

Appendix M

CMC (CARD) – Implementation approach - Overview of the CARD Services

V. 1.0 – 2015-07-02

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 (“limitations”) 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 limitations 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 Limitations

Access rights limitations are stored in the CARD and made available to Maritime Applications for enforcement. Limitations 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 receive the description of the limitations applied to a resource according to the following schema:

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

	- Types depending on the user's country.	
--	--	--

1.2 Roles

CARD uses the concept of “Role” to refer to one or more resources to be protected. Examples of EOS Roles are: “View EO Image”, “View EO Oil Spill Detection”, etc.

A Role 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 Role is sufficient to identify all the simple resources that it refers to.

For example, the Role “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 with different levels of limitations; a Complex Resource has one or more attributes that are checked by CARD in order to define the level of access limitation for a given user.

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

Data Type (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 Policy Distribution Service

CARD provides a service that distributes on request the data access policies definitions and reference data to Maritime Applications.

CARD distributes the policies by means of a Web Service. During the development of CARD, other policy distribution mechanisms may be implemented based on existing industry standards.

The distribution service includes the following requests (or equivalent):

Request
1. <code>getListOfServices()</code> : CARD provides the full list of Services including all attributes
2. <code>getListOfRoles()</code> : CARD provides the full list of Roles including all attributes
3. <code>getListOfRoles(Service)</code> : CARD provides the full list of Roles including all attributes that are associated to the given Service
4. <code>getListOfRoles(Profile)</code> : CARD provides the list of Roles associated to the given Profile, regardless of the limitations
5. <code>getListOfDataTypes()</code> : CARD provides the full list of Data Types including the corresponding Role and all other attributes
6. <code>getListOfDataTypes(Role)</code> : CARD provides the full list of Data Types for the given Role including all attributes
7. <code>getDataTypes(Country or Organization)</code> : CARD provides the list of Data Types associated to the given Country or Organization
8. <code>getListOfOperations()</code> : CARD provides the full list of Operations
9. <code>getListOfOperations(Role)</code> : CARD provides the list of Operations for the

given Role
10. getListOfProfiles(): CARD provides the full list of Profiles
11. getListOfPolicies(): CARD provides the full list of Policies, one Policy for each Profile, including all granted Roles and any Limitation
12. getPolicy(Profile): CARD provides the Policy for the given Profile, including all granted Roles and any Limitation
13. getLimitations(Profile, Role): CARD provides the Limitations for the given role and Profile
14. getListOfPolicies(User): CARD provides the full list of Policies, one Policy for each Profile, including all granted Roles and any Limitation evaluated for the given user
15. getPolicy(Profile, User): CARD provides the Policy for the given Profile, including all granted Roles and any Limitation evaluated for the given User
16. getLimitations(Profile, Role, User): CARD provides the Limitations for the given Profile, Role and evaluated for the given User

1.4 Authorization Service

CARD provides a service that, for a given user, grants or denies access to a resource, identified by a Role. 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.

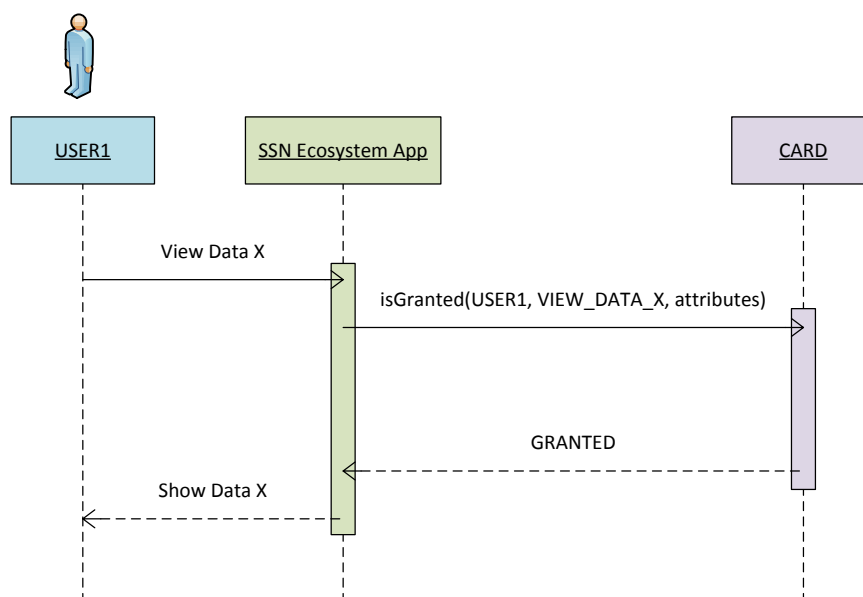


Figure 1 - Sample web-service based authorization process

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

- Web Service
- Java Authentication and Authorization Service (for Roles referring to Simple Resources only).

During the development of CARD, other authorization mechanisms may be implemented based on existing industry standards.

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

- `isGranted(User, Role)`

CARD responds with

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

- `isGranted(User, Role, resourceAttributes)`

CARD responds with

- GRANTED, if the user is granted access to the resource identified by the Role and having the given attributes; resourceAttributes is a list of (key, value) pairs that describes the specific resource that is being accessed according to **Error! Reference source not found..**
- DENIED, if the user is denied access.
- ERROR, if the user or the role 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 Profile(s) and Operation(s) and evaluates all the data access policies associated to the given Role.

If the data access policy has any limitation, CARD evaluates the limitation 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.

The details of the CARD system to system services (protocol, format) will be available by the end of 2015.

--- 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