RODEO

Co-funded by the European Union

The Provision of Open Access to Public Meteorological Data and Development of Shared Federated Data Infrastructure for the Development of Information Products and Services

RODEO Project

DIGITAL-2022-CLOUD-AI-02-OPEN-AI

Work Package 2 (User Interface)

FULL DETAILED DESIGN

Date: 22nd July 2024

Doc. Version: 1.0

Document Control Information

Settings	Value
Document Author:	Eetu Niemi
Document Owner:	Jane Wardle
Type of Document	Deliverable
Sensitivity:	Public
Document version	1.0
Date:	22nd July 2024

Document Acceptance Criteria

This certifies that the Deliverables/Milestones Acceptance Checks have been reviewed and confirmed by WP Lead and Project Manager.

Criterion	Result	Verified by	Accepted by
Detailed solution and operating model design	Version 1.0 done	Jane Wardle	

Document Approver(s) and Reviewer(s):

NOTE: All Approvers are required. Records of each approver must be maintained.

Name	Role	Action	Date
FEMDI ET Chair	External reviewer	Reviewed and suggested updates	19th June 2024
Mikko Rauhala	WP2 Chief Architect Approver	Reviewed and confirmed technical accuracy.	1st July 2024
Jane Wardle	WP2 Programme Manager Approver / reviewer	Reviewed and a final version fulfils requirements for the Deliverable.	22nd July 2024
Timo Kyntäjä, FMI	RODEO project co-ordinator, project manager Approver	Confirm conformance with EU requirement and approve	23rd July 2024

Document history:

The Document Author is authorized to make the following types of changes to the document without requiring that the document be re-approved:

- Editorial, formatting, and spelling
- Clarification and change of documentation location

To request a change to this document, contact the Document Author or Owner.

Changes to this document are summarized in the following table in reverse chronological order (latest version first).

Revision	Date	Created by	Short Description of Changes

Configuration Management: Document Location

The latest version of this controlled document is stored in the RODEO SharePoint.

Summary

This document is Deliverable 2.2 “Full Detailed Design” of the RODEO project.

This document describes the detailed solution and operating model design for the RODEO work Package 2 (WP2). This is also known as EUMETNET’s Federated European Meteorological Data Infrastructure (FEMDI) Community Components. FEMDI enables sharing hydrological and meteorological data through implementation of federated capabilities. The document is intended for all parties that are concerned with the implementation, operation, or utilisation of FEMDI, or anyone interested in FEMDI.

Contents

1. Introduction

1.1 Purpose

This is the “Full Detailed Design” deliverable for the RODEO project Work Package (WP) 2 – User Interface. The document describes detailed solution and operating model design for the EUMETNET Federated European Meteorological Data Infrastructure (FEMDI).

FEMDI enables sharing hydrological and meteorological data through implementation of federated capabilities in line with the World Meteorological Organization’s (WMO) Information System 2.0 (WIS 2.0) and the European Union’s (EU) regulation on Meteorological High Value Data (HVD).

1.2 Scope

The scope of this document is RODEO WP2 – User Interface.

This includes the development of technical components, known as the FEMDI Community Components, and the underpinning operating model.

The operating model scope covers the overarching system, ensuring it functions well together.

- Data publishers can use their own policies and processes, as long as the data provided complies with the FEMDI data requirements.
- For the Community components, the FEMDI will define the required outcomes for the hosting organisations, rather than the processes to be used, in the SLAs.

In scope

FEMDI Community Component design

These include the following components:

- Data Explorer
- API Gateway
- Identity & Access Manager
- Developer Portal
- Key Vault
- Insights Service

FEMDI Operating Model high-level design for Community Components

This includes aspects which will ensure the quality of the services provided by the FEMDI Community Components. This includes:

- FEMDI governance structures and responsibilities
- Overview of policies for FEMDI Community Component users
- Overview of processes related to Community Components

Out of scope

Local and other component design

Local and other components are only addressed in the context of understanding the operation of FEMDI as a whole. Therefore, detailed design for Local Components, such as Data Supply capabilities, and the WMO WIS 2.0 components are not included. Some of the Local components are covered, to an extent, by the other WPs of the RODEO project.

Components that are addressed in this document which are out of scope:

- Data Supply
- WMO WIS 2.0 Global Discovery Catalogue
- WMO WIS 2.0 Global Broker
- 3rd Party Identity Provider
- 3rd Party Configuration Management Tool
- Computation Service
- Data Publisher applications, that provide data to be shared through FEMDI
- Data Consumer applications, that are used to access data through FEMDI

FEMDI Operating Model details and Operating Model for Local and other components

Details of the Operating Model for Community Components, including e.g. policies, instructions, and process diagrams, are included in FEMDI documentation that is published once FEMDI is operational.

Operating Model for Local and other components is not described in this document. However, the FEMDI Operating Model touches on some aspects of operating Local components (e.g. incorporating Data Supply components into FEMDI).

1.3 Audience

In addition to EU and EUMETNET governance, this document is intended for all parties that are concerned with the implementation, operation, or utilisation of FEMDI Community Components, or anyone interested in FEMDI.

1.4 RODEO Project Work Package 2

WP2 has the following objectives:

- To provide the underpinning infrastructure and data-sharing tools, architecture, and governance mechanisms to create a European data space for meteorology, in line with the 'Design Principles for Data Spaces' paper by the end of 2025.
- To provide the foundation discovery and access capability to be used by WP3, 4, 5 and 6 to enable European public sector organisations' (NMHSs) to openly share their High Value Datasets for meteorology by the end of 2025.

The purpose of WP2 is to design and implement the critical underpinning infrastructure and data-sharing tools, architecture, and governance mechanisms required for a meteorological data space to function with federated data by the end of 2025. It provides foundation discovery and access capabilities to access shared meteorological data. It builds on and implements EUMETNET's FEMDI design.

1.5 RODEO Project Glossary

API Gateway: a FEMDI Community Component that provides managed access to shared data. It manages data requests and data access flow (by e.g., providing security, priority access, request limiting and rate limiting). The API Gateway also collects data on transactions to provide data usage and publishing information.

API Management: technical capability and process for creating and publishing APIs on the web, enforcing their usage policies, controlling access, collecting, and analysing usage statistics, and reporting on performance. FEMDI API Gateway implements API Management in FEMDI context.

API: application programming interface, see e.g. FEMDI API Guidance.

Capability Operator (Local and Community): An entity providing and operating infrastructure to allow for data to be discovered and shared. They will provide support services and manage access to the services for which they are responsible.

Community Component: FEMDI infrastructure owned and operated by EUMETNET Members which enables meteorological HVD data to be discovered and shared.

Computation service: A potential future FEMDI Community Component for enabling users to process data. Where possible, this will be offered closer to the data and may implement multiple instances to meet the requirements.

Data Consumer: An entity, such as an organisation, individual or IT application, that consumes data.

Data Explorer: a FEMDI Community capability that enables users to search and browse the data available from Data Supply components that have been registered with FEMDI.

Data Owner: An entity (individual or organisation) which owns the data. They have the authority to decide how their data can be used through rights, obligations, terms and conditions.

Data Publisher: An entity that collects and shares data with Data Consumers in line with the FEMDI terms and conditions. This role may be the Data Owner as well, or do this on behalf of the Data Owner, or provide a technical means for the Data Owner to enable data sharing with other participants.

Data Supply: a FEMDI Local Component that is used to share data, manage, and publish its metadata, and publish notifications about changed metadata and data.

ECMWF: European Centre for Medium-range Weather Forecasting.

EDR: Environmental Data Retrieval, refers to an OGC API for accessing environmental data.

EMI: European Meteorological Infrastructure.

E-SOH: EUMETNET Supplementary Observations dataHub. This is being developed by RODEO Work Package 3. The objective of E-SOH is to provide a sustainable and standardized system for sharing real-time meteorological observations in line with the World Meteorological Organization's (WMO) Information System 2.0 (WIS 2.0) and the European Union's (EU) regulation on Meteorological High Value Data (HVD).

EUMETNET: A network of 31 European NMHSs. Partially funding the RODEO work.

EUMETSAT: European Organisation for the Exploitation of Meteorological Satellites.

EWC: European Weather Cloud. A cloud-based collaboration platform for meteorological application development and operations in Europe, being developed and run by ECMWF and EUMETSAT.

FAIR Principles: Uniformly accepted principles for sharing scientific data.

FEMDI: Federated European Meteo-hydrological Data Infrastructure. The User Interface for discovering and accessing data, being partially delivered through RODEO WP2.

FEMDI Expert Team: A EUMETNET team of experts providing technical and policy recommendations and support to the FEMDI Coordinating Member

FMI: Finnish Meteorological Institute.

Global Discovery Catalogue: A WMO Component for managing metadata records that describe shared data assets and provide a mechanism to search through those records to find data assets.

Global Message Broker: a WMO Component with a subscription service for notifications about the updates to both discovery metadata and the data.

GUI: Graphical User Interface that allows users interact with information systems.

HVDs: High Value Datasets, defined in EU implementing regulation. For meteorology: observations, climate, radar, Numerical Weather Prediction, and warnings.

Identity & Access Manager: A FEMDI Community Component to control user and system access to platforms and platform services.

Insights service: A FEMDI Community Component for reporting on data discovery and publication transactions for Data Publishers to derive management information.

Local Component: FEMDI infrastructure owned and operated by Data publishers. Data Supply is a typical example of a Local Component.

NMHS: National Meteorological and Hydrological Service. Often used interchangeably with 'NMS'.

NMS: National Meteorological Service. Often used interchangeably with 'NMHS'.

OGC: Open Geospatial Consortium. Develops open API standards for providing and using geospatial data.

OSCAR: WMO application operated by MeteoSwiss that provides detailed information on observing capabilities, such as automatic weather stations.

RODEO Project: "The Provision of Open Access to Public Meteorological Data and Development of Shared Federated Data Infrastructure for the Development of Information Products and Services." 50% funding from the EU's Digital Europe Programme, with significant funding also from EUMETNET. There are 7 work packages.

WIS 2.0: WMO Information System version 2.0. This provides a framework for WMO data sharing in the 21st century, for all WMO Members and WMO programmes to embrace the Earth system approach, enable the WMO unified data policy, and support the WMO global basic observing network.

WMO: World Meteorological Organisation – a UN Agency with 193 Members.

WP Lead: Responsible for day-to-day management of their WP in the RODEO project, ensuring delivery on time, within budget and scope.

WP: Work Package – there are 7 WPs in the RODEO project.

1.6 FEMDI Stakeholders

This section describes FEMDI stakeholders and their mutual interaction.

Governance

- **FEMDI Owner:** The organisation responsible for development, operation, maintenance, and funding of the FEMDI system.
  EUMETNET is the owner of FEMDI. EUMETNET Assembly will be the topmost governing body with overarching governance for strategic, technical, financial, and legal aspects of FEMDI.
- **FEMDI Coordinating Member:** The organisation with delegated authority from the FEMDI Owner for the operation of the whole of the FEMDI Programme. This organisation will be a Member of EUMETNET and selected through a robust bidding and assessment process. This role will coordinate and govern FEMDI operations and is responsible for the FEMDI Operating Model. It includes, for example, FEMDI Programme Manager and Coordinator roles.
- **FEMDI Expert Team:** A EUMETNET team of experts providing technical and policy recommendations and support to the FEMDI Coordinating Member. The membership is open to EUMETNET Members, with observers from other organisations as appropriate.

Community Component Roles

- **FEMDI Community Capability Operators:** Provide, operate, and maintain the infrastructure to allow for data to be discovered and shared through FEMDI. They provide support services and manage access to the services they are responsible for. Community Capability Operators are selected from EUMETNET Members, ECMWF and EUMETSAT.

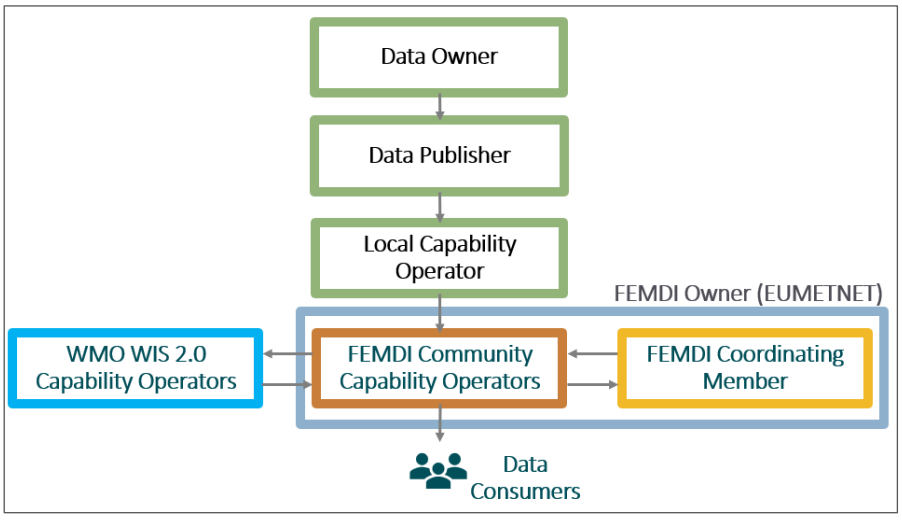
Dependency on: **WMO WIS 2.0 Capability Operator:** Provides and operates the common infrastructure for the WIS 2.0 system. There are Local capability operators that operate a WMO WIS 2.0 compliant Data Supply Component. In addition, there are Global capability operators that operate shared WMO 2.0 components, some of which are also used in FEMDI.

Data Supply Roles

- **Data Owner:** Maintains the authority to decide how their data can be used through rights, obligations, terms, and conditions. They are typically EUMETNET Members.
- **Data Publisher:** Collects and shares data using FEMDI. This role may be the Data Owner as well, or act on behalf of another Data Owner. They are typically EUMETNET Members.
- **Local Capability Operator:** Provides and operates a Data Supply Capability which integrates with the FEMDI Community capabilities. They will provide support services and manage access to the services they are responsible for. They will also have technical mechanisms to ensure others are compliant with FEMDI. Local Capability Operator can be the same party as Data Owner and/or Data Publisher. They are typically EUMETNET Members.
- **Data Consumer:** The individual or organisation that accesses shared data through FEMDI and utilises it. Data Consumers include, for example, NMHSs, public and private sector organisations, research institutions, and citizens.

3rd Party Data Publisher is a Data Publisher that shares data through FEMDI but are not EUMETNET Members (for example, private companies).

The interaction of the roles is shown in the following diagram.



Interaction between roles in FEMDI

1.7 References

This section lists and links to different kinds of references related to FEMDI and RODEO Project.

EU Direction

- EU Commission Implementing Regulation 2023/138 on High Value Datasets
- EU INSPIRE Directive (2007/2)
- EU Open Data Directive (2019/1024)
- Design Principles for Data Spaces

RODEO Project Internal Documentation

- FEMDI Overview presentation
- FEMDI Glossary
- RODEO WP2 Discovery Phase Results
- FEMDI Use cases
- RODEO WP2 User Stories as Steps in System
- FEMDI RODEO Data Explorer Paper-Based Study and Next Steps
- RODEO FEMDI Test Plan
- RODEO Quality of Service draft guidance

RODEO Project Deliverables

- RODEO Requirements Specification
- RODEO Full Detailed Design (this document)

FEMDI Documentation – to be published once FEMDI is operational

- FEMDI API Guidance
- FEMDI Data Governance Policy (draft)
- FEMDI Incident and Problem Management Policy (draft)
- FEMDI Participation Management Policy (draft)
- FEMDI Privacy Policy (draft)
- FEMDI Manual (draft)

FEMDI Community Component Repositories and Developer Documentation

- API Gateway
- Developer Portal
- Infrastructure

External Solutions

- E-SOH Requirements document
- Guide to WMO Information System (WMO No. 1061) Volume II - WMO Information System 2.0
- Manual on the WMO Information System (WMO No. 1060) Volume II - WMO Information System 2.0
- WIS2 in a box
- WIS2 Notification Message Encoding
- WMO Core Metadata Profile version 2 (WCMP2)
- WMO WIS 2.0 Discovery Metadata exchange, harvesting and search pilot: Project Report

Standards

- Discovery Metadata vocabulary

- FAIR Principles
- FEMDI Principles
- OpenAPI Specification
- OGC-API
- OGC-API-EDR
- OGC-API-Records
- MQTT Specification
- WMO Core Metadata Profile 2 (WCMP2) specification
- WMO Core Metadata Profile 2 (WCMP2) metadata examples

2. Overall Architecture

2.1 FEMDI Principles

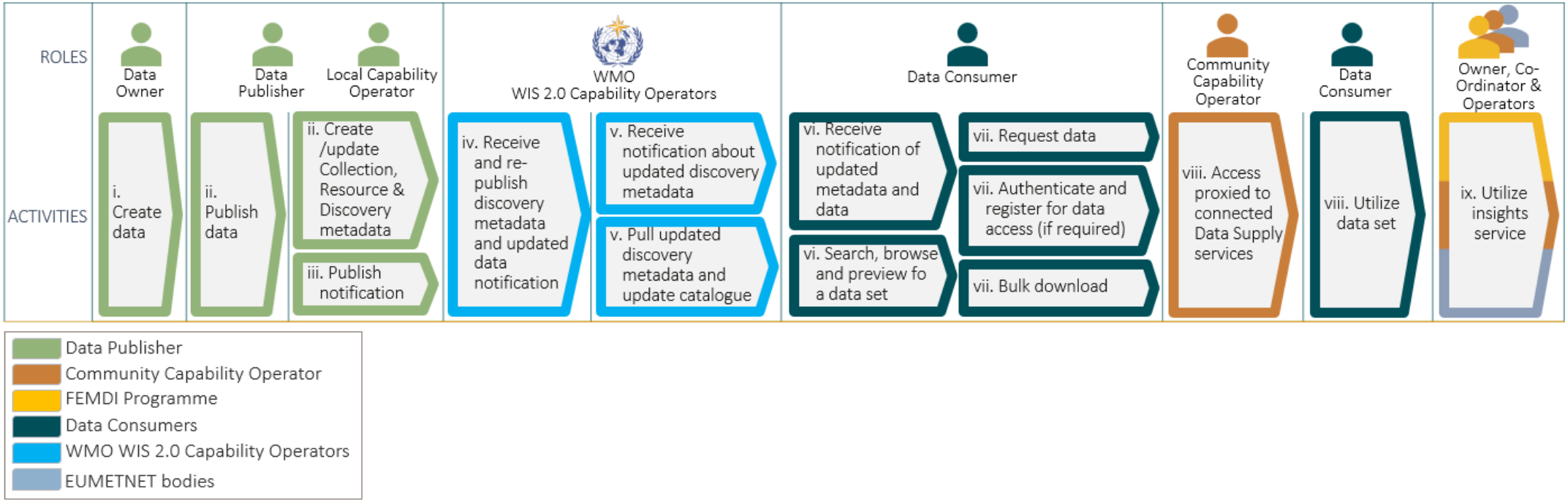
The following principles have been agreed by the EUMETNET Members to guide the development and implementation of FEMDI:

1. FEMDI will enable sharing of hydrological and meteorological data holdings both among the EMI and between the EMI and external stakeholders (global WMO community, public and private sector bodies, research institutions, citizens etc.). FEMDI will be part of the WMO Information System WIS 2.0 and will implement the WIS 2.0 principles.
2. The initial scope of the FEMDI includes sharing the following categories of data: Core Data (WMO Unified Data Policy), Meteorological High Value Data (EU Regulation 2019/1024), and Data for Official Duty[1] (ECOMET GA 13). The FEMDI will be extensible so that additional functions can be incorporated as user requirements emerge.
3. FEMDI will enable data sharing in a manner that is compliant with national and international legislation, regulation, and policy commonly applicable to the EMI, with priority given to obligatory requirements.
4. FEMDI will support the data-sharing policies commonly used within the EMI including, but not limited to, free and open data exchange.
5. FEMDI will neither affect ownership of shared data holdings nor impose additional conditions on data sharing.
6. The ownership, origin and license / usage terms of data holdings shared via FEMDI will be visible to all stakeholders.
7. Policies and technical standards ensuring interoperability and consistency of operation among components of FEMDI will be mutually agreed and maintained by European NMHSs, EUMETSAT and ECMWF under the auspices of EUMETNET.
8. FEMDI will comprise of multiple components (e.g. data sharing platforms and systems), each owned and operated by constituents of the EMI and conforming with the mutually agreed policies and technical standards. Providers of FEMDI components are encouraged to develop and/or operate them in a manner that supports the community. FEMDI components may form part of national data sharing infrastructures and vice versa.
9. FEMDI will build upon existing data sharing infrastructures, incorporating them when they conform to the mutually agreed policies and standards. FEMDI will undergo continuous development as needs arise in the EMI.
10. FEMDI will provide access to data holdings in-situ where local capability exists to do so. Moving data to a remote system only to support data sharing should be avoided.
11. FEMDI will have a single catalogue describing all its data holdings and will provide mechanisms to enable users to search for the data they need. FEMDI will make metadata contribution to the catalogue easy; aiming to avoid duplicate effort where Data Publishers contribute to multiple data sharing initiatives.

[1] Definition of Official Duty: "All activities which take place within the organization of an NMS, and external activities of the NMS resulting from legal, governmental and intergovernmental requirements relating to defence, civil aviation and the safety of life and property."

2.2 High-Level End-to-End Process

This section describes the high-level 'data publication to access' end-to-end process. It describes the flow from publishing to utilising data through FEMDI. It includes roles and activities involved in the process. The process is described in the following diagram. Each of the activities is subsequently discussed.



High-level end-to-end process for FEMDI

i. **Create Data:** In its operations, the Data Owner creates or updates data (for example, observations from automated weather stations or weather model data) in its applications.

ii. **Publish data:** The Data Publisher:
   - Collects the data (manually or automatically) and publishes it on its Data Supply component either
     - as an addition to an existing data set, for example, one update cycle worth of new data added to a data set consisting of weather observations; or,
     - if the shared data forms a completely new data set, one is created.
   - Updates the Collection-level metadata if required.
   - Creates or updates the Resource-level metadata.
   - Manually updates the Discovery metadata on the Data Supply referring to the new or updated data, if required.
     Note: Discovery metadata does not change often. It may change, for example, if there is a fundamental change in the scope of the shared data, or a change in Data Publisher information or data licensing. New discovery metadata also needs to be created for completely new data sets.

iii. **Publish notification:** The Local Capability Operator publishes a notification to advertise the new discovery metadata and/or data.

iv. **WMO re-publishes notification:** The WMO WIS 2.0 Global Broker subscribes to notifications from the Data Supply. It then re-publishes notifications about the new data and metadata to all applications which have subscribed to them.

v. **Update WMO catalogue:** The WMO WIS 2.0 Global Discovery Catalogue subscribes to notifications from the Global Broker and thus gets notified of new and updated discovery metadata. When it gets notified about such a change, the Global Discovery Catalogue fetches the updated discovery metadata and updates the catalogue accordingly.

vi. **Find data:** Data Consumers can be made aware about available data in various ways. They can:
   - Subscribe to notifications from the Global Broker and be notified about updated metadata and data.
   - Find the datasets that meet their needs using the Data Explorer by browsing or searching for datasets with specific characteristics.
   - Search and browse the WMO's Global Discovery Catalogue, in cases where a summary of the available data sets is sufficient.
   - Search via common search engines – records in the WMO Global Discovery Catalogue are indexed by the search engines enabling data consumers to find them via their favourite/normal search path.

vii. **Request data:** Using information provided in the discovery metadata, the Data Consumer can:
   - Make anonymous requests for shared data through the API Gateway.
   - When required by a data policy and in line with EU regulation, the API Gateway requires authentication from the user using an API Key. A Data Consumer can obtain an API Key by registering to FEMDI using a trusted 3rd Party Identity Provider.
   - Bulk download data.

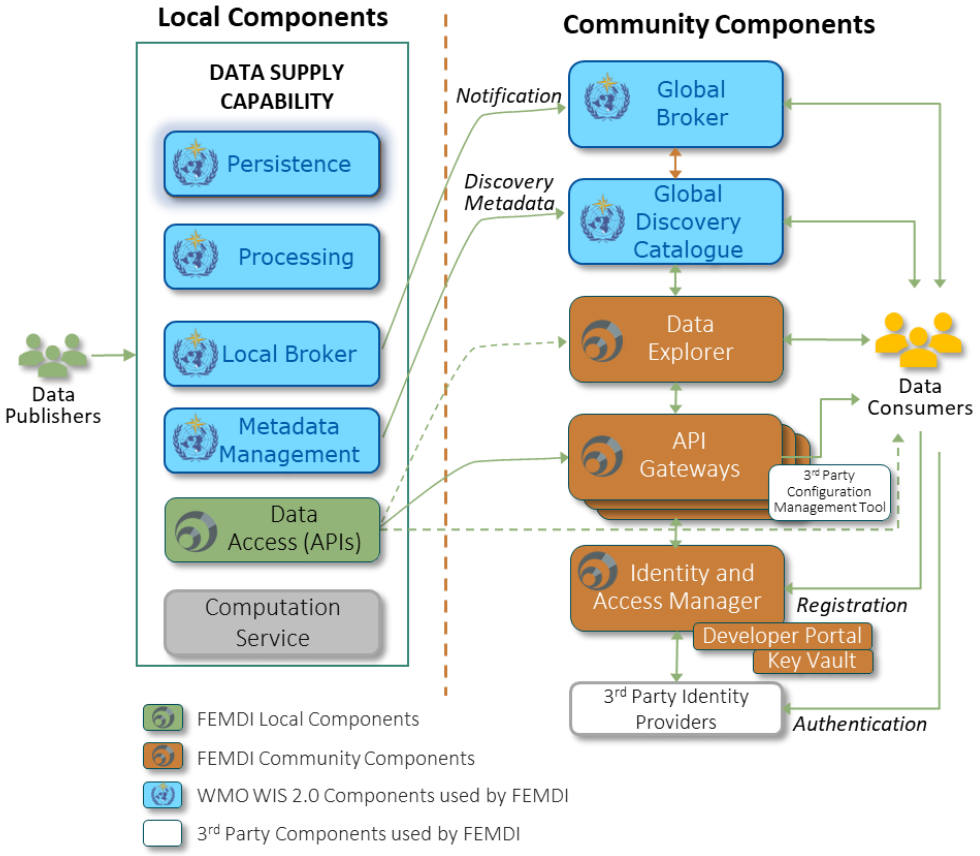
viii. **Proxied access:** The API Gateway proxies access to connected Data Supply services. The user can then utilise the data in their own applications.
   Note: Using the API Gateway is optional for the Data Publisher. They can also publish the data directly from the Data Supply (for example, if the data set is very large or if the Data Publisher already has API Management implemented as part of their Data Supply capability).

ix. **Insights service:** Community Capability Operators and other stakeholders can use the Insights service in the API Gateway to monitor data discovery and use. For example, they can observe how the data is passing through the system to be able to address any issues.

2.3 Architecture Overview

This section gives an overview of the technical components and information flows of the FEMDI solution. It contains a high-level description of the FEMDI components, how they fit together and what they need to do. Note that in addition to FEMDI-specific components, FEMDI utilises Local components, WMO WIS 2.0 components, and 3rd Party components. A more detailed description of the Community Components is given in Chapter 3, Solution Design.

An overview of the components and information flows is provided in the following diagram. Subsequently, the functionality of each component is described on a high level. The description of information flows is simplified.



Components used by FEMDI and information flows between them

RODEO WP2 Community Components

API Gateways

API Gateways provide managed access to the data shared through FEMDI. They manage data requests and data access flow by e.g., providing security, priority access, request limiting, and rate limiting measures. The API Gateway also collects data on transactions to provide data usage and publishing information through the Insights Service.

API Gateways handle data requests from Data Consumer applications, provide security and access control, and proxy access to connected Data Supply services. The API Gateway may need to identify

(authenticate) users accessing some datasets, as stated in the data policy. The API Gateway uses unique tokens (API Keys) appended to data access requests to identify users. Users must register in the FEMDI Developer Portal to obtain an API Key.

The API Gateway is a FEMDI managed service. Data Publishers can choose to register their Data Supply components with the appropriate API Gateway, based on how they have deployed/configured their service, service proximity to the API Gateway, anticipated data volumes, estimated costs, and whether they want to capture metrics or benefit from other capabilities such as rate-limiting and access control.

API Gateway instances will be deployed onto the platforms commonly used for Local Components' HVD data services, such as EWC, AWS and Azure. Selecting the platforms to be used is an architectural decision for FEMDI, impacted by e.g. where most of the Data Supply services are hosted, and cost matters.

Even though the API Gateway instances are federated, the Data Consumer can use the same API Key at every API Gateway instance. There is a centralized control and configuration process for managing the API Gateway instances.

The API Gateway supports multiple API standards.

Data Explorer

Data Explorer is a web application that enables Data Consumers to search and browse the data available through FEMDI. It also pulls in supplementary information from OSCAR/Surface. The Data Explorer uses metadata and data from both Global Discovery Catalogue and Data Supply components.

Identity & Access Manager

Some FEMDI data policies require that users register before they can access the open data. The Identity & Access Manager manages access to data through FEMDI Community Components, including Developer Portal and potentially Data Explorer.

The Identity & Access Manager provides federation capabilities to allow federated authentication using a network of trusted 3rd Party Identity Providers (i.e. authentication services). It also includes an internal user repository to allow data of registered users to be stored (user data is subject to GDPR and is kept at minimum – for example, username and email address).

Developer Portal

Users register for access to FEMDI data via a Developer Portal, a web application. In the portal, authenticated users are issued an API Key that they append to their data access requests.

Users authenticate to the portal using a 3rd Party Identity Provider, federated by the Identity & Access Manager. After the user has logged in the first time, the Developer Portal orchestrates user creation for the API Gateway and in the Key Vault. Generated API Keys are stored in a secure Key Vault.

Key Vault

API Keys issued to registered users are stored securely in the Key Vault.

Dependencies: Local Components

Data Supply

Data Supply is a Local Component that is used to share data, manage, and publish its metadata, and publish notifications about changed metadata and data. Most of the Data Supply functionalities are needed for WMO obligations rather than FEMDI.

Data Supply has the following functionalities:

- **Persistence** data for storage, allowing for shared data to be accessed through APIs.
- **Data Processing** in line with WMO regulations and FEMDI Policies, Standards and Processes (PSPs).
- **Local Broker** to send change notifications to the WMO Global Broker of new and updated discovery metadata and shared data.
- **Metadata Management** to create, publish and maintain the discovery and provenance metadata to share changes with the Global Discovery Catalogue.
- **Data Access** enabled to expose data to FEMDI users using interactive APIs through the API Gateway. Data Access APIs will be delivered by the other RODEO WPs as well as other HVD Data Publishers. In addition to FEMDI-compliant APIs, other data access methods can be implemented according to the WMO WIS 2.0 requirements.

Data is published from Data Publisher applications as data sets (collections) on the Data Supply. Data Consumer applications can access shared data through the FEMDI API Gateway. Data Supply capabilities can also be accessed directly, without proxying access from the API Gateway.

Data Publishers are free to make technology choices of their own for the Data Supply capability, but FEMDI sets certain requirements and guidelines for interoperability.

Dependencies: WMO 2.0 Components

WMO WIS 2.0 Global Discovery Catalogue

The Global Discovery Catalogue is a web application that facilitates data search and discovery by describing the data available through WIS 2.0 and FEMDI using discovery metadata. It gets notifications on changes in discovery metadata by subscribing to notifications from the Global Broker. It then retrieves updated metadata and updates the catalogue accordingly.

The catalogue metadata provide summary descriptions of the data to help Data Consumers to decide whether the data set is useful to them, as well as URLs to access shared data through the API Gateway or directly (depending on the Data Supply).

WMO WIS 2.0 Global Broker

The Global Broker is a custom application that provides notifications about discovery metadata and data changes on a subscription basis. It gets notifications on changes in discovery metadata and data by subscribing to the notifications from the Data Supply. It then republishes notifications on changes in metadata and data to Data Consumer applications that have subscribed to them.

Dependencies: 3rd Party Components

3rd Party Identity Providers

FEMDI doesn't manage passwords or user accounts, so the Developer Portal asks users to authenticate via a 3rd Party Identity Provider (IdP) when registering. IdP services can include, for example, Azure AD, Google, GitHub, or a EUMETNET Member's IdP service.

The Identity Provider will provide a limited set of attributes to the Identity and Access Manager component, including user identifier and e-mail address.

3rd Party Configuration Management Tool

In the operation of FEMDI, the registration of local Data Supply components and configuration of FEMDI API Gateway is managed by FEMDI administrators via a Configuration Management Tool provided by GitHub.

2.4 Metadata Structure

This section describes the metadata structure used in FEMDI.

- Discovery metadata
  - Points to a shared data set (collection of data)
  - Includes information for users to decide whether the dataset will be useful to them
  - Defines e.g., data set title, themes, rights and provider information
  - Includes links (URLs) to access shared data
  - Used by the Shared Catalogue
  - Notifications are published to inform on changes
  - Does not change very often
  - Updated manually
  - Encoded according to the WMO Core Metadata Profile version 2 (WCMP2)
- Collection metadata
  - Describes how a shared data set is structured and organized
  - Enables users to identify which parts of a dataset they need
  - Defines what data is available: types of queries, spatial and temporal extent, parameters
  - Stays at the Data Supply (e.g., available from API)
  - Facilitates utilisation of data (especially using smaller data sets than the whole collection)
  - Notifications are published to inform on changes
  - Updated automatically
  - Example
- File/resource-level metadata
  - Describes the content of each of the shared data files/resources
  - Describes the data on a detailed level, e.g., parameters and units of measurement
  - Stays with the file/resource: embedded in the data file, provided in a well-known location, and/or provided in a separate explicitly referenced resource
  - Notifications are published to inform on changes
  - Updated automatically

2.5 Data Publishing Patterns

Data Publishers can publish data through FEMDI in two different ways (or patterns). The data publishing models differ in how the FEMDI community API Gateway is used to access the data provided by Data Supply components. The data can be accessed and proxied through the API Gateway and/or accessed directly from Data Supply, completely bypassing the API Gateway.

Whichever data publishing pattern is chosen, the Data Publisher still needs to fulfil other FEMDI requirements, such as creating metadata, sharing it to the Global Discovery Catalogue, and publishing notifications.

The Data Publisher or Owner will decide how they want their data to be made available.

Pattern 1: Managed and proxied access

The Data Supply component is registered with an appropriate API Gateway. The data is requested from and goes through the API Gateway. This allows data requests and data flow to be managed (e.g., authorization, access control, and rate limiting). API Gateway can also collect insights on data requests and access.

When Data Publishers wish to expose their data through the FEMDI API Gateway, discovery metadata and notifications need to include an URL that points to the right API Gateway endpoint.

This pattern can be used in the following situations (not mutually exclusive):

- Data and API Gateway are on the same cloud platform or geographically close
- Includes critical and/or restricted data (e.g. need to prioritize users)
- FEMDI networking costs are acceptable
- Need for detailed insights on data use
- Want to use FEMDI Community Capabilities to manage access and provide insights
- Protection of Data Supply endpoints including rate limiting.

Pattern 2: Direct access

FEMDI API Gateway is not used at all in accessing data. Data is requested and accessed directly from the Data Supply. Therefore, the Data Supply is responsible for access management and providing insights (if required). Still, FEMDI-compliant metadata needs to be created, and Local Capabilities implemented for sharing metadata to the Global Discovery Catalogue and publishing notifications.

This pattern can be used in the following situations (not mutually exclusive):

1. Data is published through a 3rd Party platform (e.g., AWS Open Data, Microsoft Planetary Computer, Government Data Portal)
2. High performance requirements (e.g., large amount of data transferred or frequent use)
3. Serving data through a FEMDI API Gateway would be expensive due to large data volumes
4. Data Publishers want to have full control of how their data is accessed
5. Access control, request management and collection of usage metrics is handled by 3rd Party or the Data Supply (e.g. the Data Publisher already has API Management implemented as part of the Data Supply capability)

2.6 Access Levels

In FEMDI, there are three levels of access for Data Consumers:

1. Unauthenticated access – Open access for anonymous users.
2. Authenticated access – Open access with registration, this provides:
   - A higher Quality of Service; and,
   - Additional data (as decided by the Data Owner).
3. EUMETNET Members – Restricted to EUMETNET Members.

In the future, additional levels of access may be added.

3. Solution Design

This section describes detailed design for the FEMDI solution. It includes technical description of the FEMDI Community Components, solution architecture descriptions of the runtime environments, and discussion of the technical requirements.

Developer documentation for the components can be found from the FEMDI Community Component repositories (links in Section 1.7).

3.1 Components and Interfaces

A technical description of the FEMDI Community Components and interrelated 3rd Party components is provided in the following.

All components are open source[2], so they can be deployed by any EUMETNET Member.

API Gateway

API Gateway acts as a proxy between Data Consumers and API endpoints at Data Supply Components. It receives access requests from Data Consumer applications, passes them to the right Data Supply API endpoint, and passes the received data back to the consumer. It also manages rate limits and authentication for the data sources.

The discovery metadata and notifications from the Data Supply component need to include the URL to the right API endpoint at the API Gateway, so the registration of new Data Supply APIs need to be coordinated between the Data Publisher and the Community Capability Operator responsible for the API Gateway(s).

The API Gateway includes multiple API endpoints. Each of them points to a specific Data Supply API endpoint. The API Gateway supports OpenAPI-based web services, such as the Open Geospatial Consortium's API for Environmental Data Retrieval (OGC-API-EDR), which is being recommended by other WPs in the RODEO project.

When data is accessed through the API Gateway, API Gateway replaces original Data Supply links in the metadata with its own API Gateway-specific URLs which point to the data source. This is done for protecting the original Data Supply and for not exposing the Data Supply's original URL.

Registered users are created as consumers in the API Gateway by the Developer Portal. The user data include a universally unique identifier (UUID) from the Identity & Access Manager and a path to user's API Key in the Key Vault.

API Gateway uses API Keys to authenticate and authorize requests for those Data Supply API endpoints that have authentication enabled. Other APIs can be used by unauthenticated users, without an API Key. The API Key (which is a string of characters) is appended to the HTTP header of the data access request or alternatively provided as an URL parameter. API Gateway then attempts to match the API Key in the request to a user in the Key Vault. If a match is found, the user is authenticated and can access data.

API Gateway configuration (e.g. available Data Supply API endpoints, rate limiting, and authentication) is managed via the 3rd Party Configuration Management Tool in GitHub.

[2] HashiCorp Vault license is a Business Source License (BSL) for the core product, allowing limited open-source usage for non-commercial purposes.

API Gateway collects data usage metrics that can be viewed by admins. The reporting tool to be used will be selected at a later stage.

API Gateway is based on Apache APISIX open-source software product.

There are multiple API Gateway instances, one for every FEMDI runtime environment.

Data Explorer

Data Explorer is a lightweight custom web application based on the GeoWeb open-source solution. It is based on React Redux (frontend) and Python (backends).

GeoWeb is used for geo-referenced data analysis and visualization. FEMDI extends GeoWeb functionality with e.g. data discovery. GeoWeb is an open-source project by FMI, Koninklijk Nederlands Meteorologisch Instituut (KNMI – the Netherland's Met Service) and MET Norway started in 2020. It uses Apache 2.0 license.

GeoWeb uses data from multiple sources through standardized APIs, such as OGC Web Map Service (WMS) and OGC-API-EDR. Data Explorer integrates with Global Discovery Catalogue to provide the user information on what data is available. The user can then access a Data Supply they are interested in using the URL in the catalogue. The URL can either point to the API Gateway or directly to the Data Supply, whichever data access pattern is used for that Data Supply. The Data Explorer supports both anonymous and authenticated access to data.

Support for discovery metadata and OSCAR/Surface station metadata and required integrations will be added. Data Explorer includes multiple backends constructed as microservices. They are used e.g. for managing user configuration (presets).

GeoWeb is modular, so functionalities can be added. It is being developed continuously in an agile manner.

There will one Data Explorer server-side backend instance in FEMDI which is used to store user-defined configuration.

Identity & Access Manager

Identity & Access Manager manages authentication, authorization, and identity federation for FEMDI users. It intercepts user requests to the Developer Portal and potentially Data Explorer. It redirects unauthenticated users to authenticate with a 3rd Party Identity Provider.

Identity & Access Manager manages the basic data of registered users. When users authenticate for the first time, user accounts for new users are created in an internal user data store of the Identity & Access Manager. User data includes an identifier (UUID), email address (from the IdP), and first name and last name (depending on the IdP). After the user is created, Developer Portal manages the rest of the user registration process. The user identifier (UUID) created by Identity & Access Manager is also used as a user identifier in Key Vault and API Gateway. In addition, email address is unique for each user account.

Identity & Access Manager has a GUI for administrator users. Admins can view and remove users when required. Admins can also manage the set of trusted IdPs in the Identity & Access Manager.

Identity & Access Manager is based on Keycloak open-source software product. It uses OpenID Connect protocol for authentication and identity federation. Data is passed in JSON Web Tokens (JWT).

There is only one Identity & Access Manager instance in FEMDI. This allows users to use the same API Key at every API Gateway instance.

Developer Portal

Developer Portal is a custom web application where authenticated users can register to get an API Key, check API Key validity, delete API Key, and view available API endpoints (i.e. routes). It is based on Python and React.

Authentication to the Developer Portal is handled by the Identity & Access Manager. If an unauthenticated user attempts to access the portal, it redirects the user to the Identity & Access Manager which then redirects the user to authenticate with a 3rd Party Identity Provider.

Developer Portal manages the user registration process. After a new user has authenticated and wishes to obtain an API Key, the Developer Portal creates a user account in the Key Vault. In addition, the Developer Portal creates a consumer (i.e. user) at every API Gateway instance. Consequently, the user can use the same API Key at every API Gateway instance. A user account can have one API Key at a time. Developer Portal checks if the user already has an API Key and a consumer.

There is one Developer Portal instance in FEMDI.

Key Vault

Key Vault stores API Keys of registered users in a secure manner.

The Developer Portal manages the creation of new users and API Keys to the Key Vault. The Key Vault stores a user identifier (UUID) from Identity & Access Manager and user's API Key (a string of characters). The API Gateway checks user API Key validity from the Key Vault. A user account can have one API Key at a time.

FEMDI admins can view, revoke, and delete API Keys when required.

Key vault is based on the HashiCorp Vault software product.

There is only one Key Vault instance in FEMDI. This allows users to use the same API Key at every API Gateway instance.

The secrets used to configure and manage the Key Vault are stored in a 3rd Party Secret Management Service for backup and restore purposes.

3rd Party Identity Providers

Users authenticate using a trusted 3rd Party Identity Provider such as Azure AD, Google, GitHub, or a EUMETNET Member's IdP service.

The set of trusted IdPs is managed in the Identity & Access Manager by FEMDI admins.

3rd Party Configuration Management Tool

Registration of local Data Supply components and configuration of FEMDI API Gateways is managed via a 3rd Party Configuration Management Tool, provided by GitHub, by FEMDI admin users.

API Gateway route configuration is stored in GitHub in YAML (a human-friendly data serialisation language for all programming languages). Admins can update available API endpoints, and related rate limiting and authentication configuration in the file. At commit and push of the change, an updated route configuration is generated. It is much simpler than the APISIX configuration file.

A GitHub action workflow (Python code) is triggered to generate a detailed APISIX configuration (YAML) and publish it to selected API Gateway instances (e.g. EWC, AWS) by APISIX REST API. The APISIX configuration then updates the APISIX instance on the target platform.

APISIX administrator credentials for API Gateway instances are stored in GitHub repository as secrets.

3.2 Runtime Environments

The runtime environments for FEMDI are described in the following. Currently, there are two types of FEMDI runtime environments: the Main environment and other environments.

- The Main environment hosts Support services (i.e. shared components) required by the other environments. These components include Developer Portal, Key Vault, and Identity & Access Manager. Also, Data Explorer is hosted only in the Main environment. The Main environment also hosts the Main API Gateway (i.e. the first API Gateway to be implemented).
- Each of the other environments merely host an API Gateway that depends on the Supporting services in the Main environment.

FEMDI runtime environments can be hosted in a public cloud platform (e.g. AWS, Azure, Google Cloud) or a private cloud (EWC). FEMDI infrastructure has been implemented as cloud platform agnostic as possible, so the Community Components are portable to different cloud environments.

The technical implementation of the FEMDI Community Components (as described in the previous section) is similar in every environment, but cloud platform provider-specific and open-source components and services can be used for other needs (e.g. load balancing, networking, security, and reporting and analytics).

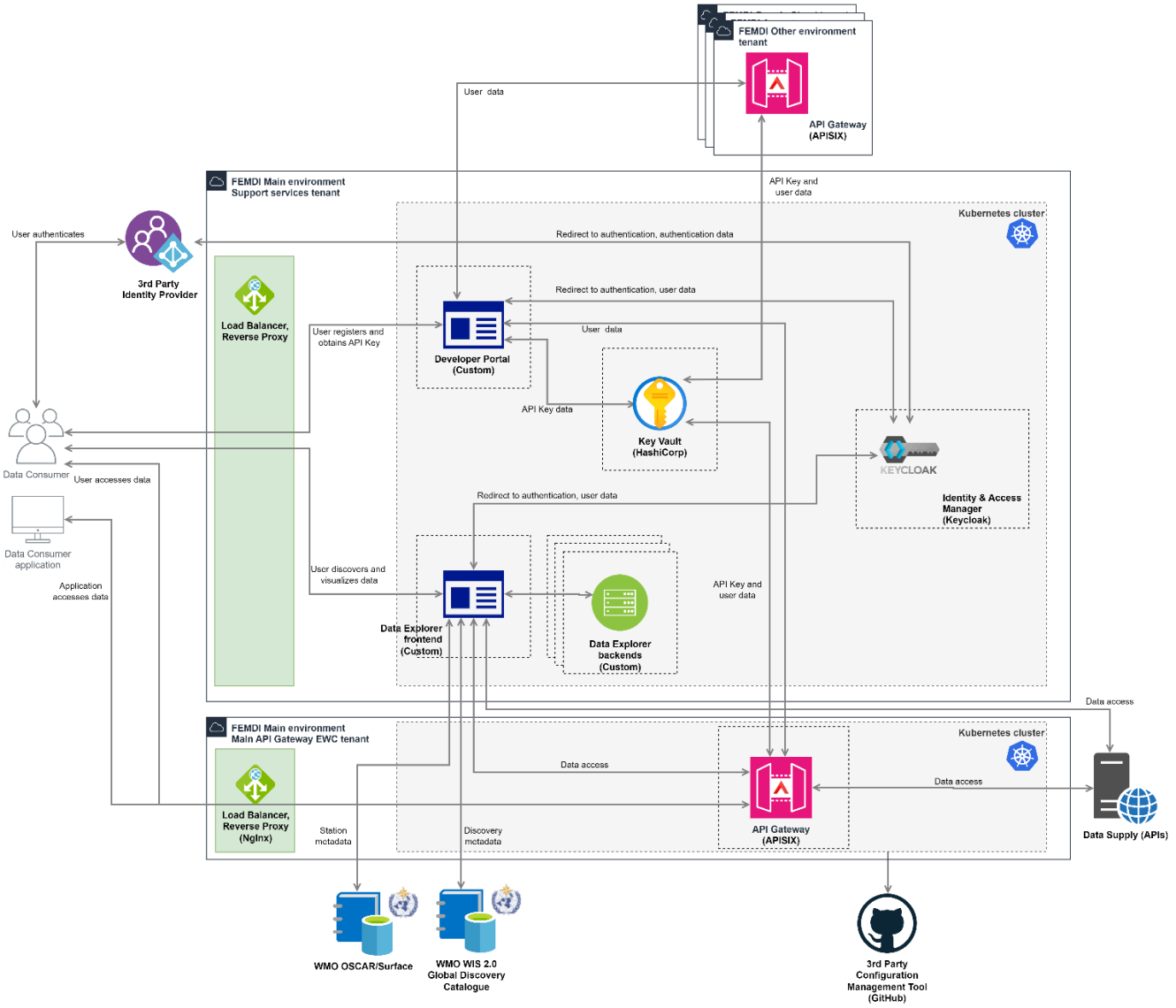
Main Environment

A solution architecture description of the FEMDI Main environment is provided in the following diagram. It includes the components that are hosted in that environment, information flows between them, and with components hosted in other environments and 3rd Party components.

The Main environment hosts all FEMDI Community Components. It is divided into two parts: Main API Gateway (i.e. the first API Gateway to be implemented) and Supporting services (i.e. the rest of the Community Components). The Main API Gateway will run on EWC. The cloud environment used to run the Supporting services will be decided at a later stage.

Each of the components is run in a container managed by Kubernetes and Rancher. Each Data Explorer backend is also run in its own container.

In EWC, each Kubernetes node runs Linux Ubuntu 22 operating system. All components are behind a load balancer and Nginx reverse proxy.



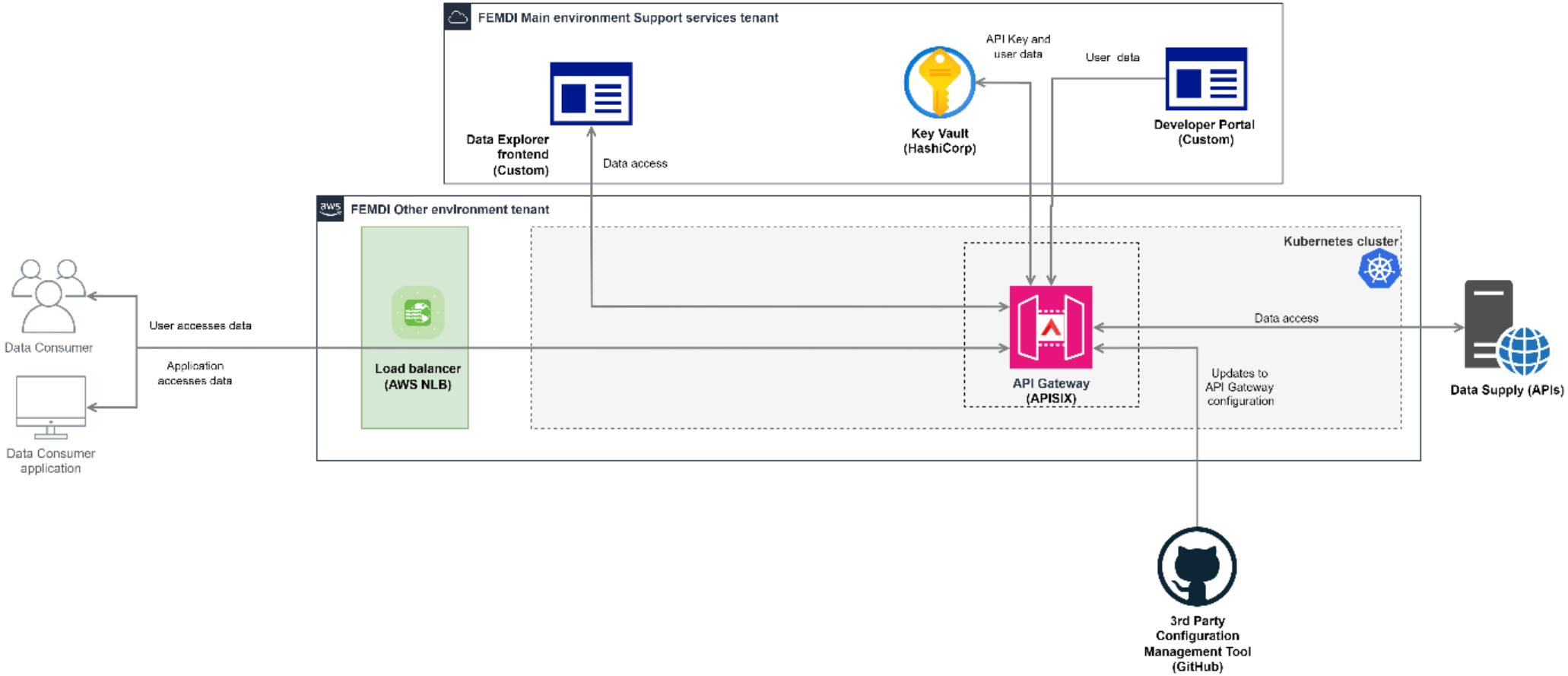
Solution architecture description of the FEMDI Main environment

Other Environments

A solution architecture description of other FEMDI environments is provided in the following diagram. The description includes the components hosted in each of the other environments, information flows between them and with components hosted in the Main environment, and 3rd Party components. Only direct dependencies are included.

Other environments can be hosted on any cloud platform. This section describes how such an environment is hosted on AWS; but the architecture is similar for other cloud platforms. The cloud environments that will be used will be decided at a later stage.

Each other environment hosts an API Gateway, which is run in a container managed by Kubernetes. In AWS, each Kubernetes node runs EKS-optimized Amazon Linux operating system. All components are behind an AWS Network Load Balancer (NLB) layer 4 proxy.



Solution architecture description of the other FEMDI environments

3.3 Data

FEMDI Community Components are implemented in a flexible manner to allow sharing many different types of data. The API Gateway supports OpenAPI-based web services, such as OGC-API-EDR, which is being recommended by other WPs in the RODEO project. It supports many web technologies, such as JSON, XML, HTML, and even MQTT. From a technical perspective, the API Gateway does not limit the content of data that is accessed through it. See FEMDI Manual and FEMDI API Guidance for information on setting up appropriate data source APIs.

Personal data is handled in compliance with GDPR and other privacy regulations. FEMDI Privacy Policy describes how personal data is managed in FEMDI. Personal data in the FEMDI solution is limited to the data of registered users, which is kept at minimum. In addition, there may be contact details in the metadata. Data Owner and Data Publisher are responsible for ensuring compliance regarding metadata and data.

Ensuring compliance with privacy regulation is part of the FEMDI Operating Model.

3.4 Security

FEMDI utilises the technical security features provided by the Community Components. Community Capability Operators are responsible for ensuring security of the technical environment (e.g. network security, hardening, denial-of-service attack protection, administrator credential protection).

FEMDI utilises authentication for Developer Portal and potentially Data Explorer using 3rd party IdP and Keycloak. Keycloak provides user email address and name. Administrators can access user data in Keycloak and prevent individual users from logging in, if required.

Data access through the API Gateway can be set up to require authentication using API Key, depending on the data policy.

API Keys are protected in the Key Vault.

Data transfer between Community Components and user applications is encrypted using HTTPS. Also, data transfer between Data Supply and Community Components is protected if the Data Supply supports HTTPS.

Discovery metadata may contain a security block that can be used to identify access-controlled data and that describes the access control mechanism (see the WCMP2 specification for more information).

3.5 Availability and Performance

FEMDI will be operated in line with the Quality-of-Service requirements published by RODEO before the end of the project. Cloud service provider and Kubernetes-specific scalability capabilities are used to ensure appropriate performance and availability. In addition, technical components can be duplicated across different availability zones and regions (in EWC, across ECMWF and EUMETSAT environments). Cloud platform-specific or open-source load balancer is used in every runtime environment.

As the EWC develops it may be possible to operate applications such as FEMDI across multiple availability zones. In this case, external load balancing will be required.

3.6 Backup and Restore

Kubernetes-specific solution is set up for backing up each environment. API Gateway consumer (user) configurations are backed up using a custom replication solution. The secrets used to configure and manage the Key Vault are stored in a 3rd Party Secret Management Service for backup and restore purposes.

Community Capability Operators are responsible establishing backup and restore solutions.

3.7 Monitoring and Error Handling

FEMDI Community Component logging features are used to provide logs. FEMDI also includes custom error pages.

Observability will be defined at a later stage.

3.8 Testing and Quality Assurance

FEMDI Community Components are tested according to the FEMDI test plan. Deployments in every new environment are tested. Existing environments are also tested after changes, as required.

3.9 Deployment and Configuration

FEMDI is being developed on EWC, but the infrastructure has been implemented as cloud platform agnostic as possible.

FEMDI is set up as infrastructure as code using Terraform. Therefore, it is more straightforward to deploy it into new environments.

When FEMDI is extended to new cloud platforms, API Gateway consumers need to be set up in each environment. FEMDI provides a tool for syncing consumer's authentication between environments. This allows using the same API Key in every environment. Data Supply routes are synced from a 3rd Party Configuration Management Tool (provided by GitHub) to given environments.

4. Operating Model Design

This section describes detailed design for FEMDI Operating Model. The Operating Model defines the policies, standards, processes, and responsibilities for governing, operating and maintaining FEMDI Community Components.

4.1 What is the Operating Model?

FEMDI stakeholders need to be able to rely on FEMDI as an operational system to deliver services and make decisions. EUMETNET Members and other users will depend on FEMDI for their products and services.

The FEMDI Operating Model, underpinned by policies, standards, processes, and responsibilities, will ensure the quality of this operational service. Where possible, the supporting policies, standards, processes, and responsibilities will be based on those already in place in the international, meteorological, and EUMETNET communities.

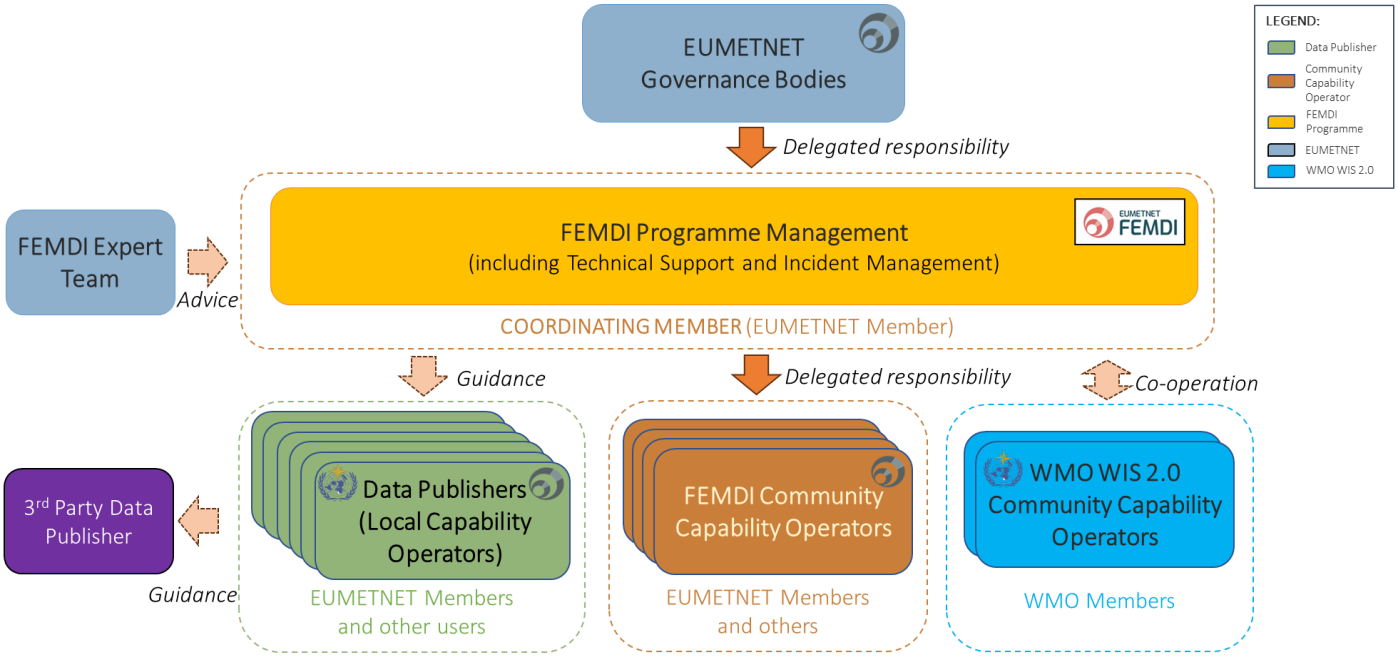
The Operating Model is meant as a practical and feasible framework for everyone involved in FEMDI governance, operation, and maintenance. It considers organisational, legal, operational, and technical aspects of FEMDI. As a result, everyone in the FEMDI community will know who is responsible for what and how FEMDI will perform. The chances for painful surprises will be lessened.

The first operational release of FEMDI is planned for the end of 2025. The Operating Model will be designed alongside the FEMDI technical capabilities so it will evolve over time as FEMDI capabilities evolves and FEMDI's use extends. Also, the Operating Model definition will be a living document that is updated when necessary.

4.2 Operating Model Responsibilities

FEMDI is expected to be run as a Programme at EUMETNET, with responsibility for delivery delegated to a EUMETNET Member as the 'Coordinating Member'. An overview of FEMDI Operating Model responsibilities is provided in the following diagram [3].

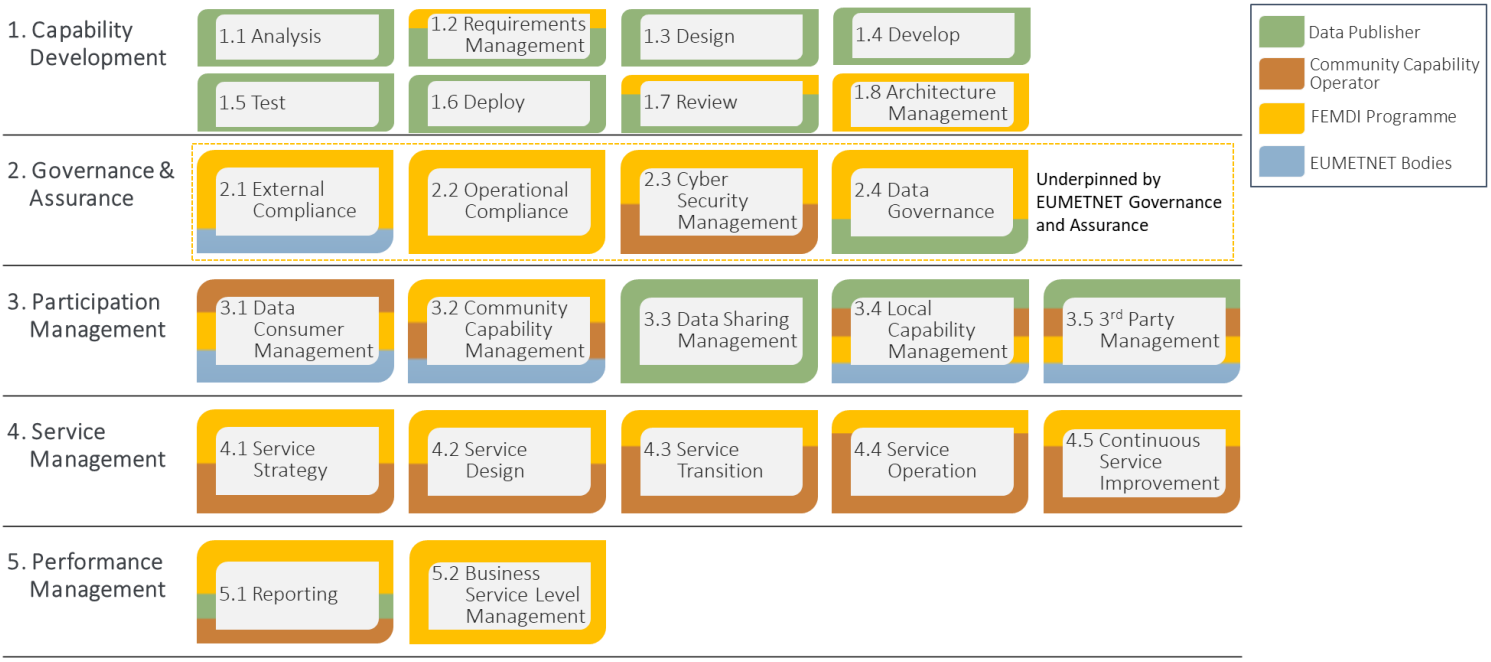
[3] See FEMDI stakeholder descriptions in section 1.7.



Overview of FEMDI Operating Model responsibilities

4.3 Operating Model Parts

An overview of the FEMDI Operating Model parts and related responsibilities is shown in the following diagram.



FEMDI Operating Model parts, sub-sections, and responsibilities

The parts of the Operating Model are described in the following.

1. Capability Development

Capability Development includes the delivery of technical solutions and changes in existing solutions needed to support future FEMDI capabilities. It closely aligns with Service Management, which ensures that technical changes and capabilities are deployed as a supportable IT services.

Developing capabilities is not a continuous activity, but initiated when new and updated capabilities are required. Capability development can be organized as a project and tasked to specific deployment teams at EUMETNET Members or IT contractors. For example, WP2 in the RODEO Project is developing the initial FEMDI Community Components.

FEMDI Coordinating Member is responsible for overseeing capability development and managing the overall FEMDI architecture and roadmap.

Capability Development includes the following sub-sections:

- **1.1 Analysis** enables understanding the focus area and beginning the requirements capture process. Also, elements of business case and business value assessed.
- **1.2 Requirements Management** ensures requirements are appropriately managed through the project, making sure there is traceability of requirements through to delivery.
- **1.3 Design** includes outlining and planning the solution and validating the design with stakeholders.
- **1.4 Develop** includes developing the technical solution or enhancement in line with the solution design.
- **1.5 Test** includes testing the solution properly to ensure that there are no defects, and that solution works as expected.
- **1.6 Deploy** ensures that new changes are released into the live environment in a way that is coordinated and eliminates disruption to users. This aligns closely with Service Transition which is responsible for making sure that technical changes and capabilities are deployed as a supportable IT services.
- **1.7 Review** ensures that changes and new solutions are monitored and evaluated to determine how successful the change has been and to help identify any improvements that need to be made. This aligns with Service Operations and Continuous Service Improvement which will ensure that any issues are resolved and that services are reviewed on an ongoing basis to identify opportunities to improve service quality.
- **1.8 Architecture Management** enables planning and safeguarding the overall FEMDI architecture. It ensures that any new capabilities being brought into FEMDI architecture follows carefully considered policies, standards, and processes (PSPs). Architecture Management seeks to enable this by outlining the PSPs that need to be followed when introducing new capability or making changes to existing capability and actively governing compliance against these PSPs.

2 Governance & Assurance

Governance & Assurance ensures compliant and secure delivery of FEMDI services.

FEMDI Coordinating Member has the main responsibility of governance and assurance. It is also underpinned by EUMETNET Governance and Assurance.

Governance & Assurance include the following sub-sections:

- **2.1 External Compliance** ensures that FEMDI capabilities are compliant with external rules, regulations, and standards (e.g. EU's Open Data Directive, HVD Act, EU NSPRIRE Directive, WIS 2).
- **2.2 Operational Compliance** ensures that FEMDI capabilities operate in line with predetermined FEMDI agreements (monitor deviations to agreed SLAs).

- **2.3 Cyber Security Management** includes development, documenting, and implementation of security policies and procedures for protection of FEMDI assets (data and capabilities).
- **2.4 Data Governance** refers to a collection of processes, roles, policies, standards, and metrics that ensure the effective, efficient, and compliant use of data.

3 Participation Management

Participation Management includes managing the onboarding and offboarding of participants, capabilities, and data within FEMDI.

FEMDI Coordinating Member has the main responsibility of participation management. It is also underpinned by EUMETNET Governance and Assurance. Data Publishers, Community Capability Operators and 3rd Parties also take part in the relevant processes.

Participation Management includes the following sub-sections:

- **3.1 Data Consumer Management** enables the onboarding and offboarding of EUMETNET Data Consumers, to access FEMDI services.
- **3.2 Community Capability Management** enables the onboarding and offboarding FEMDI Community Capabilities.
- **3.3 Data Sharing Management** enables the onboarding and offboarding data within FEMDI.
- **3.4 Local Capability Management** enables the onboarding and offboarding FEMDI Local Capabilities.
- **3.5 3rd Party Management** enables managing bi-lateral agreements between third parties and a participating NMHS agreeing to share data with them through FEMDI.

4 Service Management

Service Management includes the establishment of effective IT service management for FEMDI services. Service Management ensures that IT services related to FEMDI Community Components meet user needs and FEMDI Quality-of-Service criteria.

IT services include everyday services required to manage the Community Components, including, for example, helping users, monitoring technical components, ensuring system availability, performance and security, fixing technical problems, and reporting on service provision.

Designing and building new and upgraded Community Components is not part of IT service management.

Community Capability Operators are responsible for providing IT services related to the Community Components they are hosting. They can use their own IT service management practices if they meet FEMDI Quality-of-Service criteria and other FEMDI requirements. Community Capability Operators work together with Data Providers, other Community Capability Operators, WMO WIS2 Capability Operators and the FEMDI Coordinating Member.

FEMDI Coordinating Member is responsible for the overall governance of FEMDI Service Management. It provides FEMDI Quality-of-Service criteria and other minimum requirements for IT services, guidance to Community Capability Operators, and monitors compliance to IT service management requirements. The Coordinating Member is also responsible for providing a Central Support Function (part of 4.4 Service Operation) which is the one point of contact for FEMDI users and acts as 1st level support. The Central Support Function coordinates with other parties to fulfil user requests and solve problems.

Service Management includes the following sub-sections:

- **4.1 Service Strategy** ensures that the approach to managing FEMDI services is properly aligned with business objectives of FEMDI.
- **4.2 Service Design** includes the design of new FEMDI services, as well as changes and improvements to existing ones.
- **4.3 Service Transition** includes building and deploying FEMDI services. It also makes sure that changes to services and Service Management processes are carried out in a coordinated way.
- **4.4 Service Operation** ensures the delivery of FEMDI services to meet business requirements.
- **4.5 Continuous Service Improvement** ensures continuous improvement of the effectiveness and efficiency of FEMDI services (includes both soft Infrastructure and technical).

5 Performance Management

Performance Management includes aggregated monitoring and reporting for the performance of FEMDI services. Also see section 3.5 Availability and Performance in this document.

FEMDI Coordinating Member has the main responsibility of performance management. Also, Data Publishers and Community Capability Operators take part by adhering to the monitoring and reporting standards and providing timely reporting data to the FEMDI Coordinating Member.

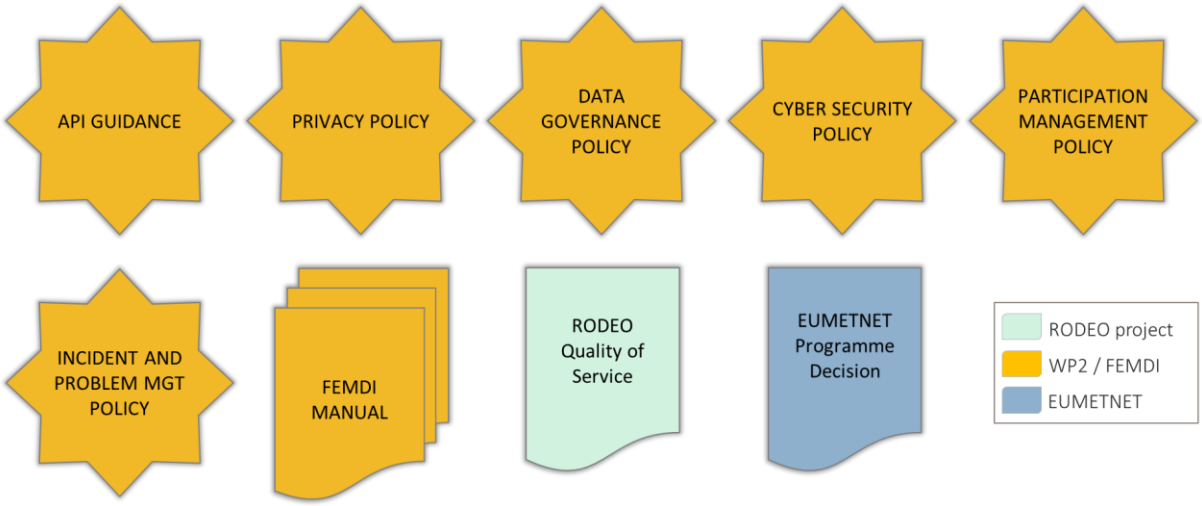
Performance Management includes the following sub-sections:

- **5.1 Reporting** ensures the reporting of overall FEMDI performance through consolidated service level reports.
- **5.2 Business Service Level Management** ensures that FEMDI services are being delivered to the specified agreed levels and that the intended outcomes and benefits of FEMDI are being realised.

4.4 Policies, Standards and Guidelines

The approach for FEMDI is to use appropriate policies and standards which are already established, only creating new ones where necessary. For example, existing EUMETNET governance patterns and structures will be used where available. In addition, there are several FEMDI-specific policies and other documentation.

The Operating Model parts will be defined in detail in the FEMDI Operating Model documents shown below. Also, key to the Operating Model is the RODEO project's Quality-of-Service agreement, and EUMETNET's Programme Decision.



FEMDI Operating Model documents and other key supporting documents

FEMDI documents

- **API Guidance:** Guidance on using APIs to make data discoverable and accessible through FEMDI.
- **Privacy Policy:** Ensures that FEMDI users' data is handled in compliance with GDPR.
- **Data Governance Policy**: Top-level policy covering FEMDI Data Governance. Its aim is to ensure that the data being shared through FEMDI is consistent, trustworthy, and does not get misused. It will help FEMDI users understand the guidelines they must adhere to when publishing and consuming data. The implementation of this policy is in the FEMDI Manual.
- **Cyber Security Policy:** Outlines EUMETNET's approach to protecting FEMDI, including its technology assets and data.
- **Participation Management Policy:** Outlines the management approach for each category of FEMDI stakeholders, including Data Publishers, Data Consumers, and Community Capability Operators.
- **Incident and Problem Management Policy:** Provides the approach on how incidents and problems will be managed across FEMDI by the Coordinating Member and Community Capability Operators, and the reporting requirements.
- **FEMDI Manual**: A comprehensive document describing, on a practical level, what FEMDI is, how to access and share data through FEMDI, and how to operate Community Capabilities. It will include the FEMDI processes, showing how to apply the policies.

RODEO Quality of Service: A project document describing the Quality-of-Service criteria to be met by the outputs of the RODEO project.

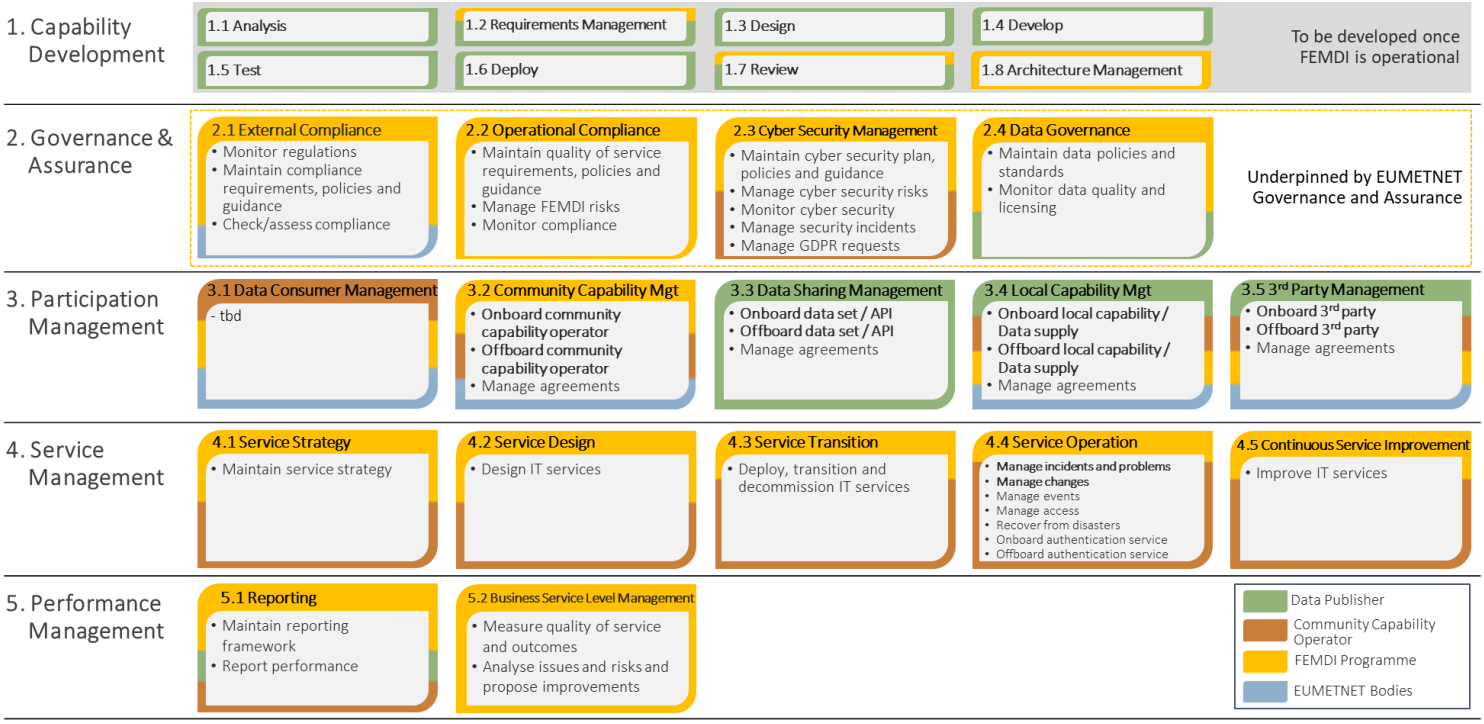
EUMETNET Programme Decision: The official agreement between EUMETNET and the FEMDI Coordinating Member for operation and maintenance of the FEMDI service, based on the FEMDI Operating Model. This will include sections such as: Requirements for managing the service, Establishment of an Expert Team, Reporting to the EUMETNET, Budget, Sub-contracting, Legal aspects, and Termination.

4.5 Processes

The FEMDI Operating Model defines a set of processes for the parts of the Operating Model. The processes define end-to-end activity flows that are required to deliver the expected outcomes. Generally, FEMDI does not define or mandate the use of a specific process, some exceptions

including Participation Management, Incident and Problem Management, and Change Management. Standard EUMETNET processes are used where available.

An overview of the FEMDI Operating Model processes is provided in the following diagram. The FEMDI Coordinating Member, Data Publishers, and Local and Community Capability Operators can use this as a recommendation to make sure that they have the required processes. FEMDI-mandated processes are bolded. For other processes, organisations can use their existing processes or design new processes, which can be FEMDI-specific.



FEMDI Operating Model parts, sub-sections, and processes

4.6 Cost Management

The costs of operating FEMDI for EUMETNET Members' data are covered by EUMETNET policies and processes which are already in place.

As FEMDI becomes operational, additional policies and processes may be needed to manage the costs of 3rd Parties exposing their data through FEMDI.