging app path to DER EMS / EV EMS. - CheckWatt (Sweden): App to DER EMS coordination for PV/batteries. - Mytilineos (Greece): App-to-EMS control for HVAC, PV and other loads.
Interface E4	- Battery optimization schedules for arbitrage and services. - Price forecasts and thresholds from backend. - State-of-charge and performance telemetry to backend.	- App backend optimization engines. - ESS EMS and BMS APIs.	- CheckWatt (Sweden): App-initiated battery scheduling to ESS EMS for VPP and customer services.
Interface E5	- Validated metering histories and identifiers. - Tariff and billing attributes per MP. - Aggregated feeder / transformer statistics for analytics.	- Member-state data hubs. - DSO measurement and billing databases. - EDDIE or AIIDA connectors.	- FHOOE (Austria): EDDIE/AIIDA connectors integrating hub data into apps. - Elektro Ljubljana (Slovenia): DSO measurement DB to backend for Moj Elektro / new app. - E-REDES (Portugal): DSO data to backend for Balcão Digital and analytics. - CEZ Distribuce (Czech Republic): Data-hub and DIP access to Proud app. - TAURON Dystrybucja (Poland): AMI / eLicznik data flows.

			- UNSTPB (Romania): National hub access to campus backend.
Interface E6	- Retail and wholesale price signals for customers. - Dynamic tariffs and time-of-use price trajectories. - Market-linked alerts and offers visible in the app.	- Energy markets, retailers and price APIs. - Energy app backend ingestion services.	- TAURON Dystrybucja (Poland): Tariff comparisons and messages in eLicznik. - E-REDES (Portugal): Tariff and price information in Balcão Digital. - i-DE Iberdrola (Spain): Smart-charging price signals. - CheckWatt (Sweden): Price-driven views for PV/battery operations. - FHOOE (Austria): Campus app and marketplace using market price signals.
Interface E7	- Service descriptors, eligibility rules and pricing from Service Marketplace. - Service offers, SLAs and acceptance status for end-users. - Feedback on service usage from apps.	- Service Marketplace platform. - Energy app backend integration services.	- FHOOE (Austria): Campus Service Marketplace integrated with customer-facing apps.
Interface E8	- Data product descriptors and schemas from Data Marketplace. - Access conditions, licences and pricing. - Usage logs for data products consumed by apps.	- Data Marketplace platform. - Energy app backend and analytics modules.	- FHOOE (Austria): Campus Data Marketplace exposing datasets to apps and services.
Interface E9	- Flexibility offers, rewards and event summaries to users.	- Flex Service Platform notification APIs.	- VOLTALIS (France): MyVoltalis messaging about flex events.

	- Notifications about upcoming flex events and results. - Customer participation status and preferences.	- Energy app backend connectors.	- D4G (France, EE, FI, DK, BE): Flex participation information for replicated demos. - i-DE Iberdrola (Spain): Smart-charging event notifications. - CheckWatt (Sweden): Flexibility offers and results to customers. - E-REDES (Portugal): Local flexibility and demand response messages. - HOPS (Croatia): Demand reduction information to users. - Mytilineos (Greece): ACCEPT/Citizen app flex-related messages. - TSOC + CINTECH (Cyprus): App messages linked to flex services.
Interface F1	- Consent tokens and metering point identifiers (MPxN). - Read schedules, near-real-time or 15-minute load curves. - Power-quality and outage event flags. - Adapter normalisation logs and data-quality KPIs.	- Smart-meter adapter service (MDMS connector). - DSO MDMS / data hubs via EDDIE/AIIDA. - Aggregator / DER Aggregation Platform data bus.	- VOLTALIS (France): Adapter-based reads supporting portfolio control. - D4G (France): EDDIE-aligned meter access for baselines. - CheckWatt (Sweden): Smart-meter streams into VPP / IoT platform. - Elektro Ljubljana (Slovenia): MDMS to adapter paths feeding apps. - E-REDES (Portugal): MDMS data to adapters for consumer services.

			- FHOOE (Austria): AIIDA adapters to P1 / data-hub providers. - CEZ Distribuce (Czech Republic): DIP / data-hub adapter access. - TAURON Dystrybucja (Poland): AMI to adapter data flows. - HOPS (Croatia): Metering feeds toward platform analytics. - UNSTPB (Romania): National data access via adapters.
Interface F2	- Raw interval reads and register values from meters. - Power-quality events and outage logs. - Firmware / communication status and meter diagnostics.	- AMI meters and concentrators. - DSO MDMS collection services.	- VOLTALIS (France): AMI reads for validation of DR actions. - D4G (France): AMI / adapter integration to support baselines. - CheckWatt (Sweden): AMI data ingested to IoT / VPP platform. - Elektro Ljubljana (Slovenia): AMI to MDMS chain for consumer analytics. - E-REDES (Portugal): AMI fleet data to MDMS. - FHOOE (Austria): adapter patterns for AMI access. - CEZ Distribuce (Czech Republic): AMI into DIP / hub. - TAURON Dystrybucja (Poland): AMI raw and validated reads.

			- Croatian pilot stakeholders (Croatia): AMI signals for awareness modules. - UNSTPB / national hub (Romania): AMI to national hub paths.
Interface F3	- Set-points, on/off commands and duty-cycle schedules for loads. - Room / zone temperature and occupancy telemetry. - Comfort bounds, opt-out logs and compliance KPIs.	- Site EMS / gateway APIs (MQTT, REST). - Smart thermostat / switch device APIs. - Home IoT hubs.	- VOLTALIS (France): Heater and appliance control via smartbox. - D4G (France): EMS control of thermostatic loads in Home Energy Station / digital-twin setups. - Mytilineos (Greece, Aspra Spitia): HVAC switching via EMS / IoT equipment. - FHOOE (Austria): EMS to device orchestration in demo homes.
Interface F4	- PV generation telemetry and forecasts. - Inverter curtailment and power-factor set-points. - Self-consumption optimization metrics.	- EMS to inverter APIs (Modbus, REST). - PV inverter telemetry feeds.	- D4G (France): PV control via EMS / Home Energy Station. - VOLTALIS (France): PV awareness in portfolio optimization. - Mytilineos (Greece, Aspra Spitia): Rooftop PV integrated with home EMS and Solarweb app. - CheckWatt (Sweden): PV telemetry within IoT / VPP platform. - FHOOE (Austria): PV data into EMS and campus app services.
Interface F5	- EV charging schedules and current limits.	- EMS orchestration to EV EMS.	- D4G (France): EMS schedules for V1G / V2X where applicable.

	- Price / tariff inputs and grid-constraint flags. - Driver preferences, departure times and state-of-charge targets. - Activation logs and acknowledgements.	- Price / tariff feeds and grid signals. - Site telemetry (SoC, charging power).	- VOLTALIS (France): Portfolio-aware EV control signals. - i-DE Iberdrola with CPO (Spain): Smart-charging EMS chain via retailer / CPO. - Mytilineos (Greece, Aspra Spitia): EV charging integrated with home EMS and Wallbox app. - FHOOE (Austria): EMS to EV optimization in demo setups.
Interface F5.1	- Charger start/stop and current set-points. - OCPP / IEC 61851 control messages. - ISO 15118 session parameters and status. - Session metering data.	- EV EMS to EVSE controller. - OCPP, IEC 61851, ISO 15118 interfaces. - EVSE metering.	- D4G (France): EVSE actuation from EV EMS. - i-DE Iberdrola with CPO (Spain): EVSE control for smart charging / V2G pilot CPs. - Mytilineos (Greece, Aspra Spitia): Wallbox control and session data. - FHOOE (Austria): EVSE sessions in pilot homes.
Interface F6	- Device discovery, capabilities and grouping. - Demand response scenes and orchestration rules. - Gateway telemetry, logs and firmware status.	- EMS orchestration APIs. - Home energy gateway (smartbox, hub, Raspberry-Pi).	- VOLTALIS (France): Smartbox as domestic control gateway. - Mytilineos (Greece): Raspberry-Pi / IoT hub as EMS gateway. - FHOOE (Austria): Home gateways linked to EMS and apps.
Interface F6.1	- Per-appliance telemetry (power, state). - Control commands (on/off, set-point).	- Gateway device APIs (MQTT, REST). - Appliance smart-plug / relay interfaces.	- VOLTALIS (France): Appliance shedding via smartbox. - Mytilineos (Greece): Shelly / Intesis device control through hub.

	- Safety / lockout states and user overrides.		- FHOOE (Austria): Appliance orchestration via gateway.
Interface F7	- Charge / discharge schedules and limits for domestic batteries. - State-of-charge, temperature and cycle metrics. - Arbitrage / peak-shaving set-points. - Response telemetry for verification.	- EMS to ESS EMS APIs. - BMS telemetry and inverter data.	- D4G (France): Home Energy Station battery control from EMS. - CheckWatt (Sweden): ESS EMS scheduling within VPP. - Mytilineos (Greece, Aspra Spitia): Domestic battery control via EMS with 5-minute PV/battery data.
Interface F7.1	- Inverter power commands and SoC targets. - BMS telemetry (voltage, current, temperature). - Charge / discharge session metering.	- ESS EMS to inverter / BMS. - Battery system APIs.	- D4G / TRIALOG (France): Home Energy Station battery actuation. - CheckWatt (Sweden): Home battery control for FCR/FFR and arbitrage. - Mytilineos (Greece): Domestic battery BMS integration.
Interface F8	- Metering point IDs, consents and load curves requested by Flex Service Platform. - Baseline and flexibility estimation inputs from smart-meter data. - Quality flags and missing-data indicators.	- Flex Service Platform meter-data connectors. - Smart-meter adapter services. - DSO MDMS / hubs providing the underlying data.	- VOLTALIS + D4G (France): Meter-driven baselines for residential flex. - CheckWatt (Sweden): AMI-driven VPP baselines. - i-DE / SIORD (Spain): Meter-based inputs to smart-charging flex. - E-REDES (Portugal): DSO AMI data supporting local flex. - HOPS (Croatia): Metering inputs for demand reduction modules.

			FHOOE (Austria), CEZ (Czech Republic), TAURON (Poland): Smart-meter data pulled via adapters for flex analytics.
Interface G1	- Validated consumption histories and MP identifiers used for flex baselines. - Consent receipts, scopes and validity periods. - Anonymised aggregates for offers and settlement.	- National smart-meter data hubs (HVD). - EDDIE / AIIDA connectors. - Flex Service Platform import pipelines.	- VOLTALIS + D4G (France): Hub data feeding flexibility baselines. - D4G (replication EE, FI, DK, BE): EDDIE-aligned / simulated hub access. - FHOOE (Austria): EDDIE / AIIDA connectors to hubs. - Elektro Ljubljana (Slovenia): MDMS / hub feeds for analytics. - E-REDES (Portugal): DSO hub data to backends. - CEZ (Czech Republic): DIP / hub access. - TAURON (Poland): AMI / hub to backend. - UNSTPB (Romania): National data-hub access.
Interface G2	- MDMS-to-hub validated load curves and events. - Tariff / billing attributes and meter metadata. - Aggregated LV feeder / transformer statistics.	DSO MDMS and measurement databases. - Member-state data hubs. - EDDIE / AIIDA data-sharing interfaces.	- FHOOE (Austria): MDMS to hub via EDDIE / AIIDA. - Elektro Ljubljana (Slovenia): MDMS to hub sharing for apps. - E-REDES (Portugal): MDMS to hub data for consumer services and grid operations.

			- CEZ (Czech Republic): MDMS to DIP / hub exports. - TAURON (Poland): MDMS to hub feeds for AMI users. - UNSTPB (Romania): MDMS to national hub. - D4G (France): MDMS to hub data consumed through EDDIE alignment.
Interface G3	- Aggregated consumption profiles and forecasts used by markets. - Tariff structures and regulated price components. - Historical statistics from hubs supporting market design / products.	- Energy market platforms and regulatory data systems. - National hubs and MDMS as historical data providers.	- France, Estonia, Finland, Denmark, Belgium, Austria via national market actors using hub data; interface is mainly conceptual from markets to HVD infrastructures.
Interface H1	- Data product catalogues for in-house energy data (P1, in-home data). - Metadata about schemas, frequency, access rights and pricing. - Usage logs for data products consumed via the bridge.	- Data Marketplace backend. - AIIDA "Bridge for in-house energy data access".	- FHOOE (Austria): AIIDA-based Data Marketplace exposing in-house energy data products.
Interface H2	- Service descriptions, eligibility, pricing and SLAs for services using in-house data. - Customer subscriptions and usage statistics.	- Service Marketplace backend. - AIIDA bridge exposing service endpoints.	- FHOOE (Austria): Service Marketplace for AIIDA-based applications.

Interface H3	- Requests from Marketplace App for in-house data and services. - User consents, scopes and time ranges. - Returned datasets and service results.	- Marketplace App frontends. - AIIDA bridge APIs.	- FHOOE (Austria): Marketplace App used by end-customers to access AIIDA-based data and services.
Interface H4	- Service search, selection and subscription from Marketplace App. - Presentation of service status and results to users.	- Marketplace App. - Service Marketplace APIs.	- FHOOE (Austria): Linkage between Marketplace App and Service Marketplace.
Interface H5	- Data product search and purchase flows. - Download or API access endpoints for selected data products.	- Marketplace App. - Data Marketplace APIs.	- FHOOE (Austria): Linkage between Marketplace App and Data Marketplace.
Interface H6	- In-house data requests from bridge to EMS (load, PV, storage, EV). - Control capabilities and discovery of controllable resources. - Returned measurements and states.	- AIIDA Bridge for in-house energy data access. - Home / site EMS.	- FHOOE (Austria): EMS integration in homes via AIIDA bridge.
Interface H7	- In-house data and control commands between bridge and Energy Management Gateway. - Per-device telemetry and actuation requests.	- AIIDA Bridge. - Energy Management Gateway in homes.	- FHOOE (Austria): Gateway-level integration of in-house devices via AIIDA.
Interface H8	- Backend requests to AIIDA bridge for in-house energy data.	- Energy App Backend.	- FHOOE (Austria): Campus Energy App

	- Returned datasets for analytics and HLUC services in apps.	- AIIDA Bridge for in-house energy data access.	Backend consuming AIIDA data for all HLUCs.

3.2.3. CATEGORIZATION OF DATA

To better understand the nature and purpose of the information exchanged across the defined interfaces, the identified data have been organised into distinct categories according to their use within the project. Table 4 (Characterization of Data for Each Interface) summarises this classification, distinguishing four complementary data types:

- Identification Data - describing the assets or entities involved
- Technical Data - defining the system configurations and specifications
- Operational Data - capturing real-time or historical system behaviour
- Training Data - supporting the development of predictive models and analytical tools.

This categorisation ensures a consistent interpretation of data flows and highlights their role in enabling monitoring, optimisation, and learning processes across the ECLIPSE DIGITAL pilots.

Table 4: Characterization of Data for Each Interface

Interface Name	**Identification Data**	**Technical Data**	**Operational Data**	**Training Data**
Interface A1	- Market participant IDs (EIC, BRP/BSP IDs)	- Market API message schemas and versions	- Day-ahead / intraday / balancing bids and offers	- Historical prices, activations and imbalance data

	- TSO control-area and bidding-zone identifiers - Balancing product IDs and codes (FCR, aFRR, etc.) - Portfolio and balancing group IDs - Bid, activation and settlement record IDs	- Time stamps, time zone and product time windows - Security artifacts (certificates, API keys, OAuth/OIDC tokens) - Supported market time resolutions and gate-closure constraints - Transport protocols and retry / error-handling policies	(volume, price, product) - TSO flexibility needs and activation requests - Dispatch results, opt-outs and penalties - Delivered energy and imbalance correction data - Settlement results and reconciliation records	- Historical portfolio response curves and availability patterns - Features for balancing product forecasting (weather, calendar, system state) - KPIs for bidding strategy optimization and risk management
Interface A2	- DSO identifiers and grid-area / feeder IDs - Local flexibility product and tariff IDs - Location identifiers for constraint zones - Contract IDs for local flexibility services	- API specifications for local flex or capacity markets - Constraint descriptors (voltage, loading, hosting capacity) - Time-window and granularity definitions for local products - Security and authentication	- Local flexibility needs by feeder or area - Published tenders, offers and acceptance notifications - Post-event measurements used for validation and settlement - DSOs' constraint cases and	- Historical local constraint and mitigation datasets - Flexibility activation effectiveness by location and product - Features linking grid conditions, prices and successful mitigation

		configuration for DSO–market links	mitigation outcomes	- Aggregated statistics to refine local product design and sizing
Interface A3	- Flex Service Platform (FSP) IDs and portfolios - Market product and contract IDs mapped to FSP services - Customer segment or portfolio segment identifiers - Bid and offer identifiers per product	- Market–FSP integration schemas (JSON, XML, CIM profiles) - Scheduling and nomination formats and horizons - Security tokens and access scopes for FSP market access - Update frequencies for prices and accepted schedules	- Price signals and product parameters sent to the FSP - Flexibility offers, nominations and accepted schedules - Event logs for activations, cancellations and penalties - Settlement reports and reward distribution inputs	- Datasets linking prices, products and FSP participation levels - Historical conversion rates from published opportunities to accepted events - Forecasting features for available flexibility versus price and time - KPIs for FSP performance on different market segments
Interface B1	- Control-area codes and balancing product IDs - Aggregator / FSP portfolio IDs and asset group IDs	- TSO messaging schemas and versions - Product time windows and granularity - Security artifacts (API keys, OAuth/OIDC	- TSO flexibility needs and activation requests - Portfolio bids, availability and opt-out logs - Dispatch acknowledgemen	- Historical activations and fleet response curves - Imbalance and price histories per balancing product - Weather and system-state

	- Bid / activation identifiers and timestamps - Metering point IDs where required by product rules	tokens, certificates) - Clock synchronization and time-zone conventions	ts and delivered energy - Baselines, deviations and settlement artifacts	features used in flex forecasting - Performance statistics for different portfolios and technologies
Interface B2	- Feeder, transformer and location IDs- DSO product and constraint identifiers - Aggregator / FSP portfolio and device-cluster IDs - Consent references where applicable	- Constraint descriptors (voltage, thermal limits, congestion zones) - Curtailment window definitions and ramp-rate limits - API and protocol specifications with QoS / latency targets - Data-quality flags and retention policies	- Local flexibility needs by area or feeder - Activation orders and acknowledgements - Verification metering and compliance KPIs - Post-event validation packages for settlement support	- LV / MV load profiles and grid state features - Event outcome logs for tuning flex products - Seasonal and behavioural features for predictability of response - Historical datasets linking constraints and mitigation success
Interface B3	- Metering point identifiers (national and DSO IDs) - Customer account references (pseudonymised)	- MDMS and data-hub schemas and quality flags - Validation, estimation and editing status codes - File / API formats (CIM,	- Validated load curves and events - Power-quality and outage indicators - Tariff and billing attributes used downstream	- Long-horizon consumption histories for baselines - Aggregated statistics for benchmarking and tariff analysis

	- Supplier / contract IDs and consent tokens	JSON, CSV) and sampling intervals	- LV / MV aggregates for analysis	- Feature sets for anomaly / fraud detection - Data-quality trend metrics for model robustness
Interface B4	- ESS asset IDs and connection points - BMS / EMS serials and firmware IDs - Feeder or zone identifiers for dispatch	- SoC, temperature, voltage telemetry channel definitions - Charge / discharge limits and safety states - Control payload formats and schedule granularity	- DSO charge / discharge requests and set-points - Acknowledgements and measured response- Cycle counts, throughput and verification logs	- Battery efficiency and aging characteristics versus duty cycle - Response-time distributions versus requested services - Price and load features for dispatch optimization
Interface B5	- Site and DER EMS IDs and device-group IDs - Feeder or node location references - Contracted product or participation IDs	- DER capability descriptors (rated power, duty cycles) - Smart-charging / curtailment command schemas - Communication protocol metadata and QoS targets	- DSO smart-charging or load-shift requests - Execution logs, compliance indicators and opt-outs - Measurement evidence used for validation and settlement	- Learned response to DSO requests per device type - Time-of-day and price-sensitivity features - Comfort-constraint models where applicable

Interface B6	- Meter serial numbers and metering point IDs - Installation metadata (coarse address or feeder) - Device firmware and model identifiers	- AMI sampling intervals and channel definitions - Event codes for outage, power quality and tamper - Communication quality statistics and retry patterns	- Raw and validated reads and load curves - Power-quality indices and outage logs - Near-real-time streams for analytics where available	- Household and building consumption pattern histories - Seasonal and weather-linked feature sets - Baseline and forecasting training datasets
Interface B7	- Mapping keys between feeders/substations and meter groups - SCADA point IDs for aggregated loads - Historian tag names and mapping tables	- MDMS-to-SCADA integration specifications and timing - Alignment rules for 15-minute MDMS data with SCADA seconds - Historian schemas and retention periods	- Aggregated demand series imported into SCADA / EMS - Alarm and event correlation datasets - Situational-awareness dashboards and export feeds	- Event libraries for predictive alerts and restoration support - Feature sets for anomaly detection and grid-state estimation - Datasets for tuning restoration and reconfiguration strategies
Interface B8	- Line and circuit identifiers, bay references - RTU and IED point lists and tag IDs	- SCADA telemetry sampling rates and scale factors - Topology models and	- Real-time line flows, voltages and breaker states - Switching plans, outage and restoration logs	- Line-loading patterns and contingency-case datasets - Weather and storm features for risk modelling

	- Topology identifiers and connectivity references	network parameters - Switching procedure templates and constraints	- Alarm streams and acknowledgements	- Post-event datasets for restoration optimization
Interface B9	- Substation, busbar and feeder IDs - IED and relay identifiers and function codes - IEC 61850 logical-node and data-model identifiers	- GOOSE and Sampled Values mapping - SCADA and EMS historian configurations - Protection and automation parameter sets	- Topology and feeder states and tap positions - VAR set-points, protection and alarm logs - Maintenance and inspection annotations	- Substation event libraries (faults, misoperations) - Predictive-maintenance feature sets - Tap and VAR optimization training datasets
Interface C1	- FSP organization IDs and portfolio IDs - DER aggregation cluster and device-group IDs (pseudonymised) - Dispatch job IDs and orchestration IDs - Consent references for using device-level data	- Southbound and northbound MQTT / REST topic structures - Message QoS, retries and time -synchronization rules- Security artifacts (OAuth tokens, API keys, certificates) - Mappings between FSP products and DER aggregation services	- Live portfolio telemetry and forecasts per cluster - Availability and opt-out states, flex baselines - Dispatch queues, ACK / NACK and error logs - Cluster-level compliance KPIs and incident records	- Historical dispatch versus response curves per cluster - Forecasting features (weather, tariffs, calendar, grid signals) - Predictability metrics and segmentation by device type or region - Datasets for improving aggregation

				strategies and portfolio design
Interface C2	- Site IDs and EMS IDs - Device inventory and capability catalogues per EMS - Pseudonymous user / contract linkage where needed	- EMS control payloads and schedule granularity - Gateway and protocol metadata (Modbus, REST, MQTT, fieldbus) - Safety and comfort constraint models per site	- Site schedules, set-points and acknowledgements - Opt-in / opt-out events and failover actions - Telemetry streams confirming compliance and device status	- Site response curves per device class - Comfort-preservation and rebound features - Data to tune local orchestration rules and constraints
Interface D1	- DER EMS IDs and device-group IDs - Connection-point and location references - Contracted product IDs and participation records	- Command schemas (power, duty cycle, ramps, set-points) - Schedule resolution and horizon parameters - Protocol metadata for EMS gateways	- Set-points and schedules issued by the FSP - ACK / NACK, compliance logs and opt-outs - Measurement evidence for validation and settlement	- Device-type response distributions vs. requested actions - Time-of-day and price-sensitivity features - Datasets for tuning FSP control strategies
Interface D2	- Device IDs (thermostats, EVSE, inverters, HVAC, etc.) - EMS–device binding IDs	- Channel definitions (power, temperature, SoC, state) - Protocols (e.g. IEC 61851, inverter	- Device telemetry and status updates - Commands (on/off, set-points, charging rates, curtailment)	- Per device behavioural models - Efficiency and comfort trade-off datasets

	- Safety and comfort policy identifiers	APIs, proprietary IoT) - Event and alert code lists	- Local constraint-enforcement logs and overrides	- Usage and response histories for different device classes
Interface D3	- ESS and EMS asset IDs and metering points - BMS serials and firmware IDs - Product and contract IDs for storage services	- SoC, voltage, temperature channels and limits - Dispatch payload formats and schedule horizons - Communication and security parameters with ESS EMS	- Charge and discharge schedules and acknowledgements - Metered response and cycle counts - Settlement, verification and exception records	- Efficiency and aging characteristics vs. schedule patterns - Response latency and accuracy versus requested power - Training sets for storage control and revenue optimization
Interface D4	- Battery pack and inverter serials - Protection-profile identifiers - BMS and inverter parameter sets	- Sampling intervals, scaling factors and telemetry mappings - Thermal-management and protection configuration - Command formats for power and SoC set-points	- Real-time power and SoC logs - Faults, alarms and protection trips - Charge/discharge execution traces	- State-of-health estimation datasets - Cycle-life and degradation features - Behaviour under different operating regimes and temperatures
Interface E1	- User and account IDs, consent tokens	- Notification payload schemas for HLUC 1-5	- Sent and received HLUC messages (economic, non-	- Personalization features based on usage patterns and preferences

	- App and device IDs, locale and profile - Pseudonymous links to metering points where applicable	- Channel metadata (push, email, in-app, SMS) - Data minimization and retention tags	economic, efficiency, alerts, tips) - App engagement and interaction metrics - A/B-test variants and outcomes	- Message effectiveness and churn models - Segment-level response to different message types
Interface E2	- Site IDs, EMS IDs and homeowner consent references - App–site linkage IDs - Automation and control policy identifiers	- Control and automation API descriptors - Alert schemas and safety constraint models - Authentication tokens and rate limits	- Control intents and executed actions from app to EMS - Critical grid alerts and user overrides - Compliance and feedback telemetry	- Automation success/failure datasets - User-comfort preference learning - Feature sets for refining automation rules
Interface E3	- DER EMS IDs and device-group identifiers - User preference profiles and service IDs - Contract IDs for DER-based services	- Command schemas (EV charging rate, HVAC set-point, PV curtailment) - Capability descriptors for each DER type - API and security configuration for DER EMS	- DER control messages and acknowledgements - Preference changes and exceptions - Telemetry used for validation of actions	- Preference and adherence models - Device-specific response datasets - Training data for user-centric optimization of DER control
Interface E4	- ESS / EMS IDs and site linkage	- Optimizations outputs (price	- Battery charge / discharge plans	- Arbitrage and FFR feature sets

	- Consent and policy identifiers for storage control - Optimizations-run IDs and schedule IDs	thresholds, schedules) and API schemas - ESS EMS / BMS integration parameters - Security and rate-limit settings	sent from backend - Execution acknowledgements and performance logs - KPIs for arbitrage and flexibility events	- Battery performance vs. schedule outcome datasets - Data for tuning algorithms and user strategies
Interface E5	- Metering point identifiers (national / DSO) - Consent tokens and access scopes - Application client IDs for hub access	- Data-hub and MDMS schemas and quality flags - Validation, estimation and status fields - Sampling intervals and file / API formats	- Validated load curves and events delivered to backend - Tariff and billing attributes and aggregates - Delivery latency and data-quality logs	- Baseline and forecast training corpora per customer cohort - Segmentation and benchmarking features for HLUC 1–3 and 5 - Data-quality features for model selection and monitoring
Interface E6	- Market area IDs and price-zone IDs - Tariff and product identifiers referenced by the app - Retail contract IDs linked	- Market and tariff API schemas (JSON/CSV/XML) - Update periods (real-time, hourly, daily) and time zones - Security configuration for	- Time series of wholesale and retail prices - Dynamic tariff tables and contract options - Event-based signals (high-price alerts, low-price windows)	- Historical prices and tariff changes - Datasets linking user reactions to different price patterns - Features for tariff recommendation and price-

	(pseudonymously) to users	backend access to price feeds	consumed by backend	response prediction
Interface E7	- Service IDs, versions and provider IDs - Customer / account IDs for subscribed services - SLA and contract identifiers	- Service catalogue schemas and API descriptors - Authentication and authorisation rules for service access - Data schemas for service usage statistics	- Service offers presented to users - Subscription, activation and cancellation events - Usage metrics and service outcome logs	- Adoption and churn datasets by service type - Features for recommending services per user segment - Performance statistics for services using energy data
Interface E8	- Dataset IDs, catalogue IDs and licence identifiers - Tenant or application IDs consuming datasets - Access-grant records for each dataset	- Data-product schemas, formats and access endpoints - Metadata about frequency, coverage and quality - Security and accounting configuration	- Dataset downloads or streaming access from backend - Query logs and data-usage statistics - Licensing and quota-consumption records	- Information on which datasets improve models - Benchmark results for different data sources - Feedback for curating and pricing data products
Interface E9	- FSP IDs and portfolio/segment IDs - Campaign or event IDs for flexibility actions - User cohort IDs for notifications	- Event and notification payload schemas - API descriptors for events, rewards and status updates	- Upcoming flex-event invitations and parameters - Results of events (participation, delivered savings, rewards)	- Behavioural datasets linking incentives and user response - Features for targeting flex offers and predicting participation

		- Security configuration between FSP and backend	- User-level or segment-level participation logs	- KPIs for effectiveness of flex campaigns
Interface F1	- Adapter IDs and portfolio / cluster IDs - Metering point identifiers linked via consent - Data-access scope and token references	- Adapter API schemas (pull/push) and sampling intervals - Security and authentication (API keys, OAuth, QoS policies) - Mapping of meter channels to portfolio entities	- Interval reads, instantaneous power and voltage, PQ events- Data -latency and quality logs, completeness flags - Availability / opt-out states used for validation and settlement	- Historical load curves for baselines and forecasts - Segment features (weekday/season patterns) - Anomaly and elasticity signatures for HLUC 1–3
Interface F2	- Meter serials and metering point IDs - HAN/WAN link identifiers	- AMI protocol metadata (DLMS/COSEM, OBIS mapping, etc.) - Sampling and granularity settings, clock sync, firmware and version info	- 15-minute / hourly reads, demand peaks, outage and tamper alarms - Voltage and power-factor where available; event logs	- Long-run profiles for forecasting and benchmarking - VEE histories (validation, estimation, editing) for robustness
Interface F3	- Device IDs, zone / room tags, thermostat model IDs - User comfort profiles (pseudonymised)	- Control schemas (set-point, mode, schedule) - Protocols (Zigbee, Z-Wave, Wi-Fi, MQTT), rate limits	- Temperature, humidity, run-time, on/off cycles - Command acknowledgements, overrides and exception logs	- Thermal response curves and occupancy patterns - Comfort vs. energy trade-off

		- Safety constraints (min/max temperature, duty cycle)		datasets for optimization
Interface F4	- Inverter and array IDs, MPPT / string IDs - Site and metering point linkage IDs	- Inverter APIs and telemetry channels (DC/AC power, voltages, currents) - Export-limit and ramp configuration, curtailment commands	- Real-time PV generation, curtailment events, alarms and faults - Import/export balances at the site level	- PV performance history (performance ratio) - Weather-aligned training sets and irradiance features - Feature stores for PV forecasting
Interface F5	- EVSE and EV EMS IDs, connector IDs - Contract or CPO site references - Pseudonymous vehicle or driver identifiers where used	- ISO 15118 and IEC 61851 parameters and charger capabilities - Schedule resolution and max current / voltage limits - EMS–EV EMS communication schemas	- Session start/stop, requested vs delivered power, SoC (if shared) - Smart-charging set-points, demand response compliance logs	- Charging-behaviour models (arrival times, initial SoC) - Price and constraint sensitivity features for scheduling
Interface F5.1	- EVSE serials, connector IDs and firmware IDs	- Pilot/PWM control parameters and min/max current settings	- Instantaneous current, voltage and energy/session counters	- Hardware reliability and failure-rate datasets

		- Error and diagnostic code lists	- Plug/unplug, error and fault events	- Response latency and tracking-accuracy statistics
Interface F6	- Gateway IDs and device-enrolment IDs - Site / household pseudonymous IDs	- Supported protocol inventory and firmware versions - Topology descriptors (scenes, groups) and QoS parameters	- Orchestration workflows and automation triggers - Latency and failure logs, device reachability information	- Automation success metrics and rebound effects - Optimal sequencing strategies across devices
Interface F6.1	- Appliance IDs, type/category and vendor/model	- Command schemas (on/off, levels, modes) and safety flags - Communication technologies (IR, RF, IP, PLC)	- Usage cycles and per-appliance energy time series - Command acknowledgements, timeouts and retry statistics	- Appliance usage patterns for NILM and shiftability - Savings potential per category and device
Interface F7	- Battery system, EMS and inverter IDs- Metering point linkage where relevant	- BMS channels (SoC, SoH, temperature) and limits - Efficiency and reserve settings - EMS-Battery EMS API descriptors	- Executed schedules, SoC traces and cycle counts - Alarms, faults and protection events	- Degradation and aging models vs. duty cycles - Response latency and round-trip efficiency datasets
Interface F7.1	- Battery pack, BMS and inverter serials	- Cell and block telemetry, thermal sensors and balancing data	- Charge/discharge execution logs, faults and protections	- Cycle-life and thermal behaviour histories

	- String and module identifiers	- Command frames for power and SoC set-points	- Balancing activity and SoH estimates	- Feature sets for predictive maintenance
Interface F8	- FSP portfolio and cluster IDs linked to meters - Metering point identifiers and consent IDs - Data-access scope and session IDs	- Integration schemas between FSP and adapter (pull schedules, push streams) - Sampling and aggregation options exposed to FSP - Security configuration and throttling rules	- Requested meter data extracts for baselines and settlement - Returned load curves, flags and quality indicators - Error, retry and fallback logs	- Baseline and flex-potential datasets per segment - Training corpora linking meter patterns and flex performance - Data-quality metrics used in model selection
Interface G1	- National metering point identifiers (pseudonymised to portfolios) - Data-access consents and scopes - Client / application IDs for hub access	- Data-hub API schemas and file formats - Sampling windows, time zones and VEE flags - Security and rate-limit policies	- Delivered datasets (validated histories) and completeness indicators- Error and retry logs, quality reports - Aggregation jobs and export manifests	- Baseline and forecast corpora per customer cohort - Segmentation and benchmarking features for HLUC 1, 2, 3 and 5 - Data-quality features for model selection and monitoring
Interface G2	- Meter IDs, metering point	- MDMS schemas (OBIS mapping, quality codes)	- Validated load curves and events	- Long-horizon historical profiles

	numbers and supplier/DSO IDs - Consent references and retention policies	- Validation, estimation and editing status and methods - Transport parameters for file/API exchanges	and tariff/billing attributes - PQ and outage events where exposed - Delivery SLAs and data-quality reports	for efficiency analytics - Tariff-aligned behavioural feature sets - Aggregated feeder/transformer statistics for non-personal analysis
Interface G3	- Market area and data-hub operator identifiers - Dataset and reporting IDs for regulatory products - Aggregation-scope identifiers (zone, tariff class, segment)	- Schemas for aggregated, anonymised market-support datasets - Time resolution, publication frequency and quality flags - Security and privacy constraints for hub–market exchanges	- Aggregated consumption, generation and flexibility indicators by zone - Historical series used for market monitoring and design - Data deliveries for regulatory and transparency obligations	- Datasets aligning aggregated load and price formation - Features for market-design studies and product sizing - Long-term statistics for policy and regulatory analysis
Interface H1	- Data-product IDs and catalogue IDs - AIIDA connector IDs and in-house data-source IDs	- Dataset schemas and descriptors (P1, in-home IoT, EMS data) - Access methods and endpoints exposed via the bridge	- Publication of in-house data products to the marketplace - Access and download logs per product	- Usage statistics for different in-house datasets - Feedback on dataset usefulness for apps and services

	- Licence and access-grant identifiers	- Security, anonymization and consent-enforcement configuration	- Error and throttling logs for data delivery	- Inputs for improving data catalogues and pricing
Interface H2	- Service IDs, provider IDs and version IDs - Linkage between services and required in-house data types - Subscription and SLA identifiers	- Service invocation schemas and parameter descriptors - Technical dependency mappings to AIIDA bridge capabilities - Security and authorisation settings	- Service execution requests routed via the bridge - Execution outcomes, performance metrics and error logs - Usage statistics per service and segment	- Adoption and churn datasets for services using in-house data - Performance metrics to refine service definitions - Input for recommending services based on household profiles
Interface H3	- App user IDs and session IDs - Selected data products and scopes per request - Consent references tied to in-house data	- Front-end to bridge API schemas - Request/response formats for data exploration - Rate limits and error-handling behaviour	- On-demand queries for in-house data via the app - Logs of user interactions with data views - Feedback and error reports from app usage	- Behavioural datasets showing which data views are most useful - Features for UX optimization and data-product design - Statistics on consent usage and revocation patterns
Interface H4	- Service IDs and categories	- Catalogue browsing and	- Browsing events, service	- Datasets for recommending

	- App user IDs and subscription IDs - Rating and review identifiers	service-selection API schemas - Order, subscription and payment message formats - Authentication/authorisation between app and marketplace	selections and purchases - Subscription lifecycle events (activation, renewal, cancellation) - Ratings, reviews and support interactions	services per user profile - KPIs for service popularity and satisfaction - Evidence for refining service bundles and UI flows
Interface H5	- Data-product IDs and categories - App user IDs and project/workspace IDs - Licence acceptance records	- Search and discovery API schemas - Ordering, download and streaming endpoints - Metadata and preview mechanisms	- Searches, filters and product selections - Dataset purchase / subscription and download events - Error and timeout logs	- Analytics on which data products are used in practice - Features to improve search, ranking and recommendation - KPIs for data-product quality and coverage
Interface H6	- EMS IDs and site IDs connected to AIIDA - Internal resource IDs (PV, battery, HVAC, EV) exposed to bridge	- EMS northbound API schemas used by AIIDA - Resource capability descriptors and telemetry channels	- Continuous or on-demand telemetry from EMS to bridge - Event-driven updates (state changes, alarms) - Control-capability	- Datasets describing EMS capabilities and typical behaviour - Features for matchmaking between EMS resources and services

		- Security configuration and authentication between bridge and EMS	discovery for services	- Statistics on data freshness and quality from EMS
Interface H7	- Gateway IDs and household/site IDs - Device-group or room identifiers exposed through gateway	- Gateway API schemas and supported protocols via bridge - Device capability and topology descriptors - Security, pairing and authorisation parameters	- Telemetry and control flows between bridge and gateways - Logs of device discovery, status changes and command results - Failure and retry statistics	- Behavioural datasets for gateway-level orchestration patterns - Metrics to optimise polling and control frequencies - Input to refine abstraction models in the bridge
Interface H8	- Backend client IDs and application IDs - Data-access scopes and consent references per user - Request IDs for data pulls and subscriptions	- API schemas used by backend to query AIIDA - Query language or filter formats for in-house data - Security configuration, throttling and pagination rules	- Data requests from backend to bridge (historical and live) - Returned datasets used to power HLUC services in apps - Error, latency and completeness logs	- Corpora of in-house measurements used in app analytics - Feature sets for energy advice, anomaly detection and forecasting - Statistics feeding decisions on caching and pre-computation

3.3. DATA CATALOGUE

The development of the data catalogue in the ECLIPSE DIGITAL project is a key task under Task T3.1 “Specifications of suitable data sets and digital environment”. Its purpose is to provide a common way to describe and organize the data used across the pilots so that CERF components and energy applications, including mobile apps, can easily find, understand, and access the relevant datasets. In Task T3.1, a common set of criteria for catalogue preparation has been defined, and a set of standards has been selected on the basis of these criteria. These standards are used to identify and shortlist open-source tools for data catalogue preparation. The shortlisted tools are then compared against the criteria and based on this comparative evaluation, a recommendation is formulated on which tool or combination of tools is most suitable for preparing the data catalogues in the ECLIPSE DIGITAL project. This recommendation will be used in Work Package WP4 “Design and development of CERF and APIs”, in particular Task T4.2 “Development of the CERF for consumer applications based on Machine learning tools and IA”, where the selected open-source tools will be integrated into CERF and the data connectors. It will also be used in Work Package WP5 “Preparation, coordination and monitoring of deployment and demonstration activities”, in particular Task T5.1 “Integration, deployment and adaptation activities”, where each pilot will apply this common approach in its local architecture while remaining aligned with the ECLIPSE DIGITAL data catalogue profile defined in WP3.

.

3.3.1. REQUIREMENTS AND EVALUATION CRITERIA FOR DATA CATALOGUE PREPARATION

In Task T3.1 “Specifications of suitable data sets and digital environment”, a common set of requirements and evaluation criteria is established to support the preparation of data catalogues across the ECLIPSE DIGITAL pilots. Task T3.1 does not implement the catalogues themselves. Instead, it provides guidance for later work by selecting a list of standards against these criteria and by identifying candidate open-source tools for data catalogue preparation that fully or partially implement those standards and meet the requirements, together with a structured description of these tools. These requirements are then used to select relevant standards and to compare open-source tools for data catalogue preparation. The requirements identified for preparing the data catalogue include:

- **Data content** (What the dataset contains)
- **Data types and sources** (Structured, semi-structured, unstructured data and where it comes from)
- **Ownership and governance** (Who owns the data and how it is managed)
- **Access rules** (Who can access the data and under what conditions)
- **Data format and access methods** (File types, APIs, and how to retrieve the data)
- **Data characteristics** (Frequency, granularity, and precision of the data)
- **Interoperability (**Ability to exchange and use data across systems and platforms)

- **Domain relevance** (Suitability for the energy sector and alignment with energy-related use cases)
- **Security and privacy** (Compliance with GDPR and implementation of secure data handling practices)
- **Scalability and flexibility** (Ability to grow, adapt, and include new datasets and data types in the future)
- **Data exchange** (Support for seamless and standardised data sharing)
- **Data versioning** (Capability to track data changes, manage different dataset versions, and ensure consistency over time)
- **Lightweight Data Base which will be applicable for the Mobile Apps.**

These requirements have been derived from the ECLIPSE DIGITAL project Grant Agreement, from WP2 “CERF use cases, requirements and services” and its deliverable D2.2 “Energy services analysis, use cases, and CERF requirements”, from pilot data assessments, and from the overall strategic needs of the project.

3.3.2. STANDARDS SELECTION AND EVALUATION

The requirements described in the previous section are used to select standards that are relevant for data catalogue preparation in the ECLIPSE DIGITAL project. Starting from a broader landscape, a subset of metadata, governance, interoperability and security standards has been retained because each of them fully or partially addresses one or more of the identified criteria. In this section, these standards are grouped into four families and briefly described:

- Metadata Standards

- Data Governance Standards
- Interoperability Standards
- Privacy Security Standards

Figure 34 provides an overview of the reviewed standards for the preparation of a data catalogue.

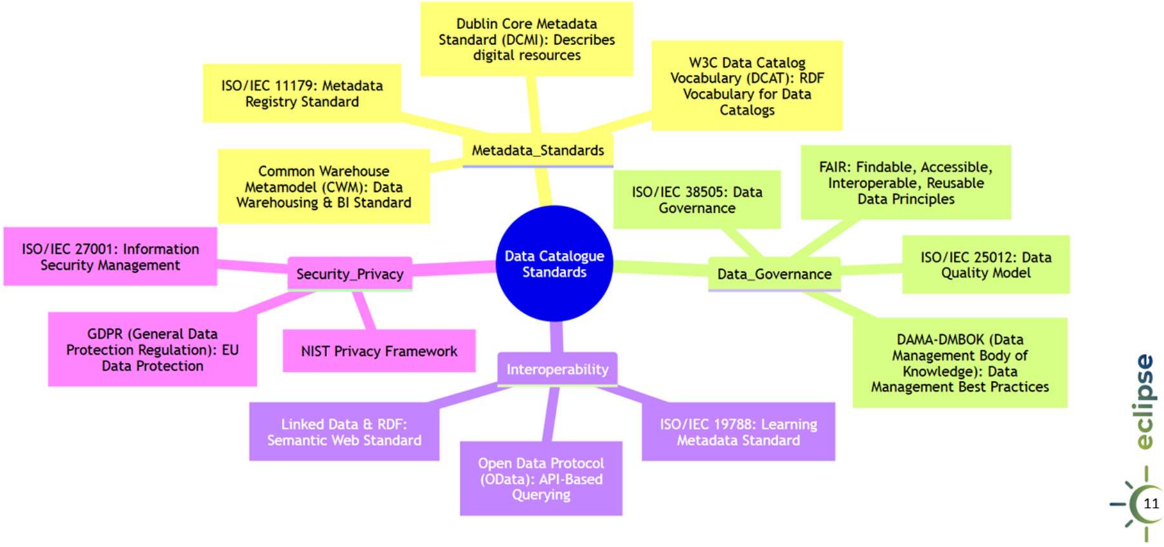


Figure 34: Review of standards for the preparation of a data catalogue

3.3.2.1. METADATA STANDARDS FOR DATA CATALOGUES

Metadata is the core of any data catalogue. These standards help in structuring metadata effectively:

a) Dublin Core Metadata Standard (DCMI) [19]

- A widely used standard for describing digital resources.
- Provides a minimal set of attributes such as Title, Creator, Subject, Description, Publisher, Date, Format, and Identifier.

- Used in libraries, data repositories, and knowledge management systems.

b) ISO/IEC 11179 - Metadata Registry Standard [20]

- Defines a framework for managing metadata.
- Helps in data governance by standardizing how metadata is collected and stored.
- Supports data interoperability across systems.

c) W3C Data Catalogue Vocabulary (DCAT) [21]

- A standard RDF vocabulary used to describe datasets in data catalogues.
- Provides metadata schemas for dataset descriptions, access policies, and distribution information.
- Used by open data portals like data.gov and European Data Portal.

d) Common Warehouse Metamodel (CWM) [22]

- Developed by OMG (Object Management Group).
- Standard for defining metadata for data warehousing and business intelligence.
- Helps in understanding data lineage and transformation history.

3.3.2.2. DATA GOVERNANCE & QUALITY STANDARDS

A well-prepared data catalogue must comply with data governance and quality frameworks:

a) ISO/IEC 38505 - Data Governance

- Defines principles for effective data governance and management.
- Ensures data security, privacy, and compliance with regulations.

b) DAMA-DMBOK (Data Management Body of Knowledge)

- Developed by the Data Management Association (DAMA).

- Provides best practices for data governance, quality, metadata management, and data architecture.
- Helps organizations implement structured data catalogue policies.

c) ISO/IEC 25012 - Data Quality Model

- Defines 15 key data quality characteristics such as accuracy, completeness, consistency, timeliness, and uniqueness.
- Helps in evaluating dataset quality in the catalogue.

d) FAIR Data Principles

- Findable, Accessible, Interoperable, Reusable (FAIR).
- Ensures that datasets in a catalogue are easy to discover, access, integrate, and reuse.
- Used in scientific research, healthcare, and open data platforms.

3.3.2.3. INTEROPERABILITY AND DATA EXCHANGE STANDARDS

A data catalogue should support data exchange between different systems:

a) Open Data Protocol (OData)

- Standard for querying and updating data over HTTP.
- Used in Microsoft, SAP, and Oracle for API-based data catalogue integration.

b) Linked Data & RDF (Resource Description Framework)

- Used for semantic web and knowledge graphs in data catalogues.
- Helps in linking related datasets across organizations.

c) ISO/IEC 19788 – Learning Metadata Standard

- Standard for cataloguing educational datasets.
- Useful in learning management systems and academic data catalogues.

3.3.2.4. SECURITY & PRIVACY STANDARDS

Data catalogues must comply with **security and privacy** regulations:

a) GDPR (General Data Protection Regulation)

- Governs personal data protection in the EU.
- Ensures that data catalogues handle user data securely and comply with privacy laws.

b) ISO/IEC 27001 - Information Security Management

- Provides best practices for data security, encryption, and access control.
- Ensures that sensitive data is protected in the catalogue.

c) NIST Privacy Framework

- Developed by the U.S. National Institute of Standards and Technology (NIST).
- Helps in managing privacy risks associated with data catalogues.

The standards listed in this section are not implemented directly in the ECLIPSE DIGITAL project at this stage. They are used as reference points to guide the selection of open-source catalogue tools.

3.3.3. DATA CATALOGUE TOOLS

3.3.3.1. SELECTION & EVALUATION PROCESS

The selection of candidate open-source data catalogue tools is based directly on the requirements and standards described in Sections 3.3.1 and 3.3.2. These criteria are used as a common checklist for assessing the tools, together with the set of metadata, governance, interoperability, and security standards retained for ECLIPSE DIGITAL. The resulting shortlist of tools is summarised in Table 5.

Table 5: Evaluation of Candidate Open-Source Data Catalogue Tools

Tool	Implemented Standard(s)	Key Capability
CKAN	DCAT-AP, DCAT-US, DCAT v2, Schema.org	FAIR-aligned portal with rich metadata
uData	DCAT v2, DCAT-AP, Hydra, JSON-LD	Modular DCAT harvester/exporter for EU-profile portals
Magda	DCAT, OpenSearch, OIDC/OAuth2, OPA	Federated metadata harvesting with policy-driven governance
DKAN	DCAT v2/3, data.json (POD), CKAN API, JSON-LD	Drupal-based portal with DCAT-US export & CKAN-compatible REST APIs
DataHub	OpenLineage v0.17, Iceberg REST, DataHub Metadata Std.	Real-time metadata graph, end-to-end lineage & governance
OpenMetadata	OpenLineage, Iceberg REST, Pegasus/PDL	Unified metadata graph with observability, quality tests & policies
Apache Atlas	OMRS/OMAS, Atlas REST v2, Kafka TagSync, OpenLineage	Enterprise lineage & classification backbone
Gravitino	Iceberg REST, OpenLineage, OpenAPI	Geo-distributed Iceberg catalogue & lightweight metadata lake
Amundsen	OpenAPI v2, OpenLineage, OAuth2/OIDC	Google-style search UI with a lightweight discovery API
ODD Platform	ODD Spec, OpenLineage, OpenAPI 3.0	Metalake for discovery, lineage visualization & data-quality monitoring
Marquez	OpenLineage v1.x, Iceberg REST	Pipeline lineage & run-time metadata repository
Metamapper	GraphQL, OpenAPI, OAuth2/SAML2	Auto-crawled schema docs with drift-alerting
Egeria	OMRS/OMAS, Kafka open-metadata, Open Metadata Type Sys.	Federated metadata backbone with bi-directional exchange

3.3.3.2. CATALOGUE TOOLS REVIEW

The following subsections provide a brief review of each shortlisted open-source catalogue tool. For every tool, we highlight the standards it implements, its main capabilities in relation to the ECLIPSE DIGITAL requirements, and any specific strengths or limitations observed during the analysis. This qualitative review complements the comparative table and supports the final recommendation on which tools are best suited for data catalogue preparation in the project.

3.3.3.2.1. CKAN

CKAN [23] is an open-source data management system that enables organizations to publish, catalogue, and share datasets through a user-friendly interface and robust APIs, widely used in public sector and research data portals. It is aligned with the following standards:

- DCAT / DCAT-AP v3 via ckanext-dcat
- Schema.org / POD-JSON mappings
- REST/JSON API & DataStore SQL API
- FAIR data principles compliant

The core features or CKAN are:

- Rich metadata & resource management
- Full Action API for data access (CRUD via JSON)
- Fine-grained roles & access control (GDPR-ready)
- SQL-backed DataStore + visual previews (tables, charts, maps)
- 300+ community extensions (e.g. versioning, harvesting)
- Scalable: supports Kubernetes, BigQuery, S3
- Plugin-based extensibility for domain-specific use

CKAN fits the following Key catalogue requirements:

Table 6: CKAN Key catalogue requirements

Requirements	Status
Interoperability	✓ DCAT, Schema.org
Metadata richness	✓ Custom fields
Governance & Access	✓ Role-based ACLs
Data versioning	(✓) via ckanext-versions
Security & GDPR	✓ Proven in production
Scalability & Flexibility	✓ Cloud/K8s-ready
Light-weight / mobile-fit	(✓) Compact JSON API; server uses Postgres + Solr

CKAN is already used in several large-scale open data portals, including Denmark's Energi Data Service, the UK's National Grid ESO open data portal, and the US federal portal data.gov.

3.3.3.2.2. UDATA

uData [24] is an open-source data portal engine developed by Etalab, enabling quick deployment of customizable, standards-compliant catalogues with modular architecture and DCAT/DCAT-AP interoperability. It is aligned with the following standards:

- W3C DCAT v2, DCAT-AP, DCAT-AP-HVD
- JSON-LD + Hydra for Linked Data APIs
- RESTful API v1/v2 for programmatic access

The core features or uData are:

- Rich metadata: tags, coverage, frequency, license, extras
- Dataset access via JSON APIs, DCAT/RDF, and direct download
- Organizations & role-based governance (private/public modes)
- CKAN & Opendatasoft harvesting; RDF export

- Scalable backend: MongoDB, Kafka + Elastic/Sonic
- Vue.js-based UI (independently themable via udata-front)
- Celery/Redis background task queue for harvesting & metrics
- GDPR-compliant (used by EU governments, e.g., data.gouv.fr)
- Docker/Kubernetes deployment-ready

uData fits the following key catalogue requirements:

Table 7: uData Key catalogue requirements

Requirements	Status
Interoperability	✓ DCAT, JSON-LD, CKAN harvesting
Metadata richness	✓ Rich core & extra fields
Governance & Access	✓ Roles, OAuth2, Read-only mode
Data versioning	(✓) Mongo history (no UI)
Security & GDPR	✓ EU compliant
Scalability & Flexibility	✓ Elastic, Docker, plugins
Lightweight API Access	✓ RESTful API for mobile use

uData is already used in production by several national open data portals, including data.gouv.fr in France and data.public.lu in Luxembourg.

3.3.3.2.3. MAGDA

Magda [25] is a federated open-source data catalogue platform developed by CSIRO/Data61, enabling organizations to unify, enrich, and search datasets from diverse sources with full metadata versioning and discovery features. It is aligned with the following standards:

- W3C DCAT for dataset & distribution modelling
- REST/JSON APIs (Registry & Search endpoints)

- OpenSearch for full-text discovery
- OpenID Connect + OAuth2 for authentication
- Open Policy Agent (OPA) for authorization policies

The core features or Magda are:

- Federated harvesting from CKAN, DCAT, data.json, etc.
- Schema-agnostic metadata registry (PostgreSQL JSONB)
- Full-text, geospatial & temporal search (OpenSearch)
- Fine-grained access via OPA policies + identity providers
- Scalable deployment with Kubernetes & Helm
- History tracking, duplication detection, lineage visibility
- Modern UI with previews (charts, maps via TerriaJS)
- Compact public APIs for mobile/web integration

Magda fits the following key catalogue requirements:

Table 8: MAGDA Key catalogue requirements

Requirements	Status
Interoperability	✓ DCAT, cross-portal harvesting
Metadata richness	✓ DCAT aspects, customizable
Governance & Access	✓ OPA policies, role-based
Data versioning	✓ History tracking
Security & GDPR	✓ Gov-grade, OIDC + OPA
Scalability & Flexibility	✓ Microservices, K8s-ready
Lightweight API Access	✓ REST/JSON for mobile use

Magda has been deployed in production environments, such as the Australian Government open data portal data.gov.au, which publishes national energy and emissions datasets.

3.3.3.2.4. DKAN

DKAN [26] is an open-source data portal framework built on Drupal that enables organizations to publish, manage, and visualise datasets using DCAT metadata, CKAN-compatible APIs, and a built-in datastore with a modern React front-end. It is aligned with the following standards:

- DCAT v2/v3, DCAT-US, Project Open Data (data.json)
- RDF, RDFa, and JSON-LD for Linked Data and SPARQL compatibility
- CKAN-style APIs (Action & DataStore)
- JSON Schema for customizable metadata fields

The core features or DKAN are:

- Metastore: schema-agnostic metadata store (DCAT-US default)
- Datastore: parses CSV into SQL; exposes queryable API
- Federated harvesting from CKAN, Socrata, data.json sources
- Governance via 6 built-in roles + group admin support
- Revision history/versioning using Drupal revisions
- Interactive previews: grid, map, graph
- React front-end, headless JSON APIs
- Scalable deployment: Docker, Kubernetes, DDEV toolchain

DKAN fits the following key catalogue requirements:

Table 9: DKAN Key catalogue requirements

Requirements	Status
Interoperability	✓ DCAT, RDFa, CKAN API
Metadata richness	✓ Metastore with extensible fields
Governance & Access	✓ Roles, Drupal auth modules
Data versioning	✓ Built-in revision history

Security & GDPR	✓ Drupal-grade security
Scalability & Flexibility	✓ Docker, Helm, DDEV
Light-weight / mobile-fit	(✓) JSON APIs are compact; underlying Drupal/PHP stack is heavier

DKAN has been deployed in several real-world portals, such as the Jamaica Open Data Portal, which publishes energy-related datasets including the “Energy Tables” series.

3.3.3.2.5. DATAHUB

DataHub [27] is an open-source data portal framework built on Drupal that enables organizations to publish, manage, and visualise datasets using DCAT metadata, CKAN-compatible APIs, and a built-in datastore with a modern React front-end. It is aligned with the following standards:

- OpenLineage v0.17 for pipeline lineage
- Apache Iceberg REST Catalogue API for table discovery
- DataHub Open Metadata Standard (PDL/GraphQL/Avro/Kafka-based)

The core features of DataHub are:

- Metadata ingestion from 80+ sources (e.g., Snowflake, BigQuery, Looker, Kafka)
- Real-time graph-based metadata store (Kafka + Elastic/Neo4j)
- Column-level lineage, schema evolution, and impact analysis
- Ownership, glossary, tags, assertions as native metadata aspects
- Policy engine for fine-grained access + OIDC/SSO authentication
- Versioned metadata with changelogs & rollback
- Triggers for governance workflows via Actions & Webhooks
- Deployable via Docker, Helm, or DataHub Lite (DuckDB)

DataHub fits the following key catalogue requirements:

Table 10: DataHub Key catalogue requirements

Requirements	Status
Interoperability	✓ OpenLineage, Iceberg, GraphQL
Metadata richness	✓ Schema, profiling, ownership
Governance & Access	✓ Roles, groups, policy engine
Data versioning	✓ Aspect history + changelogs
Security & GDPR	✓ SSO, OIDC, advisory-published
Scalability & Flexibility	✓ Stream-based microservices
Lightweight API Access	(✓) Compact JSON / GraphQL APIs; DataHub Lite (DuckDB) removes MySQL + Kafka for edge use

DataHub has been used in this example: Real-time energy consumption catalogue using DataHub and Databricks.

3.3.3.2.6. OPENMETADATA

OpenMetadata [28] is an open-source unified metadata platform that integrates cataloguing, governance, and observability into a single graph with real-time lineage, search, and policy automation across 90+ data sources. It is aligned with the following standards:

- OpenLineage v0.17 for pipeline & column-level lineage
- Apache Iceberg REST Catalogue API integration
- OpenMetadata JSON/Avro schema via REST, GraphQL, Kafka
- SSO/OIDC, SAML 2.0, LDAP for enterprise auth

The core features of OpenMetadatashare:

- Metadata 90+ ingestion connectors: DBs, lakes, ML models, dashboards

- Real-time unified metadata graph with fast search (OpenSearch)
- Column/API-level lineage via parsing or OpenLineage
- Data profiler, tests, and observability dashboards (SLAs, thresholds)
- RBAC/ABAC policies, glossary, tags, classifications
- Versioned aspect model with rollback and diff viewer
- Actions & webhooks: trigger alerts, CI/CD, remediation
- Deploy with Docker, Helm, Terraform – 4 core services only

OpenMetadata fits the following key catalogue requirements:

Table 11: OpenMetadata Key catalogue requirements

Requirements	Status
Interoperability	✓ OpenLineage, Iceberg, GraphQL
Metadata richness	✓ Profiler, tests, KPIs, lineage
Governance & Access	✓ RBAC/ABAC, SSO, team roles
Data versioning	✓ Immutable, diff & rollback
Security & GDPR	✓ Auto-PII tagging, encrypted secrets
Scalability & Flexibility	✓ Kafka-based, 4-core microservices
Lightweight API Access	(✓) Compact JSON / GraphQL APIs; server still needs MySQL + Kafka

3.3.3.2.7. APACHE ATLAS

Apache Atlas [29] is an open-source metadata management and data governance framework that catalogues, classifies, and tracks lineage of data assets across platforms, enabling real-time discovery, policy enforcement, and compliance through a graph-based model. It is aligned with the following standards:

- Atlas REST v2 (Swagger/OAS 2.0) – JSON CRUD, search, lineage
- Open Metadata Repository Services (OMRS) via Egeria connector

- Ranger TagSync JSON feed – supports ABAC policies
- OpenLineage ingestion via community hooks

The core features of Apache Atlas are:

- Flexible type system for datasets, processes, glossary, columns
- End-to-end column-level lineage with REST access
- Classification engine with auto-propagation & Ranger integration
- Audit trail & versioning for all entities
- Real-time ingestion via Kafka hooks (Hive, HBase, Spark, Kafka)
- Fast search using Solr/OpenSearch (DSL + full-text)
  Scalable deployment via Helm, Docker, or single-node profile

Apache Atlas fits the following key catalogue requirements:

Table 12; Apache Atlas Key catalogue requirements

Requirements	Status
Interoperability	✓ OMRS, REST, Kafka
Metadata richness	✓ Schema, lineage, glossary
Governance & Access	✓ Tags, RBAC/ABAC, Ranger
Data versioning	✓ Full audit log & rollback
Security & GDPR	✓ SSL/TLS, masking, audit
Scalability & Flexibility	✓ Microservices or lightweight
Lightweight API Access	(✓) REST JSON APIs; server depends on HBase + Solr

3.3.3.2.8. GRAVITINO

Gravitino [30] is an open-source, engine-agnostic metadata lake that federates technical metadata across diverse data sources and regions, enabling unified discovery, governance, and SQL access through a single REST endpoint. It is aligned with the following standards:

- Apache Iceberg REST Catalogue API – catalogue integration
- Gravitino REST API v1 – OpenAPI/Swagger with OAuth2, Basic, Kerberos auth
- OpenLineage (via community hooks) for lineage events

The core features of Gravitino are:

- Unified metalake namespace for tables, filesets, ML models across clouds
- Iceberg REST server: exposes or manages Iceberg tables
- Model & fileset catalogues with built-in versioning
- Multi-engine interoperability: Spark, Trino, Flink
- Secure REST API + Kafka notifications for real-time integration
- Geo-distributed & resilient architecture
- Quick-start Docker stack with Hive, Trino, HDFS, and Jupyter

Gravitino fits the following key catalogue requirements:

Table 13: GRAVITINO Key catalogue requirements

Requirements	Status
Interoperability	✓ Iceberg, REST, OpenLineage
Metadata richness	✓ Names, versions, tags, models
Governance & Access	✓ OAuth2/Kerberos, role fields
Data versioning	✓ Built-in (ML models, Iceberg)
Security & GDPR	✓ TLS, OAuth2, audit via Kafka
Scalability & Flexibility	✓ Geo-distributed, Docker/Helm
Lightweight API Access	✓ Compact JSON REST (edge-ready)

3.3.3.2.9. AMUNDSEN

Amundsen [31] is an open-source data discovery and metadata engine that enables fast, Google-like search across data assets, helping teams find, trust, and reuse data through a graph-based metadata model. It is aligned with the following standards:

- REST API v2 (OpenAPI/Swagger) for search & metadata CRUD
- OpenLineage support via official extractor
- OAuth 2.0 / OIDC for enterprise SSO
- Apache Atlas Proxy for metadata interoperability

The core features of Amundsenare:

- Google-style PageRank search for tables, dashboards, and streams
- Pluggable ingestion (Databuilder) for 30+ sources
- Graph storage: Neo4j, Atlas, AWS Neptune, or MySQL
- Column-level lineage with OpenLineage support
- Glossary, tags, ownership, annotations for governance
- RBAC & SSO with Helm chart configuration
- Real-time Kafka integration for metadata services
- Quick-start with Docker; scalable via Helm/K8s

Amundsen fits the following key catalogue requirements:

Table 14: AMUNDSEN Key catalogue requirements

Requirements	Status
Interoperability	✓ Atlas, OpenLineage, Kafka
Metadata richness	✓ Descriptions, usage stats, tags
Governance & Access	(✓) Basic RBAC; full enterprise RBAC via Atlas proxy

Data versioning	— Not yet available (feature in progress – GitHub #45)
Security & GDPR	✓ TLS, RBAC, GDPR use case
Scalability & Flexibility	✓ Microservices, Helm, Docker
Lightweight API Access	(✓) Compact REST JSON; backend Neo4j + Elasticsearch adds weight

3.3.3.2.10. ODD PLATFORM

ODD Platform [32] is an open-source data discovery, lineage, and observability metalake that unifies metadata from diverse systems into a searchable, lineage-aware catalogue based on the ODD Specification for cross-platform interoperability. It is aligned with the following standards:

- ODD Specification (OpenAPI 3.0) for metadata exchange
- OpenLineage v0.17 for pipeline & column-level lineage
- OAuth 2.0 / OIDC / LDAP for secure enterprise authentication

The core features of ODD Platform:

- Real-time ingestion from Postgres, Kafka, Snowflake, Feast, dbt, etc.
- Full-text search & filter – no external Solr/ES required
- Lineage diagrams for datasets, pipelines, ML jobs & dashboards
- Data quality dashboards, SLA status, alerts (Slack, webhook)
- Schema diff & versioning for datasets and columns
- Glossary, tags, business terms, and ML experiment tracking
- RBAC/ABAC policy engine with role-based permissions
- Deploys via Docker, Helm, or AWS with lightweight PostgreSQL backend

ODD Platform fits the following key catalogue requirements:

Table 15: ODD Key catalogue requirements

Requirements	Status
Interoperability	✓ ODD Spec, OpenLineage, REST/Kafka
Metadata richness	✓ Tags, profiling, glossary, lineage
Governance & Access	✓ Roles, policies, OAuth/LDAP
Data versioning	✓ Auto-versioning + schema diff
Security & GDPR	✓ TLS, audit, alerts, granular access
Scalability & Flexibility	✓ Lightweight Spring services + Helm
Lightweight API Access	✓ JSON APIs, PostgreSQL-only footprint

3.3.3.2.11. MARQUEZ

Marquez [33] is an open-source reference implementation of the OpenLineage standard that captures, stores, and visualizes data lineage and runtime metadata to support governance, auditing, and impact analysis across diverse data systems. It is aligned with the following standards:

- OpenLineage v1.33 – native lineage event model
- Marquez REST API v1 – OpenAPI-described metadata access
- Iceberg REST Catalogue API for lakehouse integration
- Avro-over-Kafka event bus for lineage streaming

The core features of Marquez:

- Universal lineage ingestion: Airflow, Spark, dbt, Flink, etc.
- Real-time lineage graph with column-level insights
- Immutable versioning of datasets & jobs
- Searchable UI: Google-style search + run-history

- Pluggable storage: PostgreSQL + OpenSearch
- REST + experimental GraphQL APIs
- Kafka notifications + webhook triggers for governance workflows
- TLS support; SSO/OIDC under development

Marquez fits the following key catalogue requirements:

Table 16: MARQUEZ Key catalogue requirements

Requirements	Status
Interoperability	✓ OpenLineage, Iceberg, Kafka
Metadata richness	✓ Schemas, tags, run stats
Governance & Access	(✓) Owners & tags; full SSO/OIDC still on roadmap
Data versioning	✓ Dataset & job snapshots
Security & GDPR	(✓) TLS + VPN today; SSO/OIDC planned
Scalability & Flexibility	✓ Helm-scalable, Docker demo
Lightweight API Access	(✓) Compact JSON APIs; single-node Postgres backend

3.3.3.2.12.METAMAPPER

Metamapper is an open-source data discovery and documentation platform that auto-scans data sources to build a searchable catalogue enriched with tags, comments, and schema change tracking, supported by GraphQL APIs and enterprise-ready RBAC/SSO. It is aligned with the following standards:

- GraphQL API for metadata CRUD/search
- OpenAPI-described REST endpoints for setup and automation
- OAuth 2.0 / OIDC / SAML 2.0 for enterprise SSO

The core features of Metamapper:

- Auto-scans 12+ databases (e.g., Redshift, Snowflake, BigQuery, Hive)
- Tracks schema drift and alerts on changes
- Full-text search UI with usage-ranked results
- Custom tags, comments & annotations on any object
- RBAC with group-level permissions
- GraphQL query API for integration and automation
- Easy Docker deployment; PostgreSQL as the only external dependency

Metamapper fits the following key catalogue requirements:

Table 17: Metamapper Key catalogue requirements

Requirements	Status
Interoperability	✓ GraphQL, SSO, Docker
Metadata richness	✓ Tags, comments, custom fields
Governance & Access	✓ Role-based, SSO integration
Data versioning	(✓) Schema-change detection & diffs (no full snapshots)
Security & GDPR	✓ TLS, audit logs, fine-grained access
Scalability & Flexibility	✓ Docker containers, PostgreSQL backend
Lightweight API Access	(✓) Compact GraphQL JSON; server needs PostgreSQL + Elasticsearch

3.3.3.2.13.EGERIA

Egeria is an open-source metadata and governance platform that enables bidirectional exchange of metadata across tools through standard models, REST APIs, and event streams, creating a vendor-neutral, federated metadata fabric. It is aligned with the following standards:

- Egeria Open Metadata Type System (800+ types)
- OMRS & OMAS REST APIs (OpenAPI, JSON)
- Apache Kafka event model for metadata streaming
- TLS-secured endpoints and Helm deployment spec
- Conformance test suite for certified interoperability

The core features of Egeria:

- OMRS: federate metadata from multiple catalogues into one view
- 50 connectors (Atlas, IGC, databases, file systems, etc.)
- Real-time lineage & classification propagation via Kafka
- Governance zones, policies, and stewardship workflows
- TLS, RBAC, and audit logs for enterprise-grade compliance
- Visual lineage across technical and business layers
- Helm charts and Kubernetes operator for scalable or local deployment
- Self-service Jupyter labs for testing and development

Egeria fits the following key catalogue requirements:

Table 18: Egeria Key catalogue requirements

Requirements	Status
Interoperability	✓ OMRS, Kafka, REST APIs
Metadata richness	✓ 800+ metadata types
Governance & Access	✓ Zones, RBAC, audits
Data versioning	✓ Immutable history, validated
Security & GDPR	✓ TLS, ABAC, governance zones
Scalability & Flexibility	✓ Helm/K8s or Docker setup
Lightweight API Access	(✓) Compact JSON REST; full server stack (Kafka + Postgres) required

3.3.3.3. COMPARATIVE ANALYSIS OF STANDARDS-ALIGNED OPEN-SOURCE CATALOGUE TOOLS

The table below summarises the implementation of the identified requirements in the catalogue tools studied.

Table 19: Comparison of catalogue tools

Requirement	**CKAN**	**UData**	**Magda**	**DKAN**	**DataHub**	**Open Metadata**	**Atlas**	**Gravito**	**Amundsen**	**ODD Platform**	**Maguez**	**Metamapper**	**Egeria**
Data content	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data types & sources	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ownership & governance	✓	✓	✓	✓	✓	✓	✓	✓	(✓)[1]	✓	(✓)[2]	✓	✓
Access rules	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	(✓)[2]	✓	✓
Data format & access methods	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data Characteristics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Interoperability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Domain relevance – energy	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security & privacy (GDPR)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	(✓)[2]	✓	✓
Scalability & flexibility	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data exchange (standardized sharing)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data versioning	(✓)[3]	(✓)[4]	✓	✓	✓	✓	✓	✓	—[5]	✓	✓	(✓)[6]	✓
Light-weight DB / mobile-fit	(✓)[7]	✓	✓	(✓)[8]	(✓)[9]	(✓)[10]	(✓)[11]	✓	(✓)[12]	✓	(✓)[13]	(✓)[14]	(✓)[11]

"✓" = native feature

"(✓)" = available through an *official* extension

"—" = missing or roadmap.

Notes:

1. **Amundsen:** Full RBAC only when fronted by the Apache Atlas proxy.
2. **Marquez:** Strong TLS + token security today; OIDC/SSO & granular policies still on the roadmap.
3. **CKAN:** Needs the ckanext-versions plug-in to expose snapshot history.
4. **UData:** Mongo keeps every revision; UI requires the udata-storage-history add-on.
5. **Amundsen:** Dataset/table versioning not yet merged.
6. **Metamapper:** Stores schema diffs, not full historical snapshots.
7. **CKAN:** Mobile apps consume bulk-JSON Action API; server remains Postgres + Solr.
8. **DKAN:** JSON APIs are slim, but Drupal/PHP stack is heavier.
9. **DataHub:** “Lite” mode swaps MySQL & Kafka for DuckDB, reducing footprint.
10. **OpenMetadata:** Slim REST/GraphQL responses; server still runs MySQL + Kafka.
11. **Atlas / Egeria:** Lightweight JSON APIs, yet depend on HBase or Postgres back-ends.
12. **Amundsen:** REST JSON is slim; Neo4j + Elasticsearch add weight.
13. **Marquez:** Single-node Docker works well; PostgreSQL required.
14. **Metamapper:** GraphQL JSON is slim; server uses PostgreSQL + Elastic.

3.3.4. FINAL RECOMMENDATIONS AND SELECTIONS

Based on the requirements, standards and tool analysis presented earlier, CKAN configured with a DCAT-AP compliant metadata model and a core FAIR catalogue profile is recommended as the reference solution for data catalogue preparation in the ECLIPSE DIGITAL project. CKAN offers mature support for DCAT-AP, rich metadata management, proven use in open data and energy portals, and compact JSON APIs that can be consumed by CERF components and by lightweight mobile applications.

The catalogue approach in the ECLIPSE DIGITAL project is decentralised but harmonised. Pilots are expected to implement a data catalogue in their local architecture rather than relying on a single central instance. Each pilot catalogue may use CKAN or another shortlisted open-source tool, provided that the chosen tool can expose metadata that is compatible with a common ECLIPSE DIGITAL data catalogue profile. In practical terms, this profile is a recommended set of mandatory and optional fields, derived from DCAT-AP and the other standards reviewed in this section, that covers elements such as dataset title and description, temporal and spatial coverage, data owner, license, access rights, pilot identifiers, HLUC tags and links to CERF components, together with basic governance and access attributes. Applying this profile ensures that catalogues created in different pilots follow a similar structure and can be queried and understood in a consistent way.

The recommendations from Task T3.1 (Specifications of suitable data sets and digital environment) will be used in later work. In Work Package WP4 (Design and development of CERF and APIs), in particular Task T4.2 (Development of the CERF for consumer applications based on Machine learning tools and IA), the selected standards and tools will guide the integration of catalogue-related functionalities within CERF and its data connectors. This may include, depending on final design decisions in WP4, preparing an example CKAN setup aligned with DCAT-AP and the ECLIPSE DIGITAL profile, and defining illustrative interfaces for publishing and querying catalogue entries. In Work Package WP5 (Preparation, coordination and monitoring of deployment and demonstration activities), in particular Task T5.1 (Integration, deployment and adaptation activities), pilots will be encouraged to follow a common approach for publishing catalogue metadata. Depending on their local systems and constraints, pilots may either deploy a CKAN instance aligned with the ECLIPSE DIGITAL profile or adapt an existing platform so that it can publish DCAT-AP compliant metadata. This will be coordinated during WP5, taking into account technical feasibility and pilot-specific needs. In this way, the work on requirements, standards and tools in WP3 is translated into concrete catalogue implementations at pilot level, while CERF and project applications benefit from a coherent way of discovering and using data across all demonstrations.

The broader comparison of tools remains useful when pilots or partners face specific technical or organizational constraints. CKAN, uData, Magda and DKAN are the preferred options when strong DCAT support and open-data style portals are required. DataHub, OpenMetadata, Apache Atlas and Egeria are better suited to environments where internal lineage and governance are the main drivers and where integration with existing data platforms is important. Gravitino, ODD Platform and Marquez are relevant when lightweight or edge deployments are needed, for example close to streaming or time-series platforms. Whatever tool is selected locally, it should implement or expose the ECLIPSE DIGITAL data catalogue profile so that the project maintains a consistent approach to data catalogue preparation across all pilots.

4. STANDARD INTERFACES AND PROTOCOLS OF THE CERF

This section aims to identify the standards, protocols and semantic models relevant for the CERF framework. These are identified through the analysis of previous projects, and discussions with the pilots.

4.1. SURVEY OF PREVIOUS PROJECTS

Within Task T3.3 “Definition of standard interfaces and protocols of the CERF” under WP3, one of the activities consisted in carrying out a structured questionnaire using a Google Form in order to identify standards, protocols and semantic models already used in related initiatives. The survey collected information on previous or ongoing projects, with a focus on the semantic methods used, the communication protocols applied, and their applicability to the three CERF interfaces: the Energy App Interface, the Data Sources Interface and the DSO Interface. Thirteen respondents described their projects, the semantic resources they developed or reused, the communication protocols they selected, the main challenges encountered, and the lessons learned.

The answers have been grouped by interface as follows:

- Table 20 summarizes the projects and methods identified in the survey that are relevant to the Energy App Interface.
- Table 21 presents the projects that contribute to the Data Sources Interface.
- Table 22 gathers the projects, semantic methods and protocols that relate to the DSO Interface.

For each project, the tables highlight the semantic methods used, the protocols applied, the main challenges reported and the lessons or future directions that are useful for defining the CERF interface profiles.

Table 20 presents the projects that are relevant to the Energy App Interface. It summarises which semantic methods and communication protocols have been used to support end user applications, the types of challenges that appeared in real deployments, and the main lessons that were reported. The focus is on how standards such as SAREF, OpenADR and related APIs have been applied in practice for smart home and flexibility services, and which gaps remain from a developer and user adoption perspective.

Table 20: Summary of surveyed projects, semantic methods and protocols relevant to the Energy App Interface

Project Name	Semantic Methods Used	Communication Protocols	Challenges Faced	Lessons Learned & Future Directions
Tomorrow's Homes Today [34]	Tailored OpenADR environment (PAS1878)	OpenADR, APIs	Different interpretations of OpenADR standard limited interoperability	Gradual implementation of interoperability via API recommendations before enforcing international standards
SYNERGY [35]	SAREF, OpenADR, USEF	OpenAPI	Different stakeholder	Standardization needs for

			interpretations of semantic concepts	improved cross-platform integration
Independent (CheckWatt) [36]	SAREF-based model for hardware resource abstraction	MQTT, REST APIs	Early-stage project, no major challenges reported	Ongoing work to improve real-time processing performance
SENDER [37]	No specific semantic methods used	OpenADR, REST API	Deployment complexities in engaging 400 households for flexibility demonstration	Need for better coordination between operators and end users to scale demand response programs
InterConnect [11]	SAREF-based Interoperability Framework (SIF), Interoperable Recommender	REST APIs, SPARQL	Engaging developers in ontology-based integration was difficult	EU-wide training needed for semantic interoperability in smart home applications
PARMENIDES [38]	PECO (PARMENIDES Energy Community Ontology), based on SAREF	OpenADR	Not finalised, but integrating with DSO systems remains a challenge	Expanding PECO ontology to cover more aspects of energy community services

Overall, the projects in Table 20 show that SAREF based models and OpenADR style protocols are already used to support Energy Apps, but that differences in interpretation and limited familiarity with ontologies can still hinder interoperability. The lessons learned will be used to guide the definition of the Energy App Interface profile in CERF.

Table 21 covers the projects that provide input for the Data Sources Interface. It brings together the semantic methods and communication protocols used to describe and exchange data from meters, assets and platforms, as well as the main challenges and lessons reported. The projects listed in this table make extensive use of CIM, IEC 61850, DLMS/COSEM, SAREF and related protocols such as MQTT and REST APIs, and they highlight practical issues such as heterogeneous formats, data throughput and the need for stronger governance and mappings.

Table 21: Data Sources Interface

Project Name	**Semantic Methods Used**	**Communication Protocols**	**Challenges Faced**	**Lessons Learned & Future Directions**
SYNERGY	IEC 61850, DLMS/COSEM, SAREF, IFC	MQTT, OpenAPI	Heterogeneous data formats across different energy actors	Need for improved semantic mappings and governance frameworks
Independent (CheckWatt)	SAREF-based model for data abstraction	MQTT, REST APIs	Project is in early stages	Ensuring data throughput efficiency while maintaining interoperability

EDDIE	CIM (European Style Market Profile - ESMP)	MQTT, REST API	Adapting CIM for different EU Member States' energy data infrastructures	Improve CIM extensions to better align with decentralised energy data hubs
InterConnect	SAREF-based Semantic Interoperability Framework (SIF)	RESTful APIs, Hyperledger Fabric (Blockchain)	Standardizing energy data exchange across IoT and energy grids	Increased regulatory alignment needed for energy data-sharing across platforms
H2020 WEDISTRICT [39]	IoT-based Smart Meter Data Exchange (non-semantic)	MODBUS RTU, MODBUS TCP, MQTT	Limited semantic integration	Move towards an ontology-based interoperability framework for better scalability
Hedge-IoT [40]	PowerCIM (Semantic Treehouse for energy data)	Not finalized	Early-stage project, no major challenges reported yet	AI-driven energy system orchestration will be a focus
OMEGA-X [41]	CIM-based model for Energy Data Spaces	Common Information Model (CIM)	No major challenges reported	Increase adoption of CIM-based interoperability in energy data exchange

The projects in Table 21: Data Sources Interface confirm that CIM and IEC 61850 are central for structured energy data exchange, but they also show that additional mappings, governance rules and performance considerations are needed when these standards are applied to data space and multi actor contexts. These findings inform the design of the Data Sources Interface profile for CERF.

Table 22 summarises the projects, semantic methods and protocols that are relevant to the DSO Interface. It focuses on how DSOs and related actors describe flexibility, manage interactions with demand side resources and exchange grid related information, using standards such as CIM, OpenADR, USEF, PECO and SHACL. For each project, the Table 22 reports the main interoperability and regulatory challenges encountered, and the lessons that can support the definition of a robust DSO oriented interface profile in CERF.

Table 22: DSO Interface

Project Name	Semantic Methods Used	Communication Protocols	Challenges Faced	Lessons Learned & Future Directions
Tomorrow's Homes Today	Tailored OpenADR (PAS1878)	OpenADR	Compatibility issues with multiple appliance types	Define a minimum data requirement for Demand Side Response (DSR) to ensure interoperability
SYNERGY	Common Information Model (CIM), OpenADR, USEF	OpenAPI	Different regulatory interpretations of flexibility services	More unified frameworks needed for demand-response programs

				across different markets
EDDIE	CIM - ESMP (European Style Market Profile)	MQTT, REST API	Differences in how Member States manage energy data exchange	Need for better standardization across EU countries for DSO interfacing
InterConnect	SAREF-based DSO Interface (DSOi)	REST APIs	Mapping smart meter data across different DSO systems was complex	Improve privacy-by-design solutions for compliance with GDPR
PARMENIDES	PECO Ontology (for Energy Communities)	OpenADR	Integration with multiple grid systems remains a challenge	PECO ontology expansion for broader use in flexibility services
Hedge-IoT	ODC Tester (SHACL-based semantic constraint validator), PowerCIM	Not finalised	Project in early stages	Enhancing federated AI/ML for improved grid flexibility services

Taken together, the projects in Table 22 show that CIM and OpenADR are already used in DSO contexts, but that differences between national frameworks and between grid systems still create fragmentation. The reported lessons help to identify common elements that can be reused in the CERF DSO Interface profile while keeping room for national specificities.

The survey shows that a small number of standards and protocols are reused across the three CERF interfaces (Energy App, Data Sources, DSO Interface). SAREF and related ontologies, CIM and its extensions, and PECO are the main semantic references, while OpenADR, MQTT and REST style APIs are the most common communication protocols.

For the Energy App Interface, SAREF and OpenADR already support smart home and flexibility services but differences in interpretation and limited semantic skills still hinder interoperability. For the Data Sources and DSO Interfaces, CIM, IEC 61850, DLMS/COSEM and MQTT are widely used for metering, asset and grid data, yet heterogeneous formats, varying national practices and weak governance of mappings continue to create fragmentation. Overall, the results confirm that CERF should reuse existing standards and provide clear, implementable interface profiles that specify how to combine these protocols and semantic methods for Energy App, Data Sources and DSO use cases.

4.2. RELEVANT PROTOCOLS AND STANDARDS

This section provides a comparative view of the main communication protocols and semantic methods used in recent energy projects. The focus is on how these technologies are applied, which benefits and limitations are reported, and what maturity level they have when mapped to the three interfaces: Energy App Interface, Data Sources Interface and DSO Interface.

For communication protocols, Table 23 compares the most relevant protocols identified in the survey and in previous EU projects. It shows, for each protocol, its role in energy systems, its main strengths, and the typical constraints that may affect its use in CERF. In particular, the table confirms that OpenADR, MQTT and REST style APIs are already widely used for demand response, telemetry and system integration, while more specialised options such as SPARQL, MODBUS and Hyperledger Fabric address specific needs related to semantic querying, legacy devices and trusted exchanges.

Table 23: Comparison of Communication Protocols

Protocol	Description	Benefits	Limitations	Maturity Level
OpenADR	Open Automated Demand Response, used for energy flexibility and demand-side response.	Standardised approach for demand response, widely adopted in smart grids.	Complexity in implementation, interoperability issues due to different interpretations.	High
MQTT	Lightweight messaging protocol for small sensors and mobile devices.	Efficient, low bandwidth, supports publish/subscribe model.	Lacks built-in security, limited support for structured data semantics.	High
REST API	Web-based communication protocol for exchanging data between systems.	Scalable, widely adopted, easy integration with existing systems.	Stateless nature can lead to inefficiencies in continuous data streams.	High
SPARQL	Query language for RDF data, used in semantic web applications.	Enables semantic querying and reasoning over linked data.	Requires ontology expertise, performance issues with large datasets.	Medium
MODBUS RTU/TCP	Protocols used for industrial control systems and smart meters.	Well-established, compatible with legacy systems.	Lacks support for semantic data structures, security vulnerabilities.	High

Hyperledger Fabric (Blockchain)	Distributed ledger technology for secure, decentralised transactions.	Provides trust and auditability in data exchange.	High computational overhead, complexity in integration.	Medium

Table 24 performs a similar comparison for semantic models and frameworks. It brings together the main ontologies and standards that support semantic interoperability in this domain, including SAREF, CIM, IEC 61850, DLMS/COSEM, PECO, PowerCIM, SIF and SHACL. For each of them, the table summarises the scope, the key benefits and the main limitations that must be considered when defining CERF interface profiles. Overall, the table highlights that SAREF and CIM are already mature and widely used in EU projects and utility contexts, while PECO, PowerCIM and SHACL provide useful capabilities for energy communities, extended power system modelling and data quality, but are still less widely deployed.

Table 24: Comparison of Semantic Methods

Semantic Model/ Framework	Description	Benefits	Limitations	Maturity Level
SAREF	Smart Appliances REFerence ontology for energy-related IoT applications.	Enables interoperability among energy applications, widely used in EU projects.	Requires alignment with domain-specific standards.	High
CIM	Standard ontology for energy management and data exchange.	Used extensively for utility data modelling and energy system interoperability.	Complexity in implementation, variations across EU member states.	High
IEC 61850	Standard for power utility automation, supports semantic interoperability.	Ensures reliable data exchange in power grids.	Complex structure, high implementation cost.	High

DLMS/ COSEM	Protocol suite for smart metering applications.	Standardized for energy metering, supports data exchange.	Limited adaptability to new semantic web standards.	High
PECO	Ontology designed for energy community services.	Supports flexible energy markets and community-based energy management.	Still evolving, requires further expansion for full implementation.	Medium
PowerCIM	Semantic extension of CIM for energy data exchange.	Enhances data interoperability in power grids.	Still in early stages of development.	Low
SIF	Semantic framework for integrating IoT and energy systems.	Supports interoperability across heterogeneous data sources.	Adoption challenges due to lack of developer familiarity.	Medium
SHACL	Used for validating RDF data against defined constraints.	Ensures data quality and consistency in semantic models.	Requires expertise in ontology modelling, limited industry adoption.	Medium

4.2.1. INTERFACE PROFILES RECOMMENDATIONS

Building on the survey of previous projects and the comparison of protocols and semantic methods, this subsection proposes initial recommendations for the three CERF interface profiles. The goal is to identify a small set of preferred protocols and semantic resources for each interface, which can be refined in later tasks when defining detailed technical specifications.

4.2.1.1. ENERGY APP INTERFACE PROFILE

For the Energy App Interface, OpenADR in combination with REST style APIs is recommended as the main protocol stack. OpenADR supports standardised demand response interactions, while REST APIs provide a simple and widely adopted way to integrate with mobile and web applications. From a semantic point of view, SAREF and the SAREF based Semantic Interoperability Framework (SIF) are recommended to describe devices, services and flexibility offerings used by Energy Apps. This combination reflects the experience of projects such as Tomorrow's Homes Today, SYNERGY and InterConnect, where SAREF based models and OpenADR style signalling were already used to support smart home and flexibility services.

- **Recommended profile for the Energy App Interface:**
    - **Protocol stack:**
        - OpenADR for standardised demand response signalling.
        - REST style APIs for integration with mobile and web applications.
    - **Semantic methods:**

        - SAREF for modelling devices, services and measurements.
        - SAREF based Semantic Interoperability Framework (SIF) for interoperable energy service descriptions and recommendations.

4.2.1.2. DATA SOURCES INTERFACE PROFILE

For the Data Sources Interface, the recommended protocol stack is based on lightweight, widely used technologies for telemetry and data access. At low level, MQTT, OpenAPI based services and RESTful APIs are suggested to support near real time and scalable data exchange from meters, assets and platforms. At higher level, the interface can reuse an ECLIPSE DIGITAL Foundation data space protocol, or resource specific profiles that will be identified in upcoming technical workshops, in order to align with emerging European data space architectures. On the semantic side, CIM and IEC 61850 are recommended as primary references for structured energy data exchange and grid related governance, complemented where relevant by DLMS/COSEM and other metering standards. This reflects the practices reported in SYNERGY, EDDIE, OMEGA X and similar projects.

- **Recommended elements for the Data Sources Interface:**
    - **Protocol stack:**
        - **Low level:**
            - MQTT for lightweight publish and subscribe telemetry.
            - OpenAPI based services and RESTful APIs for structured data access.
        - **High level:**

      - ECLIPSE DIGITAL Foundation data space protocol, when compatible with the pilot context.
  - **Semantic methods:**
    - CIM as the main reference for utility and flexibility related data models.
    - IEC 61850 for substation and grid automation semantics.
    - DLMS/COSEM and related metering standards where smart meter data is involved.

4.2.1.3. DSO INTERFACE PROFILE

For the DSO Interface, OpenADR and REST APIs are recommended to manage demand response interactions and smart grid integration between DSOs, aggregators and flexibility providers. As semantic foundations, CIM remains the main reference for grid and flexibility data, while SHACL and PECO can be used to support validation and energy community specific concepts where relevant. CIM and OpenADR are already used in DSO contexts in projects such as SYNERGY, EDDIE and PARMENIDES, while SHACL based validation and PECO style models are emerging in projects like Hedge IoT.

- **Recommended elements for the DSO Interface:**
  - **Protocol stack:**
    - OpenADR for demand response and flexibility service signalling between DSOs, aggregators and service providers.
    - REST APIs for integration with DSO IT systems and market platforms.
  - **Semantic methods and frameworks:**

- CIM as the main model for grid assets, flexibility products and related measurements.
- SHACL for validating CIM based and other RDF representations against agreed constraints.
- PECO for representing energy community concepts where DSO interactions with energy communities are in scope.

Taken together, these interface profile recommendations provide a consistent set of building blocks for CERF. They reuse mature standards where possible and take into account lessons learned on complexity, interoperability and adoption. In later tasks of WP4 (Design and development of CERF and APIs), these initial profiles will be refined into more detailed specifications and implementation guidelines that pilots can apply.

4.3. OPEN-SOURCE REUSABLE CONNECTORS

The aim of this section is to identify and assess open-source connectors that can support the objectives of Task 3.3 (Specifications of suitable data sets and digital environment). It provides an analysis of candidate solutions such as the InterConnect Generic Adapter, EDDIE Framework, and the ECLIPSE DIGITAL Foundation ESMF (ECLIPSE DIGITAL Semantic Modelling Framework) and evaluates how these can be used within the project.

The section also describes how the capabilities of each connector align with the High-Level Use Cases. This includes their relevance for economic and non-economic flexibility, device recommendations, grid alerts, and other pilot needs, so that the selected connectors can be matched to the requirements of each demonstration site.

4.3.1. POTENTIAL CONNECTOR OVERVIEWS

This section introduces each connector's fundamental purpose, scope, and architectural underpinnings.

4.3.1.1. GENERIC ADAPTER (GA) - INTERCONNECT

Before diving into detailed information about the Generic Adapter, it is important to see how the Generic Adapter (GA) addresses semantic interoperability challenges within InterConnect. In the InterConnect project, legacy systems such as traditional APIs and devices need to communicate seamlessly. However, they do not inherently support semantic interoperability.

To bridge this gap, a structured adaptation process is followed. First, the Service-Specific Adapter, or SSA, processes component-specific logic and maps API parameters. This ensures that data from different sources is standardised before further transformation.

Next, the GA plays a crucial role in enabling interoperability. It registers and initialises components through REST APIs, manages Knowledge Interactions, and ensures data is transformed into structured semantic formats. It also supports REST and native Java, making it highly adaptable.

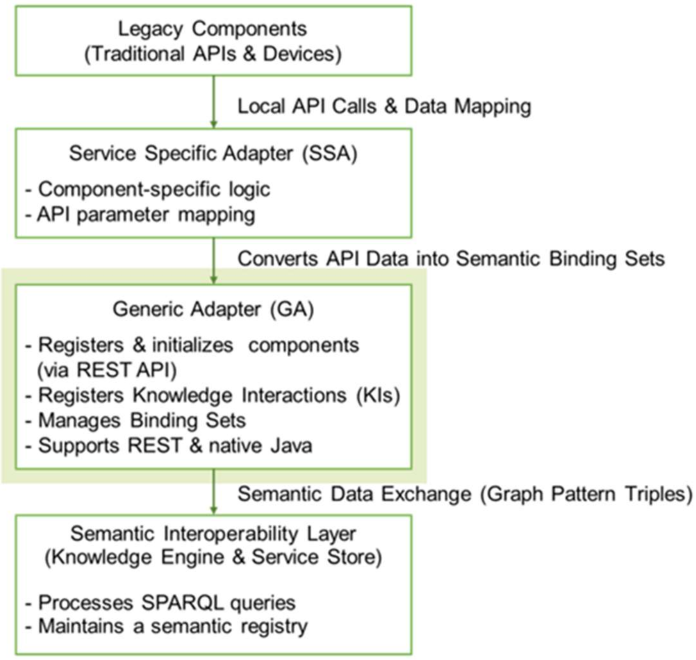


Figure 35: InterConnect semantic interoperability framework

Finally, the Semantic Interoperability Layer acts as the knowledge engine. It processes SPARQL queries and maintains a semantic registry, ensuring that data is stored and retrieved in a structured, meaningful way. Once we have seen how semantic interoperability is enabled in the InterConnect project, we can then look more closely at the Generic Adapter (GA), one of the key components facilitating this process.

The Generic Adapter plays a crucial role in enabling seamless communication between diverse systems by ensuring data interoperability. It consists of four main modules:

- **Registration & Initialization Module**: Handles authentication, smart connector creation, and adapter registration. This ensures that components can securely connect and interact within the system.

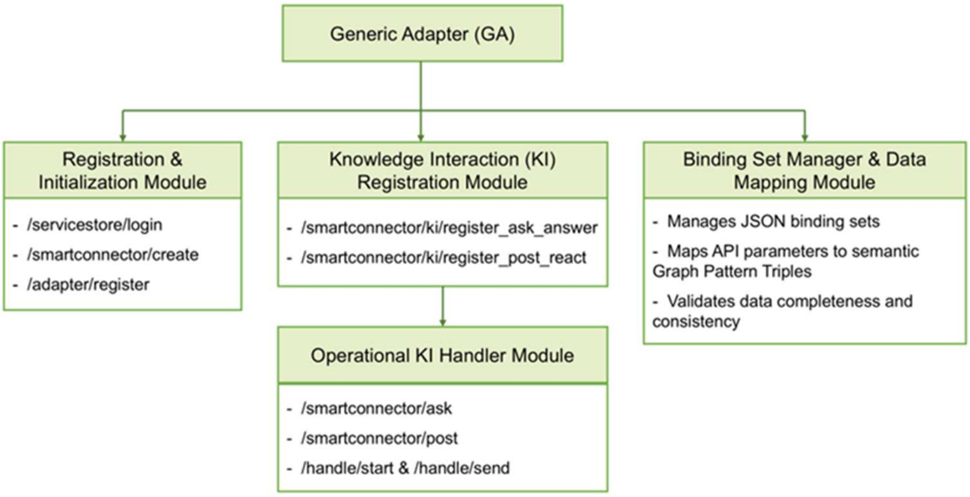


Figure 36: InterConnect Generic Adapter (GA)

- **Knowledge Interaction Registration Module**: Responsible for registering interactions between components. It supports two key types of interactions, ask–answer and post–react, allowing structured communication between services.
- **Operational KI Handler Module**: Executes the registered interactions. This module processes knowledge interactions by handling requests such as asking, posting, and executing actions.
- **Binding Set Manager & Data Mapping Module**: Takes care of JSON binding sets, maps API parameters to semantic graph pattern triples, and ensures that the exchanged data is complete and consistent.

4.3.1.2. EDDIE CONNECTOR - EDDIE PROJECT

The EDDIE Connector was first developed in the OneNet project, whose goal was to unify European electricity systems and support real time coordination between TSOs, DSOs, aggregators and prosumers. In

OneNet, particular attention was given to two main categories of data: validated historical data, which is needed for settlement and billing, and near real time (NRT) data, which is needed for fast response services such as balancing and flexibility. By aligning with IEC 62325-351 and IEC 62746, the EDDIE team ensured that all parties could exchange this data in a common, machine-readable format. This work showed how aggregator led demand response processes can be supported over a shared data infrastructure.

Building on these foundations, EDDIE (European Distributed Data Infrastructure for Energy) has been refined by D4G to cover a broader, CIM based range of energy data exchange scenarios. Its core vision can be summarised in three data exchange families, as illustrated in Figure 37: EDDIE's Core Vision.

- Smart metering validated data, which is regulated
- Flexible service providers and control units (demand), which are mostly deregulated
- Grid and market operator publications, which are regulated

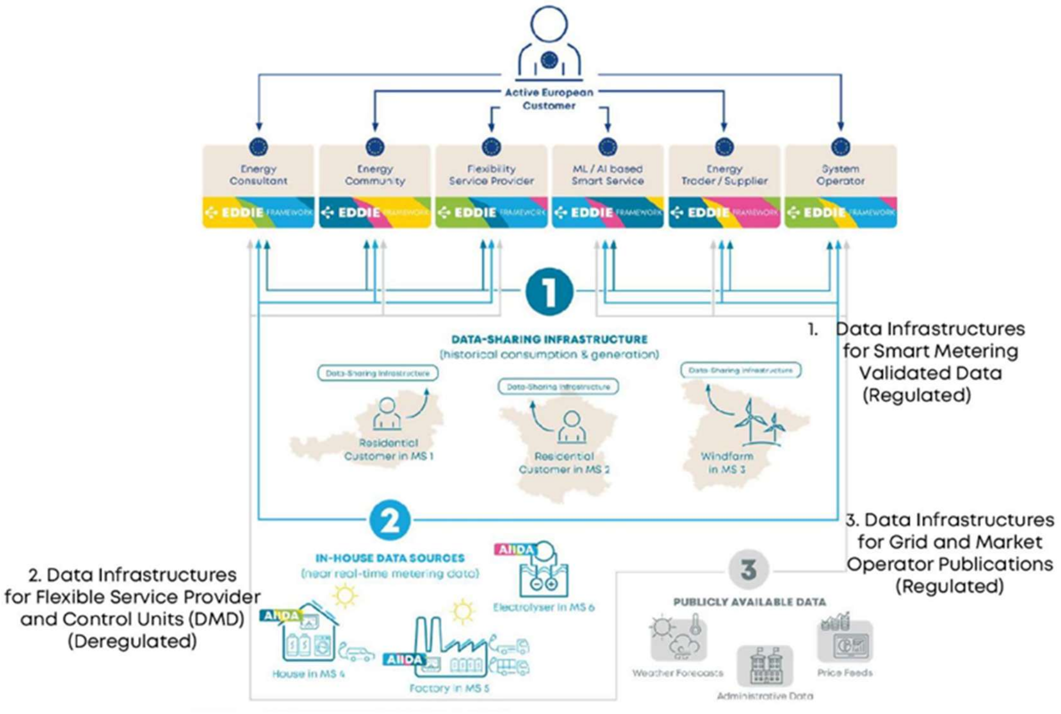


Figure 37: EDDIE's Core Vision

Through a structured data sharing infrastructure, EDDIE defines how different Member States or grid operators can interconnect across these families. It introduces validated historical data (VHD) profiles for regulated usage, NRT profiles for aggregator driven flows, and extended IEC 62325 parameters to represent consent and permission. By mapping the main domains such as metering, flexibility bidding and scheduling to CIM classes, EDDIE allows domain specific protocols like OCPP for EV charging or OpenADR for demand response to operate under a single semantic umbrella.

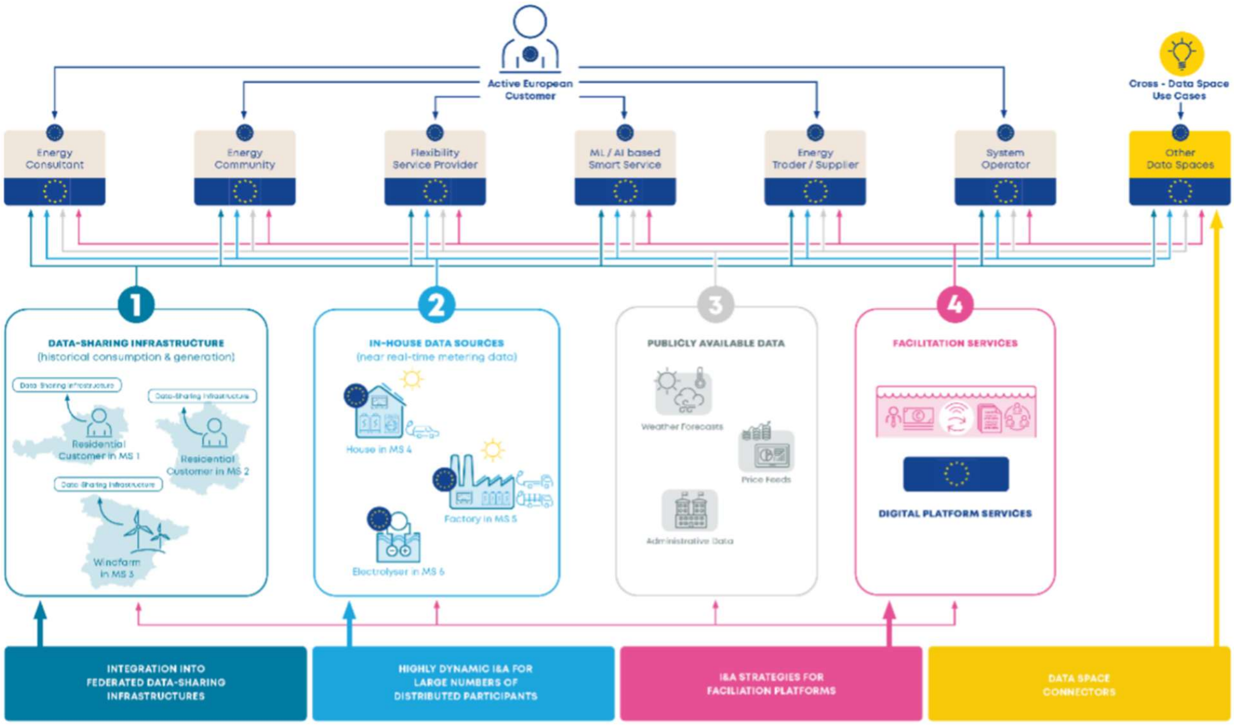


Figure 38: EDDIE Connector

As shown in Figure 38: EDDIE Connector, the EDDIE architecture is organised into four key building blocks:

- **Data driven infrastructures**. EDDIE connects data applications to existing regional infrastructures in each Member State and provides validated historical data. It acts as a technical layer that can supply VHD to eligible parties, in line with existing consent rules managed by the national Permission Administrator.
- **In house data sources**. The Administrative Interface for in house Data Access (AIIDA) provides secure access to real time data based on customer consent. It connects to in house assets such as submeters and IoT devices and can read from the customer interface of smart meters, for example the P1 port, so that near real time data is available to services.

- **Publicly available data**. EDDIE can integrate open sources such as weather forecasts, price signals and infrastructure status information that are relevant for advanced energy services.
- **Facilitation services**. EDDIE exposes connections towards data marketplaces, other dataspaces and digital platform services so that energy data can be shared and reused in a controlled way.

In operational terms, EDDIE supports four main tasks:

- Registration of flexibility service providers, during which aggregators register and supply baseline and resource data
- Delivery of validated historical data for settlement processes and analytical use
- Management of near real time data flows for aggregator and TSO processes, including baseline nomination and activation signals
- Enforcement of a consent model that allows prosumers and end users to grant or revoke access to their energy data in a dynamic way

These mechanisms have been demonstrated across multiple countries by using regional connectors that adapt local data sources and infrastructures to a common CIM based backbone.

4.3.1.3. ECLIPSE DIGITAL SEMANTIC MODELLING FRAMEWORK (ESMF) - ECLIPSE DIGITAL FOUNDATION

ECLIPSE DIGITAL Semantic Modelling Framework, which is designed to model aspects of digital twins, enabling the creation of APIs and UIs based on semantic information. ESMF focuses on digital twins, which are representations of assets using a set of submodels. Each submodel captures a specific aspect of the asset being modelled. For semantic interoperability, it is crucial to define the semantics of each submodel explicitly. ESMF provides tools and frameworks to define these semantics, ensuring interoperability and clarity in digital twin implementations. The core components of this framework are shown in Figure 39.

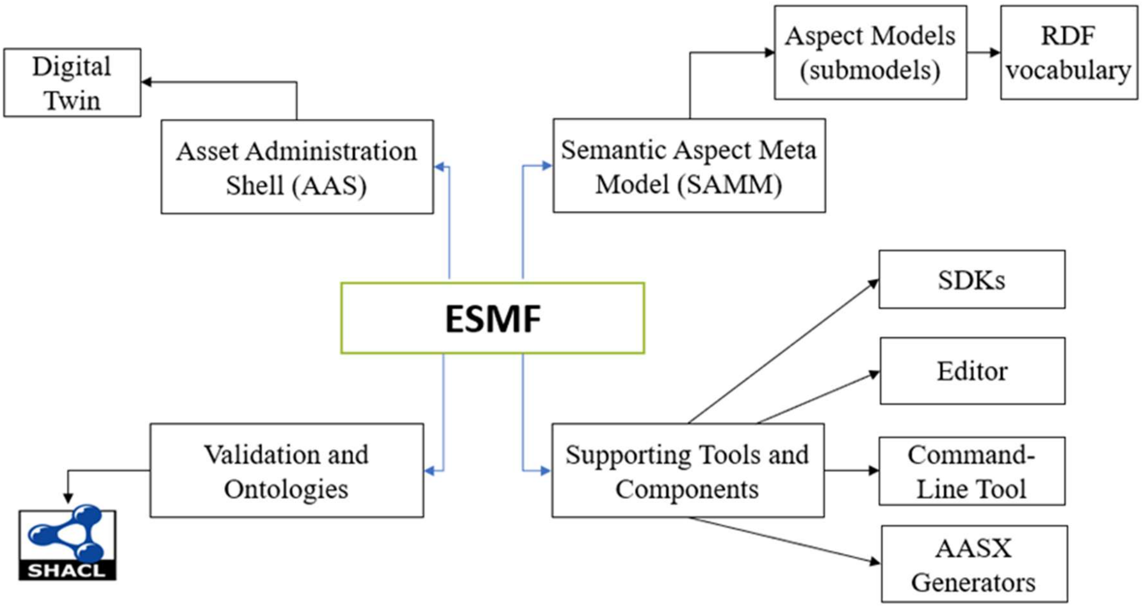
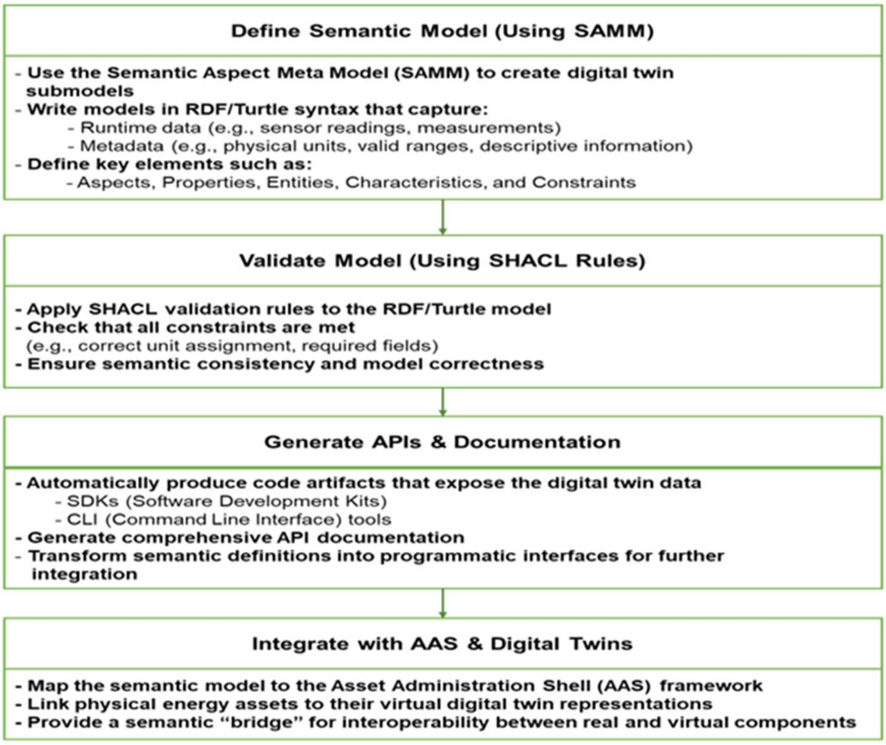


Figure 39: Core Components of the ECLIPSE DIGITAL Semantic Modelling Framework (ESMF).

At the core of ESMF is the Semantic Aspect Meta Model (SAMM), which provides a standardised language for defining the semantics of submodels also known as Aspect Models. These models define key parameters, such as a sensor's unit, range, and functionality, ensuring a structured representation. SAMM expresses these schemas using RDF vocabulary and validates them through SHACL rules, ensuring correctness and compliance with semantic standards. To facilitate usability, ESMF offers several supporting tools, including:

- SDKs for developers to integrate semantic models.
- An Editor that allows experts to create and edit Aspect Models visually.
- A Command-Line Tool for model validation, documentation, and conversions.
- AASX Generators, ensuring compliance with the Asset Administration Shell (AAS) standard for digital twins.

Validation plays a crucial role in ensuring accuracy and consistency. Aspect Models are checked against SHACL constraints, and structured ontologies are developed to maintain a common vocabulary, reducing ambiguity and ensuring smooth communication across different systems. Finally, ESMF seamlessly integrates with the Asset Administration Shell (AAS) a widely accepted standard for digital twins ensuring that all models it generates are compatible, structured, and industry-ready. This integration accelerates digital twin adoption and enhances their usability in industrial applications.



Define Semantic Model (Using SAMM)

- Use the Semantic Aspect Meta Model (SAMM) to create digital twin submodels
- Write models in RDF/Turtle syntax that capture:
  - Runtime data (e.g., sensor readings, measurements)
  - Metadata (e.g., physical units, valid ranges, descriptive information)
- Define key elements such as:
  - Aspects, Properties, Entities, Characteristics, and Constraints

Validate Model (Using SHACL Rules)

- Apply SHACL validation rules to the RDF/Turtle model
- Check that all constraints are met (e.g., correct unit assignment, required fields)
- Ensure semantic consistency and model correctness

Generate APIs & Documentation

- Automatically produce code artifacts that expose the digital twin data
  - SDKs (Software Development Kits)
  - CLI (Command Line Interface) tools
- Generate comprehensive API documentation
- Transform semantic definitions into programmatic interfaces for further integration

Integrate with AAS & Digital Twins

- Map the semantic model to the Asset Administration Shell (AAS) framework
- Link physical energy assets to their virtual digital twin representations
- Provide a semantic "bridge" for interoperability between real and virtual components

Figure 40: ESMF Workflow Overview

The workflow process begins with defining the semantic model using the Semantic Aspect Meta Model (SAMM). This allows developers to create digital twin submodels, defining key aspects such as properties, entities, characteristics, and constraints. These models are expressed using RDF/Turtle syntax, capturing both runtime data (such as sensor readings) and metadata (like physical units and valid ranges). The overall workflow is summarised in Figure 40. Once the models are created, ESMF ensures their correctness using SHACL validation rules. These rules check for semantic consistency, ensuring that constraints such as unit assignments and required fields are met. This step guarantees data reliability and compliance with industry standards. Next, ESMF automates the generation of APIs and documentation. The framework produces SDKs, command-line tools (CLI), and other software artifacts to make digital twin data accessible. It also transforms semantic definitions into programmatic interfaces, enabling smooth integration into various applications. Finally, ESMF integrates with the Asset Administration Shell (AAS) to connect real-world assets with their digital representations. This ensures that physical energy assets are linked to their virtual counterparts, providing a semantic bridge for interoperability. With this approach, organizations can develop scalable, efficient, and standards-compliant digital twins.

4.3.2. COMPARATIVE ANALYSIS

After the description of the components, Table 25 compares the three connectors (InterConnect Generic Adapter, EDDIE Connector and ECLIPSE DIGITAL ESMF) across several factors: technical scope, semantic standards, data exchange patterns, deployment complexity, maturity and ecosystem readiness. The structure of this comparison is consistent with the analysis already presented in Deliverable D4.1 ECLIPSE DIGITAL CERF for Energy Saving applications_V1, and it consolidates in a single view the main differences in scope, modelling depth and operational effort that are relevant for their potential integration within CERF and for later design choices in ECLIPSE DIGITAL.

Table 25: Connectors comparison Table

Factor	Generic Adapter (GA)	EDDIE Connector	ECLIPSE DIGITAL ESMF
Core Focus / Primary Role	Bridging service-specific adapters (SSAs) to a Knowledge Engine, enabling ontology-based data exchange (ASK/ANSWER, POST/REACT).	Standardizing energy data flows (historical, real-time, aggregator/DSO markets) via CIM alignment and ESMP-based message sets.	Enabling digital twin semantics using Aspect Models, validated by SHACL, with a strong tie-in to the Asset Administration Shell (AAS).
Key Standards & Protocols	- SPARQL-based KIs (via Knowledge Engine) - InterConnect Ontologies - Graph Pattern Triples - REST or Java integration	- IEC62325, IEC62746 - CIM (ENTSO-E) - ESMP Profile (VHD, NRT) - Potential synergy with OCPP, OpenADR	- RDF/Turtle, SHACL, SAMM - AAS alignment - Potential extension to domain ontologies - JSON/REST for aspects and submodels
Data Exchange Patterns	- Graph Pattern approach: binding sets map variables to values - Proactive (ASK/POST) & Reactive (ANSWER/REACT) interactions	- Validated Historical Data (VHD) for official meter readings - Near Real-Time (NRT) for aggregator-TSO/DSO interactions	- Aspect-based modelling: properties, operations, events - Runtime payloads enforced by SHACL rules

			-Generates OpenAPI/JSON schemas from semantic models
Semantic Depth / Modelling	- Primarily focuses on structure of interactions (KIs) rather than comprehensive domain modelling	- Uses CIM-based domain definitions (esp. for DSOs, TSOs) - Maintains comprehensive domain coverage for flexible markets	- Deep, hierarchical semantic modelling with submodels - Highly robust SHACL-based validation and inheritance rules - Focused on digital twin representation
Deployment Complexity	- Requires a Knowledge Engine (smart connectors, Service Store) - Typically deployed as a separate service or Java process	- EDDIE runs as a CIM-based connector or library that can integrate with aggregator/DSO systems - Must handle consent management data flows	- ESMF usage involves creating and maintaining Aspect Models - Tools needed: Editor, CLI, AAS environment (if used) - Possibly bigger overhead for domain modelling
Integration Overhead	- Moderate, GA approach is well-documented, but user must define SSAs and map local APIs to Graph Patterns	- Medium-High, must align local data with EDDIE’s CIM profiles. Very comprehensive but can be more complex to set up	- Medium-High, Users must design aspect models, handle SHACL validation, etc. Excellent for new developments, but more overhead for legacy systems

Maturity & Field Testing	- Used extensively in InterConnect demos/pilots - Has stable references, e.g., documented on GitLab, used by multiple SSAs	- Validated in OneNet, EDDIE, and D4G contexts - Specific TSO pilot integrations (Estonia/Elering) for balancing markets	- Open-source ECLIPSE DIGITAL project - Emphasis on industrial digital twin synergy - Maturity is good within digital manufacturing /automation contexts
Recommended Use Cases	- Rapid bridging for legacy devices/apps to a semantic environment - Multi-SSA scenarios with minimal domain-level modelling required	- Full aggregator/DSO/TSO flow (historic & NRT data, market transactions) - Demand response, consent management, advanced energy markets	- Digital twin ecosystems - Complex semantic scenarios needing domain submodels, validation, and advanced data constraints
Pros / Strengths	- Easy to add new SSAs - Good error checking on bindings - Clear “ASK/ANSWER” - Reusable architecture	- Thorough coverage of flexibility & real-time use cases - Standard-based approach for aggregator-operator interactions - Consent management is built-in	- High-level semantic rigor (SHACL, RDF) - Extensive tooling for digital twin aspects - Deep structural modelling and validation

Cons / Limitations	- Lacks direct domain coverage for energy-specific models (depends on external ontology definitions)	- Complexity can be high if smaller-scale usage - Strong dependency on CIM, which slows down onboarding for partners not aligned with CIM.	- Overhead in defining aspect models - Possibly over-engineered if only minimal data integration is needed
License / Openness	- InterConnect open-source components, GA specs are publicly available on GitLab	- D4G-based EDDIE solution references open CIM standards, docs available to partners & EU collaboration	- ECLIPSE DIGITAL Foundation open-source license, fully public repos, active developer community

4.3.3. MAPPING TO HIGH-LEVEL USE CASES AND PILOTS

ECLIPSE DIGITAL defines a set of High-Level Use Cases (HLUCs), each of which may involve several pilots. Table 26 proposes how the three connectors can support these HLUCs and illustrates this with pilot examples. For each HLUC, the table indicates which connector is best positioned to cover the required data flows, semantic modelling or digital twin aspects, and how this aligns with the roles of DSOs, aggregators and consumer applications in the pilots. This mapping extends the connector comparison by linking it to concrete project scenarios and provides an initial reference for the integration work to be refined in WP4 (Design and development of CERF and APIs) and WP5 (Preparation, coordination and monitoring of deployment and demonstration activities), in continuity with the analysis already introduced in Deliverable D4.1 ECLIPSE DIGITAL CERF for Energy Saving applications_V1.

Table 26: Mapping to High-Level Use Cases

HLUC	Description	Potential Connector Fit	Examples
HLUC1	Encourages consumer demand shift via price signals, financial rewards, tariff switching	- **EDDIE**: Good for aggregator/DSO data (real-time signals, metering) - **GA**: Could integrate consumer-facing apps easily - **ESMF**: If advanced digital twin modelling is needed	Austria Pilot (Price-driven aggregator scenario) might rely on EDDIE to handle official meter data and aggregator bidding. GA can also link small-scale consumer apps. ESMF adds deeper modelling only if needed (e.g., a digital twin of the home).

HLUC2	Focus on voluntary shifts via gamification, CO_2 footprint, badges, or social recognition	- **GA**: Quick bridging for user-facing app notifications - **ESMF**: If we want digital twin data about device usage or occupant patterns	Spain Pilot (Non-financial EV-charging incentives). If more complex occupant-level modelling is required, ESMF can help. If only simple app communication is needed, the GA might suffice.
HLUC3	Educates consumers about new technologies, efficiency potential, ROI of adoption	- **EDDIE**: Might help gather official data from DSOs to estimate ROI - **ESMF**: Detailed digital twin approach for device modelling - **GA**: Quick aggregator - knowledge-engine link	Bulgaria Pilot might use EDDIE for existing meter data and ESMF for modelling new home devices. Meanwhile, the GA would be enough if just bridging a single aggregator or consumer portal to a knowledge engine.
HLUC4	DSOs or TSOs broadcast urgent signals to reduce or shift load in critical times	- **EDDIE**: Strong real-time data flows for aggregator/DSO - **GA**: Provides a straightforward channel to push notifications to apps	Sweden Pilot (Grid vulnerability in southern region). EDDIE can handle TSO-based real-time signals. GA can integrate smaller local devices. ESMF is optional unless the pilot needs to thoroughly model assets' states over time.

HLUC5	Broad consumer guidance without direct financial or DR signals	- **GA**: Easiest if tips are short semantic messages - **ESMF**: If the pilot wants a deeper twin approach that tracks changes in building insulation or occupant behaviour	Poland Pilot might rely on GA for simple push messages to consumer apps. If the pilot aims for sophisticated building-level models (like occupant comfort modelling), ESMF can come into play. EDDIE is less relevant unless real-time DSOs data is needed

5. INTEROPERABILITY PROFILES CONSTRUCTION

This section focuses on the CERF interoperability profiles. The methodology for the definition of the interoperability profiles is first defined. One profile is then defined for each of the three main interface types:

- The energy app interface
- The data sources interface
- The DSO interface

The Behavioural and Policy interoperability layers are first defined in common for all interfaces, followed by the three interfaces profiles. Each interface is first described through its interoperability scenario, point and case, followed by the transport, syntactic and semantic layers of each profile.

5.1. METHODOLOGY

The construction of the data profiles was based on the ISO/IEC JTC 1/SC 41 standard on Internet of Things and related technologies [42]. It defines a structure for an interoperability profile, divided into five categories, as described in the figure below.

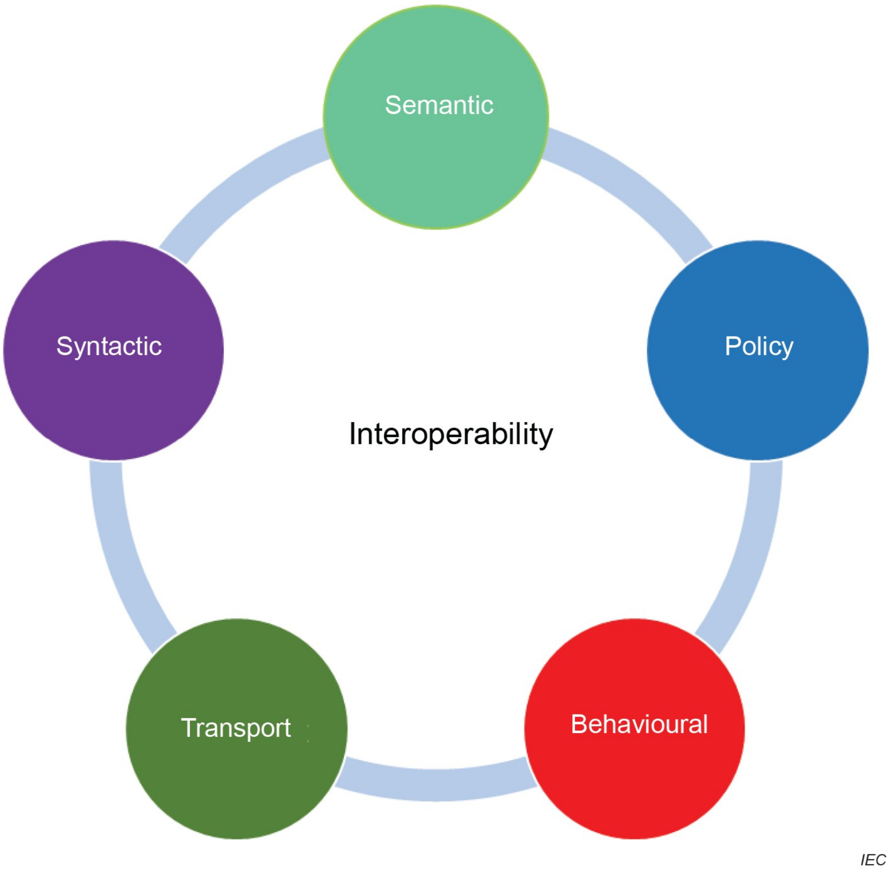


Figure 41: Interoperability profile categories

For each category, the functionalities required are first defined, then the relevant standards are reviewed to check which standards provides these functionalities. Finally, the profile defines guidelines for implementation.

5.2. INTEROPERABILITY PROFILES FOR THE CERF ARCHITECTURE

The interoperability profiles for the CERF architecture were selected based on the API interfaces that can provide services to end users and fulfil the project use cases (as identified in Deliverable D4.1 ECLIPSE DIGITAL CERF for Energy Saving applications_V1).

They represent the main interoperability points where information, control and business interactions cross organisational and system boundaries.

In the current generic implementation, these points rely on APIs and bilateral data exchanges.

In the future Data Space enabled architecture, these same points will be supported by sovereign connectors, ensuring data governance, trust, and policy enforcement in line with the principles of ISO/IEC 21823-5 (behavioural and policy interoperability).

Together, the three profiles cover the essential interoperability needs for achieving one of the ECLIPSE DIGITAL project objectives of establishing specifications for digital environments that provide real-time feedback on energy mix, grid status, consumption, and savings advice, where by applying AI and ML, ECLIPSE DIGITAL apps deliver personalised recommendations and facilitate participation in flexibility programs. The ECLIPSE DIGITAL CERF introduces standard interfaces and protocols to ensure interoperability among various energy-saving applications, reducing market barriers and enhancing consumer confidence.

5.2.1. BEHAVIOURAL INTEROPERABILITY

The behavioural interoperability layer is common for all three interoperability profiles of the CERF.

- **Technical functionality**

Enable the energy applications to integrate data space architecture, in order for the consumer to get information about the consumption and grid state, tips for optimizing the energy consumption, and express preferences.

- **Standards**
    - The Energy Transition Expertise Centre (ENTEC) has published a plan for the realisation of a Common European Energy Data Space. It outlines the use cases, data management, and business models for the development and use of a data space in a flexibility system [43].
    - Gaia-X has developed a framework for interoperability, that includes standards on architecture, access management, and data exchanges, that can be used to ensure the interoperability of complex systems, in particular for the use of data spaces in the energy sector [44].
    - PWI JTC1-SC41-8 – Behavioural and policy interoperability. This PWI is preparing a standard proposal covering trusted data sharing, leveraging the results of the European data space projects Omega-X, Enershare, and Int:net.
    - ISO/IEC PWI 25850 - Information technology — Cloud computing — Use cases for dataspaces. This PWI includes a use case on the use of data spaces in smart grids.
- **Guidelines for implementation**

The standards above should be used as guidelines to define the behaviour expected from the interface. In particular, the ENTEC documentation provides generic use-cases that should be matched to the system's use cases in order to develop a data space connector adapted to the use case of the project.

5.2.2. POLICY INTEROPERABILITY

The policy interoperability layer is common for all three interoperability profiles of the CERF.

- **Technical functionality**

Follow the mandatory requirements for the energy applications to integrate data space architecture, including mandatory components, features and interfaces.

- **Standards**
    - IDSA rulebook defines mandatory functional requirement, the regulatory framework and legal agreements to create and operate data spaces [45].
    - Gaia-X has developed a compliance document, providing rules to ensure organisational and semantic interoperability in the data exchange ecosystem. This includes design principles, contractual frameworks, data exchanges policies, cybersecurity and data protection [46].

- **Guidelines for implementation**

The IDSA rulebook and the Gaia-X compliance document should be used as guidance in order to develop a data space to be used in smart grids.

5.3. ENERGY APP INTERFACE

5.3.1. INTEROPERABILITY SCENARIO

The Energy App provides real-time feedback and personalised recommendations to end users based on consumption data, flexibility events, and market signals obtained from multiple backend systems.

The key interoperability challenge in real-life deployments is that the app sits at the edge of the system (directly with the prosumer or household) but depends on heterogeneous data flows across different actors (aggregators, DSOs, markets, platforms).

5.3.2. INTEROPERABILITY POINT

- **Generic:** The Energy App backend where APIs from DSOs, aggregators, and data sources converge to produce messages and insights for the user.
- **Data Space–enabled:** The App Connector, which mediates access to external data spaces, applying data contracts and policy enforcement.

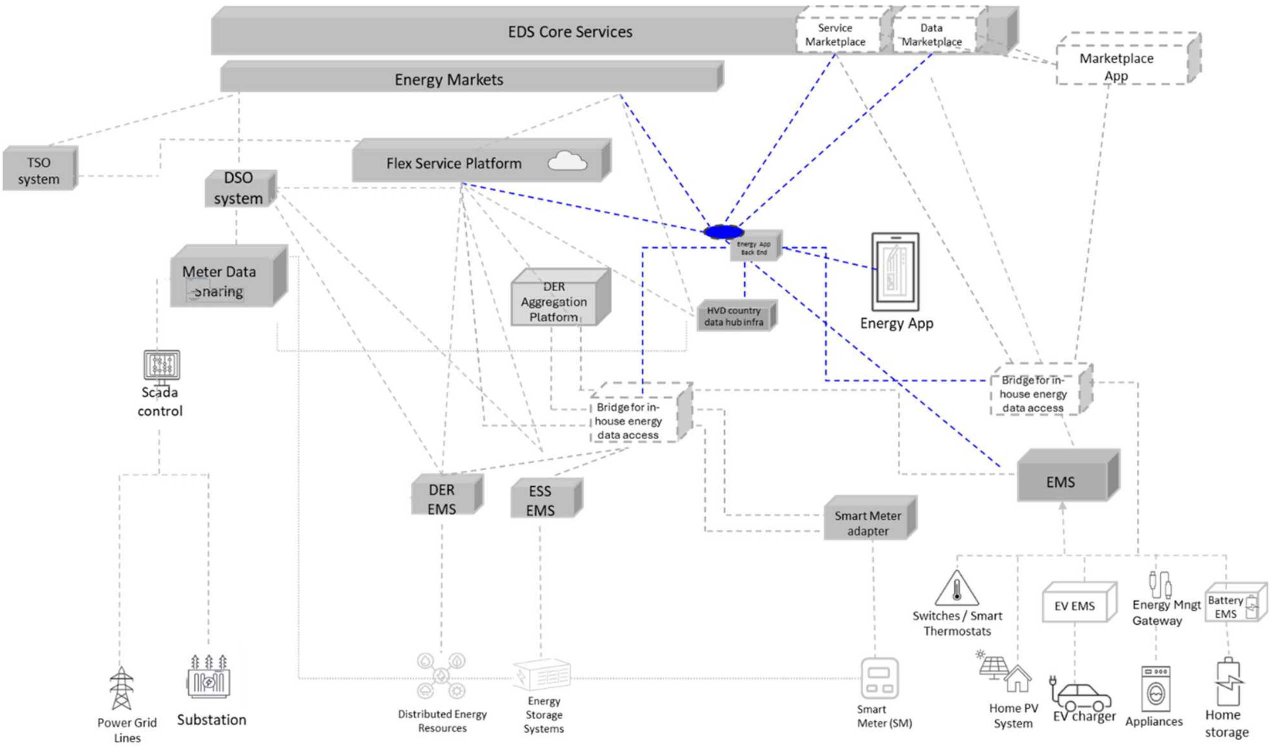


Figure 42: Energy app linked Interoperability Point

5.3.3. INTEROPERABILITY CASE

This point ensures that data from heterogeneous actors (DSO, aggregator, flexibility platform) is harmonised so that the app can deliver trusted, unified, and privacy-compliant feedback to the user.

Table 27: Energy App Interoperability Facets

Facet	Generic Implementation	Data Space–Enabled Implementation
Semantic	Harmonise terms such as *consumption*, *reward*, *flexibility event*, *notification*.	Adopt shared ontologies and Gaia-X metadata to ensure semantic alignment.
Technical	Integrate heterogeneous APIs (REST, MQTT) and handle latency/authentication differences.	Use connectors with standardised IDS/EDC interfaces, ensuring protocol compatibility and secure communication.
Organisational	Manual consent management and bilateral agreements.	Policy-driven access control and consent management governed by IDSA Rulebook and Gaia-X Compliance Framework.

5.3.4. INTEROPERABILITY PROFILE

5.3.4.1. TRANSPORT INTEROPERABILITY

- **Technical functionality:**
  1. Provide secure REST channels over HTTPS for user-facing operations such as sign-in, profile updates, tariff changes, and report uploads.

2. Support lightweights publish-subscribe channels such as MQTT over TLS for high-frequency telemetry (e.g., second-by-second metering) and rapid event notifications.
3. Stream large data flows through high-throughput backbones (e.g., Kafka) to analytics and storage modules, ensuring user traffic remains responsive.
4. Enable event-driven notifications using mechanisms such as server-sent events, webhooks, or AMQP where required by pilots, so applications can react immediately to threshold breaches or demand-response signals.
5. Enforce strong authentication with OAuth 2.0/2.1 tokens and fine-grained scopes (e.g., read meter, write report, manage profile).
6. Protect all communication with TLS 1.3 encryption and record security events (e.g., failed logins, token misuse) to support audit and GDPR compliance.
7. Provide optional VPN or mutual TLS links, backed by PKI, for DSO/TSO exchanges that require additional security assurance on critical grid messages.
8. Implement retry and quality-of-service mechanisms (e.g., MQTT QoS 0/1/2) to guarantee reliable delivery over intermittent or low-bandwidth links such as GPRS or M-Bus.
9. Apply rate limiting and denial-of-service protection mechanisms at the gateway to ensure resilience against hostile traffic while maintaining availability for normal user and device operations.
10. Provide secure device onboarding and revocation flows using certificates or access keys, with processes for issuance, renewal, and cancellation as assets join or leave the Energy App ecosystem.
11. Maintain precise clock synchronisation (e.g., NTP/PTP with redundancy) across systems so that metering data, price

curves, and user actions align accurately for billing, settlement, and audit purposes.

- **Standards:**

1. **HTTPS REST**: Secure HTTP with RESTful resource design for create/read/update/delete operations; TLS protects payloads, intermediaries support caching, and mainstream stacks (e.g., Spring, .NET, React Native) provide native support. *(Source: all pilot sheets.)*
2. **MQTT 3.1.1**: Lightweight publish/subscribe transport with 2-byte fixed header and QoS 0/1/2, well-suited to second- or minute-level metering over Wi-Fi/GSM; topics route via a broker and TLS adds confidentiality/integrity. *(Source: Pilots Austria, Croatia; Projects Independent, EDDIE, Hedge IoT, OMEGA-X.)*
3. **Apache Kafka**: Distributed commit log where readings and prices are immutable events in partitioned topics, enabling high-throughput replay for audits/AI while consumer groups process streams in real time. *(Source: Pilots Austria, Croatia, Spain; Project EDDIE.)*
4. **AMQP 1.0**: Enterprise messaging with link credits, routing, and ordering guarantees; applied as an outbound connector for bulk notifications and legacy integrations. *(Source: Pilot Austria.)*
5. **Webhooks**: Event callbacks that POST JSON to a subscriber URL on trigger (e.g., threshold breach), providing instant push without persistent client connections. *(Source: Pilots Austria, Slovenia.)*
6. **SOAP/HTTP (OpenADR 2.0b)**: XML event messages inside SOAP over HTTPS with digital signatures for authenticity and non-repudiation; required by several UK ESA deployments. *(Source: Tomorrow's Homes Today.)*
7. **NGSI-LD REST (Server-Sent Events)**: JSON-LD entity API with CRUD, subscriptions, and SSE streams to push real-time

updates of prices or metering changes to subscribers. *(Source: Projects OMEGA-X, Hedge-IoT.)*

8. **P1 smart-meter interface**: Consumer serial port (≈115 kbaud) emitting OBIS-coded telegrams every few seconds; a gateway translates serial frames to MQTT or REST for cloud ingestion. *(Source: Pilot Austria; Project EDDIE.)*
9. **Wireless M-Bus**: Sub-GHz metering radio (EN 13757-4) using AES-128 frame security; concentrators collect frames and forward them to backend services. *(Source: Pilot Poland.)*
10. **IEC 60870-5-104**: Telecontrol over TCP/IP carrying status changes and measured values between control rooms and field devices; retained as a fallback for critical switching paths. *(Source: Pilots Portugal, Spain.)*
11. **ICCP (IEC 60870-6 TASE.2)**: Inter-control-centre protocol exchanging high-rate SCADA points via predefined DataSets, with options for secure sessions. *(Source: Pilot Spain.)*
12. **Modbus TCP/RTU**: Register-based polling over Ethernet (TCP) or RS-485 (RTU); still common in inverters and heat pumps due to firmware simplicity. *(Source: Pilot Spain; Project WEDISTRICT.)*
13. **DNP3**: Event-driven protocol with source-timestamped points and Secure Authentication, used for feeder automation where latency and auditability matter. *(Source: Pilot Spain.)*
14. **OPC XML-DA / OPC UA**: OPC XML-DA exposes field data via XML/HTTP, while OPC UA adds a binary TCP stack, discovery, sessions, and built-in PKI for vendor-neutral PLC access. *(Source: Pilot Spain.)*
15. **SPARQL/HTTP**: Standards-based query endpoint over HTTP for triplestores holding CIM/SAREF graphs (e.g., “heaters in zone B with power > 2 kW”). *(Source: Project InterConnect.)*

16. **TLS 1.2 / TLS 1.3**: Transport encryption for all channels; 1.3 removes obsolete ciphers and 0-RTT is typically disabled to prevent replay. *(Source: Pilots France, Croatia, Austria.)*
17. **OAuth 2.0**: Authorization framework issuing time-limited access tokens with fine-grained scopes and refresh flows, separating authentication from API access. *(Source: Pilots Czech Republic, Austria, Croatia.)*
18. **OpenID Connect**: Identity layer on OAuth 2.0 providing signed ID tokens and standard claims, enabling single sign-on and federated identities (e.g., national eID). *(Source: Pilot Croatia.)*
19. **AES-GCM-256**: Authenticated encryption mode providing confidentiality and integrity for payloads or at-rest telemetry files. *(Source: Pilot Austria.)*
20. **HMAC-SHA-256**: Symmetric message authentication code allowing constrained devices to sign messages and enable tamper detection with minimal overhead. *(Source: Pilot Croatia.)*
21. **IPsec VPN / MPLS VPN**: Site-to-site tunnelling (IPsec ESP) or carrier-provided isolation (MPLS L3VPN) to protect grid traffic over public or shared networks. *(Source: Pilot Spain.)*
22. **CAS protocol**: Central Authentication Service enabling single sign-on via redirect and service tickets across multiple utility portals. *(Source: Pilot Poland.)*
23. **Two-phase certificate authentication**: Mutual-TLS with personal X.509 presentation followed by PIN confirmation, establishing a strong client identity before data exchange. *(Source: Pilot Slovenia.)*
24. **GPRS backhaul**: 2G data path where loggers send HTTP or SMS packets over limited bandwidth, motivating payload compression and batching strategies. *(Source: Pilot Slovenia.)*

Standards Guidelines for Implementation: This subsection provides guidelines for implementing transport standards within CERF. The evaluation and prioritisation of transport standards follows a principles-based approach built around three checks, described below. The outcome of this analysis is summarised in Table 28, which indicates which standards are recommended as defaults and which are optional or pilot specific.

- **Evaluation and Prioritisation of Transport Standards:** A principles-based selection focused on three checks:
  - **Fitness to the transport-layer technical functionalities** (secure REST, pub/sub, streaming, event notifications, authN/authZ, TLS, VPN/mTLS, QoS/retry, DDoS protection, device onboarding/revocation, time sync).
  - **Proven reuse in EU projects/pilots** (in active use in comparable contexts).
  - **Readiness to implement** (mature specifications, widely available brokers/clients/gateways, managed services, and reference configurations).

Table 28: Prioritisation of Transport Standards

Standard	When it matters most	Priority	Priority rationale & sources
HTTPS REST	Managing user profiles, device settings, tariffs, and application data	High	Widely adopted pattern for secure external APIs; protected with TLS and supported natively in all frameworks. Used across all pilot documentation.
MQTT 3.1.1	High-frequency telemetry and alerts from devices	High	Lightweights publish–subscribe with QoS options, suitable for Wi-Fi and GSM. Applied in Austria and Croatia pilots, and in EU projects Independent, EDDIE, Hedge-IoT, and OMEGA-X.
TLS 1.2/1.3	Channel encryptions for all transports	High	Mandatory for end-to-end confidentiality and integrity. TLS 1.3 preferred, TLS 1.2 allowed only for

			legacy cases. Required in France, Croatia, and Austria pilots.
OAuth 2.0	Token-based API access control	High	Provides scoped, short-lived tokens for secure API access. Used in Czech Republic, Austria, and Croatia pilots.
OpenID Connect	Federated login/SSO for user apps	High	Extends OAuth with signed ID tokens and single sign-on. Implemented in the Croatia pilot with national eID integration.
AES-GCM-256	Authenticated encryption for payloads/at-rest	High	Ensures confidentiality and integrity of sensitive data with modern encryption. Applied in Austria pilot security setups.
Apache Kafka	High-throughput streaming to analytics/storage	Medium	Provides partitioned topics, replay, and high-throughput streaming for analytics and AI. Used in Austria, Croatia, and Spain pilots and the EDDIE project.
AMQP 1.0	Enterprise queues, legacy connectors	Medium	Enables enterprise-grade queuing and ordered delivery. Demonstrated in the Austria pilot.
Webhooks	Event callbacks to third-party endpoints	Medium	Pushes JSON payloads to endpoints for instant notifications. Applied in Austria and Slovenia pilots.
NGSI-LD REST (SSE)	Real-time entity updates via SSE	Medium	JSON-LD with subscriptions and server-sent events for live updates. Implemented in OMEGA-X and Hedge-IoT projects.
SOAP/HTTP (OpenADR 2.0b)	DR where certification/legacy SOAP is mandated	Medium	XML over SOAP with digital signatures, required for certified Demand Response in the United Kingdom (Tomorrow's Homes Today pilot).
P1 smart-meter interface	Serial OBIS feed from consumer meters	Medium	Serial output of OBIS telegrams converted to MQTT/REST at the gateway. Used in Austria pilot and EDDIE project.
Wireless M-Bus	Sub-GHz metering links	Medium	Low-power radio with AES-128 security, forwarding via concentrators. Applied in Poland pilot.
IPsec VPN / MPLS VPN	DSO/TSO links requiring network isolation	Medium	Provides encrypted tunnels or carrier-grade isolation for grid traffic. Observed in Spain pilot.
HMAC-SHA-256	Lightweight message signing for constrained IoT	Medium	Ensures tamper detection with symmetric keys on small devices. Documented in Croatia pilot.
IEC 60870-5-104	Telecontrol between control room and field	Low	TCP/IP variant for telecontrol and emergency switching. Used in Portugal and Spain pilots.

ICCP (IEC 60870-6 TASE.2)	Control-centre to control-centre telemetry	Low	Exchanges SCADA data between control centres with predefined datasets. Applied in Spain pilot.
Modbus TCP/RTU	Legacy RTUs/inverters polling	Low	Register-based protocol still common in inverters and RTUs. Seen in Spain pilot and WEDISTRICT project.
DNP3	Feeder automation with source timestamps	Low	Provides secure, event-driven telemetry with timestamps. Referenced in Spain pilot.
OPC XML-DA / OPC UA	Vendor-neutral PLC/SCADA access	Low	Provides vendor-independent access to PLC/SCADA data with XML or binary encodings. Applied in Spain pilot.
SPARQL/HTTP	Querying the semantic graph store	Low	Exposes standard HTTP query endpoints for CIM/SAREF graphs. Implemented in InterConnect project.
CAS protocol	Legacy SSO in utility portals	Low	Provides single sign-on through redirects and service tickets. Still in use in Poland pilot.
Two-phase certificate auth	Strong client identity at onboarding	Low	Combines mutual TLS with personal X.509 certificates and PIN verification. Implemented in Slovenia pilot.
GPRS backhaul	2G-only sites with limited bandwidth	Low	Enables data transfer over 2G with batching and compression. Applied in Slovenia pilot.

Each standard is assigned a priority level: **High** (should be implemented by default), **Medium** (should be used when that scope appears (metering, market, substation, dataspace, buildings, optimisation)), **Low** (should be used selectively if it clearly adds value).

- **Priority-Based Implementation Guidelines:**

1. **High (should be implemented by default)**
    - **HTTPS REST:**
        - All external endpoints shall operate over TLS, with plain HTTP disabled or redirected under HSTS.
        - Resources shall follow a RESTful, resource-oriented URI design with correct method semantics (GET safe and

    idempotent; PUT idempotent; POST for creation; PATCH for partial updates; DELETE idempotent).
  - A consistent pagination style (cursor or limit/offset) shall be provided, and responses shall include navigation hints such as links.next/links.prev, and, where feasible, total or continuation indicators.
  - Cache validators (ETag, Last-Modified) and conditional requests (If-None-Match, If-Modified-Since) shall be supported to reduce bandwidth.
  - Error envelopes shall be uniform and machine-readable, including fields such as code, message, details, and correlationId.
  - Edge protections shall enforce rate limits, maximum request sizes, and strict content-type validation, returning 429 Too Many Requests with Retry-After during throttling.
  - Access, error, and audit logs shall propagate correlation IDs end-to-end while minimizing exposure of personal data.

- **TLS 1.3 (with controlled 1.2 fallback):**
  - TLS 1.3 shall be the default for all channels, with TLS 1.0 and TLS 1.1 disabled, and TLS 1.2 permitted only for explicitly authorised legacy integrations.
  - Only strong cipher suites shall be enabled (e.g., TLS_AES_128_GCM_SHA256 or TLS_AES_256_GCM_SHA384; for TLS 1.2, ECDHE_ECDSA/RSA with AES-GCM).
  - Early data (0-RTT) shall be disabled to prevent replay attacks.
  - Server certificate validation, OCSP stapling, and minimum key sizes shall be enforced.
  - Mutual-TLS (mTLS) shall be applied for broker/device links or DSO/TSO circuits where the risk assessment justifies it.

    - A managed certificate lifecycle shall be maintained for issuance, renewal, and revocation (CRL/OCSP).

- **OAuth 2.0 (access control) + OpenID Connect (identity):**
    - Grant types shall match client capabilities: Authorisation Code with PKCE for user-facing applications, Client Credentials for service-to-service traffic, and Device Authorization for headless devices.
    - Access tokens shall be short-lived, and refresh-token rotation shall be enabled.
    - JWTs shall be signed with asymmetric keys published via JWKS.
    - Scopes shall be narrowly defined (e.g., meter.read, report.write, profile.manage).
    - Token introspection and revocation endpoints shall be exposed.
    - Authentication and authorisation events shall be forwarded to a SIEM under appropriate privacy controls.
    - OIDC ID tokens shall include only the required claims to minimise data exposure

- **MQTT 3.1.1 over TLS (Device telemetry):**
    - Brokers shall terminate TLS and authenticate clients via certificates or credentials; SNI/ALPN may be used where supported.
    - Topic hierarchies shall be namespaced (for example, eu/{pilot}/{site}/{device}/telemetry), and ACLs shall strictly limit publish/subscribe rights; wildcard subscriptions shall be constrained.
    - QoS levels shall be selected according to criticality (QoS 1 for telemetry, QoS 0 for non-critical logs, QoS 2 only when essential).

  - Retained messages shall publish the last-known state, and Last-Will Testament settings shall signal offline conditions.
  - Broker protections shall cap session and inflight limits, maximum payload size, and idle timeouts.
  - Any bridges (REST↔MQTT or Kafka↔MQTT) shall enforce authentication, scope mapping, and payload validation at the boundary.

- **AES-GCM-256 (Encryption at rest / payload-level):**
  - Sensitive payloads and archival stores shall use authenticated encryption (GCM) to ensure confidentiality and integrity.
  - Encryption keys shall be generated, rotated, and stored under an HSM/KMS, with separation of duties and documented rotation schedules.
  - Data-in-motion and data-at-rest protection boundaries shall be clearly documented to avoid redundant encryption patterns that may hinder observability and operations.

- **Common transport controls (apply to all channels):**
  - Time synchronization shall be maintained using redundant NTP/PTP sources to align metering, pricing, and user actions for settlement and audit.
  - DDoS protections and back-pressure mechanisms (SYN-flood protection, connection quotas, circuit breakers) shall be configured at ingress.
  - Device onboarding shall use PKI with certificate issuance, renewal, inventory, and revocation, and all credentials shall be stored in a secure vault.
  - Security events including failed logins, token misuse, and ACL denials shall be recorded with appropriate retention to meet audit and GDPR obligations.

2. **Medium (should be used when the scope appears)**
    - **Apache Kafka (Streaming backbone):**
        - Topic naming, key selection, and partition counts shall be standardised, with idempotent producers (enable.idempotence=true) and acks=all enabled for critical streams.
        - Exactly-once processing shall be configured where required, using transactional producers and a stable transactional.id.
        - Retention and compaction policies shall be defined per topic, and TLS/SASL, ACLs, and quotas shall protect brokers and prevent noisy-neighbour effects.
        - Dead-letter topics, replay procedures, and consumer-lag alerting shall be established to support recovery and audit.

    - **AMQP 1.0 (Queues/bridges):**
        - Durable queues and exchanges shall be provisioned with clear routing keys.
        - Link credits shall govern flow control.
        - Dead-lettering with exponential backoff shall be configured for error handling.
        - Links shall be protected with TLS/SASL.
        - Per-tenant isolation shall be enforced using virtual hosts and per-link permissions to segregate partner traffic.

    - **Webhooks (HTTP callbacks):**
        - Event callbacks shall be signed (for example, HMAC over canonical headers and body).
        - An Idempotency-Key header shall be honoured to prevent duplicate processing.

    - Delivery shall use exponential retry with jitter and bounded backoff.
    - Subscription verification handshakes and server-side event filtering shall be applied.
    - Delivery outcomes (status codes, timestamps) shall be surfaced for partner monitoring and incident response.

- **NGSI-LD REST with Server-Sent Events:**
    - Supported entity types and attributes shall be documented alongside a project @context.
    - SSE endpoints shall emit text/event-stream with periodic heartbeats.
    - Last-Event-ID shall be supported for resumable delivery.
    - Notification cadence and time-series retention shall be published to help subscribers size storage and processing pipelines.

- **SOAP/HTTP (OpenADR 2.0b):**
    - WSDL and XSD artefacts shall be published.
    - TLS and XML signature verification shall be enforced on all exchanges.
    - Canonical examples for oadrDistributeEvent, opt-in/opt-out, and cancellation flows shall be provided.
    - The VTN/VEN certificate lifecycle shall be specified for onboarding, rollover, and revocation

- **P1 smart-meter interface:**
    - Serial parameters (baud rate, parity) and OBIS checksum validation shall be enforced at the gateway.
    - Telegrams shall be timestamped on ingress and buffered across disconnections.

    - Telegrams shall be normalised to the common telemetry schema.
    - Forwarding shall use TLS-protected MQTT or REST for downstream processing.

- **Wireless M-Bus (EN 13757-4):**
    - Per-meter AES-128 keys and frame counters shall be managed to prevent replay.
    - Concentrators shall implement channel hopping and store-and-forward behaviour.
    - Frames shall be converted at the edge to the common telemetry schema to unify downstream handling.

- **IPsec VPN / MPLS VPN:**
    - IPsec ESP with IKEv2, strong ciphers, PFS, and explicit lifetimes shall be configured for critical operator links.
    - Tunnel health monitoring and failover procedures shall be documented.
    - Where carrier isolation is preferred, MPLS L3VPN segmentation and demarcation shall be specified.
    - Change-control requirements for control-centre links shall be defined.

- **HMAC-SHA-256 (Message signing):**
    - Per-device symmetric keys shall be issued.
    - Each request shall include a canonical string (method, path, body hash), a nonce, and a timestamp.
    - Replay windows shall be tight.
    - Signatures shall be verified before processing.
    - This control shall complement TLS to provide payload integrity on constrained links requiring independent verification.

3. **Low (should be used selectively when value is clear)**
    - **IEC 60870-5-104:**
        - Integration shall terminate at a hardened gateway with TLS or VPN tunnelling applied.
        - Unsolicited traffic shall be throttled.
        - Command paths shall be strictly audited.
        - Mappings to the internal telemetry model shall preserve timestamps and quality flags to maintain operational integrity.
    - **ICCP (IEC 60870-6 TASE.2):**
        - Associations shall be secured.
        - DataSet definitions shall be centrally governed and mapped to internal identifiers.
        - Link supervision, failover procedures, and backlog handling shall be documented to ensure reliable inter-control-centre exchanges.
    - **Modbus TCP/RTU:**
        - Comprehensive register maps (address, type, scale, unit, endianness, polling rate) shall be published.
        - Scaling and counter rollover shall be handled at the edge.
        - Values shall be converted immediately to the structured telemetry schema.
        - TCP variants shall be protected by TLS or VPN where practical.
    - **DNP3:**
        - Secure Authentication shall be enabled.
        - Event-driven reporting and source timestamps shall be preferred over polling.

  - Limits on unsolicited traffic shall be applied.
  - Gateway translation shall preserve event flags and timestamps to maintain auditability.

- **OPC XML-DA / OPC UA:**
  - OPC UA shall be preferred.
  - Certificate-based trust and granular nodeset permissions shall be used.
  - Browsing and subscription privileges shall be separated.
  - Type-safe mappings to internal streams shall be provided to ensure consistent downstream processing.

- **SPARQL/HTTP:**
  - Read-only endpoints shall be exposed for analytics under authentication, throttling, timeouts, and query caching.
  - Common query patterns (bounded LIMIT/OFFSET, restricted federation) shall be optimised to protect the triplestore under load.

- **CAS protocol:**
  - Legacy CAS shall be terminated at an identity broker that issues OIDC/OAuth tokens to downstream APIs.
  - Session lifetimes, ticket handling, and logout propagation shall be defined to avoid orphaned sessions.

- **Two-phase certificate authentication:**
  - Client authentication shall combine mutual-TLS with presentation of a personal X.509 certificate followed by a PIN step.
  - Retry and lockout rules shall be defined.
  - Certificate renewal and revocation procedures shall be documented to maintain strong client identity.

- **GPRS backhaul:**
  - For 2G sites, payloads shall be batched and compressed.
  - Retry windows shall accommodate high latency.
  - Offline buffering policies shall be defined to prevent data loss during coverage gaps.

5.3.4.2. SYNTACTIC INTEROPERABILITY

- **Technical functionality:**

1. Fix clear data formats for meter readings, price curves, device commands, reports, and tips, so nothing is guessed.
2. Give every API a public description file that tools can read, letting developers auto-generate client code.
3. Support JSON for live calls, JSON-LD for linked-data, CSV/XLSX for ad-hoc analysis, and CIM XML for bulk grid files.
4. Allow streaming payloads for high-rate telemetry and paged payloads for history downloads.
5. Mark every field with unit's kWh, kW, €, and standard time stamps, avoiding mis-interpretation.
6. Carry optional language tags so the same message body can be viewed in any EU language.
7. Keep strict version tags so new fields (for example, a "network fee" column) appear without breaking older client code.
8. Allow compressed or binary payloads (gzip for JSON, zip for CSV, CIM XML inside a zip) to save bandwidth on low-speed links such as rural mobile networks.
9. Provide a schema-registry end-point where every message version is stored and where clients can fetch validation rules on the fly, preventing bad data from ever hitting the core platform.

10. Support partial-update messages (delta or HTTP PATCH) so large device or tariff records can change one field without resending the full payload, saving bandwidth.
11. Embed simple hyperlinks to next resources inside each response (for example, a measurement links straight to its tariff or threshold), letting client apps discover everything they need without hard-coded paths.

- **Standards:**

1. **JSON**: UTF-8 text format using objects and arrays, widely supported in REST APIs, offering small payload size, low parsing cost, and compatibility with virtually all web/mobile frameworks. *(Source: Pilots Czech, France, Croatia, Spain, Sweden; multiple projects.)*
2. **JSON-LD**: JSON with a @context that resolves fields to IRIs, enabling lightweight linked-data payloads so terms like activePower map directly to semantic identifiers (e.g., SAREF or CIM). *(Source: Projects OMEGA-X, RESONANCE.)*
3. **XML**: Schema-validated, tag-based format suited for structured and regulated exchanges such as CIM network models and OpenADR 2.0b SOAP messages, ensuring strict typing and vendor interoperability. *(Source: Pilots Austria, Croatia, Poland, Portugal.)*
4. **CSV**: Plain-text tabular format used for large-scale data exports such as readings and invoices; easy to open in BI tools or Excel, human-readable, and highly compressible. *(Source: Pilots Poland, Slovenia, Portugal, Spain.)*
5. **XLS/XLSX**: Spreadsheet containers that extend CSV tables with formulas, pivot charts, and formatting, often used for downloads that include embedded analytics or dashboards. *(Source: Pilot Poland; Pilot Slovenia.)*

6. **CIM XML (IEC 61970-552)**: Canonical XML serialization of the Common Information Model, where each class/attribute is schema-defined, allowing DSOs to validate complete grid or market files before loading. *(Source: Pilot Austria; Project EDDIE.)*
7. **CIM RDF/XML**: RDF encoding of CIM classes expressed in XML for semantic querying; enables loading grid and market data into triple stores for SPARQL analysis, e.g., topology searches. *(Source: Project SYNERGY.)*
8. **RDF/OWL (Turtle)**: Compact, text-based syntax for exchanging ontologies such as SAREF or project-specific extensions; easy to edit by humans and directly consumable by semantic tools. *(Source: Projects InterConnect, PARMENIDES, RESONANCE.)*
9. **XSD**: XML Schema Definitions specifying allowed elements, attributes, and datatypes; attached to files so malformed or non-compliant records are rejected before entering the system. *(Source: Pilot Austria.)*
10. **NGSI-LD / JSON-LD**: Context-broker API using JSON-LD to represent entities with temporal and geospatial attributes, supporting queries, subscriptions, and time-series operations for real-time streams. *(Source: Project OMEGA-X, Hedge-IoT.)*
11. **OpenAPI 3.x**: YAML/JSON specification describing endpoints, schemas, and security rules, enabling automatic client/server code generation and interactive developer documentation. *(Source: Pilot Czech; Projects SYNERGY, InterConnect.)*
12. **OpenADR 2.0b XML**: XML schemas and SOAP bindings defining DR event messages (e.g., <oadrDistributeEvent>), with digital signatures for certified ESA deployments. *(Source: Tomorrow's Homes Today; SENDER.)*
13. **OpenADR 3.0 JSON**: RESTful JSON profile carrying the same DR event semantics (IDs, signals, schedules) but with lower

overhead, better suited for mobile and IoT devices. *(Source: Tomorrow's Homes Today.)*

14. **Modbus register map (binary)**: Legacy binary protocol where fixed register offsets define measurement semantics, used to collect data from RTUs and inverters over serial or TCP links. *(Source: Project WEDISTRICT.)*
15. **ICCP DataSet structures**: IEC 60870-6 TASE.2 feature where pre-defined DataSets specify telemetry points exchanged between control centres, using compact binary frames for high-volume traffic. *(Source: Pilot Spain.)*

- **Standards Guidelines for Implementation:** This subsection provides guidelines for implementing syntactic standards within CERF. The evaluation and prioritisation of syntactic standards follows a principles-based approach built around three checks. First, candidate standards are assessed for their fitness to the technical functionalities of the syntactic layer. Second, they are checked for proven reuse in EU projects and pilots, with preference given to standards that are already applied in comparable contexts. Third, their readiness for implementation is evaluated. The outcome of this analysis is summarised in Table 29, which indicates which syntactic standards are recommended as defaults and which are optional or pilot specific.
  - **Evaluation and Prioritisation of Syntactic Standards:** We used a principles-based selection focused on three checks:
    - **Fitness to the technical functionalities of the syntactic layer** (clear payload formats, API description, streaming/paging, units & timestamps, i18n, versioning, compression, schema registry, partial updates, hyperlinks).
    - **Proven reuse in EU projects/pilots** (already used in practice within comparable contexts).

- **Readiness to implement** (machine-readable artefacts available, e.g., JSON Schema, OpenAPI 3.x, XSD, NGSI-LD API specs, example payloads).

Table 29: Prioritisation of Syntactic Standards

Standard	When it matters most	Priority	Priority rationale & sources
JSON	Day-to-day REST calls and device/app interactions	High	Ubiquitous, compact, and easy to parse across web/mobile stacks; used by multiple ECLIPSE DIGITAL project pilots for readings, tariff lookups, and commands (pilot evidence: Czech Republic, France, Croatia, Spain, Sweden).
JSON-LD	Live JSON that must carry stable identifiers for fields	High	Adds an @context without changing JSON shape so fields resolve to IRIs; applied in linked-data APIs in OMEGA-X and RESONANCE (project evidence).
OpenAPI 3.x	Public API description and client/server code-gen	High	Machine-readable contracts for endpoints/schemas/security enable SDK generation, mocks, and interactive docs (pilot evidence: CZ; projects: SYNERGY, InterConnect).
CSV	Bulk exports and ad-hoc BI analysis	Medium	Plain-text tables are universally importable and compress well for large histories and invoices (pilot evidence: Poland, Slovenia, Portugal, Spain).
XML	Regulated/structured exchanges	Medium	Namespaces plus schema validation fit regulated/structured exchanges such as CIM artefacts and OpenADR 2.0b SOAP (pilot evidence: Austria, Croatia, Poland, Portugal).
XSD	Validating XML payloads	Medium	Machine-readable definitions for XML elements/attributes/datatypes allow early rejection of malformed payloads (pilot evidence: Austria).
IEC 61970-552 (CIM XML)	Bulk grid/market files via CIM	Medium	Canonical CIM serialization validated before loading by DSO/TSO/market systems (pilot evidence: Austria; project evidence: EDDIE).
CIM RDF/XML	Triple-store/SPARQL analytics on CIM	Medium	CIM as RDF graphs enables SPARQL queries and topology analytics across pilots (project evidence: SYNERGY).
RDF/OWL (Turtle)	Exchanging ontologies/config profiles	Medium	Compact, human-readable syntax to publish ontologies and extensions consumed across partners (projects: InterConnect, PARMENIDES, RESONANCE).
NGSI-LD (JSON-LD)	Context-broker feeds (subscribe/query)	Medium	Context-broker API over JSON-LD supports real-time entities with temporal/geo attributes, queries, and subscriptions (projects: OMEGA-X, Hedge-IoT).
OpenADR 3.0 (JSON)	DR over REST/JSON	Medium	REST/JSON profile retains DR fields with lower overhead, suitable for mobile/IoT clients (project evidence: Tomorrow's Homes Today).
OpenADR 2.0b (XML/SOAP)	DR where certification/legacy SOAP is needed	Medium	Signed SOAP payloads for certified DR/ESA deployments in legacy or regulated environments

			(projects: SENDER; UK pilots such as Tomorrow's Homes Today).
XLS/XLSX	Human-friendly downloads with embedded analytics	Low	Spreadsheet downloads accompany CSV when formulas, pivots, or formatted dashboards are required (pilot evidence: Poland, Slovenia).
Modbus register map (binary)	Legacy RTUs/inverters at the edge	Low	Fixed registers over serial/TCP provide tiny, deterministic payloads for legacy RTUs/inverters, then normalised at the gateway (project evidence: WEDISTRICT).
ICCP (TASE.2) DataSet structures	Inter-control-centre telemetry	Low	Predefined DataSets in compact frames support high-volume inter-control-centre telemetry (pilot evidence: Spain).

Each standard is assigned a priority level: **High** (should be implemented by default), **Medium** (should be used when that scope appears (metering, market, substation, dataspace, buildings, optimisation)), **Low** (should be used selectively if it clearly adds value).

- **Priority-Based Implementation Guidelines:**

1. **High (should be implemented by default)**
    - **JSON:**
        - Use UTF-8 for all payloads and define a JSON Schema for each payload type so clients and validators can check requests and responses automatically.
        - Represent timestamps using ISO-8601/RFC 3339 with explicit timezone.
        - Express measurement units with UCUM; encode currency using ISO-4217 (e.g., EUR).
        - Implement predictable pagination (cursor or limit/offset).
        - Support ETag and Last-Modified headers for caching and conditional requests.
        - Enable gzip/deflate compression for large responses.
        - Support HTTP PATCH (RFC 6902 JSON Patch or RFC 7396 Merge Patch) to avoid resending full resources.
        - Include hyperlinks in responses (e.g., links.self, links.tariff) so clients can navigate without hard-coded paths.

- **JSON-LD:**
    - Expose a stable, versioned @context URL and keep older contexts resolvable.
    - Align JSON property names with the chosen semantic models so each field maps to a stable IRI.
    - Add BCP 47 language tags to translatable text.
    - Apply only backward-compatible context changes; never repurpose IRIs.
    - Mark deprecated terms clearly and publish short migration notes.
- **OpenAPI 3.x:**
    - Publish an OpenAPI 3.1 specification covering all endpoints, schemas, error envelopes, authentication scopes, and common headers.
    - Include concrete examples for typical and edge cases.
    - Mark deprecated operations and fields directly in the specification.
    - Ensure the document can generate SDKs, server stubs, and mock servers.
    - Link the OpenAPI file to the schema catalogue (JSON Schemas and SHACL shapes if applicable).
    - Version the specification with a changelog so client developers can track changes.

2. **Medium (should be used when the scope appears)**
    - **CSV:**
        - Publish CSV files as UTF-8 with a single header row and a dot (.) as decimal separator.
        - If units vary, include a dedicated unit column with UCUM codes; otherwise document fixed units in the header.

  - Provide a machine-readable CSV description (CSVW or JSON Table Schema).
  - Zip large exports.
  - Include standard columns for data-quality flags and time (start, end, granularity, timezone).
- **XML / XSD:**
  - Namespace every XML document and publish an XSD for validation.
  - Enforce XSD validation on ingestion.
  - Sign and verify XML documents when required (with TLS transport).
  - Version XML using namespaces or a top-level version attribute.
  - Provide valid and invalid sample files with expected validation messages.
- **IEC 61970-552 (CIM XML):**
  - State the exact CIM profile and version used.
  - Validate files against official IEC schemas before loading.
  - Document ESMP constraints for market-related processes.
  - Provide a mapping note showing how interface fields correspond to CIM elements and attributes.
- **CIM RDF/XML:**
  - Adopt the same CIM profile as in CIM XML.
  - Publish SPARQL query examples for common tasks (e.g., retrieving topology fragments).
  - Include guidance for identifier reconciliation so asset IDs, metering points, or market identifiers join reliably across systems.

- **RDF/OWL (Turtle):**
  - Version ontologies and publish explicit imports.
  - Maintain a short CHANGELOG for added, changed, or deprecated terms.
  - Provide minimal SHACL constraints for critical shapes so producers can catch common errors early.
- **NGSI-LD:**
  - Provide an NGSI-LD @context and document supported entity types and attributes (including temporal and geospatial properties).
  - Include subscription examples showing filters, geofencing, and temporal queries.
  - Clarify time-series retention and notification frequency so subscribers can size storage and processing.
- **OpenADR 3.0 (JSON):**
  - Define REST endpoints for creating, modifying, and cancelling events.
  - Require eventId, signalName, signalType, and intervals (explicit start and duration).
  - Use ISO-8601 timestamps throughout.
  - Publish a JSON Schema for each message type.
  - Include working examples for each flow so integrators can validate conformance quickly.
- **OpenADR 2.0b (XML/SOAP):**
  - Specify VTN/VEN roles and enforce TLS and XML signatures.
  - Publish WSDL/XSD files.
  - Provide minimal examples for oadrDistributeEvent, opt-in/opt-out, and cancellation flows with validation steps.

3. **Low (should be used selectively if it clearly adds value)**
   - **XLS/XLSX:**
     - Offer spreadsheets only as a companion to CSV for human-friendly downloads.
     - Include a clean "Data" sheet that mirrors the CSV exactly.
     - Keep formulas and visualizations on separate sheets.
     - Version the template to support troubleshooting.
     - Do not rely on XLS/XLSX for machine-to-machine integration.
   - **Modbus register map:**
     - Publish a complete register map for each device class (address, data type, scaling, unit, endianness, polling rate).
     - Handle scaling and counter overflows at the gateway.
     - Attach a trustworthy timestamp at ingress.
     - Convert readings to the project's JSON/JSON-LD format immediately for uniformity.
   - **ICCP (TASE.2) DataSets:**
     - Document DataSet definitions (identifiers, quality flags, update rates).
     - Map each point to internal fields so operators can trace values across systems.
     - Verify change-set semantics (what triggers updates).
     - Define retry/backoff and link-supervision behaviour to protect archives and dashboards during network issues.

5.3.4.3. SEMANTIC INTEROPERABILITY

- **Technical functionality:**

1. Expose a machine-readable vocabulary that lets energy apps describe user preferences (comfort bands, price ceilings, flexibility windows).
2. Capture appliance states and KPIs such as active power, energy, state of charge, tariff, run time, and health.
3. Describe event types of alerts, demand response offers, price notices, grid warnings, tips so every service reads them the same way.
4. Group heterogeneous devices into virtual assets or local communities and roll up their consumption, flexibility, and CO_2 savings.
5. Embed provenance tags (pilot site, data owner, consent ID) so later audits prove where each figure came from.
6. Provide version-controlled models so new device classes or new pilot countries plug in without breaking existing apps.
7. Attach regulatory tags (market role, grid zone, tariff code) so the same data feed can power both the user app and mandatory DSO/TSO or CO_2 reports without re-mapping.
8. Provide multilingual labels directly in the vocabulary, so the app displays the same concept correctly in every EU language and include accessibility metadata such as screen-reader descriptions or icons for inclusive use.
9. Add data quality flags (measured, estimated, missing, tampered) so optimisation engines know how much trust to place in each value before taking action.
10. Mark every value with a time validity window (start, end, granularity) so the app can safely mix real time feeds, day ahead forecasts and multi-year history in one screen.

- **Standards:**

1. **IEC CIM (IEC 61970, IEC 61968 core, IEC 62325-351 market)**: Reference information model for grid, metering, and market data used across EU TSO/DSO ecosystems; maintained in UML and available in RDF/OWL for semantic queries. *(Source: Pilot Austria; Projects SYNERGY, EDDIE.)*
2. **ETSI SAREF family (SAREF, SAREF4ENER/4BLDG/4CITY)**: Lightweight OWL vocabularies for devices, sensors, services, and buildings; well suited to JSON-LD and fine-grained appliance semantics. *(Source: Projects InterConnect, Independent, OMEGA-X; referenced in several pilot sheets.)*
3. **ESMP (European Style Market Profile)**: EU market profile that narrows CIM options (roles, IDs, documents) to improve cross-border interoperability; aligned with IEC 62325-351 and adopted in projects like EDDIE. *(Source: Project EDDIE.)*
4. **PAS 1878 / PAS 1879**: UK BSI specifications defining Energy Smart Appliance capability semantics and DR signal semantics (often paired with OpenADR 2.0b/3.0). *(Source: Tomorrow's Homes Today.)*
5. **IEC 61850**: Logical-node semantics for substation automation (measurements, states, events) frequently bridged to CIM for end-to-end data flows. *(Source: Pilot Croatia; Project SYNERGY.)*
6. **DLMS/COSEM (IEC 62056)**: OBIS-coded smart-meter semantics commonly mapped into CIM-based metering exchanges. *(Source: Project SYNERGY.)*
7. **OpenADR event model**: Fixed DR event vocabulary (e.g., *eiEventID, optType, signalName*) used in the Croatian pilot and

in projects such as SENDER and PARMENIDES. *(Source: Pilots Croatia; Projects SENDER, PARMENIDES.)*

8. **USEF (Universal Smart Energy Framework)**: Role/process model and semantic definition of flex offers for market-based demand response. *(Source: Project SYNERGY.)*
9. **IFC (ISO 16739)**: Building information semantics (floors/rooms/zones) providing spatial context for devices and NILM/HVAC use cases. *(Source: Project SYNERGY.)*
10. **PECO ontology**: SAREF-aligned community semantics (actors, assets, governance artefacts) for energy-community scenarios. *(Source: Project PARMENIDES.)*
11. **OMEGA-X Common Semantic Data Model (CSDM)**: Dataspace-oriented model aligning CIM and SAREF with data-sovereignty metadata. *(Source: Project OMEGA X.)*
12. **SHACL (Shapes Constraint Language)**: Semantic constraint language to enforce required properties/types/ranges on RDF/JSON-LD payloads. *(Source: Project Hedge IoT.)*
13. **RESONANCE ontology**: Combines SAREF/SEAS/CSDM to cover P2P and DSO-coordinated energy exchanges. *(Source: Project RESONANCE.)*
14. **SEAS (Smart-Energy Aware Systems) ontology**: Ontology for energy services, objectives, and context (e.g., optimization goals and time windows). *(Source: Project RESONANCE.)*

- **Standards Guidelines for Implementation:** This subsection provides guidelines for implementing semantic standards within CERF. The evaluation and prioritisation of semantic standards follows a principles-based approach built around three checks. The outcome of this analysis is summarised in Table 30, which indicates which semantic standards are recommended as defaults and which are optional or pilot specific.

- **Evaluation and Prioritisation of Semantic Standards:** We used a principles-based selection focused on three checks:
  - **Fitness to the technical functionalities of the Semantic standards layer** (does the standard directly enable the required capabilities?).
  - **Proven reuse in EU projects/pilots** (is it already used in practice within comparable contexts?).
  - **Readiness to implement** (are machine-readable artefacts available, e.g., RDF/OWL, JSON-LD contexts, SHACL shapes?).

Table 30: Prioritisation of Semantic Standards

Standard	When it matters most	Priority	Priority rationale & sources
ETSI SAREF / SAREF4ENER / 4BLDG / 4CITY	Canonical device/app semantics (assets, states, KPIs, preferences)	High	Referenced by project requirement DAT_021 in Deliverable “D2.2 Energy services analysis, use cases, and CERF requirements” for adopting standard ontologies for the Energy App; applied in InterConnect; used in SYNERGY; aligned with CIM in OMEGA-X CSDM; and used as a taxonomy in int:net.
SHACL	Semantic validation and conformance for all payloads	High	Used across EU work: ENERSHARE pilot shapes, IDS Dataspace Protocol response compliance, data.europa.eu MQA for DCAT-AP, and the ETSI SAREF Pipeline (CI checks). Recommended in ECLIPSE DIGITAL project as the semantic conformance gate.
IEC CIM (61970/61968, 62325-351)	Aligning with DSO/TSO systems or market artefacts	Medium	Referenced by project requirement DAT_023 in Deliverable D2.2 (CIM + 62325 for market exchanges) and reinforced by APP_030 in Deliverable D2.2 (apps should support CIM/ESMP); implemented in SYNERGY/SYNERGIES and used by the Austria pilot.

ESMP (CIM market profile)	Cross-border market documents, roles/IDs	Medium	Covered in DAT_023 (Deliverable D2.2) acceptance criteria (consistency with IEC 62325 ESMP) and APP_030 in Deliverable D2.2 acceptance criteria (ESMP version of CIM), adopted in EDDIE for accounting-point master data, and applied in the Austria pilot as the basis for CIM-based exchanges.
OpenADR (event terms)	Demand-response events/offers/ alerts/requests	Medium	Fit in the ECLIPSE DIGITAL requirements DAT_020 in Deliverable D2.2 (use standard protocols and data models) when DR is in scope, used in SENDER, implemented in the Croatia pilot, and applied in PARMENIDES for EMS/DSO/HEMS messaging.
DLMS/ COSEM (IEC 62056)	Smart-meter OBIS data is ingested	Medium	Listed in the ECLIPSE DIGITAL Grant Agreement among the standardised formats to be evaluated and implemented in SYNERGY/SYNERGIES as the semantic model for smart-meter data.
IEC 61850	Substation/SCADA semantics are ingested	Medium	Listed in the Grant Agreement among standardised formats to evaluate, referenced in SYNERGY/SYNERGIES for logical-node semantics, and in the Croatia pilot.
OMEGA-X CSDM	Operating in a dataspace with policy/sovereignty metadata	Medium	OMEGA-X CSDM is aligned with the ECLIPSE DIGITAL project requirement (DAT_020 (Deliverable D2.2): semantic interoperability for energy dataspaces), merging CIM with SAREF and adding sovereignty metadata for dataspace exchange.
IFC (ISO 16739)	Floor/room/zone spatial context is needed	Medium	IFC is applied in SYNERGY/SYNERGIES to provide spatial semantics (floors/rooms/zones) for NILM/HVAC and UI mapping.
SEAS	Optimization goals/constraints are exposed	Medium	Project evidence (RESONANCE) where SEAS is combined with SAREF/CSDM to express optimisation objectives/constraints.
USEF	Modelling DR market processes/roles in the app	Low	USEF is referenced in SYNERGY/SYNERGIES as part of semantic frameworks, supporting role and process modelling in demand-response scenarios. (no direct DAT_ requirement, but aligned with APP_018–022 (Deliverable D2.2) on flexibility offers and aggregators)
PAS 1878 / 1879	UK Energy-Smart Appliance semantics are specifically needed	Low	PAS 1878/1879 appear in the ECLIPSE DIGITAL requirements (APP_038 (Deliverable D2.2): semantic models for smart appliances and flexibility services) and are applied in Tomorrow’s

			Homes Today with OpenADR for UK-specific demand-side response.
PECO (PARMENIDES)	Energy-community actors/assets/governance	Low	PECO is defined in PARMENIDES as a SAREF-aligned ontology for community actors, assets, and governance artefacts. (no explicit DAT_ requirement, but relevant to APP_064–066 (Deliverable D2.2) on community/collective energy services)
RESONANCE ontology	Hybrid P2P + DSO semantics	Low	RESONANCE integrates SAREF, SEAS, and OMEGA-X CSDM, introducing an MQTT-based Semantic Resource Interface for hybrid P2P/DSO coordination. (not linked to a specific DAT_ requirement, but relevant to APP_073–076 (Deliverable D2.2) on hybrid flexibility)

Each standard is assigned a priority level: **High** (should be implemented by default), **Medium** (should be used when that scope appears (metering, market, substation, dataspace, buildings, optimisation)), **Low** (should be used selectively if it clearly adds value).

- **Priority-Based Implementation Guidelines:**
  1. **High (should be implemented by default)**
     - **ETSI SAREF family (SAREF, SAREF4ENER/4BLDG/4CITY):**
       - Publish versioned JSON-LD contexts for each payload type (e.g., Device, MeterReading, TariffPeriod, Preference).
       - Use SAREF/SAREF4ENER classes and properties consistently to represent assets, operational states, KPIs, and user preferences or flexibility windows.
       - Maintain a compact crosswalk per payload (interface field → SAREF term) so implementers can trace every field to its semantic identifier and manage changes without breaking clients.

     - **SHACL:**

  - Provide SHACL shapes for each payload specifying target class, required properties, datatypes, value ranges, and controlled vocabularies.
  - Supply one valid and one invalid example per shape.
  - Execute SHACL checks in CI/CD so semantic conformance is verified on every release.

Common requirements (apply to all payloads):

  - Use UCUM for units and SKOS concept schemes with multilingual labels for enumerations.
  - Add OWL-Time instants and intervals with validity windows, resolution, and timezone.
  - Attach PROV-O provenance (source, site, derivation).
  - Add DPV/ODRL only where consent, purpose, or usage constraints are relevant.

2. **Medium (should be used when the scope appears)**
   - **CIM / ESMP (market & operator alignment):**
     - Keep SAREF as the primary vocabulary when exchanging data with DSOs/TSOs or market platforms.
     - Provide mappings only for exchanged artefacts.
     - Maintain a compact crosswalk (interface field → SAREF term → CIM/ESMP class.property).
     - Reuse standard identifiers such as EIC codes and ESMP role codes.
     - Include one worked conversion example for each used document type.
     - Document the exact ESMP profile choices (roles, IDs, document variants).
     - Verify round-trip integrity (interface → CIM/ESMP → interface) in tests.

- **OpenADR (demand response):**
  - Bind DR payloads to OASIS Energy Interoperation terms (eiEventID, signalName, optType, marketContext, start/duration) in JSON-LD.
  - Publish a DR event SHACL shape that makes these fields mandatory and constrains enumerations, with valid and invalid examples.
  - Ensure ISO-8601 timestamps, explicit windows, and alignment with SAREF-based semantics.

- **DLMS/COSEM (IEC 62056) - smart metering:**
  - Provide an OBIS→SAREF/CIM crosswalk for common registers.
  - Represent quantities with SAREF properties and UCUM units (kWh, kW).
  - Include the original OBIS code as a code value.
  - Add a SHACL shape requiring OBIS, numeric value, unit, and timestamp.
  - Map to CIM MeterReading/ReadingType where relevant.

- **IEC 61850 (substation/SCADA):**
  - Map IEC 61850 Logical Nodes and data attributes to SAREF/CIM terms.
  - Publish a mapping table (LN.DA → SAREF/CIM).
  - Carry timestamp and quality/status flags and normalise units to UCUM.
  - Provide examples for typical feeds (measurements, status, alarms).
  - Verify sampling rate and quality semantics across the mapping.

- **OMEGA-X CSDM (data spaces)**:
    - Attach OMEGA-X CSDM policy and sovereignty metadata alongside SAREF/CIM terms.
    - Supply a SHACL shape for policy fields with MUST/SHOULD severities.
    - Provide example payloads showing policy-aware sharing.
    - Expose DCAT-AP metadata at catalogue level for dataset discovery and enforcement.

- **IFC (ISO 16739) (built environment)**:
    - Link devices to IFC spaces using persistent URIs and available room/floor identifiers or geometry.
    - Maintain a minimal mapping note (device → IFC space/zone).
    - Ensure location updates are versioned.
    - Align location properties with the SAREF device model.

- **SEAS (optimization semantics)**:
    - Annotate objectives and constraints with SEAS terms (cost/CO_2 targets, time windows, comfort bounds).
    - Link SEAS annotations to user preferences represented in SAREF.
    - Provide an example optimization request/response.
    - Provide a SEAS SHACL shape fixing required fields and allowed operators.
    - Ensure explicit time semantics (intervals, horizons) and units.

3. **Low (should be used selectively if it clearly adds value)**
    - **USEF:**
        - Apply only where market role or process semantics are required for flexibility workflows.

  - Keep USEF terms in a separate namespace and provide a mapping back to SAREF.

- **PAS 1878/1879:**
  - Use for UK Energy-Smart Appliance contexts.
  - Map appliance capabilities and DR signal semantics to SAREF/OpenADR terms.
  - Activate conditionally based on country or regulatory scope.

- **PECO (PARMENIDES):**
  - Use for energy-community scenarios (actors, assets, governance).
  - Map roles to application permissions or entitlements.
  - Provide a SAREF mapping note to avoid fragmentation of core payloads.

- **RESONANCE ontology:**
  - Reuse only minimal terms needed for hybrid P2P + DSO coordination.
  - Document compatibility with SAREF/SEAS/CSDM.
  - Include a mapping back to SAREF to keep interoperability deterministic.

5.4. DATA SOURCES INTERFACE (FLEXIBILITY & AGGREGATION)

5.4.1. INTEROPERABILITY SCENARIO

Energy resources (DERs, EMSs, smart meters) share operational and consumption data to allow the aggregator to analyse incentives and integrate participants into flexibility programs and reward schemes within the ECLIPSE DIGITAL ecosystem.

5.4.2. INTEROPERABILITY POINT

- **Generic**: The edge of the Technical Aggregator, where data from energy resources is collected, formatted, and sent toward the flexibility management system.
- **Data Space–enabled**: The Aggregator Connector, which intakes resource data and manages its sovereign publication into the Energy Data Space for flexibility and market analysis.

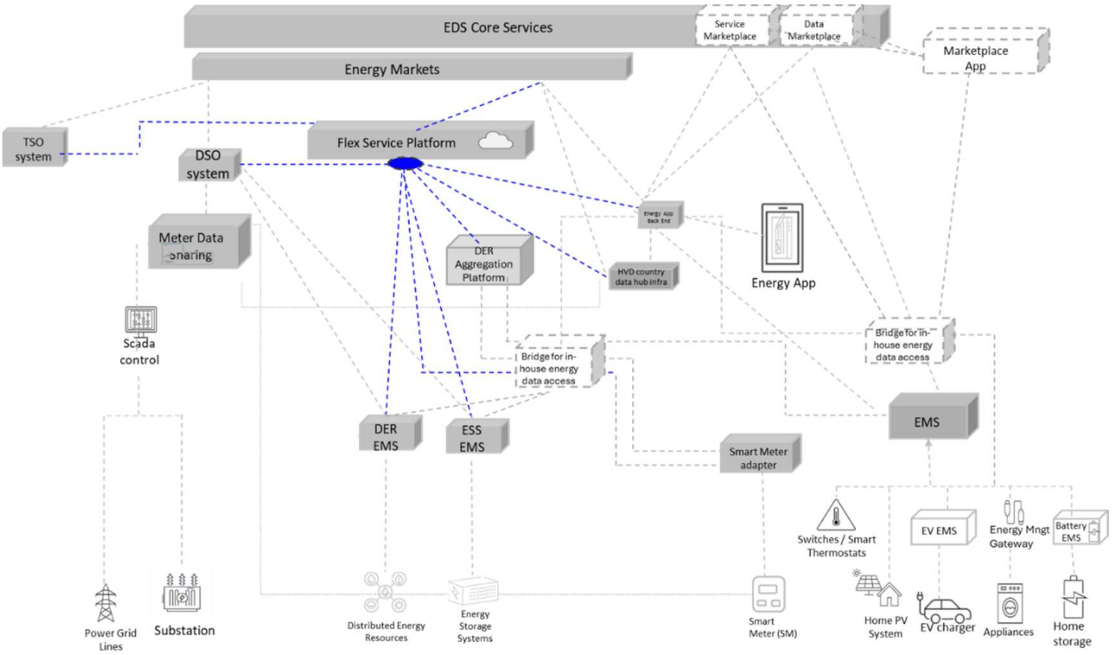


Figure 43: Data Sources Interface (Flexibility & Aggregation) Interoperability Point

5.4.3. INTEROPERABILITY CASE

This point enables distributed resources to interoperate with the aggregation and market platforms. It ensures that consumption, production, and flexibility potential are correctly shared and evaluated under consistent technical and contractual conditions.

Table 31: Interoperability Facets

Facet	Generic Implementation	Data Space–Enabled Implementation
Semantic	Normalise data models for load, flexibility availability, and incentive signals.	Apply CIM and SAREF-for-Energy ontologies with semantic annotations in data contracts.
Technical	Different APIs and file-based exchanges between resources and aggregator.	Connectors expose harmonised IDS/EDC interfaces and perform API translation while enforcing latency and security requirements.
Organisational	Bilateral NDAs and informal participation agreements.	Machine-readable usage control policies embedded in connectors define access rights, obligations, and retention periods.

5.4.4. INTEROPERABILITY PROFILE

5.4.4.1. TRANSPORT INTEROPERABILITY

- **Technical functionality:**
  1. Serve all Data-Sources endpoints (catalogue discovery, dataset metadata, data retrieval, consent) over encrypted transport with cache and precondition controls.
  2. Provide low-overhead pub/sub for near-real-time streams (metering series, price updates, device heartbeats) with configurable QoS, retained last state, and offline/last-will signalling.

3. Support high-throughput ingestion for bulk histories and event flows into analytics/settlement pipelines with scalable consumer groups and replay.
4. Deliver notifications (new/changed data, schema updates, consent changes, SLA alerts, emergency advisories) via signed push with retries, back-off, and de-duplication.
5. Enforce token-based access with short-lived, scoped tokens, per-tenant policies, and optional federated identity for operator portals and partner onboarding.
6. Tolerate intermittent gateways with buffering, batching, store-and-forward, and adaptive retry/QoS; harden ingress with rate limits, size limits, schema/content-type checks, circuit breakers, and DDoS shielding.
7. Operate certificate/key lifecycle for endpoints and brokers; keep clocks synchronised so timestamps align for verification/settlement; record security and delivery events with correlation IDs for audit and GDPR obligations.

- **Standards:**

1. **HTTPS REST**: Secure HTTP with RESTful resource design for create/read/update/delete operations; TLS protects payloads, intermediaries support caching, and mainstream stacks (e.g., Spring, .NET, React Native) provide native support. *(Source: all pilot sheets.)*
2. **MQTT 3.1.1**: Lightweight publish/subscribe transport with 2-byte fixed header and QoS 0/1/2, well-suited to second- or minute-level metering over Wi-Fi/GSM; topics route via a broker and TLS adds confidentiality/integrity. *(Source: Pilots Austria, Croatia; Projects Independent, EDDIE, Hedge IoT, OMEGA-X.)*
3. **Apache Kafka**: Distributed commit log where readings and prices are immutable events in partitioned topics, enabling high-throughput replay for audits/AI while consumer groups

process streams in real time. *(Source: Pilots Austria, Croatia, Spain; Project EDDIE.)*

4. **AMQP 1.0**: Enterprise messaging with link credits, routing, and ordering guarantees; applied as an outbound connector for bulk notifications and legacy integrations. *(Source: Pilot Austria.)*
5. **Webhooks**: Event callbacks that POST JSON to a subscriber URL on trigger (e.g., threshold breach), providing instant push without persistent client connections. *(Source: Pilots Austria, Slovenia.)*
6. **SOAP/HTTP (OpenADR 2.0b)**: XML event messages inside SOAP over HTTPS with digital signatures for authenticity and non-repudiation; required by several UK ESA deployments. *(Source: Tomorrow's Homes Today.)*
7. **NGSI-LD REST (Server-Sent Events)**: JSON-LD entity API with CRUD, subscriptions, and SSE streams to push real-time updates of prices or metering changes to subscribers. *(Source: Projects OMEGA-X, Hedge-IoT.)*
8. **P1 smart-meter interface**: Consumer serial port (≈115 kbaud) emitting OBIS-coded telegrams every few seconds; a gateway translates serial frames to MQTT or REST for cloud ingestion. *(Source: Pilot Austria; Project EDDIE.)*
9. **Wireless M-Bus**: Sub-GHz metering radio (EN 13757-4) using AES-128 frame security; concentrators collect frames and forward them to backend services. *(Source: Pilot Poland.)*
10. **IEC 60870-5-104**: Telecontrol over TCP/IP carrying status changes and measured values between control rooms and field devices; retained as a fallback for critical switching paths. *(Source: Pilots Portugal, Spain.)*
11. **ICCP (IEC 60870-6 TASE.2)**: Inter-control-centre protocol exchanging high-rate SCADA points via predefined DataSets, with options for secure sessions. *(Source: Pilot Spain.)*

12. **Modbus TCP/RTU**: Register-based polling over Ethernet (TCP) or RS-485 (RTU); still common in inverters and heat pumps due to firmware simplicity. *(Source: Pilot Spain; Project WEDISTRICT.)*
13. **DNP3**: Event-driven protocol with source-timestamped points and Secure Authentication, used for feeder automation where latency and auditability matter. *(Source: Pilot Spain.)*
14. **OPC XML-DA / OPC UA**: OPC XML-DA exposes field data via XML/HTTP, while OPC UA adds a binary TCP stack, discovery, sessions, and built-in PKI for vendor-neutral PLC access. *(Source: Pilot Spain.)*
15. **SPARQL/HTTP**: Standards-based query endpoint over HTTP for triplestores holding CIM/SAREF graphs (e.g., "heaters in zone B with power > 2 kW"). *(Source: Project InterConnect.)*
16. **TLS 1.2 / TLS 1.3**: Transport encryption for all channels; 1.3 removes obsolete ciphers and 0-RTT is typically disabled to prevent replay. *(Source: Pilots France, Croatia, Austria.)*
17. **OAuth 2.0**: Authorization framework issuing time-limited access tokens with fine-grained scopes and refresh flows, separating authentication from API access. *(Source: Pilots Czech Republic, Austria, Croatia.)*
18. **OpenID Connect**: Identity layer on OAuth 2.0 providing signed ID tokens and standard claims, enabling single sign-on and federated identities (e.g., national eID). *(Source: Pilot Croatia.)*
19. **AES-GCM-256**: Authenticated encryption mode providing confidentiality and integrity for payloads or at-rest telemetry files. *(Source: Pilot Austria.)*
20. **HMAC-SHA-256**: Symmetric message authentication code allowing constrained devices to sign messages and enable tamper detection with minimal overhead. *(Source: Pilot Croatia.)*

21. **IPsec VPN / MPLS VPN**: Site-to-site tunnelling (IPsec ESP) or carrier-provided isolation (MPLS L3VPN) to protect grid traffic over public or shared networks. *(Source: Pilot Spain.)*
22. **CAS protocol**: Central Authentication Service enabling single sign-on via redirect and service tickets across multiple utility portals. *(Source: Pilot Poland.)*
23. **Two-phase certificate authentication**: Mutual-TLS with personal X.509 presentation followed by PIN confirmation, establishing a strong client identity before data exchange. *(Source: Pilot Slovenia.)*
24. **GPRS backhaul**: 2G data path where loggers send HTTP or SMS packets over limited bandwidth, motivating payload compression and batching strategies. *(Source: Pilot Slovenia.)*

- **Standards Guidelines for Implementation:** This subsection provides guidelines for selecting transport standards in CERF. The evaluation uses a small set of checks covering relevance to CERF data sources, support for required transport functions, reuse in EU projects and implementation readiness. The resulting shortlist, which includes HTTPS REST, Webhooks, MQTT over TLS, Kafka and other widely deployed protocols, is prioritised for CERF use in Table 32.
- **Evaluation and Prioritisation of Transport Standards:** A principles-based selection focused on three checks:
  - **Data-Source relevance shortlist** (does it directly serve: catalogue/metadata & discovery, historical/NRT time-series, prices/tariffs, flexibility datasets, consent/policy; across REST, batch, and notifications/subscriptions?).
  - **Fitness to the technical functionalities of the transport standards layer** (does it enable: secure

request/response, pub/sub, streaming, push notifications, authN/authZ, reliability, PKI/time-sync?)

- **Proven reuse in EU projects/pilots** (is it already used in practice within comparable contexts?)
- **Readiness to implement** (are specifications mature and stable, with tooling, services, configurations, and test kits readily available?)

- **Shortlisted standards:** HTTPS REST, Webhooks (HTTP push), MQTT 3.1.1 over TLS, Apache Kafka, AMQP 1.0, NGSI-LD REST, OpenADR 3.0 JSON / 2.0b SOAP *(where mandated)*, TLS 1.3 *(with controlled 1.2 fallback)*, OAuth 2.0/2.1 + OpenID Connect, IPsec VPN / MPLS VPN *(where required).*

Table 32: Prioritisation of Transport Standards

Standard	When it matters most	Priority	Priority rationale & sources
HTTPS REST	Core request/response for catalogue,metadata, retrieval, consent	High	Required for machine-readable catalogue/discovery and dataset retrieval, supports cache validators and conditional requests to reduce load, already used by multiple pilots for public/partner APIs.
TLS 1.3 (1.2 fallback)	Encryption & integrity for every endpoint/stream	High	Meets the “all personal/sensitive data must be encrypted” requirement, supported by cloud/API gateways across pilots.
OAuth 2.0/2.1 + OIDC	Scoped API access; SSO for operator/partner portals	High	Provides short-lived, scope-based access aligned with consent and role controls; integrates with existing IdPs used by pilots; enables token revocation/introspection for audits.
Webhooks (HTTP push)	Push of dataset/metadata changes, consent updates, SLA/emergency notices	High	Delivers near-real-time updates without polling, supports signed delivery, retries, and de-duplication so partners can safely process once, used in pilot notification paths.
PKI lifecycle + time sync (NTP/PTP)	Certificates/keys; aligned timestamps for verification/settlement	High	Ensures certificate issuance/rotation/revocation for endpoints and brokers, time sync keeps timestamps consistent across providers for verification and reporting.
MQTT 3.1.1 over TLS	Low-overhead NRT telemetry/price feeds into the data space	Medium	Efficient over constrained links, QoS/retain/last-will suit gateways and HEMS, adopted in pilots for near-real-time ingestion.

Apache Kafka	High-throughput ingestion, replay, consumer groups for analytics/settlement	Medium	Handles large historical streams and event bursts, built-in replay and consumer isolation support audits and AI pipelines, used in project backbones.
AMQP 1.0	Enterprise queue bridges and legacy connectors	Medium	Provides interop with existing message brokers in operator environments, flow control and dead-lettering ease large-scale outbound notifications.
NGSI-LD REST	Dataspace/entity subscriptions with temporal/geo attributes	Medium	Matches dataspace patterns where entities and subscriptions are required, SSE offers lightweight streaming of changes, seen in dataspace-oriented pilots.
OpenADR 3.0 / 2.0b	Regulated DR event transport as data-source notifications	Medium	Kept for jurisdictions demanding certified DR message transport, otherwise REST/Webhooks cover notifications with lower overhead.
IPsec VPN / MPLS VPN	Private operator backhaul or partner links needing network isolation	Medium	Adds network-level isolation where policy or risk assessment requires it, aligns with operator practices observed in pilots.

Each standard is assigned a priority level: **High** (should be implemented by default), **Medium** (should be used when that scope appears (metering, market, substation, dataspace, buildings, optimisation)), **Low** (should be used selectively if it clearly adds value).

- **Priority-Based Implementation Guidelines:**

1. **High (implement by default):**
    - Serve all Data-Source endpoints over HTTPS with TLS 1.3; disable plaintext HTTP and enforce HSTS.
    - Apply a consistent REST style with resource URIs, correct methods, cache validators (ETag/Last-Modified), and conditional requests to reduce load.
    - Protect access with OAuth 2.0/2.1 and OpenID Connect: use short-lived, scoped tokens for APIs, enable federated identity for operator/partner portals, and support token introspection/revocation.
    - For outbound change notifications (dataset created/updated, schema change, consent change,

SLA/emergency advisory), use signed webhooks with a canonical event envelope (id, type, version, subject, time, data), HMAC signature header, exponential back-off with jitter, de-duplication keys, and an explicit subscription verification handshake.

  - Operate a managed PKI for servers, clients, and brokers (issuance, renewal, revocation/OCSP), and maintain redundant time synchronization (NTP/PTP) so timestamps align for verification and settlement.
  - Harden ingress with rate limits, request-size limits, schema/content-type validation, circuit breakers, and DDoS shielding, and expose Retry-After where applicable.
  - Record security and delivery events with correlation IDs, retaining only the minimum personal data required for GDPR-compliant audit.

2. **Medium (activate when the scope appears):**
  - When near-real-time device or market feeds must be ingested, deploy MQTT 3.1.1 over TLS with namespaced topics, strict ACLs, QoS levels chosen by criticality (e.g., QoS 1 for telemetry), and retained messages and last-will for session awareness.
  - For high-volume analytics or settlement pipelines, use Apache Kafka with TLS/SASL, idempotent producers (acks=all), consumer-group isolation, retention and compaction policies, dead-letter topics, and documented replay procedures.
  - Where enterprise queues already exist, bridge via AMQP 1.0 with TLS/SASL, link-credit flow control, and dead-lettering.
  - If a dataspace or entity-style API is required, expose NGSI-LD REST with Server-Sent Events for live updates

(heartbeats, Last-Event-ID, resumable delivery), ensuring a 1:1 mapping to Data-Source entities.
- In jurisdictions that mandate certified DR transport, support OpenADR 3.0 JSON (preferred) or OpenADR 2.0b SOAP behind a gateway and publish onboarding material (API description or WSDL/XSD) together with certificate procedures.
- For operator backhaul isolation or partner-specific links, configure IPsec VPN (IKEv2, PFS) or carrier MPLS VPN with documented failover and monitoring.

Cross-cutting transport practices (apply to all):

- Apply mutual TLS whenever the risk level requires strong client authentication, such as for brokers or partner circuits.
- Prefer modern cipher suites like AES-GCM or ChaCha20-Poly1305 and disable TLS 0-RTT to prevent replay risks.
- Define explicit retry and replay rules for each channel:
  - Idempotency keys for HTTP and webhooks
  - QoS and retained messages for MQTT
  - Transactional or idempotent producers for Kafka
- Publish a partner conformance kit (OpenAPI, webhook signer/verifier, sample topics or records, Postman/CLI tests) so providers can validate their integrations before onboarding.
- Document SLOs for latency, throughput, and delivery guarantees to ensure verification and settlement processes rely on predictable message delivery.

5.4.4.2. SYNTACTIC INTEROPERABILITY

- **Technical functionality:**

1. Publish one versioned API specification for all Data-Sources endpoints so paths, parameters, headers, security scopes, and examples are consistent (e.g., OpenAPI 3.1).
2. Attach strict schemas to every request and response so messages are validated the same way across providers (e.g., JSON Schema for JSON/JSON-LD; XSD for XML; CSVW/JSON Table Schema for CSV; Avro/JSON-Schema for streams).
3. Fix common data conventions so files and APIs parse uniformly: timestamps with time zone (ISO-8601/RFC 3339), units (UCUM), currency codes (ISO-4217), numeric precision, identifier formats, and explicit null/NA rules.
4. Standardise time-series access with start/end filters and fixed granularities, server-driven pagination with navigation links (self/next/prev), and negotiated compression for large results (e.g., gzip).
5. Protect concurrent updates and enable caching by supporting partial updates where relevant (JSON Merge Patch / JSON Patch) and enforcing HTTP preconditions (ETag/If-Match; Last-Modified/If-Modified-Since).
6. Return a uniform error format and support safe retries using a standard problem body (e.g., RFC 7807) with type/code/title/detail and a correlation ID; make writes idempotent via an Idempotency-Key header.
7. Define standard batch and notification contracts: CSV import/export with machine-readable descriptors and checksums; webhook events with a canonical event format (id, type, version, time, subject, data), signed delivery (e.g., HMAC), retry with backoff, and de-duplication keys.

- **Standards:**

1. **JSON**: UTF-8 text format using objects and arrays, widely supported in REST APIs, offering small payload size, low parsing cost, and compatibility with virtually all web/mobile frameworks. *(Source: Pilots Czech, France, Croatia, Spain, Sweden; multiple projects.)*
2. **JSON-LD**: JSON with a @context that resolves fields to IRIs, enabling lightweight linked-data payloads so terms like activePower map directly to semantic identifiers (e.g., SAREF or CIM). *(Source: Projects OMEGA-X, RESONANCE.)*
3. **XML**: Schema-validated, tag-based format suited for structured and regulated exchanges such as CIM network models and OpenADR 2.0b SOAP messages, ensuring strict typing and vendor interoperability. *(Source: Pilots Austria, Croatia, Poland, Portugal.)*
4. **CSV**: Plain-text tabular format used for large-scale data exports such as readings and invoices; easy to open in BI tools or Excel, human-readable, and highly compressible. *(Source: Pilots Poland, Slovenia, Portugal, Spain.)*
5. **XLS/XLSX**: Spreadsheet containers that extend CSV tables with formulas, pivot charts, and formatting, often used for downloads that include embedded analytics or dashboards. *(Source: Pilot Poland; Pilot Slovenia.)*
6. **CIM XML (IEC 61970-552)**: Canonical XML serialization of the Common Information Model, where each class/attribute is schema-defined, allowing DSOs to validate complete grid or market files before loading. *(Source: Pilot Austria; Project EDDIE.)*
7. **CIM RDF/XML**: RDF encoding of CIM classes expressed in XML for semantic querying; enables loading grid and market data into triple stores for SPARQL analysis, e.g., topology searches. *(Source: Project SYNERGY.)*

8. **RDF/OWL (Turtle)**: Compact, text-based syntax for exchanging ontologies such as SAREF or project-specific extensions; easy to edit by humans and directly consumable by semantic tools. *(Source: Projects InterConnect, PARMENIDES, RESONANCE.)*
9. **XSD**: XML Schema Definitions specifying allowed elements, attributes, and datatypes; attached to files so malformed or non-compliant records are rejected before entering the system. *(Source: Pilot Austria.)*
10. **NGSI-LD / JSON-LD**: Context-broker API using JSON-LD to represent entities with temporal and geospatial attributes, supporting queries, subscriptions, and time-series operations for real-time streams. *(Source: Project OMEGA-X, Hedge-IoT.)*
11. **OpenAPI 3.x**: YAML/JSON specification describing endpoints, schemas, and security rules, enabling automatic client/server code generation and interactive developer documentation. *(Source: Pilot Czech; Projects SYNERGY, InterConnect.)*
12. **OpenADR 2.0b XML**: XML schemas and SOAP bindings defining DR event messages (e.g., <oadrDistributeEvent>), with digital signatures for certified ESA deployments. *(Source: Tomorrow's Homes Today; SENDER.)*
13. **OpenADR 3.0 JSON**: RESTful JSON profile carrying the same DR event semantics (IDs, signals, schedules) but with lower overhead, better suited for mobile and IoT devices. *(Source: Tomorrow's Homes Today.)*
14. **Modbus register map (binary)**: Legacy binary protocol where fixed register offsets define measurement semantics, used to collect data from RTUs and inverters over serial or TCP links. *(Source: Project WEDISTRICT.)*
15. **ICCP DataSet structures**: IEC 60870-6 TASE.2 feature where pre-defined DataSets specify telemetry points exchanged between control centres, using compact binary frames for high-volume traffic. *(Source: Pilot Spain.)*

- **Standards Guidelines for Implementation:** This subsection provides guidelines for selecting syntactic standards in CERF. The evaluation follows four checks that cover relevance to CERF data sources, support for the required syntactic functions, reuse in EU projects and implementation readiness. Based on these checks, a shortlist of high-level API and file formats is retained, while low level constructs such as Modbus register maps and ICCP DataSet structures are excluded and expected to be normalised through the selected syntactic standards. The resulting prioritisation is summarised in Table 33.

- **Evaluation and Prioritisation of Syntactic Standards:** We used a principles-based selection focused on four checks:
  - **Data-Source relevance shortlist** (does it directly serve catalogue/metadata & discovery, historical and near-real-time time-series, prices/tariffs, flexibility datasets, and consent/policy objects across REST endpoints, batch import/export, and notifications/subscriptions?).
  - **Fitness to the technical functionalities of the syntactic standards layer** (does it support one versioned API spec, strict schemas, shared data conventions, time-window filters with predictable pagination/compression, partial updates with HTTP preconditions, a uniform error format, and idempotent writes?)
  - **Proven reuse in EU projects/pilots** (is it already used in practice within comparable contexts?)
  - **Readiness to implement** (are specifications mature and stable, with validators/examples, code-generation or schema registries, and clear versioning/deprecation?)

- **Shortlisted standards:** We did not retain Modbus register maps and ICCP DataSet structures in the syntactic shortlist, as these are low-level transport or control-centre protocols. Their data should instead be normalised and published through the retained API and file formats for interoperability.

Table 33: Prioritisation of Transport Standards

Standard	When it matters most	Priority	Priority rationale & sources
OpenAPI 3.x	One machine-readable contract for all Data-Source endpoints (paths, schemas, headers, security, examples)	High	Enables consistent clients, testing and docs across providers, used in CZ pilot gateways, aligned with D4.1 ECLIPSE DIGITAL CERF for Energy Saving applications_V1 API approach and WP3 (Architecture of a scalable and interoperable European open-source CERF and data sets) profiles.
JSON	Default wire format for REST responses/requests across catalogue, time-series, prices/tariffs, flexibility datasets	High	Universally supported and lightweight, widely used in CZ/FR/HR/ES/SW pilots and project stacks referenced in D4.1.
CSV (+ CSVW/JSON Table Schema descriptors)	Bulk export/import of historical metering and KPI tables and audit extracts	High	Human-friendly, compressible, standard in PL/SI/PT/ES pilots, descriptors make columns and types of machine-checkable (D4.1 data exchange patterns).
XML	Regulated or archival file exchanges where strict schema-validated typing is required	Medium	Applied in AT/HR/PL/PT pilots, complements JSON for batches, pairs with XSD for early rejection of malformed files.
XSD	Validation of XML datasets (e.g., CIM files or regulated payloads) before ingest	Medium	Ensures conformance at file boundaries, cited in AT pilot practices and D4.1 regulated exchanges.
CIM XML (IEC 61970-552)	Canonical XML serialization for grid/master data and market-adjacent batches published as datasets	Medium	Used in AT pilot and EDDIE lineage, ensures complete model validation prior to load, aligns with DAT_020/DAT_023 (Deliverable D2.2) “use standard models”.
CIM RDF/XML	Loading CIM graphs into triple stores for topology/market analysis and cross-source joins	Medium	Used in SYNERGY, useful when semantic analytics are required while retaining XML tooling.
JSON-LD	Embedding semantic identifiers in JSON payloads via @context for portability across sources	Medium	Applied in OMEGA-X/RESONANCE, keeps JSON while linking to CIM/SAREF terms where needed.

NGSI-LD (JSON-LD API style)	Context-broker entity streams for near-real-time datasets with temporal/geo attributes	Medium	Used in OMEGA-X/Hedge-IoT contexts, adopt when a broker pattern is in scope for Data-Source exposure.
OpenADR 3.0 JSON / 2.0b XML	Publishing demand-response event datasets where jurisdiction or partners require OpenADR	Medium	Seen in SENDER/THT contexts, include only when DR datasets are part of the Data-Source catalogue.
RDF/OWL (Turtle)	Exchanging controlled vocabularies/contexts referenced by the API (not runtime data)	Low	Used in InterConnect/RESONANCE, appropriate for publishing the vocabulary itself rather than operational payloads.
XLS/XLSX	End-user oriented downloads that need formulas/pivots (not system-to-system)	Low	Convenience over CSV in PL/SI pilots, keep for analyst exports, not for integration.

Each standard is assigned a priority level: **High** (implement by default), **Medium** (use when that scope appears (metering, market, substation, dataspace, buildings, optimisation)), **Low** (use selectively if it clearly adds value).

- **Priority-Based Implementation Guidelines:**

1. **High (implement by default):**
   - Publish a single versioned OpenAPI 3.x document covering all Data-Source endpoints: catalogue/metadata, dataset discovery, historical and near-real-time time-series, prices/tariffs, flexibility datasets, and consent/policy objects.
   - Ensure the specification defines paths, parameters, headers, security scopes, request/response bodies, worked examples, and includes a clear versioning and deprecation policy.
   - Use JSON as the default operational format and attach JSON Schema definitions to every request and response so providers validate messages consistently.
   - For bulk exchanges, offer CSV with CSVW/JSON Table Schema descriptors, fixed column order, explicit timezone columns, and checksums for data integrity.

- Standardise data conventions across all formats, including ISO-8601/RFC 3339 timestamps with timezone, UCUM units, ISO-4217 currency codes, numeric precision rules, identifier formats, and explicit guidelines for null/NA values.
- Implement time-series access with start/end filters, fixed granularities, server-driven pagination (self/next/prev links) and negotiated compression for large responses.
- Support partial updates where relevant (JSON Merge Patch / JSON Patch) and enforce HTTP preconditions (ETag/If-Match; Last-Modified/If-Modified-Since) to protect concurrency.
- Return a uniform problem-details error body with type, code, title, detail, and a correlation identifier.
- Make all write operations idempotent using an Idempotency-Key header.

2. **Medium (activate when that scope appears):**
    - Support XML with XSD validation for regulated or archival exchanges so that invalid files are rejected before ingestion.
    - For grid or master data batches, accept or publish CIM XML (IEC 61970-552) with the related profile documentation and sample files; when semantic analytics are needed, support CIM RDF/XML to enable graph queries on the same data model.
    - When JSON sources must carry semantic identifiers, use JSON-LD @context so each term resolves to the correct CIM/SAREF identifier without altering the API structure.
    - If a context-broker pattern is required, expose NGSI-LD entity payloads and SSE/streaming endpoints for subscriptions, maintaining a strict one-to-one mapping with the Data-Source entities defined in the specification.

  - When demand-response datasets are mandated, publish OpenADR 3.0 JSON or OpenADR 2.0b XML alongside the canonical API, and provide examples and validation artefacts so partners can integrate reliably.

3. **Low (use selectively when it clearly adds value)**:
   - When the API defines its own vocabulary or controlled lists, publish RDF/OWL (Turtle) files for those vocabularies and keep them properly versioned; avoid using Turtle for operational data exchanges.
   - Provide XLS/XLSX files only for analyst-focused downloads that require formulas, pivot tables, or visualization; use JSON, XML, or CSV for all system-to-system data transfers to ensure predictable and deterministic behaviour.

Cross-cutting syntactic practices (apply to all):

- Ensure every endpoint and file includes both a schema version and a resource version so the API can evolve without breaking existing clients.
- Keep pagination, filtering, and compression behaviour consistent across all providers to guarantee predictable client interactions.
- Fully specify batch and notification mechanisms, including:
  - CSV imports/exports with machine-readable descriptors and checksums.
  - Webhook notifications using a canonical event structure (id, type, version, time, subject, data), with signed deliveries, bounded retries using backoff and jitter, and de-duplication keys.
- Publish a complete conformance kit OpenAPI file, JSON Schemas or XSDs, CSV descriptors, example payloads, and

validator scripts, so both data providers and consumers can self-test integrations before onboarding.

5.4.4.3. SEMANTIC INTEROPERABILITY

- **Technical functionality:**

1. Publish machine-readable metadata for every source so requests can be routed correctly (e.g., stable source ID, owner, data type, coverage period, routing key, contact URI).
2. Represent core entities with recognised models so payloads are portable across providers (e.g., metering series, price/tariff periods, flexibility artefacts, market roles/IDs using CIM/ESMP or IEC 62746-4 bindings).
3. Attach explicit policy metadata to every dataset to enable access control and audit (e.g., consentId, purpose/usage policy, lawful basis, data-owner reference, retention class).
4. Encode the trust signals consumers need to assess and verify figures (e.g., SLA target, validation status, baseline method, flags such as measured/estimated/missing/tampered, cross-validation reference).
5. Carry complete temporal context and lifecycle rules with the data (e.g., start/end, resolution, timezone, calendar alignment, retention period, archival status).
6. Include identifiers and locality so data can be correlated across networks and actors (e.g., role codes, EIC/EAN/MPxN, grid zone/feeder, location polygon, cross-DSO sharing marker).
7. Expose provenance and service health signals so consumers can monitor reliability (e.g., source system ID, update frequency, freshness/lag indicator, lastUpdated timestamp, availability metric, lineage hash).

- **Standards:**

1. **IEC CIM (IEC 61970, IEC 61968 core, IEC 62325-351 market)**: Reference information model for grid, metering, and market data used across EU TSO/DSO ecosystems; maintained in UML and available in RDF/OWL for semantic queries. *(Source: Pilot Austria; Projects SYNERGY, EDDIE.)*
2. **ETSI SAREF family (SAREF, SAREF4ENER/4BLDG/4CITY)**: Lightweight OWL vocabularies for devices, sensors, services, and buildings; well suited to JSON-LD and fine-grained appliance semantics. *(Source: Projects InterConnect, Independent, OMEGA-X; referenced in several pilot sheets.)*
3. **ESMP (European Style Market Profile)**: EU market profile that narrows CIM options (roles, IDs, documents) to improve cross-border interoperability; aligned with IEC 62325-351 and adopted in projects like EDDIE. *(Source: Project EDDIE.)*
4. **PAS 1878 / PAS 1879**: UK BSI specifications defining Energy Smart Appliance capability semantics and DR signal semantics (often paired with OpenADR 2.0b/3.0). *(Source: Tomorrow's Homes Today.)*
5. **IEC 61850**: Logical-node semantics for substation automation (measurements, states, events) frequently bridged to CIM for end-to-end data flows. *(Source: Pilot Croatia; Project SYNERGY.)*
6. **DLMS/COSEM (IEC 62056)**: OBIS-coded smart-meter semantics commonly mapped into CIM-based metering exchanges. *(Source: Project SYNERGY.)*
7. **OpenADR event model**: Fixed DR event vocabulary (e.g., *eiEventID, optType, signalName*) used in the Croatian pilot and in projects such as SENDER and PARMENIDES. *(Source: Pilots Croatia; Projects SENDER, PARMENIDES.)*

8. **USEF (Universal Smart Energy Framework)**: Role/process model and semantic definition of flex offers for market-based demand response. *(Source: Project SYNERGY.)*
9. **IFC (ISO 16739)**: Building information semantics (floors/rooms/zones) providing spatial context for devices and NILM/HVAC use cases. *(Source: Project SYNERGY.)*
10. **PECO ontology**: SAREF-aligned community semantics (actors, assets, governance artefacts) for energy-community scenarios. *(Source: Project PARMENIDES.)*
11. **OMEGA-X Common Semantic Data Model (CSDM)**: Dataspace-oriented model aligning CIM and SAREF with data-sovereignty metadata. *(Source: Project OMEGA X.)*
12. **SHACL (Shapes Constraint Language)**: Semantic constraint language to enforce required properties/types/ranges on RDF/JSON-LD payloads. *(Source: Project Hedge IoT.)*
13. **RESONANCE ontology**: Combines SAREF/SEAS/CSDM to cover P2P and DSO-coordinated energy exchanges. *(Source: Project RESONANCE.)*
14. **SEAS (Smart-Energy Aware Systems) ontology**: Ontology for energy services, objectives, and context (e.g., optimization goals and time windows). *(Source: Project RESONANCE.)*

- **Standards Guidelines for Implementation:** This subsection provides guidelines for selecting semantic standards in CERF. The evaluation and prioritisation follow four checks that assess relevance to Data-Sources payloads, fitness for the required semantic functions, reuse in EU projects, and implementation readiness with machine-readable artefacts. All collected standards were retained and then classified with a High/Medium/Low priority to reflect their applicability within the

Data Sources Interface. The outcome of this prioritisation is summarised in Table 34.

- **Evaluation and Prioritisation of Semantic Standards:** We used a principles-based selection focused on four checks:
  - **Data-Source relevance shortlist** (must directly serve Data-Sources payloads (catalogue/metadata, historical/NRT metering, prices/tariffs, flexibility artefacts, consent/policy))
  - **Fitness to the technical functionalities of the semantic standards layer** (does the standard enable routing/identities, common vocabulary, policy/consent tags, data-quality & validation, time/retention, multi-operator context, and provenance/health?)
  - **Proven reuse in EU projects/pilots** (is it already used in practice within comparable contexts?)
  - **Readiness to implement** (are specifications mature, machine-readable artefacts available (RDF/OWL/contexts, shapes/profiles)?).
- **Shortlisted standards:** We retained all collected standards and then prioritised them (High/Medium/Low) to reflect their specific applicability within the Data Source interface.

Table 34: Prioritisation of Semantic Standards

Standard	When it matters most	Priority	Priority rationale & sources
IEC CIM (61970/61968 core)	Common identities and structures for grid assets, meter points, readings, and providers across sources	High	Required for cross-provider alignment and portability, aligns with 'use standard data models' and 'latest CIM' expectations (DAT_020, DAT_023 (Deliverable D2.2 Energy services analysis, use cases, and CERF requirements)), and supports routing/cataloguing (DAT_001, DAT_019 (Deliverable D2.2)). Applied in EDDIE.
ESMP (IEC 62325-351 profile)	Market roles/IDs and documents behind price series, bids/schedules, settlement-adjacent datasets	High	Narrows CIM for EU market consistency, mentioned in interoperability goals (DAT_020, DAT_023 (Deliverable D2.2)). Ensures cross-border portability of market-related data.
SHACL	Semantic conformance for all published datasets	High	Enables dataset-level rules and data-quality gates (DAT_005, DAT_006, DAT_010 (Deliverable

	(metering, prices, flexibility, consent/policy)		D2.2)); supports auditable acceptance criteria and automated validation before onboarding.
SAREF / SAREF4ENER / 4BLDG	Device/asset KPIs and states when sources originate from IoT/HEMS/field gateways	Medium	Bridges edge semantics to CIM-based exchanges, used in InterConnect/OMEGA-X, activates where device-level feeds are exposed.
DLMS/COSEM (IEC 62056)	Smart-meter OBIS series published as datasets or streams	Medium	De-facto meter semantics, maps cleanly into CIM/SAREF, underpins historical/NRT availability (DAT_002, DAT_008 (Deliverable D2.2)).
IEC 61850	Substation/SCADA signals published as data sources	Medium	Logical-node semantics are commonly bridged to CIM, relevant where SCADA telemetry feeds the data space.
OpenADR event model	DR events/offers/alerts exposed as datasets	Medium	Fixed DR terms ease reuse, support near-real-time follow-up for flexibility contexts (DAT_008 (Deliverable D2.2)).
OMEGA-X CSDM	Dataspace exchange needs policy/sovereignty metadata on datasets	Medium	Complements consent/usage/contract tags (DAT_004, DAT_011, DAT_013, DAT_016 (Deliverable D2.2)), aligns with ‘use standards’ (DAT_020 (Deliverable D2.2)).
USEF	Process/role semantics when a USEF-style DR process is part of the source	Low	Helpful where process semantics are needed, optional for core catalogue/series publication.
IFC (ISO 16739)	Building/floor/room context within a source	Low	Adds fine-grained spatial context when needed.
SEAS	Expressing optimization goals/constraints as part of a published dataset	Low	Useful where sources expose objectives/constraints, otherwise optional.
PECO	Community actors/assets/governance data as a source	Low	Project-specific community semantics, include only where applicable.
RESONANCE ontology	Hybrid P2P + DSO semantics within particular sources	Low	Optional mapping path, keep separate from the core profile.

Each standard is assigned a priority level: **High** (implement by default), **Medium** (use when that scope appears (metering, market, substation, dataspace, buildings, optimisation)), **Low** (use selectively if it clearly adds value).

- **Priority-Based Implementation Guidelines:**
  1. **High (implement by default):**
     - Define a compact CIM profile covering data-source objects such as data provider, dataset, meter point, time

series/reading, and grid context, and use stable identifiers (for example EIC, EAN, or MPxN where applicable).

  - Publish JSON-LD contexts that map each exposed field to the correct CIM IRI and provide at least one worked example for each dataset type (historical time series, near-real-time feeds, price/tariff periods).
  - For market-related datasets, align with ESMP: use its role codes and identifiers, document the exact ESMP version and profile choices, and include a simple mapping table showing how each dataset field corresponds to the CIM/ESMP element.
  - Include an example demonstrating equivalence between a dataset and the corresponding ESMP document fragment.
  - Use SHACL as the semantic conformance gate for all dataset classes (metering series, price/tariff, flexibility artefact, consent/policy bundle). Shapes must define required properties, datatypes, units, allowed code lists, and time-window rules.
  - Provide one valid and one invalid example for each shape, and run SHACL validation automatically in the build and release pipeline.
  - Register every dataset in the Data Catalogue, exposing discovery metadata (source ID, owner, type, coverage, routing key) so requests route correctly and assets remain searchable across CERF.
  - When JSON-LD cannot be used, provide a field-to-IRI mapping document so consumers can resolve each field to its CIM identifier with the same fidelity.

2. **Medium (use when the scope appears):**
  - When sources originate from devices or HEMS, bridge device states and KPIs to SAREF/SAREF4ENER while

keeping CIM as the backbone and publish a clear SAREF-to-CIM mapping table so downstream consumers work with one main vocabulary.

- If smart-meter data is exposed, provide an OBIS-to-CIM/SAREF mapping for common registers and validate that each reading includes the OBIS code, numeric value, UCUM unit, and timestamp; retain the original OBIS code in the payload for traceability.
- For SCADA-derived datasets, document how IEC 61850 Logical Nodes and Data Attributes map to CIM/SAREF terms and ensure timestamps and quality flags are preserved; include small examples for measurements, status, and alarms.
- If demand-response data is included, publish event datasets using OpenADR terms (identifiers, signals, options, intervals) and validate them using a dedicated shape that constrains enumerations and lifecycle states.
- When operating inside a dataspace, attach OMEGA-X style policy and sovereignty metadata (provider, permitted purpose, contractual basis, region, usage constraints) to each dataset and validate these fields with a small policy shape containing clear MUST and SHOULD rules.

3. **Low (use selectively when it clearly adds value):**
   - Add USEF terms only when a dataset must carry explicit demand-response process or role semantics and provide a short mapping back to ESMP/CIM identifiers to avoid divergence.
   - Apply IFC links only when building-level detail is required; connect devices or meter points to IFC spaces using persistent URIs and keep those bindings versioned as locations evolve.

- Use SEAS terms only when the dataset includes optimization objectives or constraints and reference any user preferences stored elsewhere to keep responsibilities clear.
- For community or hybrid P2P + DSO datasets, reuse only the minimal terms needed from PECO or RESONANCE, and include a brief mapping note back to CIM/SAREF so consumers maintain a predictable data model.

Cross-cutting practices (apply to all semantic payloads):

- Every dataset must include policy and consent information: a consent identifier, lawful basis, permitted purpose or usage policy, retention class, and a reference to the data owner, ensuring access control and audit checks are enforceable.
- All values must include time and quality context: start and end instants, resolution, timezone, calendar alignment, and data-quality flags (measured, estimated, missing, tampered), along with any baseline or validation status required for verification.
- Expose provenance and service health in metadata, including the source system identifier, update frequency, freshness or lag indicator, last-updated timestamp, and simple availability metrics; add a checksum or hash where feasible for lineage tracking.
- Manage versioning and change control for contexts, shapes, and mapping tables; never repurpose IRIs, and publish short migration notes with each change so existing consumers continue to function.
- Publish a conformance kit containing contexts, SHACL shapes, sample payloads, and lightweight validator scripts

so providers and consumers can self-test semantic compliance before onboarding.

5.5. DSO INTERFACE

5.5.1. INTEROPERABILITY SCENARIO

The DSO connects to the data space to obtain information on users and appliances and to send flexibility requests or grid-related recommendations to aggregators and energy apps.

5.5.2. INTEROPERABILITY POINT

- **Generic**: The interfaces linked to the DSO System, where grid data, flexibility signals, and user consumption information are exchanged with aggregators, market operators, and EMS infrastructures. This is effectively a central interoperability point of the architecture.
- **Data Space–enabled**: The DSO Connector, managing trusted access to and from the DSO's systems, ensuring data exchange follows regulatory and operational policies.

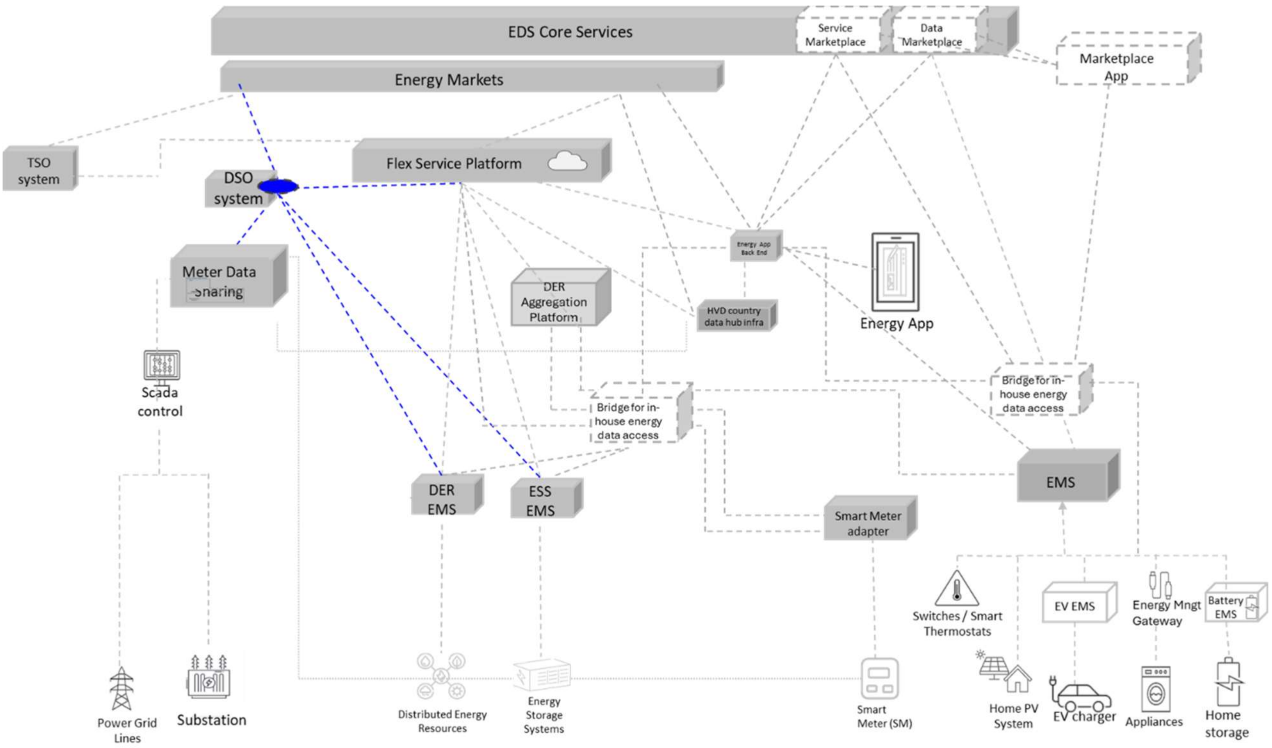


Figure 44. DSO Interface Interoperability Point

5.5.3. INTEROPERABILITY CASE

This point ensures coordinated and reliable information flow between grid operators and flexibility actors, enabling efficient demand response and grid stability services while respecting data governance rules.

Table 35: Interoperability Facets

Facet	Generic Implementation	Data Space–Enabled Implementation
Semantic	Differences in how DSOs and aggregators describe flexibility products or grid events.	Apply CIM and IEC 62325 models for harmonised representation of grid and flexibility data.
Technical	Point-to-point APIs or secure FTP data transfers.	Federated connector APIs with policy enforcement for traceable, auditable exchanges.

Organisational	Data governed through bilateral contracts and service agreements.	Connectors enforce organisational trust through IDSA Rulebook and Gaia-X Trust Framework, automating compliance and governance.

5.5.4. INTEROPERABILITY PROFILE

5.5.4.1. TRANSPORT INTEROPERABILITY

- **Technical functionality:**

1. Provide a secure request-response channel for DSOi endpoints (registration, grid zones, metering, flexibility needs/offers/baselines/activation plans) with encrypted HTTP and caching controls.
2. Enable low-overhead publish/subscribe for telemetry and grid signals (e.g., metering series, activation status, device heartbeats) with configurable QoS, retained state, and last-will.
3. Support high-throughput streaming for bulk metering and flexibility event flows into analytics/settlement backbones via scalable consumer groups.
4. Deliver event notifications (flexibility needs, activation plans, HLUC4 emergency notices) to external parties using signed push mechanisms with retries and deduplication.
5. Enforce strong authentication and authorisation for DSO-FSP/app exchanges using short-lived, scoped tokens and optional federated identity for operator portals.
6. Provide robustness over intermittent field links (GPRS/wM-Bus gateways) via QoS, batching, buffering, and replay, and harden gateways with rate limits, size limits, circuit breakers, and DDoS protection.

7. Operate PKI-based certificate/key lifecycle for devices/brokers and maintain precise time synchronization for verification/settlement, recording security events to meet audit and GDPR obligations.

- **Standards:**

1. **HTTPS REST**: Secure HTTP with RESTful resource design for create/read/update/delete operations; TLS protects payloads, intermediaries support caching, and mainstream stacks (e.g., Spring, .NET, React Native) provide native support. *(Source: all pilot sheets.)*
2. **MQTT 3.1.1**: Lightweight publish/subscribe transport with 2-byte fixed header and QoS 0/1/2, well-suited to second- or minute-level metering over Wi-Fi/GSM; topics route via a broker and TLS adds confidentiality/integrity. *(Source: Pilots Austria, Croatia; Projects Independent, EDDIE, Hedge IoT, OMEGA-X.)*
3. **Apache Kafka**: Distributed commit log where readings and prices are immutable events in partitioned topics, enabling high-throughput replay for audits/AI while consumer groups process streams in real time. *(Source: Pilots Austria, Croatia, Spain; Project EDDIE.)*
4. **AMQP 1.0**: Enterprise messaging with link credits, routing, and ordering guarantees; applied as an outbound connector for bulk notifications and legacy integrations. *(Source: Pilot Austria.)*
5. **Webhooks**: Event callbacks that POST JSON to a subscriber URL on trigger (e.g., threshold breach), providing instant push without persistent client connections. *(Source: Pilots Austria, Slovenia.)*
6. **SOAP/HTTP (OpenADR 2.0b)**: XML event messages inside SOAP over HTTPS with digital signatures for authenticity and non-repudiation; required by several UK ESA deployments.

(Source: Tomorrow's Homes Today.)

7. **NGSI-LD REST (Server-Sent Events)**: JSON-LD entity API with CRUD, subscriptions, and SSE streams to push real-time updates of prices or metering changes to subscribers. *(Source: Projects OMEGA-X, Hedge-IoT.)*
8. **P1 smart-meter interface**: Consumer serial port (≈115 kbaud) emitting OBIS-coded telegrams every few seconds; a gateway translates serial frames to MQTT or REST for cloud ingestion. *(Source: Pilot Austria; Project EDDIE.)*
9. **Wireless M-Bus**: Sub-GHz metering radio (EN 13757-4) using AES-128 frame security; concentrators collect frames and forward them to backend services. *(Source: Pilot Poland.)*
10. **IEC 60870-5-104**: Telecontrol over TCP/IP carrying status changes and measured values between control rooms and field devices; retained as a fallback for critical switching paths. *(Source: Pilots Portugal, Spain.)*
11. **ICCP (IEC 60870-6 TASE.2)**: Inter-control-centre protocol exchanging high-rate SCADA points via predefined DataSets, with options for secure sessions. *(Source: Pilot Spain.)*
12. **Modbus TCP/RTU**: Register-based polling over Ethernet (TCP) or RS-485 (RTU); still common in inverters and heat pumps due to firmware simplicity. *(Source: Pilot Spain; Project WEDISTRICT.)*
13. **DNP3**: Event-driven protocol with source-timestamped points and Secure Authentication, used for feeder automation where latency and auditability matter. *(Source: Pilot Spain.)*
14. **OPC XML-DA / OPC UA**: OPC XML-DA exposes field data via XML/HTTP, while OPC UA adds a binary TCP stack, discovery, sessions, and built-in PKI for vendor-neutral PLC access. *(Source: Pilot Spain.)*
15. **SPARQL/HTTP**: Standards-based query endpoint over HTTP for triplestores holding CIM/SAREF graphs (e.g., "heaters in zone B

with power > 2 kW"). *(Source: Project InterConnect.)*

16. **TLS 1.2 / TLS 1.3**: Transport encryption for all channels; 1.3 removes obsolete ciphers and 0-RTT is typically disabled to prevent replay. *(Source: Pilots France, Croatia, Austria.)*
17. **OAuth 2.0**: Authorization framework issuing time-limited access tokens with fine-grained scopes and refresh flows, separating authentication from API access. *(Source: Pilots Czech Republic, Austria, Croatia.)*
18. **OpenID Connect**: Identity layer on OAuth 2.0 providing signed ID tokens and standard claims, enabling single sign-on and federated identities (e.g., national eID). *(Source: Pilot Croatia.)*
19. **AES-GCM-256**: Authenticated encryption mode providing confidentiality and integrity for payloads or at-rest telemetry files. *(Source: Pilot Austria.)*
20. **HMAC-SHA-256**: Symmetric message authentication code allowing constrained devices to sign messages and enable tamper detection with minimal overhead. *(Source: Pilot Croatia.)*
21. **IPsec VPN / MPLS VPN**: Site-to-site tunnelling (IPsec ESP) or carrier-provided isolation (MPLS L3VPN) to protect grid traffic over public or shared networks. *(Source: Pilot Spain.)*
22. **CAS protocol**: Central Authentication Service enabling single sign-on via redirect and service tickets across multiple utility portals. *(Source: Pilot Poland.)*
23. **Two-phase certificate authentication**: Mutual-TLS with personal X.509 presentation followed by PIN confirmation, establishing a strong client identity before data exchange. *(Source: Pilot Slovenia.)*
24. **GPRS backhaul**: 2G data path where loggers send HTTP or SMS packets over limited bandwidth, motivating payload compression and batching strategies. *(Source: Pilot Slovenia.)*

- **Standards Guidelines for Implementation:** This subsection provides guidelines for selecting transport standards for the DSO Interface within CERF. The evaluation and prioritisation follow four checks: relevance to DSOi channels and endpoints, fitness for the required transport-layer capabilities, proven reuse in comparable EU projects, and implementation readiness with mature tooling and configurations. Based on these checks, a set of transport standards has been shortlisted and prioritised for use in ECLIPSE DIGITAL. The result of this analysis is summarised in Table 36.
- **Evaluation and Prioritisation of Transport Standards:** A principles-based selection focused on four checks:
  - **DSO relevance shortlist** (must directly serve DSOi channels/endpoints (registration, grid zones, metering series, flexibility needs/offers/baselines/activation plans, subscriptions/notifications, authorisation)).
  - **Fitness to the technical functionalities of the transport standards layer** (does the transport directly enable the secure REST, pub/sub, streaming, event push, authN/authZ, reliability, and PKI/time-sync controls listed for the transport layer?)
  - **Proven reuse in EU projects/pilots** (is it already used in practice within comparable contexts?)
  - **Readiness to implement** (are specifications mature and stable, with tooling, services, configurations, and test kits readily available?)

- **Shortlisted standards:** HTTPS REST, Webhooks (HTTP push), MQTT 3.1.1 over TLS, Apache Kafka, AMQP 1.0, NGSI-LD REST (+SSE), OpenADR 3.0 JSON / 2.0b SOAP (where mandated), TLS 1.3 (with controlled 1.2 fallback), OAuth 2.0/2.1 + OpenID Connect, IPsec VPN / MPLS VPN (where required).

Table 36: Prioritisation of Transport Standards

Standard	When it matters most	Priority	Priority rationale & sources
HTTPS REST	Core request-response for all DSOi endpoints (/Generic, /Data, /Flexibility/*)	High	Universally supported, cache controls and intermediaries available, used across pilots, underpins DAT_008 (Deliverable D2.2 Energy services analysis, use cases, and CERF requirements) follow-up and SVC_023 (Deliverable D2.2) availability.
TLS 1.3 (1.2 fallback)	Encryption and integrity for every channel	High	Mandatory transport protection 1.3 preferred, used in France/Croatia/Austria pilot.
OAuth 2.0/2.1 + OIDC	Scoped access to APIs; SSO for operator portals	High	Used in CZ/AT/HR pilots, short-lived tokens + claims suit APP_044 (Deliverable D2.2) comms and /Data/Authorization in D4.1.
Webhooks (HTTP push)	Push of needs/activation plans and status from /Flexibility/Subscribe	High	Matches D4.1, signed delivery + retry/dedup satisfy DAT_008 (Deliverable D2.2) near-real-time follow-up and SVC_016 (Deliverable D2.2) verification.
PKI lifecycle + time sync (NTP/PTP)	Cert issuance/rotation; aligned timestamps for settlement	High	Needed for audit/GDPR and SVC_016 (Deliverable D2.2) proof windows, common DSO ops practice.
MQTT 3.1.1 over TLS	Low-overhead pub/sub for telemetry or device/grid signals feeding DSOi	Medium	Applied in AT/HR and multiple projects, enable only if ingesting edge data into backend, maps to DAT_008 (Deliverable D2.2) monitoring.
Apache Kafka	High-throughput streaming to analytics/settlement backbones	Medium	Used in AT/HR/ES and EDDIE, enables replay and consumer groups for audits/AI.
AMQP 1.0	Enterprise queue bridges/legacy back-office connectors	Medium	Present in AT pilot, enable when existing brokers must be integrated.
NGSI-LD REST (+SSE)	Dataspace/entity subscriptions with temporal/geo attrs	Medium	Used in OMEGA-X/Hedge-IoT, adopt only if exposing entity-style streams beyond core DSOi.
OpenADR 3.0 JSON / 2.0b SOAP	Regulated DR exchanges where OpenADR is mandated	Medium	Used in UK/THT and SENDER, switch on when jurisdiction/certification requires it, otherwise keep REST/webhooks.

IPsec VPN / MPLS VPN	Private operator links (e.g., DSO-TSO backhaul)	Medium	Observed in ES pilot, use for site-to-site isolation where risk analysis demands network-level protection.

Each standard is assigned a priority level: **High** (should be implemented by default), **Medium** (should be used when that scope appears (metering, market, substation, dataspace, buildings, optimisation)), **Low** (should be used selectively if it clearly adds value).

- **Priority-Based Implementation Guidelines:**

1. **High (implement by default):**
    - Use HTTPS over TLS 1.3 for every DSOi endpoint; disable plaintext HTTP and enforce HSTS.
    - Expose a consistent REST style with resource URIs, correct method semantics, and standard cache validators (ETag/Last-Modified) with conditional requests to reduce load.
    - Enforce OAuth 2.0/2.1 with OIDC by using Authorization Code + PKCE for user-facing portals, Client Credentials for service-to-service communication, rotating asymmetric-signed JWTs via JWKS, keeping scopes narrow and tokens short-lived, and exposing introspection and revocation.
    - Implement signed webhooks for /Flexibility/Subscribe with a canonical event envelope (id, type, version, subject, time, data), an HMAC signature header, exponential back-off with jitter, deduplication keys, idempotent processing, and a subscription verification handshake.
    - Harden the API edge with gateway resilience measures including rate limits, request-size caps, schema/content-type validation, circuit breakers, and DDoS shielding, and surface Retry-After where applicable.
    - Run a managed PKI for servers, brokers, and clients, covering issuance, renewal, revocation, and OCSP; maintain redundant

NTP/PTP so timestamps align across metering, bids, activations, and verification windows.

- Log security and delivery events with correlation IDs to meet audit and GDPR requirements while minimizing personal data in logs.

2. **Medium (activate when the scope appears):**
    - When ingesting device or grid telemetry, deploy MQTT 3.1.1 over TLS with namespaced topics and strict ACLs, select QoS based on criticality (QoS 1 for telemetry), use retained messages and last-will for session awareness, and terminate MQTT at an integration layer that validates and forwards into the DSOi model.
    - For high-volume analytics or settlement pipelines, use Apache Kafka with TLS/SASL, idempotent producers (acks=all), consumer-group isolation, retention/compaction policies, dead-letter topics, and replay procedures.
    - Where enterprise queues exist, bridge via AMQP 1.0 with TLS/SASL, link-credit flow control, and dead-lettering.
    - If a dataspace or entity-style interface is required, expose NGSI-LD REST with SSE for live updates (heartbeats, Last-Event-ID, resumable delivery), ensuring a 1:1 mapping to DSOi entities.
    - In jurisdictions mandating OpenADR, support OpenADR 3.0 JSON (preferred) or OpenADR 2.0b SOAP behind a gateway and publish WSDL/XSD or OpenAPI specifications with onboarding and certificate procedures.

  - For operator backhaul isolation, configure IPsec VPN (IKEv2, PFS, strong ciphers) or carrier MPLS VPN with documented failover and monitoring.

Cross-cutting transport practices (apply to all):

  - Apply mutual TLS where risk justifies strong client authentication, such as for brokers or operator circuits.
  - Prefer modern cipher suites such as AES-GCM or ChaCha20-Poly1305 and disable TLS 0-RTT.
  - Define explicit retry and replay policies per channel, including idempotency keys for HTTP/webhooks, QoS/retained behaviour for MQTT, and transactional producers for Kafka.
  - Document SLOs for latency and delivery guarantees so flexibility verification and settlement (SVC_016) can rely on predictable behaviour.
  - Provide a partner conformance kit including an OpenAPI specification, webhook signer/verifier, sample topics and records, and Postman/CLI tests so FSPs can self-validate before onboarding.

5.5.4.2. SYNTACTIC INTEROPERABILITY

- **Technical functionality:**

1. Standardise request and response payloads in a widely adopted, machine-readable format with per-endpoint schemas and consistent timestamp, unit, and currency conventions (e.g., ISO-8601/RFC 3339, UCUM, ISO-4217), or equivalent profiles agreed with stakeholders.
2. Publish a versioned, machine-readable API description for all DSOi endpoints (registration, grid zones, metering, flexibility

needs/offers/baselines/subscriptions), including security scopes, headers, and worked examples (e.g., OpenAPI 3.1).

3. Provide predictable filtering and pagination for historical datasets (zone/user, time windows, fixed granularities), enable negotiated compression for large payloads (e.g., gzip/deflate), and include hypermedia navigation fields (e.g., links.self/next/prev).
4. Support partial updates and standard cache/precondition controls to minimise bandwidth and protect concurrency (e.g., JSON Patch or Merge Patch; ETag/Last-Modified with If-Match / If-None-Match workflows).
5. Define a uniform error envelope and idempotent write semantics, using a problem-details format (e.g., RFC 7807) and an Idempotency-Key header to guarantee safe retries.
6. Specify a webhook/notification contract for subscriptions with a canonical event shape, explicit type/version fields, signed delivery (e.g., HMAC), back-off with jitter, deduplication keys, and idempotent processing.
7. Offer bulk import/export alongside the API in standard tabular or domain formats with machine-readable descriptors and audit fields (e.g., CSV + CSVW/JSON Table Schema; CIM/XML where mandated), including data-quality flags and timezone metadata.

- **Standards:**

1. **JSON**: UTF-8 text format using objects and arrays, widely supported in REST APIs, offering small payload size, low parsing cost, and compatibility with virtually all web/mobile frameworks. *(Source: Pilots Czech, France, Croatia, Spain, Sweden; multiple projects.)*

2. **JSON-LD**: JSON with a @context that resolves fields to IRIs, enabling lightweight linked-data payloads so terms like activePower map directly to semantic identifiers (e.g., SAREF or CIM). *(Source: Projects OMEGA-X, RESONANCE.)*
3. **XML**: Schema-validated, tag-based format suited for structured and regulated exchanges such as CIM network models and OpenADR 2.0b SOAP messages, ensuring strict typing and vendor interoperability. *(Source: Pilots Austria, Croatia, Poland, Portugal.)*
4. **CSV**: Plain-text tabular format used for large-scale data exports such as readings and invoices; easy to open in BI tools or Excel, human-readable, and highly compressible. *(Source: Pilots Poland, Slovenia, Portugal, Spain.)*
5. **XLS/XLSX**: Spreadsheet containers that extend CSV tables with formulas, pivot charts, and formatting, often used for downloads that include embedded analytics or dashboards. *(Source: Pilot Poland; Pilot Slovenia.)*
6. **CIM XML (IEC 61970-552)**: Canonical XML serialization of the Common Information Model, where each class/attribute is schema-defined, allowing DSOs to validate complete grid or market files before loading. *(Source: Pilot Austria; Project EDDIE.)*
7. **CIM RDF/XML**: RDF encoding of CIM classes expressed in XML for semantic querying; enables loading grid and market data into triple stores for SPARQL analysis, e.g., topology searches. *(Source: Project SYNERGY.)*
8. **RDF/OWL (Turtle)**: Compact, text-based syntax for exchanging ontologies such as SAREF or project-specific extensions; easy to edit by humans and directly consumable by semantic tools. *(Source: Projects InterConnect, PARMENIDES, RESONANCE.)*

9. **XSD**: XML Schema Definitions specifying allowed elements, attributes, and datatypes; attached to files so malformed or non-compliant records are rejected before entering the system. *(Source: Pilot Austria.)*
10. **NGSI-LD / JSON-LD**: Context-broker API using JSON-LD to represent entities with temporal and geospatial attributes, supporting queries, subscriptions, and time-series operations for real-time streams. *(Source: Project OMEGA-X, Hedge-IoT.)*
11. **OpenAPI 3.x**: YAML/JSON specification describing endpoints, schemas, and security rules, enabling automatic client/server code generation and interactive developer documentation. *(Source: Pilot Czech; Projects SYNERGY, InterConnect.)*
12. **OpenADR 2.0b XML**: XML schemas and SOAP bindings defining DR event messages (e.g., <oadrDistributeEvent>), with digital signatures for certified ESA deployments. *(Source: Tomorrow's Homes Today; SENDER.)*
13. **OpenADR 3.0 JSON**: RESTful JSON profile carrying the same DR event semantics (IDs, signals, schedules) but with lower overhead, better suited for mobile and IoT devices. *(Source: Tomorrow's Homes Today.)*
14. **Modbus register map (binary)**: Legacy binary protocol where fixed register offsets define measurement semantics, used to collect data from RTUs and inverters over serial or TCP links. *(Source: Project WEDISTRICT.)*
15. **ICCP DataSet structures**: IEC 60870-6 TASE.2 feature where pre-defined DataSets specify telemetry points exchanged between control centres, using compact binary frames for high-volume traffic. *(Source: Pilot Spain.)*

- **Guidelines for Implementation:** This subsection provides guidelines for selecting syntactic standards for the DSO Interface within CERF. The evaluation and prioritisation follow four checks: relevance to DSOi payloads and endpoints, fitness for the required syntactic capabilities, proven reuse in comparable EU projects and pilots, and implementation readiness based on available artefacts and tooling. All collected syntactic standards were retained and then prioritised (High, Medium, Low) according to their applicability to DSO needs. The outcome of this analysis is presented in Table 37: Prioritisation of Syntactic Standards.
- **Evaluation and Prioritisation of Syntactic Standards:** A principles-based selection focused on four checks:
  - **DSO relevance shortlist** (must directly serve DSOi payloads/endpoints (registration, grid zones, metering series, flexibility needs/offers/baselines/subscriptions, authorisation, notifications))
  - **Fitness to the technical functionalities of the Syntactic standards layer** (does the standard directly enable the required capabilities?)
  - **Proven reuse in EU projects/pilots** (is it already used in practice within comparable contexts?)
  - **Readiness to implement** (has mature artifacts (schemas/specs/examples), validators, and good tooling (generators/IDEs/linters)?)

- **Shortlisted standards:** We retained all collected standards and then prioritised them (High/Medium/Low) to reflect their specific applicability within the DSO interface.

Table 37: Prioritisation of Syntactic Standards

Standard	When it matters most	Priority	Priority rationale & sources
JSON	Default wire format for DSOi endpoints (/Generic/, /Data/, /Flexibility/*).	High	Native to REST, minimal overhead, universal tooling, cited across pilots (Czech, France, Croatia, Spain, Sweden) and projects. Supports DAT_008/SVC_023 (Deliverable D2.2 Energy services analysis, use cases, and CERF requirements) data-availability expectations.
OpenAPI 3.x	Single machine-readable contract for all endpoints, schemas, headers, and examples.	High	Enables client/server codegen, test stubs, and docs, present in pilots/projects (Czech, SYNERGY, InterConnect). Underpins predictable pagination/filters, error shapes, and security scopes.
CSV	Bulk exports/imports of metering and KPI tables.	High	Human-friendly, compressible, easy to ingest in BI, used in Portugal, Spain, Poland, Slovenia pilots. Fits DAT_008 (Deliverable D2.2) follow-up tooling and SVC_023 availability. Pair with CSVW/JSON Table Schema descriptors.
XML	Regulated/bulk exchanges where strict typing is required.	Medium	Used in Austria, Croatia, Poland, Portugal pilots, aligns with XSD validation and archival needs; complements JSON for day-to-day API traffic.
XSD	Validation of XML payloads (CIM, OpenADR 2.0b, regulated files).	Medium	Rejects malformed records early, mentioned in Austria pilot. Critical when agencies require schema conformance.
CIM XML (IEC 61970-552)	Canonical files for grid/metering master data and market-adjacent batches.	Medium	Applied in EDDIE, common in Austria, ensures complete model validation prior to load, aligns with DSOi metering and zone catalogues.
CIM RDF/XML	Loading CIM graphs into triple stores for topology/market analysis.	Medium	Used in SYNERGY, useful where semantic analytics are needed while keeping XML tooling.
JSON-LD	Lightweight linked data for DSOi JSON (semantic identifiers in payloads).	Medium	Named by OMEGA-X/RESONANCE, bridges to SAREF/CIM IDs without leaving JSON, helps portability across pilots.
NGSI-LD / JSON-LD	Context-broker style entity API for subscriptions/time-series views.	Medium	Seen in OMEGA-X and Hedge-IoT, optional pathway to publish metering/flex entities with temporal + geo attributes.
OpenADR 3.0 JSON	REST/JSON DR messages where DSO publishes needs/events via modern payloads.	Medium	Tomorrow's Homes Today roadmap; lighter than 2.0b, aligns with DSO notifications and APP_044 (Deliverable D2.2) exchanges when DR is in scope.
OpenADR 2.0b XML	Certified ESA/DR exchanges in SOAP/XML environments.	Medium	Used in SENDER/THT contexts, pairs with XML/XSD, keep for jurisdictions requiring certification.

RDF/OWL (Turtle)	Exchanging ontologies and vocabularies used by the API (not runtime data).	Low	Used in InterConnect, PARMENIDES, RESONANCE, mainly for publishing the controlled vocab/contexts, not for the operational API.
XLS/XLSX	End-user oriented downloads with formulas/pivots.	Low	Poland/Slovenia pilots, convenience layer over CSV, not a system-to-system format.
Modbus register map (binary)	Legacy device polling registers are represented in files/specification.	Low	Applied in the WEDISTRICT project, include only as mapping docs, not a public DSOi exchange syntax.
ICCP DataSet structures	Control-centre to control-centre point lists and dataset definitions.	Low	Used in Spain pilot, keep as mapping reference for bridging to DSOi, not a public JSON/XML API format.

Each standard is assigned a priority level: **High** (should be implemented by default), **Medium** (should be used when that scope appears (metering, market, substation, dataspace, buildings, optimisation)), **Low** (should be used selectively if it clearly adds value).

- **Priority-Based Implementation Guidelines:**
  - **High (implement by default):**
    - Use JSON as the canonical payload for all DSOi endpoints and provide per-endpoint JSON Schemas that define field names, types, required/optional properties, allowed enumerations, and constraints for timestamps, units, and currencies.
    - Publish a versioned OpenAPI 3.x document that references those schemas, defines security scopes and headers, specifies pagination and filtering (zone/user, start–end, granularity), and includes worked examples for both success and error scenarios.
    - For large result sets, standardise pagination using cursor or limit/offset, provide hypermedia navigation fields (links.self/next/prev), and support content negotiation for compression.
    - Define a uniform error envelope using a problem-details format (RFC 7807 style) and make all write operations idempotent

through an agreed header and idempotency keys returned in responses.
  - For bulk tabular exchanges, provide CSV with machine-readable descriptors (CSVW / JSON Table Schema), including timezone columns, data-quality flags, and audit fields, and reserve CSV strictly for batch interfaces and downloads to keep the operational API consistent.

- **Medium (use when that scope appears):**
  - For bulk or regulated exchanges, deliver XML payloads validated by XSD.
  - For grid or metering master-data batches, provide CIM XML (IEC 61970-552) with profile documentation and sample files; where semantic analytics are needed, also support CIM RDF/XML for the same data models.
  - When JSON needs to carry semantic identifiers, enrich the operational JSON with JSON-LD @context documents so terms resolve to IRIs without altering the API surface.
  - If a context-broker pattern is required, expose NGSI-LD / JSON-LD entities with temporal attributes and subscription endpoints, ensuring the entity payloads map 1:1 to the DSOi model.
  - Where demand-response is in scope, support OpenADR 3.0 JSON as the preferred REST/JSON option and keep OpenADR 2.0b XML only when certification or legacy requirements mandate it.
  - Ship schemas, examples, and conformance tests across all medium pathways so partners can validate their integration before onboarding.

- **Low (use selectively when it clearly adds value):**

- Use RDF/OWL (Turtle) only to publish vocabularies referenced by JSON/JSON-LD, and do not use Turtle for operational API responses.
- Offer XLS/XLSX only for user-facing downloads that require formulas or pivot tables; avoid using it for system-to-system integration.
- Where legacy or control-centre systems are involved, keep Modbus register maps and ICCP DataSet definitions as boundary documentation and convert those datasets into the canonical API schemas before entering the DSOi. These Low items act as compatibility aids, not core parts of the public API.

Cross-cutting syntactic practices (apply to all):

- Keep timestamps consistent using ISO-8601 with timezone, and include explicit granularity and interval fields in history queries; carry units using a shared code list such as UCUM.
- Use stable identifiers and version tags in every payload (schema version and resource version).
- Support partial updates (JSON Merge Patch / JSON Patch) and enable cache/precondition controls (ETag/Last-Modified with If-Match/If-None-Match) to reduce bandwidth and prevent concurrency issues.
- Provide a webhook/notification contract with a canonical event shape (type, version, id, timestamp, subject, data), signed deliveries, retries with jitter, and deduplication keys.
- Publish a conformance kit containing the OpenAPI file, JSON Schemas/XSDs, example payloads, and validator scripts so pilot partners can self-test before connecting. This directly supports follow-up and near-real-time expectations in DAT_008, data-availability performance in SVC_023, verification needs in SVC_016, and DSO-customer exchanges in APP_044.

5.5.4.3. SEMANTIC INTEROPERABILITY

- **Technical functionality:**

1. Provide a machine-readable grid model that names DSOs/TSOs/FSPs, grid zones, feeders, and metering points with stable IDs so "who/where" is unambiguous.
2. Define a common vocabulary for the flexibility lifecycle-needs/requests, offers, activation plans, baselines, and results with states, links, and timestamps.
3. Standardise metering semantics (quantities, units, granularity, timezone, intervals) and aggregation rules for user-level and zone-level data.
4. Encode verification and settlement evidence using clear thresholds, durations, baseline methods, and data-quality flags to support KPI calculation.
5. Attach provenance, consent/authorization, and usage-policy tags so access checks and audits are enforceable across parties.
6. Publish cross-model mappings (CIM/ESMP, SAREF, OpenADR/USEF) so the same objects are portable across pilots and Member States.
7. Model spatial targeting for emergencies using zones/polygons with validity windows and severity for HLUC4-type notices.
8. Provide a controlled event taxonomy (alerts, curtailment notices, market requests) with severities and statuses for consistent messaging.

- **Standards:**

1. **IEC CIM (IEC 61970, IEC 61968 core, IEC 62325-351 market)**: Reference information model for grid, metering, and market data used across EU TSO/DSO ecosystems; maintained in UML and available in RDF/OWL for semantic queries. *(Source: Pilot Austria; Projects SYNERGY, EDDIE.)*

2. **ETSI SAREF family (SAREF, SAREF4ENER/4BLDG/4CITY)**: Lightweight OWL vocabularies for devices, sensors, services, and buildings; well suited to JSON-LD and fine-grained appliance semantics. *(Source: Projects InterConnect, Independent, OMEGA-X; referenced in several pilot sheets.)*
3. **ESMP (European Style Market Profile)**: EU market profile that narrows CIM options (roles, IDs, documents) to improve cross-border interoperability; aligned with IEC 62325-351 and adopted in projects like EDDIE. *(Source: Project EDDIE.)*
4. **PAS 1878 / PAS 1879**: UK BSI specifications defining Energy Smart Appliance capability semantics and DR signal semantics (often paired with OpenADR 2.0b/3.0). *(Source: Tomorrow's Homes Today.)*
5. **IEC 61850**: Logical-node semantics for substation automation (measurements, states, events) frequently bridged to CIM for end-to-end data flows. *(Source: Pilot Croatia; Project SYNERGY.)*
6. **DLMS/COSEM (IEC 62056)**: OBIS-coded smart-meter semantics commonly mapped into CIM-based metering exchanges. *(Source: Project SYNERGY.)*
7. **OpenADR event model**: Fixed DR event vocabulary (e.g., *eiEventID, optType, signalName*) used in the Croatian pilot and in projects such as SENDER and PARMENIDES. *(Source: Pilots Croatia; Projects SENDER, PARMENIDES.)*
8. **USEF (Universal Smart Energy Framework)**: Role/process model and semantic definition of flex offers for market-based demand response. *(Source: Project SYNERGY.)*
9. **IFC (ISO 16739)**: Building information semantics (floors/rooms/zones) providing spatial context for devices and NILM/HVAC use cases. *(Source: Project SYNERGY.)*

10. **PECO ontology**: SAREF-aligned community semantics (actors, assets, governance artefacts) for energy-community scenarios. *(Source: Project PARMENIDES.)*
11. **OMEGA-X Common Semantic Data Model (CSDM)**: Dataspace-oriented model aligning CIM and SAREF with data-sovereignty metadata. *(Source: Project OMEGA X.)*
12. **SHACL (Shapes Constraint Language)**: Semantic constraint language to enforce required properties/types/ranges on RDF/JSON-LD payloads. *(Source: Project Hedge IoT.)*
13. **RESONANCE ontology**: Combines SAREF/SEAS/CSDM to cover P2P and DSO-coordinated energy exchanges. *(Source: Project RESONANCE.)*
14. **SEAS (Smart-Energy Aware Systems) ontology**: Ontology for energy services, objectives, and context (e.g., optimization goals and time windows). *(Source: Project RESONANCE.)*

- **Guidelines for Implementation:** This subsection provides guidelines for selecting semantic standards for the DSO Interface within CERF. The evaluation and prioritisation follow four checks: relevance to DSOi objects, fitness for the required semantic capabilities, proven reuse in comparable EU projects and pilots, and implementation readiness based on available machine-readable artefacts. On this basis, a shortlist of semantic standards has been retained and then prioritised (High, Medium, Low) according to their applicability to DSO needs. The outcome of this analysis is presented in Table 38: Prioritisation of Semantic Standards.

- **Evaluation and Prioritisation of Semantic Standards:** We used a principles-based selection focused on four checks:

  - **DSO relevance shortlist** (must directly support DSOi objects: grid zones, metering, flexibility lifecycle, authorisation/consent, emergency targeting)
  - **Fitness to the technical functionalities of the Semantic standards layer** (does the standard directly enable the required capabilities?)
  - **Proven reuse in EU projects/pilots** (is it already used in practice within comparable contexts?)
  - **Readiness to implement** (are machine-readable artefacts available, e.g., RDF/OWL, JSON-LD contexts, SHACL shapes?)

- **Shortlisted standards:** IEC CIM (61970/61968), ESMP (62325-351 profile), SHACL, SAREF (incl. SAREF4ENER/4BLDG), DLMS/COSEM (IEC 62056), IEC 61850, OpenADR event model, USEF, OMEGA-X CSDM, SEAS, IFC (ISO 16739).

Table 38: Prioritisation of Semantic Standards

Standard	When it matters most	Priority	Priority rationale & sources
IEC CIM (61970/61968)	Modelling DSOs, grid zones/feeders, metering points, and identities for /Generic/gridZones and /Data/Metering.	High	Canonical DSO/TSO model across the EU, used in Austria pilot and SYNERGY/SYNERGIES, supports inter-DSO sharing (DAT_009 (Deliverable D2.2 Energy services analysis, use cases, and CERF requirements)) and standardization intent (GEN_023 (Deliverable D2.2)).
ESMP (IEC 62325-351 profile)	Market roles/IDs and document semantics across the flexibility lifecycle and settlement.	High	Narrows CIM choices for cross-border consistency, adopted in EDDIE, aligns with verification criteria (SVC_016 (Deliverable D2.2)) and catalogue of standard services (GEN_023 (Deliverable D2.2)).
SHACL	Machine-checkable conformance for metering,	High	Machine-checkable constraints needed for data quality KPIs (SVC_023

	needs/offers/plans, baselines, settlement, and authorisation.		(Deliverable D2.2)) and follow-up tools (DAT_008 (Deliverable D2.2)), fit D4.1 /Data/Authorization.
SAREF (SAREF4ENER/ 4BLDG)	Bridging device/asset KPIs referenced by DSO signals and activation plans to app/IoT semantics.	Medium	Used in InterConnect/Independent; aligned with OMEGA-X CSDM, supports automated actions (APP_002 (Deliverable D2.2)) and DSO-customer exchange (APP_044 (Deliverable D2.2)).
DLMS/COSEM (IEC 62056)	Normalizing OBIS smart-meter data (quantities/units/intervals/timezone) into /Data/Metering.	Medium	Implemented in SYNERGY/SYNERGIES, underpins data availability (SVC_023 (Deliverable D2.2)) and monitoring needs (DAT_008 (Deliverable D2.2)).
IEC 61850	Bringing SCADA/substation values, quality and status into DSO data space and emergency contexts.	Medium	Frequently bridged to CIM, used in the Croatia pilot and the SYNERGY project, and relevant for conveying grid-status inputs and emergency notices to end-users.
OpenADR event model	Normalizing DR terms (eiEventID, signalName, optType, time windows) for needs/activations.	Medium	Used in Croatia pilot and SENDER, supports DSO-customer communication (APP_044 (Deliverable D2.2)) and economic signals (SVC_025 (Deliverable D2.2)).
USEF	Role/process semantics when a market-based flexibility process model is adopted.	Low	Helpful where a USEF process model is adopted (SYNERGY), complements GEN_023 (Deliverable D2.2), optional for core DSOi.
OMEGA-X CSDM	Dataspace exchange with sovereignty/policy metadata on DSO datasets.	Low	Aligns CIM+SAREF with policy tags, relevant when operating in a dataspace, complements inter-DSO sharing spirit (DAT_009 (Deliverable D2.2)).
SEAS	Expressing optimization goals/constraints attached to needs/activation plans.	Low	Used in RESONANCE, can refine SVC_016 (Deliverable D2.2) conditions, optional in core DSOi.
IFC (ISO 16739)	Building/space context when targeting goes beyond grid zones (fine-grained spatial notices).	Low	Applied in SYNERGY, useful for fine-grained spatial semantics, not mandatory for DSOi core.

Each standard is assigned a priority level: **High** (should be implemented by default), **Medium** (should be used when that scope appears (metering, market, substation, dataspace, buildings, optimisation)), **Low** (should be used selectively if it clearly adds value).

- **Priority-Based Implementation Guidelines:**
  - **High (implement by default)**
    - Publish a compact IEC CIM (61970/61968) profile covering grid zones, feeders, metering points, readings, and actor roles with stable identifiers and a JSON-LD @context that maps every DSOi field to a CIM IRI.
    - Adopt ESMP (62325-351) codes for market roles, identifiers, and document headers, document the exact ESMP version/profile choices, and provide a field-to-CIM/ESMP crosswalk for the flexibility lifecycle, so offers/plans/settlement artefacts are portable.
    - Provide a SHACL shape per payload (grid zone, metering series, flexibility need/offer/activation plan, baseline, settlement result, authorisation), enforcing required properties, datatypes, units, and time windows; ship one valid and one invalid example per shape and run them in CI (e.g., FlexOfferShape requires amount (kW, ≥0), timeInterval (start/end), zoneId, actorId).
    - Express time using OWL-Time (instants/intervals with timezone and resolution) and carry data-quality flags that SHACL validates.
    - Version the JSON-LD contexts, SHACL shapes, and mapping tables; avoid IRI repurposing; mark deprecated terms and include a short migration note per release (e.g., “v1.2 adds baselineMethod, v1.3 deprecates offerPower in favour of offerQuantity”).

- **Medium (use when that scope appears)**
    - Map device KPIs and states referenced by DSO signals to SAREF/SAREF4ENER while keeping CIM as the backbone; publish a minimal SAREF↔CIM crosswalk so app/IoT payloads stay consistent.
    - Provide an OBIS→CIM/SAREF mapping for common registers and validate with SHACL that each reading includes OBIS code, unit, value and timestamp.
    - Map logical nodes/data attributes (values, quality, status) to interface terms and preserve quality/timestamp semantics, with examples for measurements, status and alarms.
    - When DR is in scope, express eiEventID, signalName/signalType, optType, intervals and market context in JSON-LD with a dedicated DR SHACL shape and examples for create/modify/cancel.
    - Represent emergency regions as grid zones or polygons with validity windows and severity, reusing CIM location references and a controlled event taxonomy.
- **Low (use selectively when it clearly adds value)**
    - If a market-based process model is required, reuse USEF roles and processes and keep a short mapping back to ESMP/CIM identifiers to avoid duplicating semantics.
    - In data-space exchanges, attach policy/sovereignty metadata (provider, contract/purpose, region) per OMEGA-X CSDM and validate with a small policy SHACL.
    - Where optimization is exposed, annotate objectives/constraints with SEAS and link them to SAREF preferences.
    - If targeting must go below grid zone granularity, link devices/meter points to IFC spaces via persistent URIs and version the bindings.

Cross-cutting (apply to all semantic payloads)

- Use UCUM units, optional SKOS multilingual labels for user-facing terms, and PROV-O/consent references for auditability.
- Provide round-trip tests for each mapping (interface → CIM/ESMP/SAREF → interface) and a conformance kit (contexts, shapes, examples) so partners can self-validate before onboarding (e.g., a Postman/pytest bundle that runs SHACL and field-level checks).

5.6. INTEGRATED VIEW

The three recommended interfaces (Energy App, Data Sources, and DSO Interface) together cover all interoperability needs in ECLIPSE DIGITAL project by linking end-user interaction, flexibility and resource management, and grid-level coordination. At this stage, WP3 Architecture of a scalable and interoperable European open-source CERF and data sets focuses on studying and recommending the foundations for future interoperability profiles by identifying required functionalities, mapping relevant standards across all interoperability layers, and proposing practical guidelines. These outputs serve as the methodological starting point for later work packages, which will implement, validate, and refine the recommendations in real pilot environments. The final interoperability profiles will only be achieved after integration, validation, field feedback, and consolidation in WP4-7.

Table 39: ECLIPSE DIGITAL project recommended interfaces

Profile	Role in Architecture	Primary Interoperability Point	Possible contribution to Project Objectives
Energy App	Edge interface with the end user.	App backend (possibly) Data Space Connector.	Enables personalised feedback and behavioural incentives.
Data Sources (Flexibility & Aggregation)	Middle layer managing resource data and flexibility.	Technical Aggregator and Flexibility/Market platforms.	Supports AI/ML analytics for rewards and flexibility participation.
DSO Interface	Core coordination layer linking operational and market actors.	DSO System and Aggregator/EMS/Meter infrastructure.	Ensures reliable, policy-governed grid interaction and flexibility management.

5.7. REFINEMENT AND VALIDATION

These recommended interoperability points define the behavioural and policy interactions across ECLIPSE DIGITAL's system-of-systems. Initially implemented through APIs and shared data models, they will evolve toward Data Space–enabled interoperability profiles, where connectors embody semantic alignment, technical compatibility, and organisational governance fully aligned with the ISO/IEC 21823-5 methodology for behavioural and policy interoperability.

However, the work carried out in WP3 Architecture of a scalable and interoperable European open-source CERF and data sets (Tasks 3.3) represents the construction and recommendation phase toward the future interoperability profiles of the Common European Reference Framework (CERF).

At this stage, the activities focus on studying, structuring, and recommending not yet defining the final interoperability profiles. The main objective of WP3 is to provide a methodological foundation for building the profiles. This includes:

- Identifying relevant functionalities from WP2 and pilot inputs.
- Mapping applicable standards across the policy, behaviour, semantic, syntactic, and transport layers.
- Recommending practical guidelines for implementation.

These results from the starting point for further development and validation in the next stages.

A true interoperability profile can only be achieved through implementation, validation, and agreement among pilot partners. Therefore, the outputs of WP3 Architecture of a scalable and interoperable European open-source CERF and data sets describe how to build the profiles and propose recommended standards and options, while the final, validated profiles will be produced after real implementation and feedback from pilots. At this stage, WP3 provides the methods, standards mapping, and guidelines needed to build the profiles, whereas the subsequent work packages (WP4-7) will transform these recommendations into validated and agreed interoperability profiles. The refinement process will take place in the following tasks:

- Task 4.2 (Development of the CERF for consumer applications based on Machine learning tools and IA): Integration and Implementation: Application of the WP3 recommendations in pilot environments to identify missing elements and required technical refinements.
- Task 4.4 (Verification, validation and maintenance of the CERF): Verification and Validation: Practical validation of interoperability and collection of pilot feedback to adjust and improve the initial guidelines.

- Task 5.3 (Demonstration activities by real pilots): Field Feedback and Demonstration: In-field verification of interoperability under operational conditions, ensuring that profiles work as expected.
- Task 7.3 (Exploitation plans and IPR activities): Exploitation and Publication: Consolidation, validation, and publication of the final interoperability profiles, integrating the specifications effectively implemented in the pilots.

6. GOVERNANCE OF THE CERF

This section aims at defining the governance of the CERF framework, in order to keep it relevant and interoperable. Governance scheme was included in D4.1 “ECLIPSE DIGITAL CERF for Energy Saving applications_V1” likewise and the full completion is expected by the end of the project.

The energy apps are part of an ecosystem composed of several building blocks. The goal of the CERF is to provide interoperability across these building blocks. Its relevance therefore requires the involvement of several parties.

The goal of this section is to define an agreement process for the upkeep of the CERF, including its functions, components, and interoperability features.

The CERF specification will initially be constituted of the architecture, data exchanges and interoperability profiles defined in this document, along with the cybersecurity, privacy and trustworthiness aspects defined in D3.2: “Energy services analysis, use cases, and CERF requirements”. Further details, such as datasets, APIs, and semantic models may be included at a later date.

6.1. STAKEHOLDERS

The stakeholders involved in the governance of the CERF for energy-saving applications are:

- The developers of the framework: Trialog and ETRA
- The users of the framework: all users of the framework, including ECLIPSE DIGITAL pilots

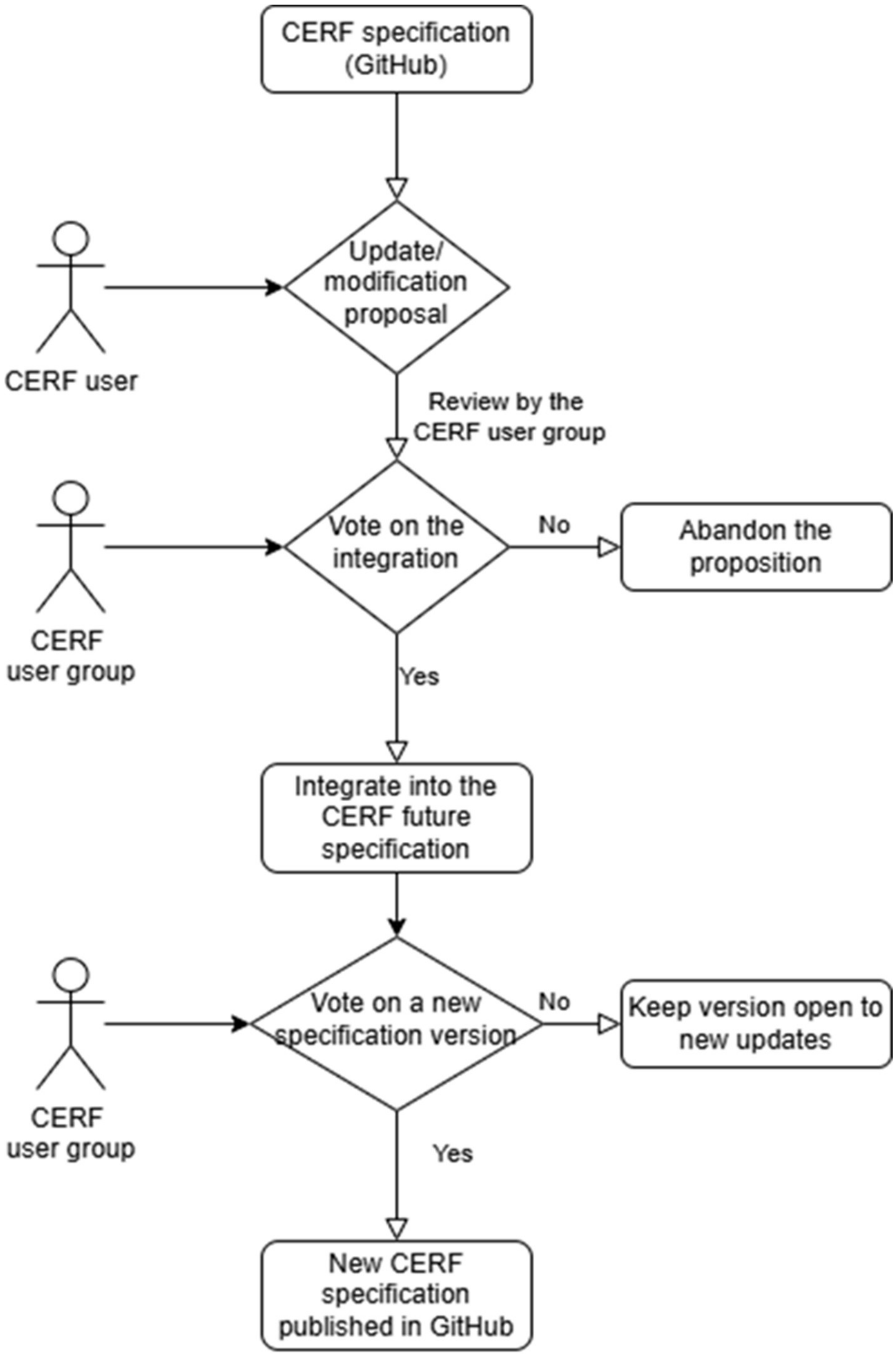
6.2. GOVERNANCE STRUCTURE

The governance of the CERF will be organised through the creation of the CERF user group. This structure will be composed by all voluntary stakeholders who are interested in following the development of the framework. Individual roles such as contributors, validators, will be defined upon members registration.

6.3. AGREEMENT PROCESS

The CERF user group will in particular be responsible for sharing and maintaining the CERF specifications. Updates and modifications of the CERF framework should be submitted to the CERF user group. The CERF user group will review their relevance and integration into the framework and vote on its integration. It the modification is accepted the new specifications of the CERF will be made available on the CERF GitHub.

Table 40: CERF agreement process



7. CONCLUSION

D3.1 consolidates the architectural foundations of the CERF from initial architecture to proposed inclusion of Data Spaces in the ECLIPSE DIGITAL project CERF, and demonstrates how these foundations are instantiated, validated, and extended within the ECLIPSE DIGITAL project. Across its sections, the document positions interoperability, data governance, and modularity as the central enablers for scalable, consumer-centric energy services. By mapping stakeholders to functional capabilities through models such as the hourglass and DERA, the deliverable clarifies how data exchanges, interfaces, and technical components interact across layers, supporting both Data Space–based integration and alternative interoperability pathways already in use.

The analysis highlights how the ECLIPSE DIGITAL CERF architecture accommodates evolving market and policy requirements, covering the roles of Energy Apps, aggregators, data sources, and DSOs. It shows how these components can be aligned with emerging European developments such as CEEDs, INSIEME project High-Value Datasets, provenance metadata, and connector-enabled data sharing. The result is a future-proof architectural blueprint capable of supporting behavioural feedback, flexibility markets, smart-meter analytics, and trustworthy data exchange.

Overall, D3.1 provides a clear and actionable reference architecture for ECLIPSE DIGITAL, while demonstrating its practical relevance through pilot implementations and its readiness to evolve towards full interoperability frameworks, including Energy Data Spaces. It establishes the technical and conceptual grounding for subsequent work on reusable connectors, data governance, and integration patterns that will guide the project’s technical development in later stages.

Complementary, the deliverable D3.2 (Specific Data Protection analysis) describes cybersecurity, privacy, and trustworthiness aspects that can be applied to the CERF. The work done in the WP3 Architecture of a scalable and interoperable European open-source CERF and data sets will be further detailed in refined in the development and operation phases of the project in WP4 Design and development of CERF and APIs and WP5 Preparation, coordination and monitoring of deployment and demonstration activities.

8. REFERENCES AND ACRONYMS

8.1. REFERENCES

[1] EDDIE European project, grant agreement No. 101069510, “EDDIE European Distributed Data Infrastructure for Energy,” 2025. [Online]. Available: https://eddie.energy/. [Accessed 2025].

[2] CEN-CENELEC-ETSI Smart Grid Coordination Group, “Smart Grid Reference Architecture,” 11 2012. [Online]. Available: https://syc-se.iec.ch/wp-content/uploads/2019/10/Reference_Architecture_final.pdf. [Accessed 23 11 2023].

[3] Bridge Data management working group, “European (energy) data exchange reference architecture 3.1,” 2024. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/48792d77-b544-11f0-b37f-01aa75ed71a1/language-en. [Accessed 2025].

[4] B. D. M. W. GROUP, “European (energy) data exchange reference architecture 3.1,” Publications Office of the European Union, Luxembourg, 2024.

[5] CEI Sphere European project, Grant Nb 101189683, “Hourglass Model,” 2025. [Online]. Available: https://ceisphere.eu/hourglass-model. [Accessed 2025].

[6] OASC, “MIMs,” 2025. [Online]. Available: https://oascities.org/minimal-interoperability-mechanisms/. [Accessed Nov 2025].

[7] ISO/IEC/IEEE, “ISO/IEC/IEEE 42010:2022,” 2022. [Online]. Available: https://www.iso.org/standard/74393.html. [Accessed 17 11 2025].

[8] H2020 InterConnect Project, “A Common European Reference Framework for energy saving applications for consumers,” May 2023. [Online]. Available: https://interconnectproject.eu/wp-content/uploads/2023/05/20230510_InterConnect_CERF-and-energy-applications-technical-overview_clean.pdf. [Accessed 18 11 2025].

[9] E.DSO, “The new ECLIPSE DIGITAL project will facilitate energy consumption reduction and support the stability and resilience of European power grids through the implementation of an open-source reference framework,” 14 October 2024. [Online]. Available: https://www.edsoforsmartgrids.eu/the-new-ECLIPSE DIGITAL-project-will-facilitate-energy-consumption-reduction-and-support-the-stability-and-resilience-of-european-power-grids-through-the-implementation-of-an-open-source-reference-framework.

[10] E.DSO, "ECLIPSE DIGITAL," 2025. [Online]. Available: https://www.edsoforsmartgrids.eu/eu-projects/ECLIPSE DIGITAL/.

[11] InterConnectProject, "InterConnect," November 2023. [Online]. Available: https://interconnectproject.eu/energy-applications.

[12] W. S. S. G. C. S. G. H. Shievam Kashyap, "Energy Data Governance Fragmentation in Europe: Challenges, Models, and Pathways to Integration," *21st International Conference on the European Energy Market (EEM) - IEEE,* pp. 1-6, 2025.

[13] Smart Energy Expert Group (SEEG)/ Data for Energy (D4E) , " Use Case 3: Flexibility aggregation and activation," 2025.

[14] ENTSO-E, "The Harmonised Electricity Market Role Model," ENTSO-E, 2025.

[15] ETSI, "The Smart Applications REFerence Ontology (SAREF)," 2025. [Online]. Available: https://saref.etsi.org/. [Accessed 2025].

[16] Interoperability Network for the Energy Transition (int:net), "Blueprint of the Common European Energy Data Space Version 3.0," September 2025. [Online]. Available: https://intnet.eu/images/Blueprint_CEEDS_v3.0.pdf. [Accessed 18 11 2025].

[17] C.-C.-E. S. G. C. Group, "SGAM User Manual - Applying, testing & refining the Smart Grid Architecture Model (SGAM)," M/490 Mandate Smart Grids, EU, 2014.

[18] CEI Sphere, "Hourglass model," 2025. [Online]. Available: https://ceisphere.eu/hourglass-model. [Accessed 2025].

[19] ISO, “ISO 15836-1:2017 Information and documentation — The Dublin Core metadata element set,” 2017. [Online]. Available: https://www.iso.org/standard/71339.html. [Accessed 2025].

[20] ISO, “ISO/IEC 11179-1:2023 Information technology — Metadata registries (MDR),” ISO, 2023. [Online]. Available: https://www.iso.org/standard/78914.html. [Accessed 2025].

[21] W3C, “Data Catalogue Vocabulary (DCAT) - Version 3,” 2024. [Online]. Available: https://www.w3.org/TR/vocab-dcat-3/. [Accessed 2025].

[22] CWM, “Common Warehouse Metamodel (CWM) Specification,” 2023. [Online]. Available: https://www.omg.org/spec/CWM/1.1/PDF/. [Accessed 2025].

[23] CKAN, “CKAN 2.11.3,” 2025. [Online].

[24] data.gouv.fr, “Guides et documentations,” 2025. [Online]. Available: https://guides.data.gouv.fr/.

[25] Magda, “Magda,” 2025. [Online]. Available: https://magda.io/. [Accessed 2025].

[26] DKAN, “DKAN documentation,” 2024. [Online]. Available: https://dkan.readthedocs.io/en/latest/. [Accessed 2025].

[27] DataHub, “What is DataHub?,” 2025. [Online]. Available: https://docs.datahub.com/docs/features. [Accessed 2025].

[28] OpenMetadata, “Local Docker deployment,” 2025. [Online]. Available: https://docs.open-metadata.org/quick-start/local-docker-deployment. [Accessed 2025].

[29] Apache Atlas, “Overview,” 2025. [Online]. Available: https://atlas.apache.org/#/. [Accessed 2025].

[30] The Apache Software Foundation, “Gravitino,” 2025. [Online]. Available: https://gravitino.apache.org/. [Accessed 2025].

[31] Amundsen, “Amundsen,” 2020. [Online]. Available: https://www.amundsen.io/amundsen/. [Accessed 2025].

[32] ODD platform, “about ODD,” 2024. [Online]. Available: https://docs.opendatadiscovery.org/. [Accessed 2025].

[33] Marquez, “Quickstart,” 2025. [Online]. Available: https://marquezproject.ai/docs/quickstart/. [Accessed 2025].

[34] Tomorrow's Homes Today project, “Tomorrow's Homes Today - THT,” 2024. [Online]. Available: https://www.linkedin.com/company/tomorrow-s-homes-today-tht/posts/?feedView=all. [Accessed 2025].

[35] SYNERGY European project Grant Agreement No 872734, “SYNERGY - A Big Data and AI Analytics Platform,” 2025. [Online]. Available: https://synergyh2020.eu/. [Accessed 2025].

[36] CheckWatt, “Increase the value of your flexible energy resources,” 2025, [Online]. Available: https://checkwatt.com/en/. [Accessed 2025].

[37] SENDER European Project grant agreement No. 957755, “SENDER Sustainable Consumer Engagement and Demand Response,” 2025. [Online]. Available: https://www.sender-h2020.eu/. [Accessed 2025].

[38] Parmenides European Project, “Parmenides Plug&plAy eneRgy ManagEmeNt for hybrID Energy Storage,” 2025. [Online]. Available: https://parmenides-project.eu/. [Accessed 2025].

[39] WE DISTRICT European project grant agreement N°857801, “Heating & cooling solutions,” 2025. [Online]. Available: https://www.wedistrict.eu/. [Accessed 2025].

[40] European project HEDGE-IoT , “HEDGE-IoT Holistic Approach towards Empowerment of the DiGitalization of the Energy Ecosystem through adoption of IoT solutions,” 2025. [Online]. Available: https://hedgeiot.eu/. [Accessed 2025].

[41] OMEGA-X European Project Grant Agreement No. 101069287, “Orchestrating an interoperable sovereign federated Multi-vector Energy data space built on open standards and ready for GAia-X,” 2025. [Online]. Available: https://omega-x.eu/. [Accessed 2025].

[42] ISO/IEC JTC 1/SC 41, “Internet of Things and related technologies,” 2018.

[43] ENTEC Energy Transition Expertise Centre, “Common European Energy Data Space,” October 2023. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/43b8d2d1-6975-11ee-9220-01aa75ed71a1 . [Accessed 18 11 2025].

[44] Gaia-X, “Deliverables & Gaia-X Standard,” Gaia-X, [Online]. Available: https://gaia-x.eu/services-deliverables/deliverables/. [Accessed 18 11 2025].

[45] “IDSA Rulebook,” International Data Spaces, [Online]. Available: https://docs.internationaldataspaces.org/ids-knowledgebase/idsa-rulebook/idsa-rulebook/1_introduction. [Accessed 18 1 2025].

[46] Gaia-X, “Gaia-X Compliance Document - 25.03 Release,” [Online]. Available: https://docs.gaia-x.eu/policy-rules-committee/compliance-document/25.03/. [Accessed 18 11 2025].

[47] IEC, “IEC Use Case - D4E Flexibility Usecase V1.3,” 2025.

8.2. ACRONYMS

Table 41 : Acronyms

Acronym	Signification
aFRR	Automatic Frequency Restoration Reserves
AI	Artificial Intelligence
AIIDA	Administrative Interface for In-house Data Access
API	Application Programming Interface
App	Application
BMS	Building Management System
BSP	Balancing Service Provider
CEEDS	Common European Energy Data Space
CEM	Customer Energy Management
CIM	Common Information Model
CO_2	Carbon
CPO	Charge Point Operator
CRUD	Create Read Update Delete
CSVW	CSV on the Web
DC	Direct Current
DCAT-AP	Data Catalogue Application Profile (EU)
DER	Distributed Energy Resources
DERA	Data Exchange Reference Architecture
DLMS/COSEM	Device Language Message Specification / Companion Specification for Energy Metering
D4E	Data for Energy
DPV	Data Privacy Vocabulary
DSM	Demand-Side Management
DSO	Distribution System Operator
EAN	European Article Number
EDDIE	European project EDDIE
EIC	Energy Identification Code
EMF	ECLIPSE DIGITAL Modelling Framework
EMS	Energy Management System

ECLIPSE DIGITAL ESMF	ECLIPSE DIGITAL Semantic Modelling Framework
ESMP	European Style Market Profile
ESS	Energy storage system
EV	Electric Vehicle
FFR	Frequency Firming Reserve
FCR	Frequency Containment Reserve
GA	Generic Adapter
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HEMS	Home Energy Management System
HLUC	High-Level Use Case
HTTP / HTTPS	HyperText Transfer Protocol (Secure)
HVAC	Heating Ventilation and Climatization
HVD	High Value Data
IEC	International Electrotechnical Commission
IED	
IFC	Industry Foundation Classes
IoT	Internet of Things
IDP	Identity Provider
ISO	International Organization for Standardization
JSON / JSON-LD	JavaScript Object Notation / for Linked Data
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
MDMS	Meter Data Management System
MIM	Minimum Interoperability Mechanism
MQTT	Message Queuing Telemetry Transport
MPxN	Meter Point Number
NGSI-LD	Next Generation Service Interface – Linked Data
OBIS	Object Identification System
ODRL	Open Digital Rights Language
OMEGA-X CSDM	Common Semantic Data Model from the project OMEGA-X
OMAS / OMRS	Open Metadata Access / Repository Services

OPA	Open Policy Agent
OpenADR	Open Automated Demand Response
OWL-Time	Time ontology in OWL
P2P	Peer-to-Peer
PAS 1878 / 1879	UK Smart Appliance & DR specs
PECO	PARMENIDES Energy Community Ontology
PKI	Public Key Infrastructure
PROV-O	Provenance Ontology
POD	Public Open Data
QoS	Quality of Service
RDF	Resource Description Framework
PV	Photovoltaic
RA	Reference Architecture
RESONANCE Ontology	Hybrid P2P & DSO semantic ontology
REST	Representational State Transfer
RM	Resource Manager
SCADA	Supervisory Control and Data Acquisition
SDK	Software Development Kit
SEAS	Smart Energy Aware Systems
SEEG	Smart Energy Expert Group
SGAM	Smart Grid Architecture Model
SHACL	Shapes Constraint Language
SLA	Service Level Agreement
SM	Smart Meter
SKOS	Simple Knowledge Organization System
SAREF	Smart Applications REFerence
SPARQL	SPARQL Protocol and RDF Query Language
SPOF	Single Point of Failure
SSL / TLS	Secure Sockets Layer / Transport Layer Security
SYNERGIE	European project SYNERGIE
TASE.2 / ICCP	Inter-Control Centre Protocol
TSO	Transmission System Operator
UCUM	Unified Code for Units of Measure

UML	Unified Modelling Language
URI / IRI	Uniform / Internationalized Resource Identifier
USEF	Universal Smart Energy Framework
V1G	Smart charging
V2X	Vehicle to anything
VPP	Virtual Power Plant
W3C	World Wide Web Consortium
XML / XSD	eXtensible Markup Language / XML Schema Definition

Thank

You

If you have any questions, please get in touch with us.

eclipse

www.ECLIPSE DIGITAL-

info@ECLIPSE DIGITAL-

@ECLIPSE

@ECLIPSE

@ECLIPSE