

# **Appendix Q to Tender Specifications EMSA/OP/15/2016 “Development of New European Marine Casualty Information Platform”**

## **Overview of the CARD Services**

# 1 Introduction

The Central Access Rights Database (CARD) is the repository of the policies that govern the access to EMSA Maritime information.

Maritime Information is composed of “resources”, e.g. the AIS position reports sent by a ship, the incident report provided by a Port Authority, a radar image of the sea surface, etc.

The typical user of a Maritime Application has limited access to resources. Restrictions on access rights (“policies”) are related to the characteristics of the resource to be protected, like for instance the data provider or the geographical area in the case of geo-spatial data.

Some examples of access rights policies are:

- a user with profile “Frontex” has access to Sat-AIS data on the Mediterranean Sea only
- a user with profile “PSC” has access to the Port Call messages of ships bound to the port associated to his/her Organization
- a user with profile “Pollution Control” has access only to Incident Reports of type POLREP

## 1.1 Data Access Policy

Data Access Policies are stored in the CARD and made available to Maritime Applications for enforcement. Policies are based on the user’s Profiles and may be dependent on the attributes of the user: Country, Organization, and Operations.

CARD provides to Maritime Applications a request/response service (system to system interface) to grant or deny access to a resource according to the following schema:

Condition Type	Description	Example
<b>No Conditions</b>	User has unrestricted access to the resource. This is the default approach.	User has unlimited access to METOCEAN data
<b>Source</b>	The access is restricted to resources provided by: <ul style="list-style-type: none"> <li>- Selected group of countries, or</li> <li>- The user’s country.</li> </ul>	Data source is a Country that belongs to the EU EFTA group of countries
<b>Location</b>	The access is restricted to resources associated to a list of Locations.	Access limited to Port Calls of ships bound to the user’s Country
<b>Area</b>	The access is restricted to resources which coordinates are within selected geographical areas.	Access limited to ship positions in the Baltic Sea
<b>Operation</b>	The access is restricted to resources related to the selected operation(s).	Access limited to the SAFEMED resources
<b>Data Type</b>	The access is restricted to resources of: <ul style="list-style-type: none"> <li>- Specific types,</li> <li>- Types depending on user’s organization, or</li> <li>- Types depending on the user’s country.</li> </ul>	Access limited to Incident Reports of type “POLREP”.

## 1.2 Target

CARD uses the concept of “Target” to refer to a resource to be protected. A Target is associated to a specific action, e.g. “view”, “edit”, “stop”, etc. Examples of targets are: “*View EO Image*”, “*Provide Feedback on EO Oil Spill Detection*”, etc. (the action is indicated in *italics*).

A Target may refer to two categories of resources.

- **Simple Resource:** a basic type of information or function (page, button) that the user can fully access or not at all; a Simple Resource does not have any specific attribute: the Target name is sufficient to identify all the simple resources that it refers to.

For example, the Target “View METOCEAN data” refers to all available meteorological resources (information layers). The “METOCEAN data” is a Simple Resource and the user can either view all the METOCEAN information layers or none at all.

- **Complex Resource:** a complex type of information or function that the user can access only partially; a Complex Resource has one or more attributes that are checked by CARD in order to define the access level for a given user.

For example, the Target “View VMS data” refers to the positions of fishing vessels; this resource has “source” and “coordinates” attributes that are checked by CARD. It is a complex resource and a user may access it only for some source countries or in some specific geographical areas.

A Complex Resource may have the following attributes.

Attribute	Type	Description	Example
<b>Source</b> (optional)	<Country_Code>	Country Code that identifies the source of the resource (from CCD)	IT
<b>Location</b> (optional)	<Location_Code>	Code of the location associated to the resource (from CLD), generally defined with a UN/LOCODE.	FRLEH
<b>Coordinates.Lat</b> (optional)	String “^[+-][0-9]{2}(\.[0-9]{1,6})?\$”	The Latitude of the coordinates of the resource.	-12.123456
<b>Coordinates.Lon</b> (optional)	String “^[+-][0-9]{3}(\.[0-9]{1,6})?\$”	The Longitude of the coordinates of the resource.	+123.123456
<b>Operation</b> (optional)	<Operation_Code>	The code of the Operation to which the resource is associated to (from CARD).	“Safemed”
<b>Data Type</b> (optional)	<Data_Type_Code>	The code of the Data Type of this resource (from CARD).	PROVIDE_INCIDENT.WASTE

CARD does not store the list of resources and their attributes. The Authorization Service of CARD however responds to requests from a Maritime Application and evaluates the resource attributes provided as request parameters. CARD therefore needs to compare the values of the relevant attributes with the Data Access Policies applicable to the user account before granting or denying access to a resource.

### 1.3 Authorization Service

CARD provides a service that, for a given user, grants or denies access to a resource, identified by a Target. This is in fact an implementation of the policies stored in CARD itself, in a way that the Maritime Application fully relies on CARD for policy enforcement and for taking a decision on granting, or not, access to its resources.

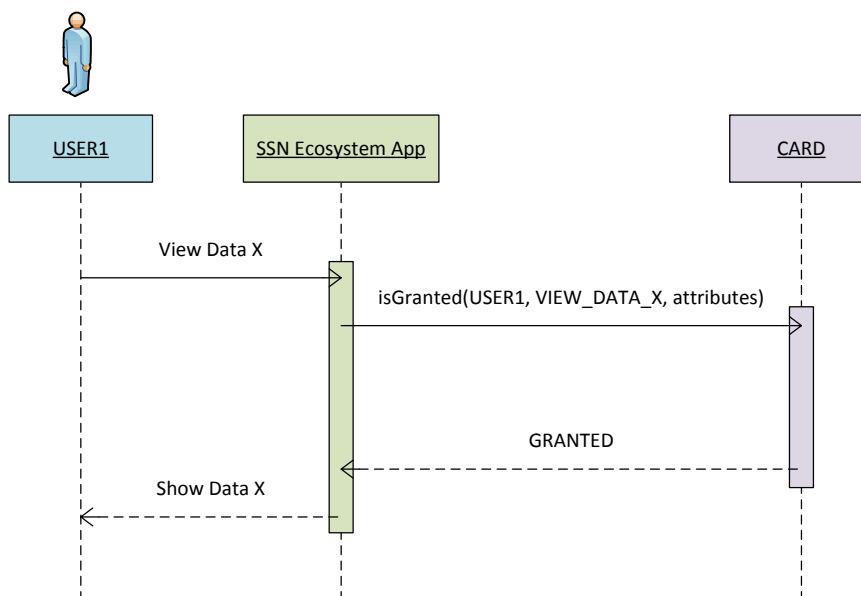


Figure 1 - Sample web-service based authorization process

CARD provides the Authorization Service by means of the following mechanism:

- Web Service (REST)

The Authorization Service includes the following requests (or equivalent):

- `isGranted(User, Target)`

CARD responds with

- GRANTED, if the user is granted access to the *simple resource* identified by the Target
- DENIED, if the user is denied access to the *simple resource* identified by the Target
- ERROR, if the User or the Target do not exist or if the Target refers to a complex resource; sample error message: "Target refers to a complex resource, resource attributes are required to evaluate the data access policy".

- `isGranted(User, Target, resourceAttributes)`

CARD responds with

- GRANTED, if the user is granted access to the resource identified by the Target and having the given attributes; resourceAttributes is a list of (key, value) pairs that describes the specific resource that is being accessed.
- DENIED, if the user is denied access.
- ERROR, if the user or the Target do not exist or the request parameters are not valid.

Example:

```
isGranted("USER123",
        "PROVIDE_INCIDENT",
        "{source=FR, location=FRLEH, data-type=PROVIDE_INCIDENT.BANNED}")
```

CARD retrieves the user details and evaluates all the data access policies associated to the given Target.

If the data access policy has any condition, CARD evaluates the policy by setting, if applicable, the dynamic criteria (USER\_COUNTRY, USER\_ORGANIZATION, USER\_OPERATION) and retrieving the corresponding information from the Central Databases and the local CARD database.

## 2 CARD Interface – Draft Technical Specifications

This chapter contains the technical specifications of the REST services exposed by CARD.

**Important Note:** this is a DRAFT technical specification provided for Tender evaluation purposes only; the final interface implementation may differ from the one described in this document.

**Note:** All described services, if not specified, produce a response in JSON format.

**Note:** Requests listed below, if not with specific annotation, are of type **HTTP GET**.

**Note:** ALL dates in input or output for the following services are in **YYYY-MM-dd'T'hh:mm:ss'Z'** format (UTC time).

### 2.1 Standard JSON service response

When not specified, the service provides a standard JSON response.

The structure is the following:

Argument	Type	Occurs	Description
status	String	1..1	Indicates the status of the request. It can be: <ul style="list-style-type: none"> <li>• success</li> <li>• error</li> </ul>
result	Object	0..1	An optional service invocation result. This is a nested JSON object. Object is described by each service specifications if it uses this kind of response.
message	String	0..1	An optional additional message of the server

2.2 Authorization services

In this paragraph are described all services concerning authorization concepts.

CARD Module

card-authorization-service

Methods summary

Name	Description
getAuthorization	Request the authorization for an user to perform an action on a particular resource

### 2.2.1 Standard Authorization service response

All authorization services (described in this section) will return a response in JSON format.  
The response is a JSON Object that contains the following elements

#### Elements

Name	Type	Occurs	Description
allowed	Boolean	1..1	<i>true</i> if the user is allowed to perform the specified request, <i>false</i> otherwise
obligations	JSON Array of JSON Objects	0..1	List of JSON Objects representing the obligation that the caller has to parse to proceed with the authorization process, this array is present only if the “allowed” element has “true” value

Each JSON Object contained into the “obligations” array is composed by the following elements.

Name	Type	Occurs	Description
name	String	1..1	Obligation identifier
values	JSON Array of JSON Objects	1..1	List of JSON Objects (key-value pairs) representing the obligation content

Each JSON Object contained into the “values” array is composed by the following elements

Component	Type	Occurs	Description
key	String	1..1	Obligation key
value	String	1..1	Obligation content for current key

Here follows some examples of an authorization response

## Examples

Allowed with no obligations:

```
{
  "allowed": "true"
}
```

Not allowed:

```
{
  "allowed": "false"
}
```

Allowed with obligation:

```
{
  "allowed" : true,
  "obligations" : [
    {
      "name" : "Obligation1",
      "values" : [
        {
          "oblVal1Key2" : "oblVal1Key2Val",
          "oblVal1Key1" : "oblVal1Key1Val"
        },
        {
          "oblVal2Key1" : "oblVal2Key1Val",
          "oblVal2Key2" : "oblVal2Key2Val"
        }
      ]
    }
  ]
}
```



## 2.2.2 getAuthorization service

### Description

Returns the authorization for the specified user to perform an action on a resource. This service can also respond to an authorization request in attribute based mode.

### Action

```
http://{host:port}/card-authorization-service/services/
  getAuthorization.do?user=<string>&service=<string>&resource=<string>&action=<string>
  &attributes=<json_string>
```

### Input

The inputs of this method are the arguments defined by the following table.

Argument	Type	Occurs	Description
user	String	1..1	Name of the user requesting the authorization
service	String	1..1	Service code of the service that the user is using
resource	String	1..1	Name of the resource that the user wants to use
action	String	1..1	Name of the action that the user wants to perform on the specified resource
attributes	JSON Object	0..1	Optional attributes that the user provides for the current invocation, this is a list of key-value pairs in JSON format (see example)

### Output (JSON)

The response of this service is the standard authorization response described in section 2.2.1: *Standard Authorization service response*.

### Example

An invocation example is the following (**non attribute based**):

```
http://tcardwls01:7020/card-authorization-service/services/getAuthorization.do?
  user=BILL
  &service=IMDATE
  &resource=VESSELS_SERVICE
  &action=INVOKE
```

Or (**attribute based**):

```
http://tcardwls01:7020/card-authorization-service/services/getAuthorization.do?
  user=BILL
  &service=IMDATE
  &resource=SAR_SURPIC
  &action=EDIT
  &attributes={"sarsurpicFlag":"IT","MemberState":"IT","sarsurpicOwner":"BILL"}
```

--- End of the Document ---

## ABOUT THE EUROPEAN MARITIME SAFETY AGENCY

The European Maritime Safety Agency is one of the European Union's decentralised agencies. Based in Lisbon, the Agency provides technical assistance and support to the European Commission and Member States in the development and implementation of EU legislation on maritime safety, pollution by ships and maritime security. It has also been given operational tasks in the field of oil pollution response, vessel monitoring and in long-range identification and tracking of vessels.

### **European Maritime Safety Agency**

Praça Europa 4  
1249-206 Lisbon, Portugal  
Tel +351 211209 200  
Fax +351 211209 210  
[emsa.europa.eu](http://emsa.europa.eu)