Whitepaper of DEMETER Technology Integration Tools (D3.4)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 857202.

DEMETER Technology Integration Tools – Release 2

1 Abstract

DEMETER has released a second version of a suite of components and tools that enable solution integration, interoperability with external platforms and deployment support for pilot cases. The main components and tools, depicted in the diagram below, are:

- Stakeholders Open Collaboration Space (SOCS): a knowledge base and co-creation space where farmers, advisors and providers connect.
- DEMETER Enabler HUB (DEH): collects all the resources that are available to be used by a solution and enables access to them.
- Agricultural Interoperability Space (AIS): provides interoperability mechanisms to develop and deploy a solution.
- Dashboards: sole entry points to the DEMETER ecosystem.
- DEMETER-enhanced Entity (DEE): A Service, Application, Platform, or Thing wrapped with DEMETER enabler functionalities to act as a DEMETER consumer and/or producer. Many of these DEE's interoperate with each other to form an application solution.
- Agriculture Information Model (AIM): a common semantic data model to be used for the information exchange.

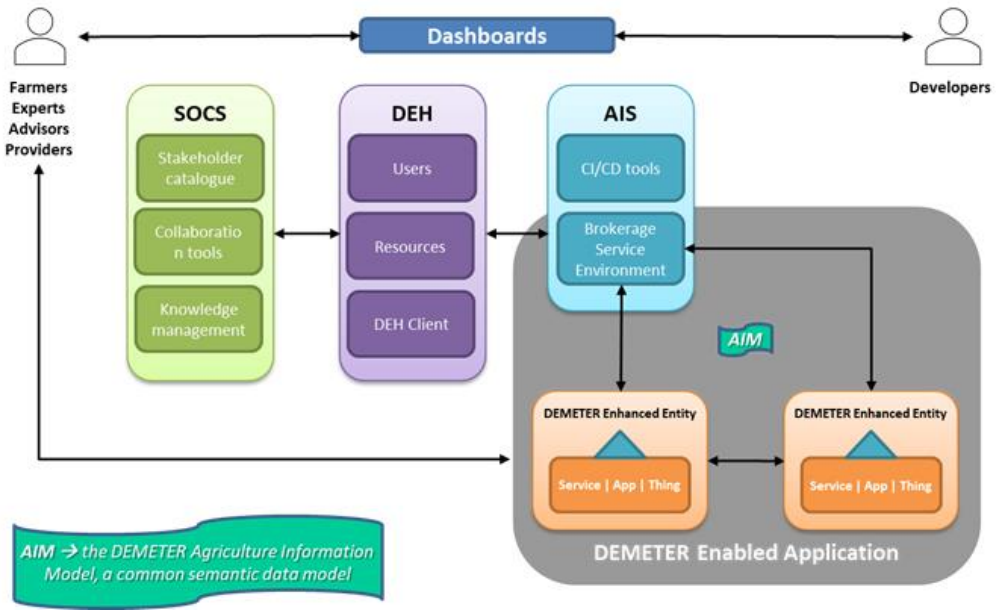


Figure 1: DEMETER main elements

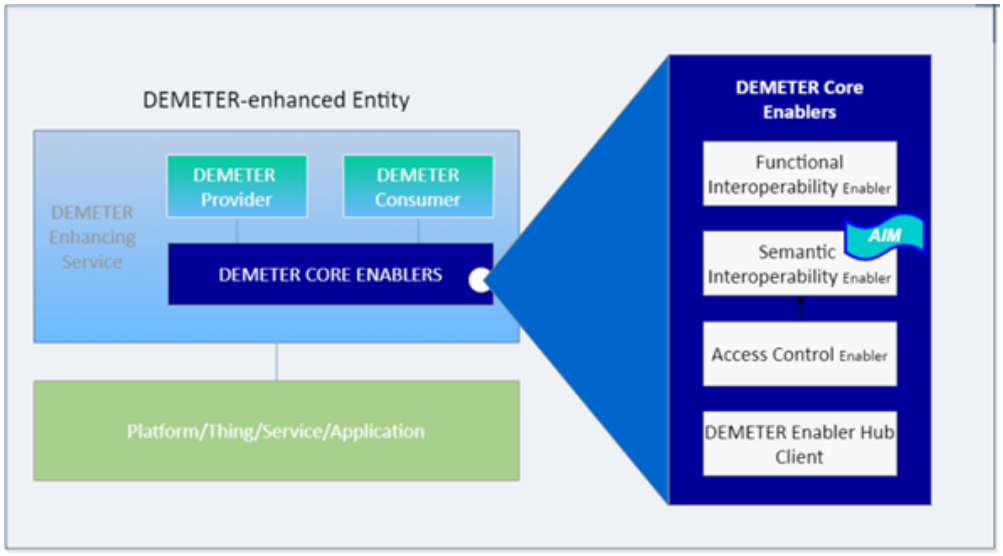


Figure 2: DEMETER Core Enablers

2 Overall architecture of the DEMETER reference implementation

Figure 3 describes the 3 major modules of DEMETER platform, namely Stakeholder Open Collaboration Space, DEMETER Enabler HUB and Brokerage Service environment. Included in these three major modules lies, the Security module (or Access Control Server module). In addition, it illustrates the interoperation activities between DEMETER Enhanced Entities (DEE) and DEMETER's Reference

Implementation. DEE consists of a set of either an app, a service, or a device along with a set of core Enablers and Advanced Enablers.

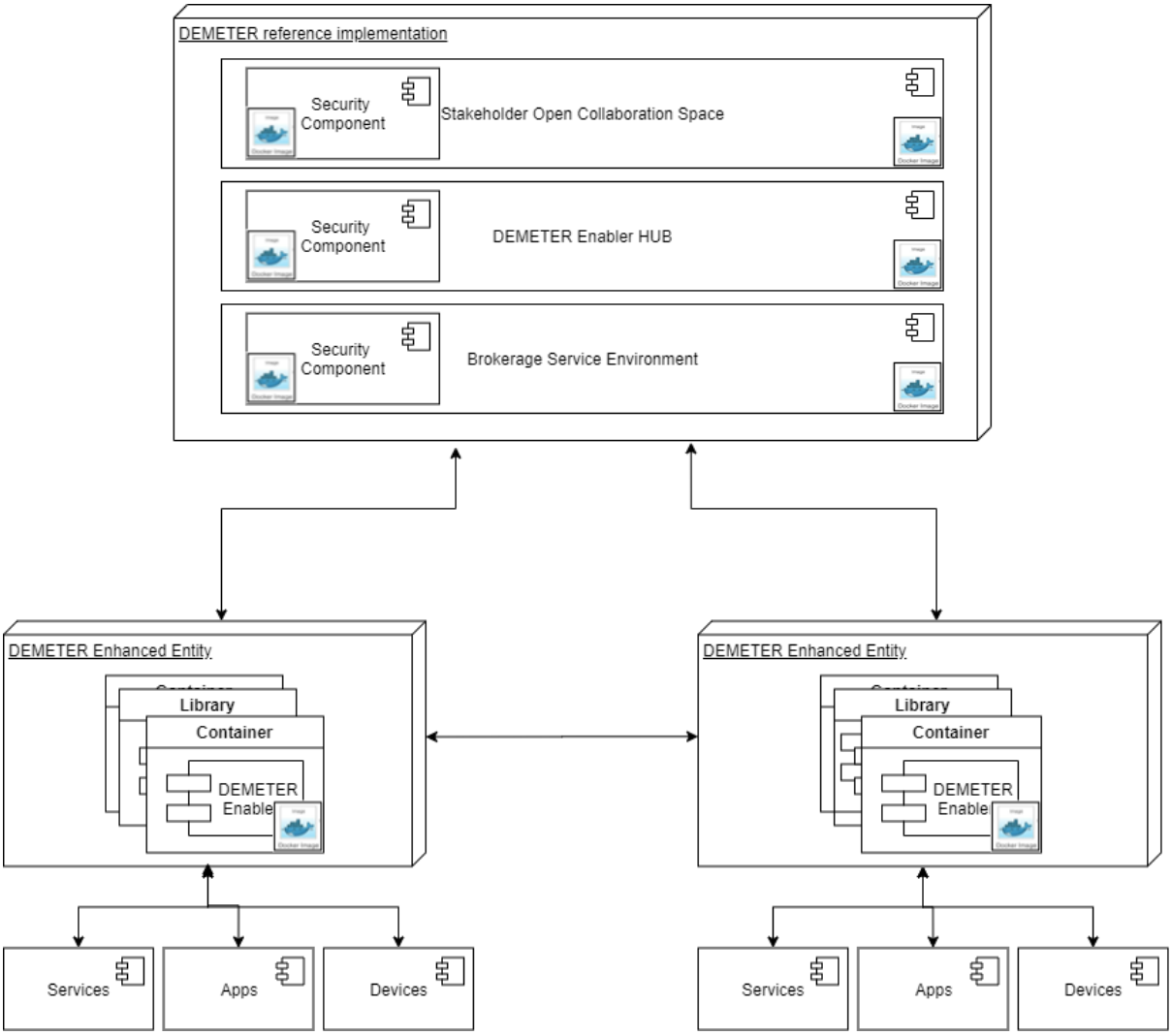
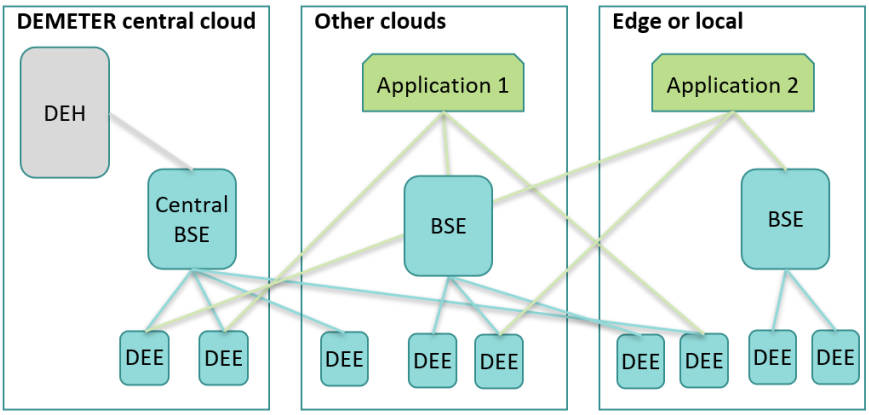


Figure 3: Reference Implementation Deployment diagram

DEMETER allows application to be deployed in many ways (from cloud to edge to local infrastructure), according to the business needs, as depicted in the diagram below:



3 Brokerage Service Environment

The Brokerage Service Environment (BSE) facilitates the registration, discovery and ultimately communication process for the DEMETER-enabled resources in a secure and privacy preserving manner. In the framework of DEMETER, a resource coupled with the necessary enablers is named a DEMETER enhanced entity (DEE). A DEE, once authenticated and authorised by the BSE, can register as a service with the BSE specific registry. Subsequently, it becomes discoverable by all the other registered DEE's. Finally, based on the suitable core and advanced enablers that each DEE implement and after resource provisioning information from the BSE, DEE's can communicate directly with each other.

The BSE is implemented as a self-contained application that enables an external party to deploy it as a complete brokerage service solution. Each DEMETER-enabled application should utilise at least one BSE. The BSE accompanied by a publish-subscribe communication mechanism that addresses the required communication data throughput realises the backbone of the DEMETER reference architecture.

The major components of the BSE are the Access Control Server (ACS), the Brokerage Server (BS) and the Service Registry (SR). While the ACS provides for the authentication and the authorisation of the DEE's that request to be included in the BSE, the BS realises the DEE registration, discovery, and the provisioning functionality

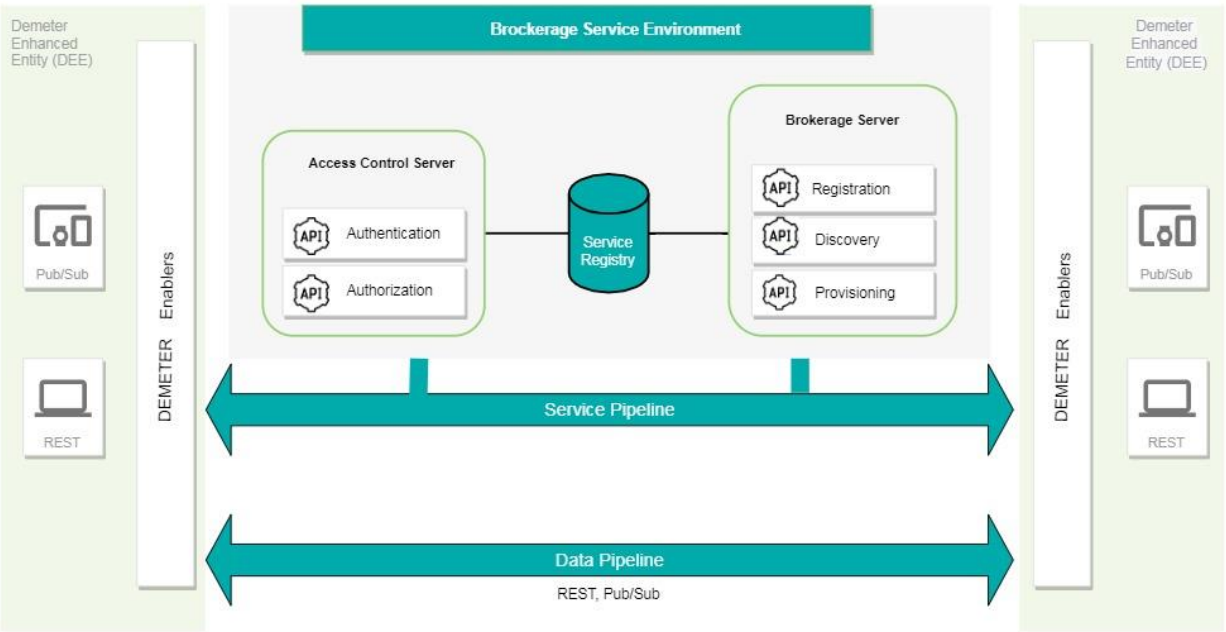


Figure 4: BSE component diagram

4 Access Control Server

The security components provide the following three functionalities to other DEMETER components and pilots implementations:

- Authentication
- Authorisation
- Traceability

These functionalities have been implemented in six main security components: Identity Manager (IdM), XACML PDP, Capability Manager, PEP Proxy, Traceability Agent and Traceability blockchain repository. These components expose methods using a REST API.

- IdM is based on the FIWARE Keyrock GE[1] and provides the Keyrock's REST API for authentication based on the OAuth 2.0 protocol.
- The XACML PDP manages the access control policies and decides who can access a resource and what actions they can perform with that resource.

[1] https://fiware-idm.readthedocs.io/en/7.4.0/

- The Capability Manager is the component for generating capability tokens for the user in the event of an affirmative authorisation decision from the XACML PDP following a request about an action or access to a resource.
- The PEP (*Policy Enforcement Point*) is responsible for validating a generated assertion in an authentication token (X-AUTH-TOKEN) with the capability token that was already generated in a response by the Capability Manager to a user's authorization request.
- The authentication and authorisation traceability component will log the access to DEMETER resources by logging the issue and use of authentication and authorisation tokens. These tokens contain the information about the user who is logged on to the system and the resources the user is intending to access.
- A permissioned blockchain repository has been chosen to provide the characteristics of immutability, privacy and compatibility required by the DEMETER Traceability Component.

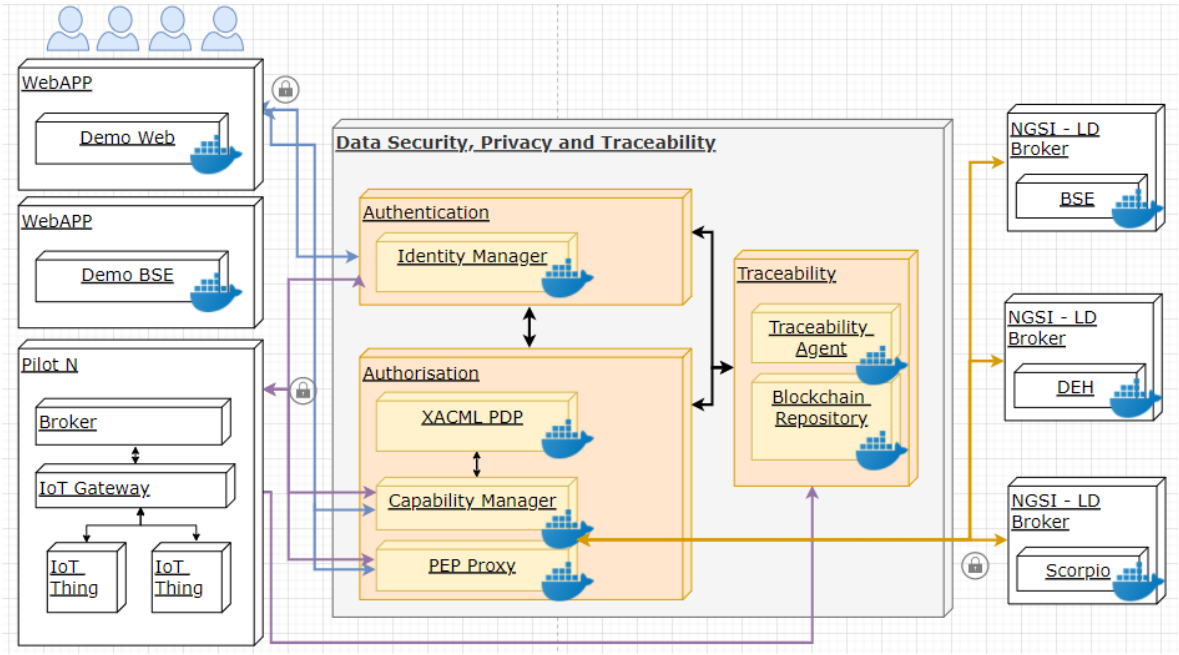


Figure 5: Security component diagram

5 DEMETER Enabler Hub (DEH)

The DEH represents the digital space where (technically capable) end users of DEMETER are able to create and register their own resources. Users have two roles; they act as DEMETER Provider and DEMETER Consumer. A DEMETER Provider is able

to offer and manage his resources (components, services, data sources, devices, platforms, etc), while DEMETER Consumers will be able to browse it and find suitable resources matching their requirements.

DEH Components is composed of three main modules:

- DEH Dashboard functional module is in charge of User Interaction & Data Visualisation. It allows users to login to DEH, discover, register and manage DEH Resources.
- DEH Authentication & Authorization functional module is in charge of User Authentication and Authorization. It contains information related to users.

DEH Resource Registry Management functional module is in charge for managing DEH Resources. It manages creating, validating, editing, deleting, discovery and consumption of DEH Resources.

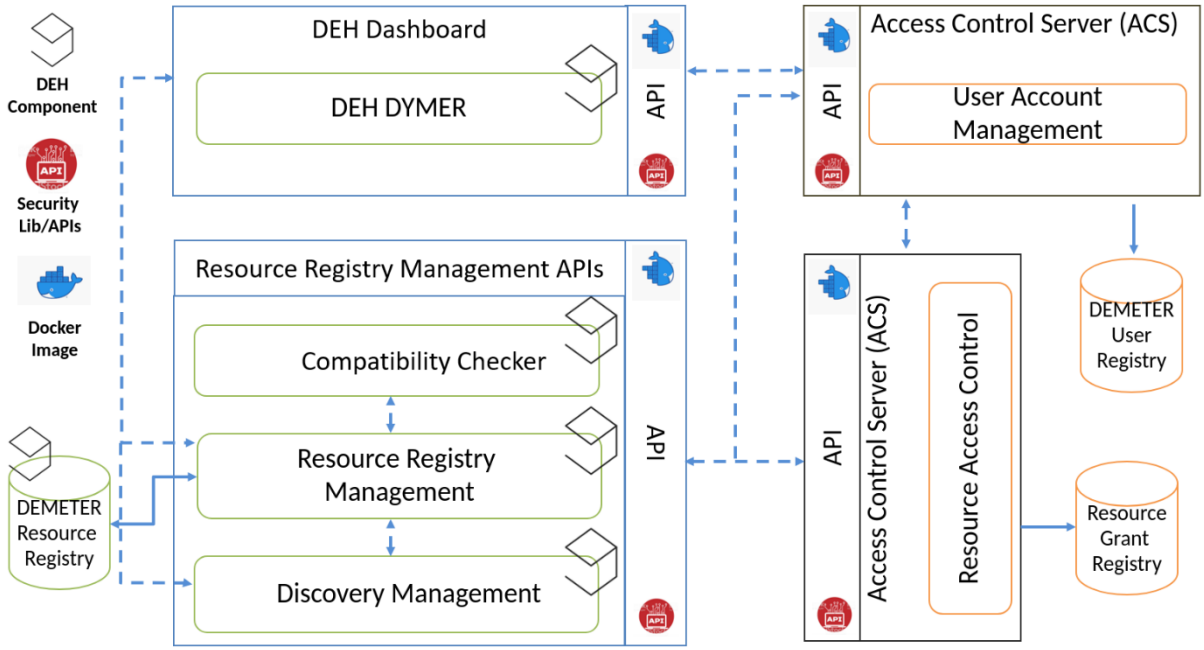


Figure 6: DEH Functional Architecture

Secured communication among all components is provided by a Security Enabler, more specifically by the Identity Manager, and Access Control Server (Capability Manager) components.

The DEH Dashboard communicates with Resource Registry Management (RRM), where all data related to future DEH Resources is inserted by the user, and passed to be verified by Compatibility Checker, and if the data satisfies all necessary requirements, it will be stored inside the DEMETER Resource Registry. In the end, the

DEH Dashboard is able to show these resources to the end-users of DEMETER, who intend to view them.

All Hub components are made available for deployment via Docker containerisation. This increases the configurability of the API's and the flexibility of the DEH components by allowing different deployment modes such as cloud-centric or Pilot environments.

6 Core Enablers for Integration

6.1 Functional Interoperability Enabler (FIE)

Functional Interoperability core Enabler (FIE) can be regarded as the client-side of the Brokerage Service Environment. This Enabler provides all the services of the BSE to the rest of the DEMETER modules and enablers, and also to the Consumer's application. It serves as a wrapper for the Registration, Discovery, and Provisioning services offered by the BSE, but also offers the compatibility check feature, i.e., a compatibility check of a service to be registered, with the BSE data model. The FIE is bundled with the BSE module and provides its functionality along with the BSE module.

6.2 Access Control Enabler

The Access Control Enabler is composed by:

- The ***Authentication Security Enabler***: provides the DEMETER components and the pilots developers with an abstract way to access to the Authentication OAuth 2.0 functionalities exposed by the DEMETER Authentication component REST API. This library provides the following functions: authentication by username and password, refresh authentication and revoke authentication token.
- The ***Authorisation Security Enabler*** provides a solution for controlling the access to the resources stored in an information repository. It is based on a technology called Distributed Capability-Based Access Control, which basically decouples the traditional XACML framework, into two phases: one for receiving the authorisation, which is represented by the receipt of an authorisation token called Capability Token, and a second one for accessing the information repository where basically, the user/service inserts the previous Capability Token in the corresponding query so that a Policy

Enforcement Point Proxy (PEP_Proxy) could check if the query matches the content of the Capability Token. In case of a positive answer, the PEP_Proxy acts as a mere intermediary between the user/service and the information repository.

- The ***Communications and Networking Enabler*** provides confidentiality properties through TLS/DTLS protocols, as well as providing encryption and decryption of JSON and XML.

6.3 DEH Client Enabler

The *DEH Client Enabler* enables discovering, monitoring, and generating resource consumption metrics of DEH Service containers deployed on a Docker Host. The metrics data is visualised with the DEH Dashboard. The DEH Client Module is also deployed as a Docker container, thus enabling an external party to deploy DEH Client solution as a stand-alone Docker Container and start monitoring containers on any Docker Host hosting DEH Service Containers.

demeter

CONTACT US

Kevin Doolin, Project Coordinator

Kevin.Doolin@WaltonInstitute.ie

or email **INFO@H2020-DEMETER.EU**

For more information visit **WWW.H2020-DEMETER.EU** and follow us on social media:

H2020DEMETER **H2020DEMETER** **h2020-demeter** **h2020-demeter**