D4.13

Communications and Information Sharing - Specification

Instrument	Collaborative Project
Call / Topic	H2020-SEC-2016-2017/H2020-SEC-2016-2017-1
Project Title	Multi-Hazard Cooperative Management Tool for Data Exchange, Response Planning and Scenario Building
Project Number	740689
Project Acronym	HEIMDALL
Project Start Date	01/05/2017
Project Duration	42 months
Contributing WP	WP 4
Dissemination Level	PU
Contractual Delivery Date	M18
Actual Delivery Date	01/04/2019
Editor	Benjamin Barth (DLR)
Contributors	Benjamin Barth, Tomaso de Cola, Monika Friedemann, Christian Knopp, Michaela Bettinger, Sandro Martinis, Alberto Viseras Ruiz, (DLR), Alexandros Bartzas, Spyros Pantazis (SPH), Miguel Mendes (TSYL), Stéphanie Battiston (UNISTRA), Jose A. Navarro (CTTC), Claudia Abanco (ICGC), Eva Trasforini, Flavio Pignone (CIMA)

Document History			
Version	Date	Modifications	Source
0.1	26/01/18	First draft	DLR
0.2	10/02/18	Technical requirements generated	DLR
0.3	18/12/18	Update if the requirements form EUW2	DLR
0.4	30/01/19	Update of the specification	DLR
0.5	01/02/19	First review of the specification	SPH
0.6	14/03/19	Naming structure added	All partners
0.7	15/03/19	Added content of section 1,3 and 4	DLR
0.8	19/03/19	QA ready	DLR
0.9	29/03/19	QA version	SPH
1.0.D	29/03/19	First Issue	DLR
1.0.F	01/04/2019	Final version submitted	DLR

Table of Contents

List of Figures

List of Tables

List of Acronyms

ACP	Access Control Provider
API	Application Programming Interface
CD	Content Descriptor
EO	Earth Observation
COPSS	Content Oriented Pub/Sub System
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IA	Impact Assessment
ICN	Information Centric Network
IP	Internet Protocol
LU	Local Unit
P2P	Peer to Peer
Pub	Publish
RP	Rendezvous Point
SP	Service Platform
Sub	Subscribe
UeRM	User and Role Management
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
VPN	Virtual Private Network
WG	Working Group

Intentionally blank

Executive Summary

This document provides the requirements and specification of the HEIMDALL catalogue module. The module is part of Task 4.4 which designs and develops components and services which can be used by various Local Units (LUs) in order to facilitate the cooperation among end-users. The catalogue organizes the data sharing and communication of end users without direct access to the data. The specified design follows a content orient approach with publication and subscription mechanism that allows for data exchange and discovery and enables a multi-disciplinary network of users. The data exchange is done in a peer to peer manner; in this way the users have full control about who has access to their data. Mapping services can be used to transform HEIMDALL data to standard data exchange protocols e.g. PDF, EDXL standards and other formats defined, as developed by WP6 Task 6.3 situation assessment services and presented in D6.7 [1]. It must be noted that this document treats the communication between different organisations. Information about communication within a single organisation (e.g. to users in the field) can be found in D4.16 [2].

1 Introduction

One main goal of HEIMDALL is to foster data and information sharing among multi-disciplinary stakeholders of multiple organisations also in international context in order to improve the cooperation capabilities. For this, HEIMDALL sets up a federated architecture of multiple local units (LU) for sharing data and information and provide collaboration services. A LU is an instance of a HEIMDALL system owned by a single organisation, e.g. fire fighters in Catalonia or France, or medical services, police, civil protection, command and control. This LU generates data belonging to this organisation which can include for instance, scenarios, sensor data, simulations, impact assessment data (IA) and Earth observation (EO). For collaboration users might want to share the data where there are three potential use cases:

- First, in most cases of an actual ongoing incident, multiple organizations are usually involved. This also applies in an international context where cross border scenarios could engage multiple organizations from more than one country. In all cases, information exchange and communication among the organizations is critical, e.g. in a forest fire situation, the fire can approach a road, so the police needs the information to block the road. Information exchange is the key in building and maintaining a common operational picture.
- Second, preparedness and training for such an incident. Scenarios can e.g. be generated in cooperation and common response plans can be prepared and shared.
- Third, is to build a network of end users to exchange experiences and information for instance about hazards, scenarios and response plans. Organizations could e.g. exchange scenarios and lessons learnt in order to support others with their knowledge in similar situations and with this strengthen the capability to respond in these situations.

A global catalogue to which all LUs can connect organises the communication and data sharing of the LUs. The catalogue itself has no access to the data itself, the data is transmitted from LU to LU in a peer to peer (P2P) mode. The principle can be seen in Figure 1-1. This approach provides opportunities for future implementations: on one hand, different services can be available in each local unit and made accessible to users accessing other local units by means of publishing them in the catalogue. On the other hand, additional external services can be easily added to the overall architecture by publishing the corresponding services or information in the catalogue and establishing the corresponding connection, without additional integration efforts.

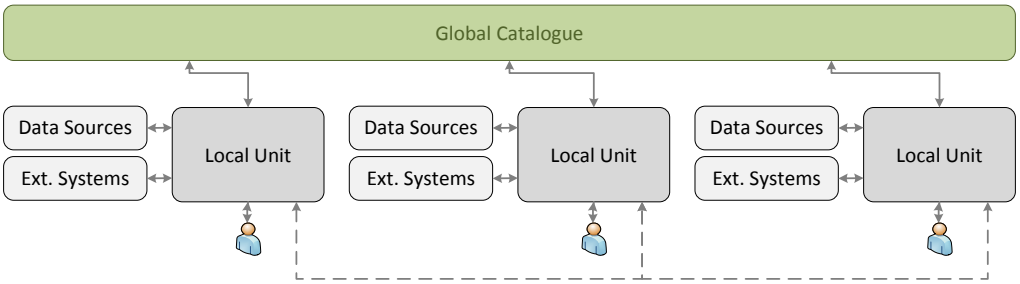

Figure 1-1: Data sharing in HEIMDALL

The architecture is organised in a content-oriented way which increases the efficiency of data sharing. Publish and subscribe services are provided by the catalogue. Users can grant access to data and always keep an overview of who can access their data. The catalogue also enable the discovery of data and with this supports the connection to other authorities. The system takes care to tailor the data so that every user can access it in his/her preferred or mandatory format. HEIMDALL makes use of common data formats, mostly based on open standards for this.

This document, giving the specification of the catalogue services, is organised as follows:

- Section 2 presents the technical requirements that have been derived from HEIMDALL user and system requirements [3].
- Section 3 sorts the catalogue in the overall HEIMDALL architecture.
- In section 4 the functionality of the catalogue is described in detail.
- Section 5 specifies the catalogue module.
- Finally, section 6 summarizes and concludes the document.

2 Technical Requirements

2.1 Interface Requirements

2.1.1 **Hardware Interfaces**

The catalogue services run in a virtual machine on a server farm on DLR premises, in principle could also be hosted on a single server. The machines are connecting via Ethernet.

2.1.2 **Software Interfaces**

The catalogue provides RESTful web services for all local units.

2.1.3 **Communication Interfaces**

The protocol to communicate with the catalogue service shall be either HTTP or, for secured connection, HTTPS.

2.2 Functional Technical Requirements

2.2.1 **Short-Term Features**

It has been decided to implement the Catalogue services not in short term in order to allow a higher level of development of the other services which outputs the catalogue requires for the sharing.

2.2.2 **Mid-Term Features**

Table 2-1: Technical Requirement TR_DSC_1

Requirement ID:	TR_DSC_1
Related SR(s):	• Sys_DSC_1 • Sys_DSC_2 • Sys_DSC_3 • Sys_DSC_13 • Sys_DSC_14 • Sys_DSC_17 • Sys_DSC_20 • Sys_DSC_24
Description: The catalogue shall be able coordinate data exchange among LUs.	
Rational: In order to exchange the data of multiple organisations a coordination module is needed which is the catalogue.	
Stimulus: LUs try to establish connections for data exchange.	
Response: The catalogue provides the necessary information to establish the connections.	
Verification Criterion: multiple LUs can be connected to the catalogue and are able to exchange information. Their users will be able to publish data and subscribe to ones already published.	
Notes: none	

Table 2-2: Technical Requirement TR_DSC_2

Requirement ID:	TR_DSC_2
Related SR(s):	• Sys_DSC_1 • Sys_DSC_2 • Sys_DSC_3 • Sys_DSC_13 • Sys_DSC_14 • Sys_DSC_17 • Sys_DSC_24
Description: The catalogue shall enable to search for specific data.	
Rational: In order to facilitate discovery information a search feature is necessary.	
Stimulus: a search request with dedicated parameters is sent.	
Response: results for the search requests are returned that fit the parameters.	
Verification Criterion: data can be searched and found using the catalogue.	
Notes: none	

Table 2-3: Technical Requirement TR_DSC_3

Requirement ID:	TR_DSC_3
Related SR(s):	• Sys_DSC_1 • Sys_DSC_2 • Sys_DSC_3 • Sys_DSC_13 • Sys_DSC_14 • Sys_DSC_17 • Sys_DSC_20 • Sys_DSC_24
Description: The catalogue shall offer means to distribute data that has been granted access by a local unit.	
Rational: In order to exchange data where access has been granted a unit must be able to distribute the data.	
Stimulus: access to data is granted.	
Response: The data can be shared with the ones having access rights.	
Verification Criterion: access to data is granted and the reference of the data is distributed to the ones with proper access rights requesting the data.	
Notes: none	

Table 2-4: Technical Requirement TR_DSC_4

Requirement ID:	TR_DSC_4
Related SR(s):	• Sys_DSC_1 • Sys_DSC_2 • Sys_DSC_3 • Sys_DSC_13 • Sys_DSC_14 • Sys_DSC_17 • Sys_DSC_20 • Sys_DSC_24
Description: The local unit shall be able to connect to the catalogue.	
Rational: in order to share the data a LU must be able to request this at the catalogue.	
Stimulus: the LU sends a request to the catalogue.	
Response: the catalogue response to the request.	
Verification Criterion: The LU and catalogue can communicate	
Notes: none	

Table 2-5: Technical Requirement TR_DSC_5

Requirement ID:	TR_DSC_5
Related SR(s):	• Sys_DSC_12 • Sys_DSC_14 • Sys_DSC_24
Description: The cataloque/LU shall be able to share information with authorities from other countries.	
Rational: in order to solve crisis on an international level the system must be usable from different countries	
Stimulus: The user grants access to data sets to other organisations.	
Response: The sharing procedure is activated	
Verification Criterion: Sharing is possible among LUs in different countries.	
Notes: none	

Table 2-6: Technical Requirement TR_DSC_6

Requirement ID:	TR_DSC_6
Related SR(s):	• Sys_DSC_1 • Sys_DSC_2 • Sys_DSC_3 • Sys_DSC_13 • Sys_DSC_14 • Sys_DSC_17 • Sys_DSC_20 • Sys_DSC_24
Description: The LUs shall be able to directly exchange information.	
Rational: To enable the users having full control about their data, it should be stored locally in the system instance of the user. To enable sharing in this circumstance, the LUs must be able to connect directly.	
Stimulus: a LU tries to get data from another LU.	
Response: data is exchanged.	
Verification Criterion: data can be exchanged directly between LUs.	
Notes: Linked to TR_DSC_3, since the access rights have to be respected	

Table 2-7: Technical Requirement TR_DSC_7

Requirement ID:	TR_DSC_7
Related SR(s):	• Sys_DSC_14 • Sys_DSC_24 • Sys_DSC_38
Description: The cataloque/LU shall provide means to share all data or specific data sets with command and control centers and forward command posts managed or used by other authorities.	
Rational: To be able to have a coordinated response to a disaster situation it is crucial that the information is shared to all possible actors involved.	
Stimulus: data is shared with another LU.	
Response: the shared information can be accessed by the FCP and the C&C of another authority.	
Verification Criterion: data can be shared among C&Cs. The FCPs can access the shared data according to their access rights.	
Notes: none	

Table 2-8: Technical Requirement TR_DSC_8

Requirement ID:	TR_DSC_8
Related SR(s):	• Sys_DSC_14 • Sys_DSC_16 • Sys_DSC_20 • Sys_DSC_24
Description: The LU shall offer means to configure data access and information sharing, specifying which data can be accessed by each user/profile.	
Rational: in order to provide access control the corresponding settings must be enabled.	
Stimulus: sharing/access settings for user profiles are requested to be modified.	
Response: the settings are modified and the sharing tool implements the modifications. The sharing/access rights are adapted accordingly.	
Verification Criterion: Access rights for dedicated users or user profiles can be modified and the system implements the modifications for sharing.	
Notes: none	

Table 2-9: Technical Requirement TR_DSC_9

Requirement ID:	TR_DSC_9
Related SR(s):	• Sys_DSC_14 • Sys_DSC_16 • Sys_DSC_24
Description: The catalogue shall be able to communicate with the user and role management of each LU.	
Rational: In order to check access rights the catalogue must be aware of the roles of an organization and the level of access they are granted.	
Stimulus: the catalogue contacts the role management of a LU with a request.	
Response: a respond to the request is send.	
Verification Criterion: request and response are sent and received.	
Notes: none	

Table 2-10: Technical Requirement TR_DSC_10

Requirement ID:	TR_DSC_10
Related SR(s):	• Sys_DSC_1 • Sys_DSC_2 • Sys_DSC_3 • Sys_DSC_13 • Sys_DSC_14 • Sys_DSC_17 • Sys_DSC_20 • Sys_DSC_24
Description: The LU shall be able to allow users to access data that has been generated or published by other system entities.	
Rational: In order to share data the LU must provide the basic features for this.	
Stimulus: data available at the LU can be shared or published.	
Response: the data is shared or published.	
Verification Criterion: data is shared or published.	
Notes: none	

Table 2-11: Technical Requirement TR_DSC_11

Requirement ID:	TR_DSC_11
Related SR(s):	• Sys_DSC_1 • Sys_DSC_2 • Sys_DSC_3 • Sys_DSC_13 • Sys_DSC_14 • Sys_DSC_17 • Sys_DSC_20 • Sys_DSC_24
Description: The LU shall be able to connect to other instances of the system via a dedicated interface.	
Rational: the system must provide an interface in order to enable the information sharing.	
Stimulus: a LU tries to connect to another LU via a dedicated interface.	
Response: a LU reacts as specified, e.g. a connection can be established if access rights have been granted.	
Verification Criterion: Two LUs can connect via a dedicated interface. o	
Notes: none	

Table 2-12: Technical Requirement TR_DSC_12

Requirement ID:	TR_DSC_12
Related SR(s):	• Sys_DSC_1 • Sys_DSC_2 • Sys_DSC_3 • Sys_DSC_13 • Sys_DSC_17 • Sys_DSC_24 • Sys_DSC_38
Description: The data that can be shared shall include risk predictions, incident predictions, lessons learnt and historical incident data.	
Rational: Specific data sets must be made available among other data.	
Stimulus: risk predictions, incident predictions, lessons learnt or historical incident data are shared by the user.	
Response: Risk predictions, incident predictions, lessons learnt or historical incident data can be accessed by other LUs that have been granted access.	
Verification Criterion: Risk predictions, incident predictions, lessons learnt and historical incident data can be accessed by other LUs that have been granted access.	
Notes: none	

Table 2-13: Technical Requirement TR_DSC_13

Requirement ID:	TR_DSC_13
Related SR(s):	• Sys_DSC_1 • Sys_DSC_2 • Sys_DSC_3 • Sys_DSC_13 • Sys_DSC_14 • Sys_DSC_17 • Sys_DSC_24
Description: The local unit shall inform the catalogue about the data where access has been granted and the access rights of that data.	
Rational: In order to get aware of an update on new data the catalogue must be informed by the LU.	
Stimulus: the LU informs the catalogue about an update on data access.	
Response: the catalogue enables the sharing features for that data.	
Verification Criterion: The LU informs the catalogue about an update.	
Notes: none	

Table 2-14: Technical Requirement TR_DSC_15

Requirement ID:	TR_DSC_15
Related SR(s):	• Sys_DSC_14 • Sys_DSC_24
Description: The cataloque shall offer a mapping feature that helps to communicate with other authorities and is able to map between standards.	
Rational: in order to work in multi-disciplinary environment mapping capabilities can ease the work of the user and avoid misunderstanding due to different terms used in the discipline.	
Stimulus: data in standard format and with standard values is shared among actors having different profile settings.	
Response: the data is mapped to the standard values of the other profile.	
Verification Criterion: Standard values that are able to be translated are translated by the system.	
Notes: none	

Table 2-15: Technical Requirement TR_DSC_16

Requirement ID:	TR_DSC_16
Related SR(s):	• Sys_DSC_23 • Sys_DSC_24 • Sys_DSC_25
Description: The catalogue shall provide a chat function so that communication with forward command posts and C&Cs of other authorities is possible.	
Rational: it is a fast way to establish direct communication of different persons in front of a PC.	
Stimulus: user initiates chat procedure.	
Response: other users receive notification about the chat and can answer.	
Verification Criterion: people can exchange text messages.	
Notes: none	

Table 2-16: Technical Requirement TR_DSC_17

Requirement ID:	TR_DSC_17
Related SR(s):	• Sys_DSC_36
Description: The catalogue shall be able to provide information about who has access to which data.	
Rational: In order to allow the user to have a good picture of the situation it is necessary that	

the user knows who has access to the data.
Stimulus: user requests an overview for a data set about who the access rights.
Response: the catalogue answers with the access rights.
Verification Criterion: The correct access rights for the data set are shown.
Notes: none

Table 2-17: Technical Requirement TR_DSC_18

Requirement ID:	TR_DSC_18
Related SR(s):	• Sys_DSC_36 • Sys_DSC_24 • Sys_DSC_25
Description: The catalogue shall be able to show the incident commander who has accessed the data already	
Rational: In this way the incident commander can have an overview if there is a lack of information at some point.	
Stimulus: The incident commander asks about the status of distribution for some information.	
Response: System returns if someone with access rights already had accessed the data.	
Verification Criterion: The incident commander can identify if a data set has been accessed by another user.	
Notes: none	

Table 2-18: Technical Requirement TR_DSC_19

Requirement ID:	TR_DSC_19
Related SR(s):	• Sys_DSC_42
Description: The catalogue shall provide a function to request assistance from other organisations also internationally if access rights allow for it.	
Rational: the system information sharing provides a fast way of request for assistance.	
Stimulus: user request assistance from another organisation.	
Response: the catalogue forwards the request.	
Verification Criterion: The request is received at another system instance.	
Notes: none	

Table 2-19: Technical Requirement TR_DSC_20

Requirement ID:	TR_DSC_20

Related SR(s):	• Sys_DSC_43
Description: The catalogue shall allow adding manual translations.	
Rational: in international context it is sometimes necessary to translate.	
Stimulus: user adds a translation	
Response: the catalogue stores the translation which can be accessed by other users with proper access rights.	
Verification Criterion: The translation can be accessed.	
Notes: none	

2.2.3 **Long-Term Features**

Table 2-20: Technical Requirement TR_DSC_17

Requirement ID:	TR_DSC_17
Related SR(s):	• Sys_DSC_4
Description: The catalogue shall offer means to trigger simulations on demand for users.	
Rational: In order to share not only data but also services the simulations can be triggered remotely.	
Stimulus: a simulation result is requested via the catalogue by another LU.	
Response: the simulation is triggered and the result is returned.	
Verification Criterion: a simulation is requested and the result is returned.	
Notes: none	

2.3 Other Requirements

2.3.1 **Short-Term Requirements**

Table 2-21: Technical Requirement TR_DSC_19

Requirement ID:	TR_DSC_19
Related SR(s):	• Sys_DSC_6 • Sys_DSC_14 • Sys_DSC_17
Description: The catalogue/LU shall be able to connect to communication networks.	
Rational: In order to forward messages and connect first responders the catalogue/LU must be able to connect to communication networks.	
Verification Criterion: The catalogue/LU can establish a connection to other system components according to the overall system architecture.	

Notes: Standards should be used.

Table 2-22: Technical Requirement TR_DSC_20

Requirement ID:	TR_DSC_20
Related SR(s):	• Sys_DSC_26
Description: The catalogue/LU shall be connected to secure communications links.	
Rational: The links to and from the catalogue/LU must be secured to ensure security of the whole system.	
Verification Criterion: An attacker outside of the secured network tries to access the catalogue/LU which shall not be successful.	
Notes: Standards should be used.	

2.3.2 **Mid-Term Requirements**

Table 2-23: Technical Requirement TR_DSC_21

Requirement ID:	TR_DSC_21
Related SR(s):	• Sys_DSC_1 • Sys_DSC_2 • Sys_DSC_3 • Sys_DSC_12 • Sys_DSC_13
Description: The cataloque/LUs shall make use of international standards as much as possible for data sharing.	
Rational: In order to increase the use of the system and enable communications with other platforms standards are needed especially in international environment.	
Verification Criterion: The system can exchange information according to a standard and is compliant with this.	
Notes: Standards should be used.	

Table 2-24: Technical Requirement TR_DSC_22

Requirement ID:	TR_DSC_22
Related SR(s):	• Sys_DSC_12 • Sys_DSC_14
Description: The catalogue shall be able to support multiple local units in a scalable manner.	
Rational: In order to have a system that can be used on international and national level with a lot of actors a lot of LUs will be active. In order to be able to interconnect all this LUs the	

catalogue must be designed scalable.
Verification Criterion: The catalogue can be run on platforms that can be extended in terms of resources.
Notes: Standards should be used.

2.3.3 **Long-Term Requirements**

No long term requirements have been identified.

3 Reference Architecture

In Figure 3-1 the general HEIMDALL system architecture is shown. On the left hand side there are the system inputs that are used within the HEIMDALL system to provide products. The main HEIMDALL system products are generated by the simulators, the risk assessment, impact summary, the decision support and the scenario management module. For communication to users in the fields an app is provided and the so called information gateway module provides services for this. All these modules generate products (i.e. data) that are of potential interest to be shared with other organisations which is performed via the catalogue and an interface to other instances (marked in green). The catalogue controls the data sharing and offers the necessary services. The interface connected to the HEIMDALL service platform (SP), is then used to actually transmit the data.

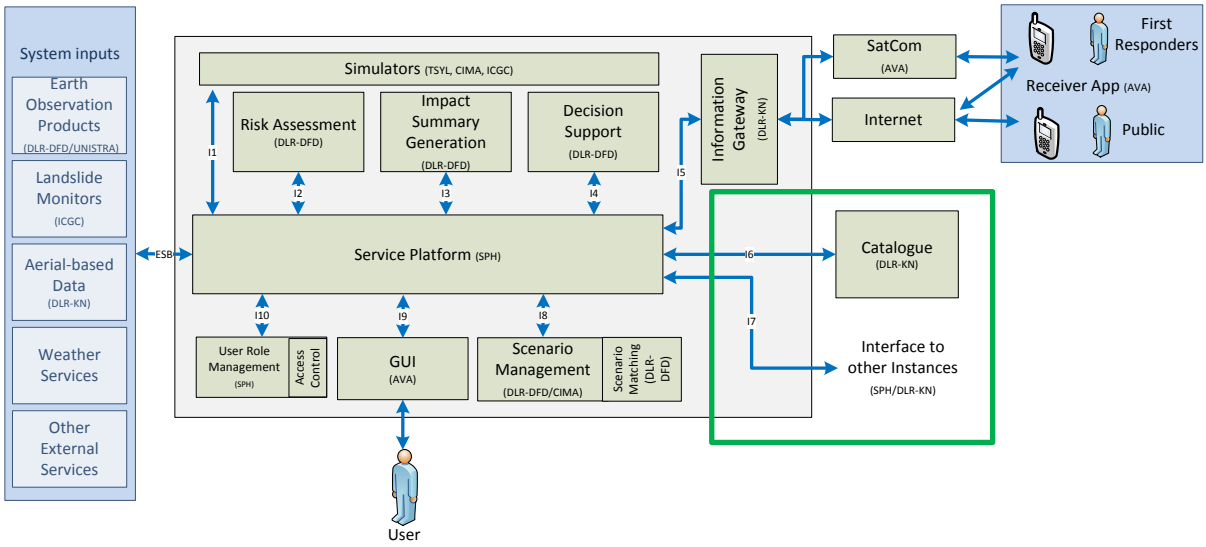

Figure 3-1: Local unit architecure

Figure 3-2 shows an example with two connected LUs, for user A and user B but the setup can in principle be extended for multiple users. The HEIMDALL approach is a federated architecture based on content-oriented design which offers efficient communication and at the same time ensures security. The data and service catalogue helps with the information discovery and the connection to other authorities. The system takes care to tailor the data so that every user can access it in his/her preferred or mandatory format. As mentioned, HEIMDALL makes use of common data formats, mostly based on open standards for this.

The catalogue is the core unit for the interconnection of multiple LUs. It will provide several services that enable efficient communication among the end users which are:

- As basis for the interconnection the catalogue manages the addresses of the LU and provides them for P2P connection if the permission has been given.
- By the use of standards for cross-national interoperability and information exchange HEIMDALL will provide a mapping of standardized formats.
- End users can publish their data to other users using the system. They grant access of specific data sets or all data. HEIMDALL offers an information discover service for this published data.
- A working group service enables live collaboration of the different organisations.

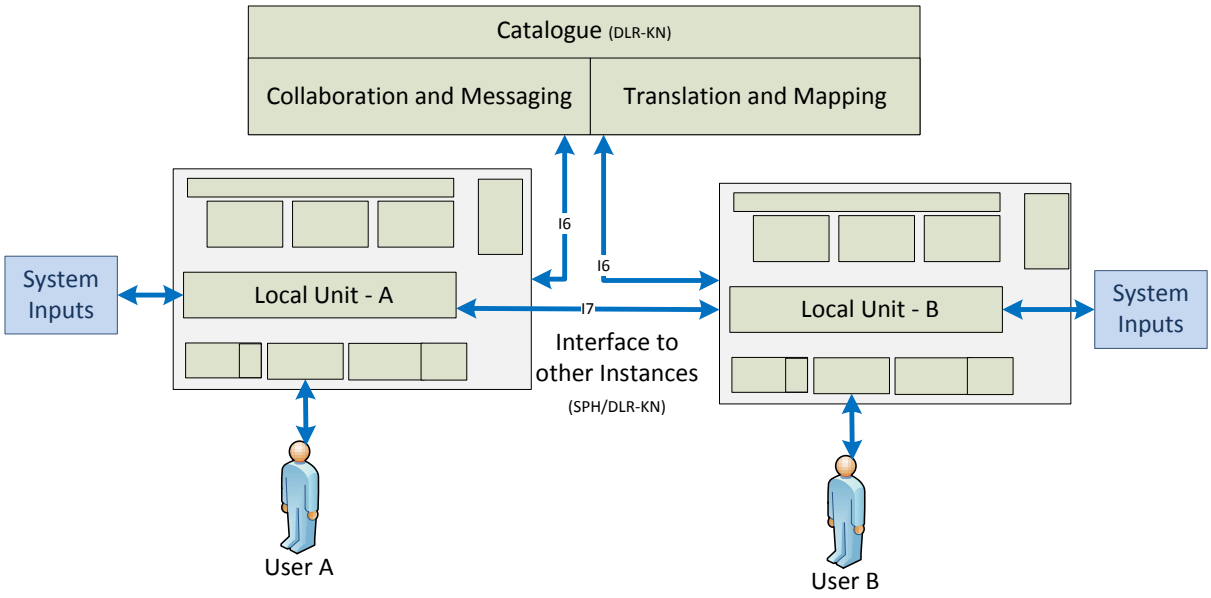

Figure 3-2: Federated architecture example

Table 3-1 summarises the services and the required inputs as well who uses the services and the modules providing it.

Table 3-1: Catalogue inputs/outputs

Products and/or Services	**Inputs needed**	**Provided by**	**Used by**
Connection to other LU	Connection Parameters	Interfaces to LU	Interface to LU
Information Discovery	Shared Content and metadata	GUI LU	GUI LU
Mapping service	Shared Content and metadata	GUI LU	GUI LU
Collaboration	Data input by the user	GUI	GUI

4 Module Functionality

The Catalogue is a webserver offering RESTful web services for which an application programmable interface (API) connects to other HEIMDALL components. The request is forwarded to dedicated system methods that process the request. If needed, a reply or other connections are created and forwarded by a return function (RTN). The structure and the available methods can be seen in Figure 4-1. The server includes a database with the tables (presented in section 5.2) required to provide the services. The functionality presented in this report is a first version; updates can still be performed and will be presented in the final version of this document D4.14 due at M38. The approach followed is a content oriented one where data is exchanged based on the name of the data; this is further described in section 4.2.

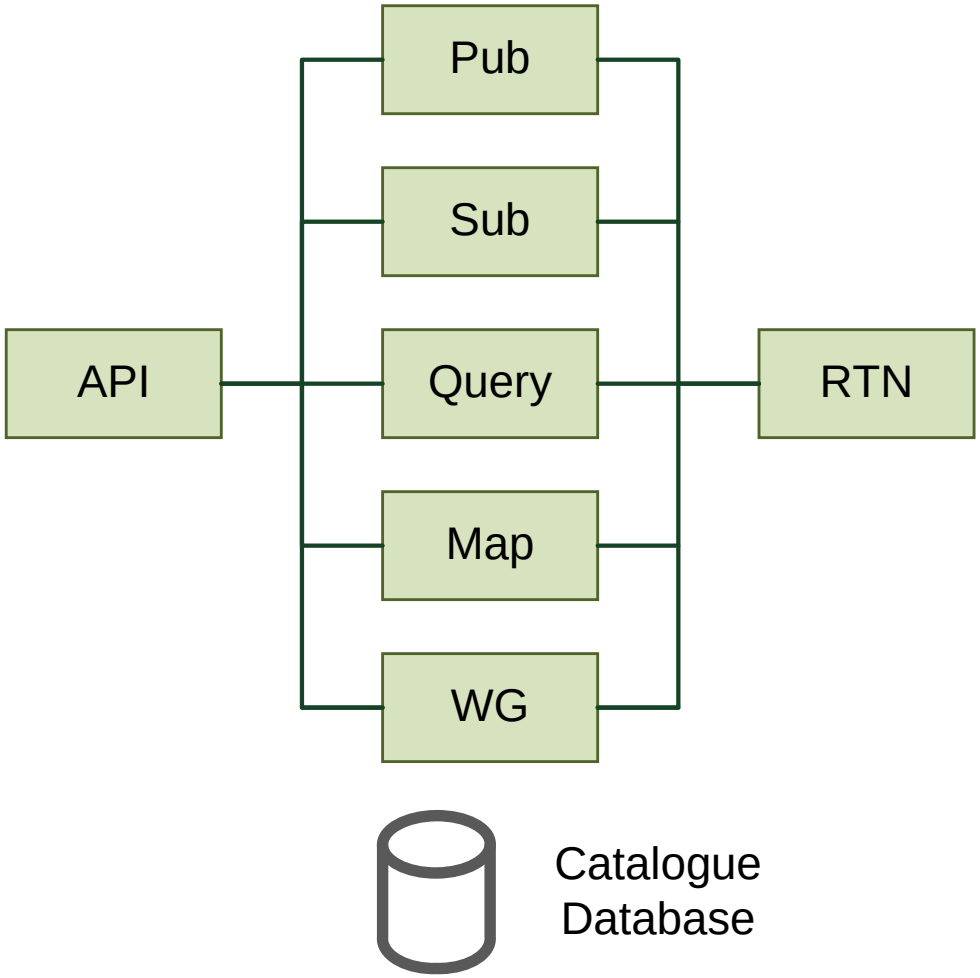

Figure 4-1: Catalogue API structure

Publish (Pub): this can be used if a data owner wants to share data with other entities or stop sharing data. The name of the data shall be send. The publications table in the database is updated (see Table 5-2).

Subscription (Sub): this can be called if a user wants to un-/subscribe to a dedicated topic. If subscribed, the user will receive available data once available in the system, i.e. someone published fitting content. If for instance subscribed to:

```
Simulation/Fire/Catalonia
```

The user receives all messages for which the access is enabled and that include the attributes fire and Catalonia. The catalogue is not directly sharing or storing the data, only the name is used for subscription.

Query: in contrast to subscription where there are continuous updates, a query is a single request of fitting data available in the network. Queries are performed by name where search parameters are attached to corresponding part of the name. There are two different kinds of queries: the first checks for an exact match using the equals sign (“=”) and the second checks for a range of numbers using either a logical operator (“<”, “>”, “>=”, “<=”) or curved brackets to directly set the range (“{”, “}”). The query can include multiple names to detail the query and improve the match result. An example would be:

```
Scenario/Fire/Wind speed{50-100}/Catalonia/
```

which would return all shared scenario data matching a fire hazard with wind speed between 50-100 in the area of Catalonia. The catalogue does not hold the data. Consequently, it cannot perform a complete match itself. But it uses the publications table to determine a list of possible matches. If the data fits and access control allows data is transmitted using the P2P link.

Map: this method can be used to map some data structures to another. Specifically it is foreseen to map the situation report or scenario structure to PDF in order to share it with other organisations or for example politicians. The data is transmitted to the catalogue with the supported and desired format and the catalogue returns the converted data. Optionally a list of addresses can be added. In this case the catalogue automatically shares the converted data with the addresses. The last item needs to be evaluated if it will be implemented.

Temporal Working Group (WG): This offers all functionality needed for forming a temporal working group (WG). The idea is that in response mode (during a disaster situation) all or some involved organisations can form a WG that lasts for this incident. The WG works on a synchronized scenario object. If the incident is over the group is resolved and included organisations keep their local copy of the scenario object.

To start this process an organization sends a reference to a scenario object to the catalogue and invites other organizations to join. Also references to an empty scenario object can be transmitted. All organizations can now perform updates on their scenario object which are automatically updated via the P2P links. The catalogue supports with the synchronisation.

Translation: translation was a feature that we first considered for the platform. But it was a requirements by our users that only manual translation shall be done. Since there is no need for translations provide by the system we did not considered this point in the design.

Chat: Chat function refers to TR_DSC_16 and can be used for collaboration and direct communication of involved personal. Initially, it was planned to have this service provided by the catalogue, but it was agreed that the notification service provided by the SP can also be used to provide an instant messaging service. The basic features are already available at the SP and the GUI.

4.1 Content Oriented Approaches

Content oriented approaches describe a new paradigm of networking that has drawn quite big attention in the research community. The goal is to overcome problems of the host-centric approach of today’s internet with high request for digital content of the modern society by using a content centric approach. Users looking for content, request it directly from the network and not from a specific host. The content is identified by its name where there can be multiple copies of it in the network. The closest one to the requester is usually delivered which increases the efficiency of the network. In principle, the new paradigm needs a dedicated network consisting of nodes that are able to perform content oriented routing and provide caching, but it is also possible to run such a network on top of TCP/IP.

In [4] they presented how information centric networks (ICN) can be used during disaster situations with the focus being on damaged communication infrastructures. Open research topics are pointed out. Accordingly, the benefits of an ICN approach during disaster situation on the fields are:

- Routing by name
- Authentication of named data objects
- Content-based access control
- Caching
- Sessionless
- Potential to run IP-based services
- Traffic prioritisation

The scenario matches more the one considered for data sharing to users in the field and among the users in the field, which is handled in D4.16 [2]. But here a classic host centric approach is selected since necessary access to network resources is missing during the project. For the HEIMDALL communication and data sharing is a different scenario since the data is shared among different HEIMDALL LUs that are usually placed outside the disaster area. Nevertheless, some of the benefits are still interesting for this scenario given the user requirements. In using content based approach we see the following advantages for HEIMDALL system:

- Authentication of named data objects
- Decentralised content-based access control
- publish/subscribe mechanism
- Sessionless
- Discovery by name

4.2 Network

The selected approach is based on the Content Oriented Pub/Sub System (COPSS) [5]. The network structure can be seen in Figure 4-2. The catalogue serves as a so called rendezvous point (RP) that deals in our case with data related to hazards and disaster management. But in principle it is not limited to this.

The basic idea is that if a content owner wants to share data it is publishing the data using the catalogue by sending a content descriptor (CD), in our case the name of the data, following a well-defined naming scheme (Section 5.1). The catalogue maps between the content oriented world and the internet protocol (IP) world by maintaining a table with all CDs and the corresponding IPs and user IDs. If a user wants to subscribe to content, it sends a subscription message (containing a CD to which the user wants to subscribe) to the catalogue which initiates the next steps for this subscription. In contrast to [5] data is not transmitted via the RP, the peers directly exchange the data which on the other hand means that the publisher and subscriber are not decoupled.

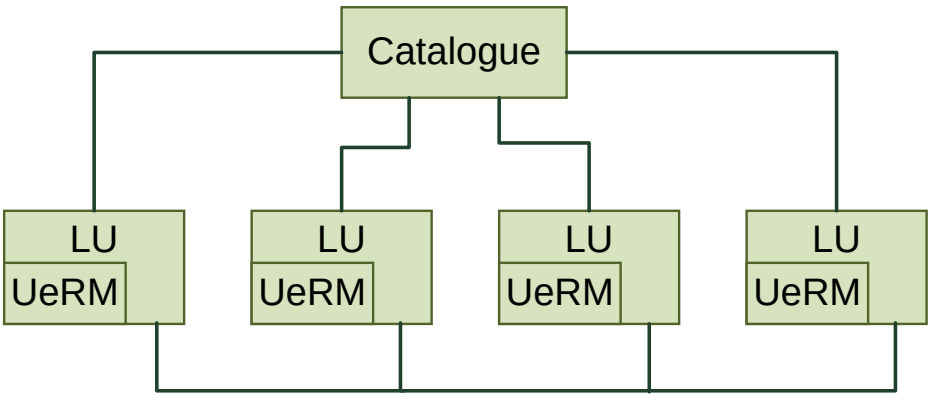

Figure 4-2: HEIMDALL network

All nodes are within the HEIMDALL virtual private network (VPN) which means that communication links are secured. Furthermore, authentication is guaranteed since

communication is organized by the catalogue in a closed network. Only authorized users will have access to the catalogue.

4.2.1 **Access Control**

For access control three alternative approaches have been identified. For initial implementation the first one is selected since it is the approach avoiding modifications at the LU as much as possible. However, for completion also the others are presented since they also offer advantages and could be considered at later stages.

In the first approach, the access control rights are included in the name when data is published. With this it is on the catalogue to check queries and subscriptions requests for the necessary access rights. If access rights are updated at the LU, the updated rights must be forwarded to the catalogue. The access rights will just be used at the catalogue and not be included in the naming scheme for query or subscription matching. On query or subscription the catalogue sends a list of publishers that offer data fitting the request to the subscriber. This approach is currently considered in the current naming design presented in section 5.1 and in the specification.

The second approach considers the design presented in [6] where the access control provider (ACP) is the user and role management (UeRM) services from the HEIMDALL system, i.e. a distributed ACP approach. The catalogue does not receive any information about access rights. Receiving a query or subscription it forwards the request to the publishers which then check on their side if they grant access to this request. The check is consequently moved to the LU and allows for a maximum of control. It further would allow for more detailed queries since the LUs actually know the data and can match better as it would be the case at the catalogue based on the naming.

Last approach for access control is attribute-based encryption [7], which is the one affecting the LU design the most, so could only be considered for further evolutions of the system. In this approach the data is authenticated and encrypted at the same time. A key authority distributes keys based on the access roles set by the data owner. The access roles depend on so called attributes. Only subscribers fulfilling the attributes can decrypt the data. Attribute for example can be the role, discipline, area or any logical combination.

5 Technical Specification

5.1 Naming

For HEIMDALL we define a URI like naming where the name can be selected by the data owner keeping the communication infrastructure transparent to any names and structures. An example would be:

```
Data/Hazard/Attribute 1/Attribute 2/Attribute 3/
```

Nevertheless, for efficient data discovery and sharing it is recommended to follow the guidelines from the following sections. The name shall be unique for a dedicated content and needs to describe the content as much as possible.

Any UTF-8 character is valid besides a slash (“/”), logical operators (“=”, “<”, “>”, “>=”, “<=”) and curved brackets (“{”, “}”) to avoid confusion. If still these signs should be used they need to be encoded; the encoding format still needs to be decided on and will be presented in D4.14 at M38.

All naming fields are optional from the catalogue side, which as a communication system it is agnostic to the data. However, for usability some naming fields are defined. The following presented name elements consist of multiple sub-elements, forming a tree structure as shown in the following example:

- Tree
    - Branch 1
        - Leaf 1.1
        - Leaf 1.2
    - Branch 2
        - Leaf 2.1
        - Leaf 2.2

The complete name of this tree would be:

```
Tree/Branch 1/Leaf 1.1/Leaf 1.2/Branch 2/Leaf 2.1/Leaf 2.2/
```

Not all fields need to be set but the more fields are set the better the discovery will work. Only rule for naming is that if a sub-element is used the parent element needs to be added as well. So the name can for instance also be:

```
Tree/Branch 2
```

or

```
Tree/Branch 1/Leaf 1.2
```

With this, the user can follow the tree in the GUI and stop at any point s/he wishes, for query and subscription operations. Some subtrees can be skipped if the users are not interested in or if they are interested in all parts of the tree. For instance, a user is interested in `Leaf 1.1` and `Leaf 1.2` data, can just subscribe to `Branch 1` since this includes the two nodes. If a user is interested in `Leaf 1.1` and `Leaf 2.1` and `Leaf 2.2` the subscription or query should look like:

```
Tree/Branch 1/Leaf 1.1/Branch 2
```

For publication the name should always be as complete as possible.

5.1.1 General Structure and fields

For usability the naming structure should in general follow the following example:

```
Local Unit ID / Access Rules / Language / Area / HEIMDALL Product /
```

The local unit ID is unique to the LU and shall be added to the name automatically by the system when data is shared. The ID identifies the publisher and can be used as a search filter, e.g. if a subscriber only is interested in the publications of a dedicated entity.

The access rules are generated and attached to the name by the UeRM module. They are used internally by the catalogue to perform the access control and cannot be used for the discovery or subscription, i.e. this field only can be set for publication.

The sub-elements in the general naming structure are defined as:

- Area
    - Country
    - State
    - Region
- HEIMDALL Product
    - Impact assessment
    - EO data
    - Simulation
    - Impact summary
    - Scenario

At the moment only English is considered as language during the project. However, for a Europe-wide use the system must provide multi-language capabilities hence the “Language” field is already considered in the naming structure. We currently define a not set language field in the name as default value set to “en-GB”.

To identify the HEIMDALL products specific naming details are presented in the following sections. In this specific naming there are some fields that are used for several HEIMDALL products and which are defined as follows:

- Timestamp (in UTC)
    - hh
    - mm
    - ss
- Date
    - Year
    - Month
    - Day
- Hazard Type
    - Forest fire
    - Flood
    - Flash flood
    - Terrain movement
    - Landslide

5.1.2 **Impact Assessment**

The following naming structure is proposed for the impact assessment products.

```
LU ID / Language / Area / Impact Assessment / Hazard Type / Mode / Date
```

- Mode
    - Simulation based
        - Simulation (see section 5.1.6)
        - IA Product Type
            - Human
            - Economic
            - Physical
        - Hazard level

- EO based
  - EO Data (see section 5.1.4)
  - Timestamp
  - IA Product Type
    - Human
    - Impact assessment on population
    - Physical
    - Building impact assessment
    - Road network impact assessment
    - Impact assessment on land cover

5.1.3 **Impact Summary**

The following naming structure is proposed for the impact summary products.

```
LU ID / Language / Area / Impact Summary / Impact Assessment / Date / Summary Products
```

Impact Assessment and Mode according to impact Assessment (see section 5.1.2)

Summary products tree:

- Summary Products
  - Total human population
  - Total economic values
  - Total physical numbers
  - Total mean damage in percentage
  - Total max damage in percentage
  - Total min damage in percentage
  - List of total quantities of damaged assets
    - Number of Buildings
    - Kilometres of roads
    - Hectares of LULC
  - List of damaged asset types
    - Buildings
      - Residential
      - Service Infrastructure
      - Non-residential
    - Roads
      - Primary
      - Secondary
    - LULC
      - Grassland
  - Maximum hazard level
  - Maximum risk

5.1.4 **Earth Observation**

The following naming structure is proposed for the earth observation products.

```
LU ID / Language / Area / EO Data / Hazard Type / Sensor Name / Tiles / Product Type / Date / Timestamp
```

- Sensor Name
  - Sentinel-1
  - Sentinel-2
  - TerraSAR-X
  - Modis
  - Pléiades

    - SPOT-6
    - SPOT-7
- Tiles with same timestamp only for Sentinel-2, unique otherwise.
- Product Type
    - flood extent or flood delineation
    - reference water extent
    - burned area or burnt area or burn scar
    - landslide extent or landslide delineation
    - landslide activity
    - fire severity
    - fire hot spots

For the sensor names and EO products, a mapping between possible values is agreed and presented in Table 5-1. Both values can be used at the catalogue which automatically maps them in queries, publication and subscription commands.

Table 5-1: EO naming mapping to abbreviation

Name Element	Possible Values	Abbreviation
Sensor Name	Sentinel-1	S1
	Sentinel-2	S2
	TerraSAR-X	TSX
	Modis	MODIS
	Pléiades	
	SPOT-6	
	SPOT-7	
Product Type	flood extent, flood delineation	FE
	reference water extent	RWE
	burned area, burnt area, burn scar	BA
	landslide extent, landslide delineation	LE
	landslide activity	LA
	fire severity	FS
	fire hot spots	FHS

5.1.5 **Sensor Data**

The following naming structure is proposed for the sensor data products.

```
LU ID / Language / Area / Sensor Data / Sensor Type / Sensor Product /
```

- Sensor Type
    - Geotechnical sensor
        - Sensor Product
            - Geotechnical sensor data
                - Station
                - Sensor name
                - Date
                - Timestamp

        - Type of geotechnical sensor
            - Battery level sensor
            - Thermistor
            - Extensometer
            - Crackmeter
            - Anemometer
            - Rain gauge
            - Piezometer
    - Geotechnical report
        - Date
        - Timestamp
    - Deformation Map
        - Format
            - CSV
            - JPEG
            - Shape file
        - Type
            - Accumulated
            - Instantaneous
        - Time
    - Closest place
- Drone System
    - Sensor Product
        - Pictures
            - Type
                - Thermal
                - visual
            - Hotspot
            - Time
        - Drone
            - Drone ID
            - Date
            - Timestamp

5.1.6 **Simulation**

The following naming structure is proposed for the simulation products.

```
LU ID / Language / Area / Simulation / Hazard Type / Simulation Mode
Simulation Product / Date / Input Parameters / Simulation ID / Scenario
```

- Hazard Type
    - Forest Fire
        - Simulation mode
            - Fire spread mode
                - Simulation product
                    - Arrival time of the fire: “arrivaltime”
                    - Flame length of the fire: “simflamelength”
                    - Rate of spread of the fire: “simros”
                    - Minimum travel time fire paths: “firepaths”
                    - Areas of out of suppression capacity: “supression”
                    - Flame Intensity: “simflameintensity”
                    - Fire Perimeter
                - Input parameters
                    - Time and date of simulation start
                    - Number of hours

- Simulation description
- ExtentCols
- ExtentRows
- Moisture type
- Weather type
- Temperature in degree Celsius
- Air moisture in percentage
- Shadow in percentage
- Wind speed in km/h
- Wind direction in degree

- Landslide
  - Simulation mode
    - Susceptibility
      - Simulation product
        - Susceptibility simulation
      - Input parameters
        - Type of landslide
          - Rock falls
            - Size
              - Small
              - Medium
              - Large
            - Precision
              - High
              - Medium
          - Landslide
            - Size
              - Small
              - Medium
              - Big
              - Very big
            - Type of soil
              - Gravel
              - Sand
              - Silt
              - Clay
            - Soil humidity
              - Dry
              - Low
              - Medium
              - Wet
          - Debris flow
            - Size
              - Small-medium
              - Large
            - Precision
              - High
              - Medium
            - Type of material
              - Coarse
              - Coarse and fine
              - Fine
    - Rainfall
      - Simulation product
        - Susceptibility simulation
      - Input parameters

                - Name of event
                - Day
                - Timestamp
            - Complete (it is the concatenation of susceptibility + rainfall)
    - Flood
        - Simulation mode
            - Real time simplified
                - Simulation product
                    - Real time flood extension
                    - Real time water depth
                    - Dynamic of flooding
                - Input parameters
                    - Peak discharge value
                    - Peak discharge timing
                    - Flood duration
                    - Possible interaction with sea
            - Complete 2D hydraulic
                - Simulation product
                    - flood extension
                    - water depth
                    - water velocity
                    - dynamic of flooding
                - Input parameters

5.1.7 **Scenario**

The following naming structure is proposed for the scenario management products.

```
LU ID / Language / Area / Scenario / Hazard Type / Status / Urgency / Casualties / Conditions / Date / Scenario ID
```

- Scenario
    - Hazard Type
    - Status
        - Unknown
        - Actual
        - Exercise
    - Urgency
        - Unknown
        - Immediate
        - Future
        - Past
        - NoAppropriateDefault
    - Casualties
    - Conditions
        - Progr
        - Verified
        - Temperature
        - Dewpoint
        - Humidity
        - Rainfallfor
        - Windspeed
        - Accrainfall24h
        - Windgust
        - Datetime
        - Winddirection

5.2 Database

In order to provide its services the catalogue maintains the following tables in a database.

Table 5-2: Catalogue database tables

Table name	Description	Fields
Publications	Table that holds all shared/published data and the corresponding host addresses. This enables basically the ICN overlay over TCP/IP.	• Data name • Access rights • LU_ID
Subscriptions	Table that stores all subscriptions and the corresponding interested addresses.	• Data name • LU_ID
WG	In order to manage the WGs the catalogue stores the members for the time the groups exist.	• WG ID • Members • Performed updates • Timestamp of updates

5.3 API Specification

5.3.1 Publish

Table 5-3: Catalogue service Cat_Pub_01

Service ID	Cat_Pub_01
Description	Publish data. This method is called if a data owner wants to share data with other entities. The name of the data shall be send. The publications table in the database is updated and subscribers are informed.

Input	JSON with data name and User ID; an example follows:
	`{`
	`“LU ID” : “Bomberos de Catalunya”,`
	`“CD” : ”name as defined in section 5.1”,`
	`}`

Communication Protocol	HTTP POST `http://<<IP>>/catalogue/pub`
Response on success	HTTP code 200

Response on error	HTTP code 400
	JSON with error
	`{`
	`“error” : “error message as string”`
	`}`

Notes	

Table 5-4: Catalogue service Cat_Pub_02

Service ID	Cat_Pub_02
Description	Undo publication of data. This method is called if a data owner wants to stop sharing data with other entities. The name of the data or data sets shall be send. The publications table in the database is updated.

Input	JSON with data name and User ID
	{
	“LU ID” : “Bomberos de Catalunya”,
	“CD” : “name as in section 5.1”
	}

Communication Protocol	HTTP DELETE http://<<IP>>/catalogue/pub
Response on success	HTTP code 200

Response on error	HTTP code 400
	JSON with error
	{
	“error” : “error message as string”
	}

Notes	

Table 5-5: Catalogue service Cat_Pub_03

Service ID	Cat_Pub_03
Description	This method can be used to check published data and the according access rights. If all data of a LU needs to be checked, as name the LU_ID needs to be checked. Access rights are only sent as return value if the publisher is requesting it.

Input	JSON with data name and User ID
	{
	“LU ID” : “Bomberos de Catalunya”,
	“CD” : “name as in section 5.1”
	}

Communication Protocol	HTTP GET http://<<IP>>/catalogue/pub
Response on success	HTTP code 200 { “publications” : [{ “LU ID” : “user 1”,

	<pre>"CD" : "name as in section 5.1",
	"AccessRights": ["list of UI IDs"]
	},
	{
	"LU ID" : "user 1",
	"CD" : "name as in section 5.1"
	"AccessRights": ["list of UI IDs"]
	}
	]
	}</pre>

Response on error	HTTP code 400
	JSON with error
	<pre>{
	"error" : "error message as string"
	}</pre>

Notes	

5.3.2 **Subscribe**

Table 5-6: Catalogue service Cat_Sub_01

Service ID	Cat_Sub_01
Description	Subscribe to data. This method is called if a user wants to subscribe to content.

Input	JSON with data name and User ID
	<pre>{
	"LU ID" : "Bomberos de Catalunya"
	"CD" : "name as in section 5.1",
	}</pre>

Communication Protocol	HTTP POST <pre>http://<<IP>>/catalogue/sub</pre>

Response on success	HTTP code 200
	List with publisher where the access is granted including the address to contact and the CD to identify the data.
	<pre>{
	"publications" : [
	{
	"LU ID" : "user 1",
	"CD" : "name as in section 5.1"</pre>

	}, {
	“LU ID” : “user 2”,
	“CD” : “name as in section 5.1”
	}
	]
	}

Response on error	HTTP code 400
	JSON with error
	{
	“error” : “error message as string”
	}

Notes	The catalogue contacts at the same time publishers to share data if access rights are granted.

Table 5-7: Catalogue service Cat_Sub_02

Service ID	Cat_Sub_02
Description	Unsubscribe to data. This method is called if a user wants to unsubscribe content. No updates will be received anymore.

Input	JSON with data name and User ID
	{
	“LU ID” : “Bomberos de Catalunya”,
	“CD” : “name as in section 5.1”
	}

Communication Protocol	HTTP DELETE http://<<IP>>/catalogue/sub
Response on success	HTTP code 200

Response on error	HTTP code 400
	JSON with error
	{
	“error” : “error message as string”
	}

Notes	

5.3.3 **Query**

Table 5-8: Catalogue service Cat_Que_01

Service ID	Cat_Que_01

Description	This method is used to query the network for data

Input	JSON with data name and User ID
	{
	“LU ID” : “Bomberos de Catalunya”,
	“CD” : “name as in section 5.1”
	}

Communication Protocol	HTTP POST http://<<IP>>/catalogue/query
Response on success	HTTP code 200

Response on error	HTTP code 400
	JSON with error
	{
	“error” : “error message as string”
	}

Notes	The catalogue contacts at the same time publishers to share data if access rights are granted.

5.3.4 **Map**

Table 5-9: Catalogue service Cat_Map_01

Service ID	Cat_Map_01
Description	This method is used to map situation report to PDF
Input	EDXL – SitRep
Communication Protocol	HTTP POST http://<<IP>>/catalogue/map/topdf
Response on success	HTTP code 200 PDF file

Response on error	HTTP code 400
	JSON with error
	{
	“error” : “error message as string”
	}

Notes	

5.3.5 **Workgroup**

Table 5-10: Catalogue service Cat_WG_01

Service ID	Cat_WG_01

Description	This method is used to create a workgroup.

Input	References to scenario as JSON Object
	{
	“LU ID” : “Bomberos de Catalunya”,
	“scenario” : “name as in section 5.1”
	}

Communication Protocol	HTTP POST http://<<IP>>/catalogue/wg

Response on success	HTTP code 200
	JSON object with a generated WG ID
	{
	“WG” : ”ABCD1”
	}

Response on error	HTTP code 400
	JSON with error
	{
	“error” : “error message as string”
	}

Notes	

Table 5-11: Catalogue service Cat_WG_02

Service ID	Cat_WG_02
Description	This method add entities to a workgroup

Input	References to WG group name and user to be added to the WG as JSON Object
	{
	“WG” : “ABCD1”,
	“users” : [
	{
	“LU ID” : “user 1”
	},
	{
	“LU ID” : “user 2”
	}
	]
	}

Communication Protocol	HTTP PATCH

	`http://<<IP>>/catalogue/wg`
Response on success	HTTP code 200

Response on error	HTTP code 400
	JSON with error
	`{`
	`“error” : “error message as string”`
	`}`

Notes	Only users known to the system can be added. The invitation is forwarded to the invited entities

Table 5-12: Catalogue service Cat_WG_03

Service ID	Cat_WG_03
Description	This method forwards a modification of the scenario object to the other members of the WG

Input	References to WG and the modified variables of the scenario as JSON Object
	`{`
	`“WG” : “ABCD1”,`
	`“Scenario” : [`
	`{`
	`“variable 1” : “value 1”`
	`},`
	`{`
	`“variable 2” : “value 2”`
	`}`
	`]`
	`}`

Communication Protocol	HTTP PATCH `http://<<IP>>/catalogue/wg`
Response on success	HTTP code 200

Response on error	HTTP code 400
	JSON with error
	`{`
	`“error” : “error message as string”`
	`}`

Notes	The catalogue forwards the request to the other entities of the WG.

Table 5-13: Catalogue service Cat_WG_04

Service ID	Cat_WG_04
Description	This method closes a WG and informs the members about the entities to a workgroup

Input	References to scenario as JSON Object
	Either only the WG is send, in this case the WG is closed
	`{`
	`“WG” : “ABCD1”,`
	`}`
	Or user ID(s) are send. In this case the users with the ID are removed.
	`{`
	`“WG” : “ABCD1”,`
	`“user” : [`
	`{`
	`“UserId” : “user 1”`
	`},`
	`{`
	`“UserId” : “user 2”`
	`}`
	`]`
	`}`

Communication Protocol	HTTP DELETE `http://<<IP>>/catalogue/wg`
Response on success	HTTP code 200

Response on error	HTTP code 400
	JSON with error
	`{`
	`“error” : “error message as string”`
	`}`

Notes	The catalogue forwards the request to the other entities of the WG. They keep their local copy of the scenario

6 Conclusion

In this document, the first specification of the catalogue module for data sharing was presented. The catalogue is the connecting unit enabling a federated architecture of multiple local units (LUs). The catalogue is based on a content orient approach and does offer services for data publication, subscription and query. Furthermore, it offers options to map data to standardized formats and a working group feature for cooperative management of scenario files.

The technical requirements for this module were described and the module was shown on the overall context of the HEIMDALL system architecture. Finally the API of the catalogue based on RESTful web services was shown and specified. An implementation report and update of the specification is given in deliverable D4.14 due at M38. This presented specification will be considered for HEIMDALL system release C and will be evaluated at demo C.

7 References

[1] Monika Friedemann et al., HEIMDALL Deliverable 6.7: “Situation Assessment, Impact Summary Generation and sCOP/SITREP Specification and Implementation Report – Draft“, 10.2018

[2] Diana Mathew et al., HEIMDALL Deliverable 4.6: “Communications to Remote Areas – Design and Specifications – Draft “, 2019

[3] Benjamin Barth et al., HEIMDALL Deliverable 2.7: “HEIMDALL Requirements Report – Issue 2”, 03.2019

[4] irtf-icnrg-disaster-03, Jan Seedorf et al., “Research Directions for Using ICN in Disaster Scenarios”, Work in Progress, Internet Engineering Task Force, Feb. 2018

[5] Chen et al., “COPSS: An Efficient Content Oriented Publish/Subscribe System”, Seventh ACM/IEEE Symposium on Architectures for Networking and Communications Systems, 2011

[6] Nikos Fotiou, Giannis F. Marias, George C. Polyzos, “Access Control Enforcement Delegation for Information-Centric Networking Architectures”, Aug. 2017

[7] M. Ion, J. Zhang, M. Schuchard, E. M. Schooler, “Toward content centric privacy in ICN: Attribute-based encryption and routing,” Aug. 2013