BLUEMASSMED PILOT PROJECT

LESSONS LEARNED TOWARDS A TECHNOLOGICAL SOLUTION FOR THE IMPLEMENTATION OF C.I.S.E.

04/07/2012

Table of Contents

1 Introduction

The *BlueMassMed* experimental demo has proven the effective exchange of basic real data and simulated sensitive data among 16 out of 39 partners, belonging to 6 different nations (Italy, France, Spain, Portugal, Malta and Greece).

The direct and deep involvement of Maritime policies stakeholders in the experimental demo has allowed to verify under the best suited technical-operational conditions the potential benefits of integrating the EU surveillance networks, as well as to identify the best candidate technological solution for the C.I.S.E. implementation.

The experimentation has ultimately demonstrated a technical architecture capable to integrate National Surveillance Systems into an "*European Maritime Surveillance Network – EMSN*" complying with the following key operational needs:

- ✓ allowing Users to share their own maritime information according to a "*Responsibility-To-Share*" policy
- ✓ allowing Users to exchange added value information about Ships, not only Ship Positions & Reports
- ✓ supporting the exploitation of Military and Civilian Cooperation for Maritime Awareness Improvement
- ✓ optimizing the exploitation of Large Scale Monitoring Assets (e.g. Satellites and Aero- naval patrols)

At National level, each EU MS has evidenced data policies restrictions on sensitive and classified information, that have not hindered the demonstration but will need to be taken into account in the future operational validation. Also Sectorial Communities, who are subject to EU directives that generally imply data centralization by EU agencies and data distribution regulated by need-to-know information sharing policies, have evidenced restrictions on data distribution policies outside their domains, that will need to be taken into account.

Outside the national and the EU sectorial communities, National authorities are generally willing to share their own maritime information, subject to the following conditions:

- ✓ their own roles and responsibilities are maintained wrt the subscription to third parties data
- ✓ no further responsibility is assumed due to the data sharing wrt their data subscribers
- ✓ selective data access and data distribution can be granted to different categories of Users, according to national regulations and sectorial agreements
- ✓ a "responsibility-to-share" policy is enforced so that the overall exchange of information is inherently balanced

On the systems side, interoperability constraints have been faced in the BMM experimental demonstration, because **it is not possible to design from scratch a new, top-down, interoperable network connecting all the European Maritime Domain Stakeholders.**

Integration of National Maritime Surveillance Systems is a long running on-going process:

- ✓ at MS level (e.g. IT, FR) for Maritime Situational Awareness purposes
- ✓ at EU level, in support of the implementation of EU sectorial policies (e.g. EDA, EFCA, EMSA, FRONTEX, etc.)

Both integration dimensions rely generally on a central controlling entity which regulates the data exchange and distribution among participating systems and on the definition of standardized interfaces and data models in support of systems' interoperability.

Very differently from a sectorial context, in the C.I.S.E. the interoperability cannot be guaranteed by the adherence of all the participant entities to a common technical baseline or data model imposed by a regulatory framework through a Central Controlling Entity. In operational terms, we could say that the "C.I.S.E." shall be interoperable for "*Newcomers*" while the sectorial networks are interoperable for the Competent Authorities empowered by the relevant sectorial policy.

The big step forward required from the C.I.S.E. implementation is to allow all Maritime Data/Systems owner to contribute on a volunteer base to the enrichment of a cross-sector cross-border maritime picture:

- ✓ without delivering their own information to any central repository or controlling entity but only directly to the subscribers
- ✓ maintaining the traceability of the information provided
- ✓ maintaining full independence in the design, exploitation and evolution of their own maritime surveillance systems and networks

In technical terms, the C.I.S.E. will and shall be an environment of "*loosely interconnected systems*", where the capability to interoperate shall not hinder in any way the core mission, the specific design and the growth potential of the single cooperating systems.

- **The BMM project has demonstrated an open, flexible, secure and decentralized architecture capable to integrate National Surveillance Systems owned by the participating Administrations and satisfying the identified C.I.S.E. implementation needs**

2 The BMM Technological Solution for C.I.S.E.

The BMM solution for C.I.S.E. is based on the basic concept that systems owned and operated by National Competent Authorities shall be adapted to exchange information through a completely decentralized approach, without implying data transfer to any central controlling entity or central data base, but rather an end-to-end transparent, traceable and secure bilateral information exchange mechanism, implemented through a harmonized frontend interface that implies no major interference or impact with the owner agency duties execution and own systems' evolution policies implementation.

In the BMM vision, the CISE will be implemented connecting all the surveillance systems owned/operated by participating authorities (so called Primary Nodes) over the TCP/IP public network, in https over SSL with certificates provided by the respective National Security Authorities, in order to ensure a secure, transparent and guaranteed end-to-end transport layer among the network nodes. A full SOA-based web-service system-to-system interface (the BMM front-end) is implemented at each Primary Node level, for information and data exchange among all BMM Primary Nodes, protected with 2-way SSL certificates and WS-Security standard for encryption at WS level. Moreover, a light-client access user interface (BMM web-interface) is implemented at each Primary Node, in order to make available information exchange over the CISE also to Users not owning legacy maritime surveillance systems, or not willing to implement the BMM front-end on their systems (the so called Secondary Nodes).

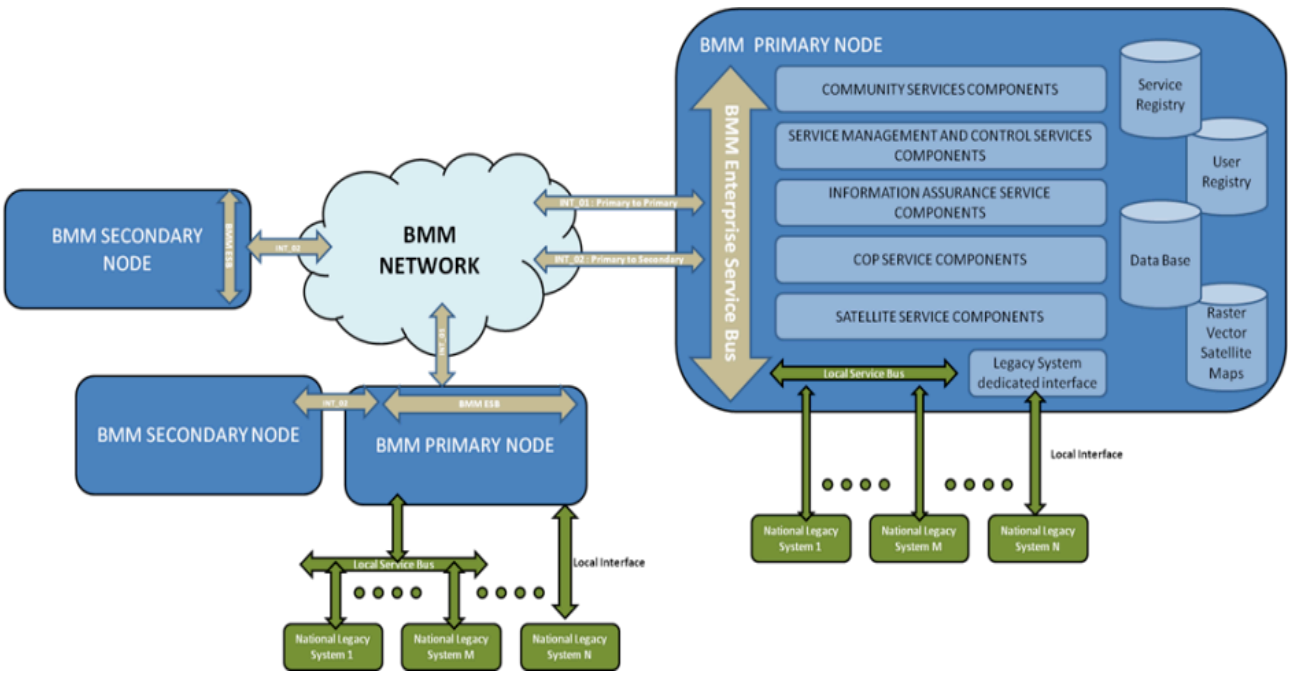


Fig. 1 – The BMM vision of CISE implementation

The basic enabling components of such frontend have been designed, developed and demonstrated in the BMM project in an operational context involving more than 20 Maritime Surveillance and Monitoring systems owned by 16 different authorities in 6 different Countries.

These components are depicted in Fig. 2 (from the lower to the higher level of connection):

1. a SOAP over https as platform independent protocol stack for exchanging structured information
2. a set of Harmonized Infrastructural Services ("Core Services") implementing User and Service Access federation (Uddi Registry) as well as the necessary information protection mechanisms (Directory Service, User Profiling) and basic cooperative tools (portal server, web server, map server, GIS server, chat server, etc.)
3. a set of added value services ("Common Services"), built on Web Services technology, implementing information exchange services according to the specific data sources and functional capabilities available in the respective back-ends, but adhering to a common set of minimal semantic rules and service specifications
4. an harmonized procedure ("SBCMP Procedure") to compile at each node a Shared Basic Common Maritime Picture and solve conflicts and ambiguities in areas where multiple reporting of the same ships occur.

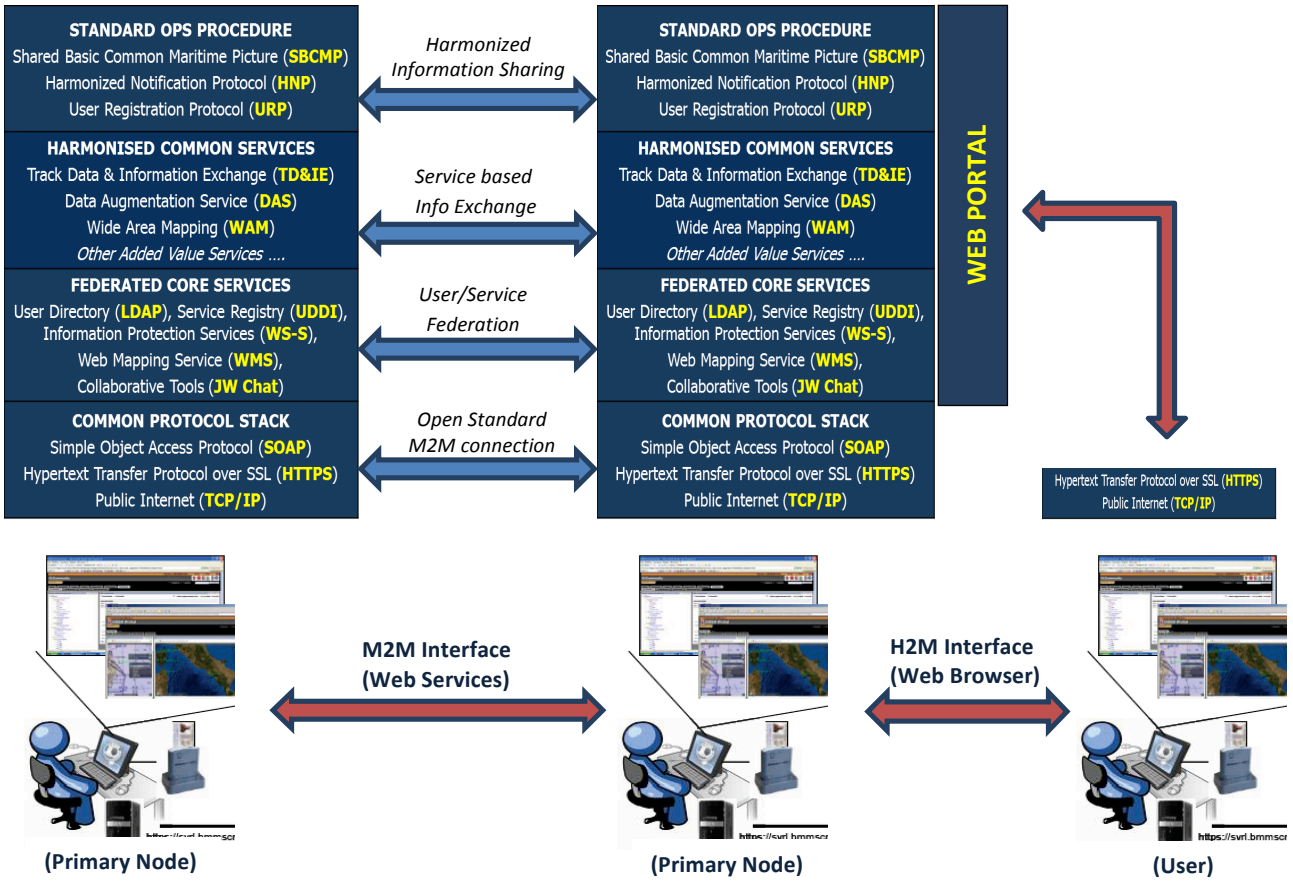


Fig. 2 – Proposed Network Protocol Architecture for CISE

As depicted in the above figure, the Legacy Surveillance Systems are connected on the CISE through the BMM frontend at four different levels. At the bottom level, a machine independent network connection is implemented over the Public Internet with https over 2-way SSL and the SOAP protocol.

On top of this basic connectivity, a so-called "core services" layer is implemented, which provides a group of harmonized services that allow the Legacy Surveillance Systems to share an open SOA-based infrastructure based on users and service federation mechanisms, as well as on WS-Security protocol for information protection, and on various collaborative tools complementing the information exchange capabilities with Users cooperation functionalities.

At the third level, the proper set of "common service" layer is implemented, which makes the Legacy systems connected to the network able to selectively exchange track information, notifications and other added value services residing in the respective back-ends, according to the established data distribution plan and security policies.

At the top level, standard operational procedures for maritime picture compilation, notifications and new users registration are implemented, making the Legacy systems connected to the network not only fully interoperable and able to exchange information in a controlled and selective way, but also able to follow harmonized rules for information exchange in order to collectively compile an understandable maritime picture and support an effective decision making mechanism across the network.

Finally, the results of the information exchange among the primary nodes, as well as Human Machine Interfaces to the core and common services implemented by the Primary Nodes is published at each Primary Node on a Web Portal, in order to allow a simpler interface (simple web browser over a 1-way SSL protocol https) to be implemented at Operational Nodes which require CISE interconnection without owning legacy systems to be adapted with the full BMM front-end interface.

The four basic components (layers) of the BMM front-end for the CISE are fully described in the "*BMM CCTP document"* and "*BMM System View document*", which follow the well-known NATO Architectural Framework methodology for the specifications of system-of-systems.

Moreover during the implementation of the project, the BMM Front-End has been designed and developed on 5 different legacy systems in Spain, France, Italy and Portugal, leading to 5 different "*Target Architectures Document*" all aligned to the *BMM System View Document*, as well as to 5 prototypes of the BMM Primary Nodes, which have been extensively validated and exploited during the experimentation phase by more than 20 Users.

While we redirect to the cited documents for the detailed specifications and validation of the implemented components, the main concept and added value of such components are outlined in the following sections, in order to emphasize the contribution of the BMM project to the CISE implementation strategy.

2.1 The BMM Protocol Stack & Technical Standards

The BMM protocol stack is composed by:

- ✓ Standard Web Services (WSDL, XSD) and potentially evolutions to WS-S
- ✓ Simple Object Access Protocol (SOAP)
- ✓ Hypertext Transfer Protocol over Secure Socket Layer (HTTP / HTTPS)
- ✓ TCP/IP

The technical standards, to which the protocol stack and the whole Front End architecture shall strictly adhere to avoid interoperability problems, are listed in the Table above.

Important lessons learned on the technical standards side have included:

- the promotion of standard solutions, based on open source or equivalent, has proven to be a key factor to achieve true interoperability among systems at cross-sectorial level
- the use of commercial platform solutions should be limited (due to restrictions introduced by non-standard extension and vendor optimization)
- a full SOA-paradigm based on standard Web Services technology (preferably built on Java platform) has been proven as the best solution to allow machine independent interoperability
- the use of proprietary standards solutions shall be avoided.

Primary Node Services	Standards / Interface	Standard (Applications)	Open Source Solution
Common Services : • Track data / information exchange • Regional Corrrelation • Wide Area Mapping • Data Augmentation	Web Services (XML, SOAP, WSDL)	Java	JDK 1.6
		JAX-WS	Glassfish Tomcat
		SQL	MySQL PostgreSQL
Web Portal	JSR 168 (1.0) JSR 286 (2.0) WSRP	Java	Liferay
Web GIS	WGS84 Mercator Projection AIS symbols Web Services (SOAP, WSDL)	PHP (Apache)	
Map Server	WMS 1.1.1 ADRG, ASRP, CADRG, USRP, CIB, SRG-IGM, GEOTIFF Rev.6.0, TIF + tfw/tab, JPG + jpw, Tiff + tab	PHP (Apache)	MapServer
	WFS 1.0.0 Shape File	PHP (Apache)	MapServer
Identity & Access Management	WS-Security (username/password) SSL (https) SAML / XACML		
Directory Service	LDAP v3		Open LDAP
Service Registry Management	UDDI v3		jUDDI
Regional correlation		Java SQL	JDK 1.6

Wide Area Rapid Mapping (content)	WMS 1.1.1 GIF, JPG, PNG ADRG, ASRP, CADRG, USRP, CIB, SRG-IGM, GEOTIFF Rev.6.0, TIF + tfw/tab, JPG + jpw, Tiff + tab

Table 1 – BMM Front End Technical Standards

2.2 The BMM Federated User & Service Management

The basic feature of the BMM Core Service layer, is the implementation of standard mechanisms for federated user and service management over the network.

The basic concept in BMM (and so it should be also in CISE) is that an User can be either:

- a *legacy system*, connected to the other legacy systems over the network according to the scheme depicted in Fig. 2 (primary-to-primary node interface), i.e. through a M2M SOA interface
- an *operator*, connected to a legacy system over the network through a H2M web browser interface

The User Federation mechanism ensures that both kinds of Users can access each point of the network with same credentials and access privileges, **regardless the Node that initially gave the User the credentials**.

This is achieved by implementing a standard LDAP user registry service, which synchronizes the User Credentials directory across the Nodes in the network, based on a "replication" or "referral" mechanism. When a User is authenticated on another Node he gets access credentials to some or all the services and functionalities available on that Node. If the User is a Primary Node (M2M), the services are published in the UDDI service registry of the Host Node, otherwise the services and functionalities are available on the pages or portlets of the Web Portal of the Host Node.

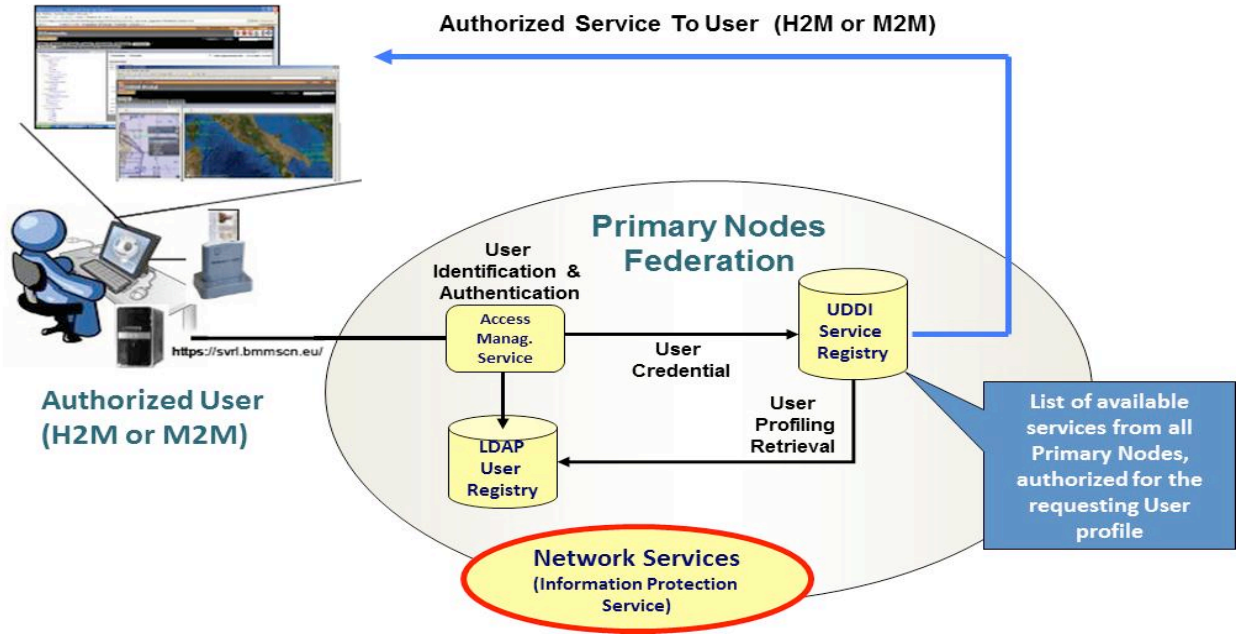


Fig. 3 – Concept of the User and Service Federation

In the same way, the UDDI service registry is federated by a replication mechanism across the Network, so that available services at all Primary Nodes are listed in the UDDI of each Node and are always presented to the Users, whichever the point of access to the Network is.

In the BMM experimentation, the Users have been subdivided in Super Users (i.e. Users having sufficient credentials on a Primary Node to configure service subscriptions and modify user profiles) and Normal Users (i.e. Users who don't).

In a C.I.S.E. perspective, the same mechanism could be extended to deploy whatever access policies established at National, Sectorial or EU level.

2.3 The BMM Harmonized Common Services

The Common Services are the set of standard platform independent Web Services that implement the basic Machine-to-Machine interoperable interface among Primary Nodes connected to the BMM Network.

The Common Services are the innovative solution to perform information exchange among cross sectorial systems w.r.t. to plain data exchange because each data transfer operation is encapsulated into a specific service request/response or publish/subscribe transaction that can be tailored:

- ✓ *On the specific situation in the moment of the request*
- ✓ *On the specific user performing the request*

Thus allowing ***in each operational situation*** the selection of the best **adding value** data to be exchanged and the segregation of **sensitive data** not allowed to be exchanged

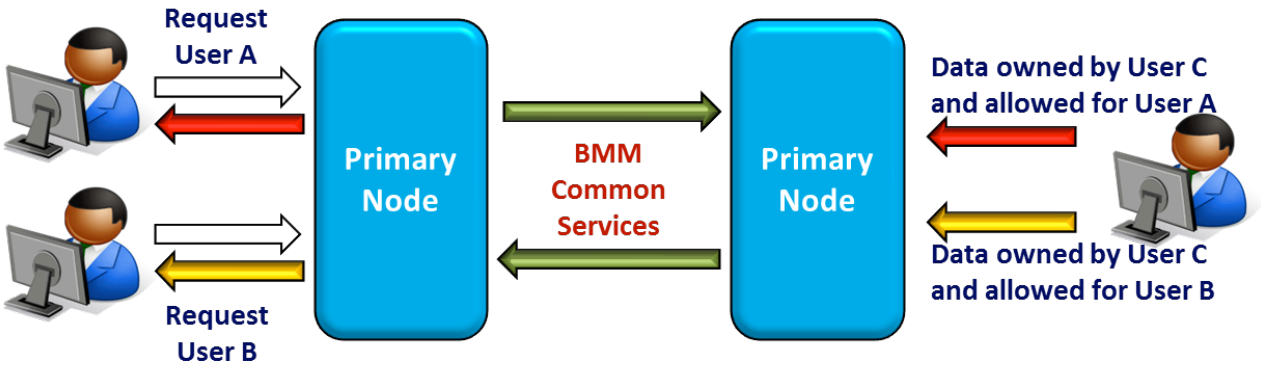


Fig. 4 – Principle of the BMM Common Services

The Synchronous Operations

Synchronous Operations are based on standard *Web Services* and the Request / Reply paradigm

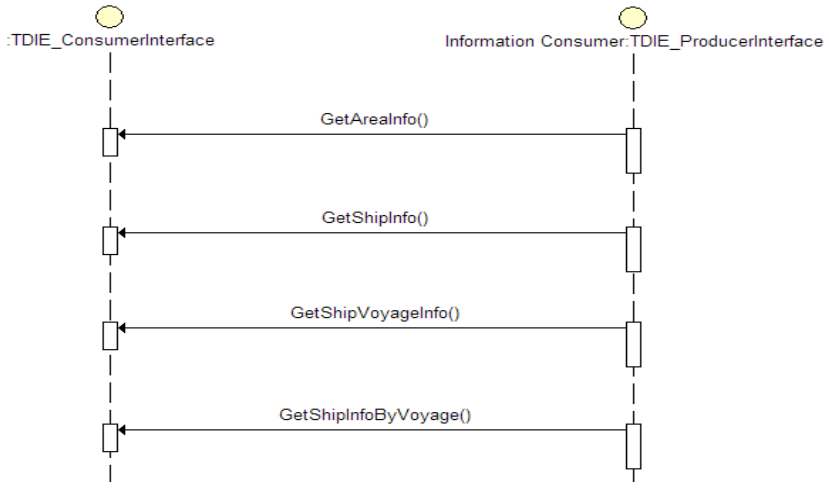


Fig. 5 – Common Services – Synchronous Operations

TRACK DATA & INFORMATION EXCHANGE CS

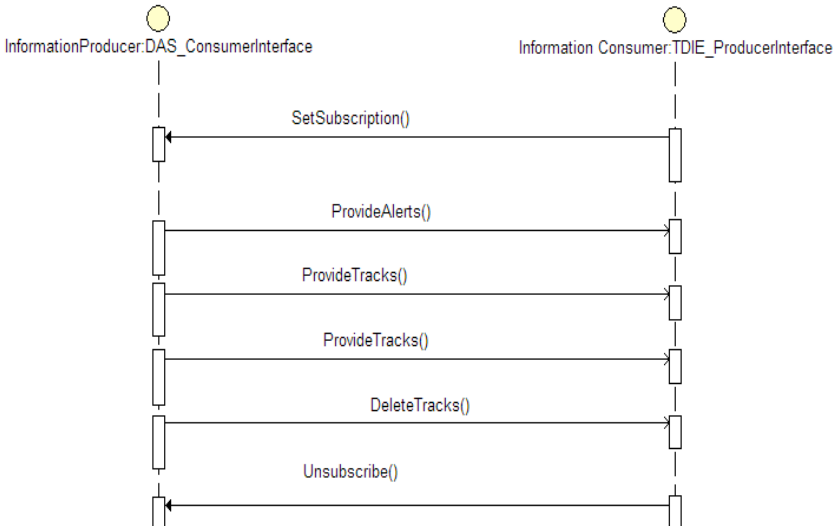
- ✓ GetAreaInfo(): *Request Tracks Data in a given Area of Interest and in a given Time window*
- ✓ GetShipInfo(): *Request Tracks Data on a specific Ship known by an Id parameter*
- ✓ GetShipVoyageInfo(): *Request Track history on a specific ship known by an Id parameter*

The Asynchronous Operations

Include Operations for the exchange of notification and alerts on tracks or on an Area of Interest

DATA AUGMENTATION CS

- ✓ ProvideTracks(): *Transmit track data to subscribing nodes, as soon as they are updated*
- ✓ ProvideAlerts(): *transmit alerts to subscribing nodes, as soon as they are generated*
- ✓ ProvideTargetInfo(): *Transmit additional information about tracks to subscribing nodes, as soon as they are updated*
- ✓ ProvideMetocData(), ProvideSafetyData(), ProvideMPRData(): *transmit to subscribing nodes Meteo Data, Safety Data and Maritime Pollution Data*



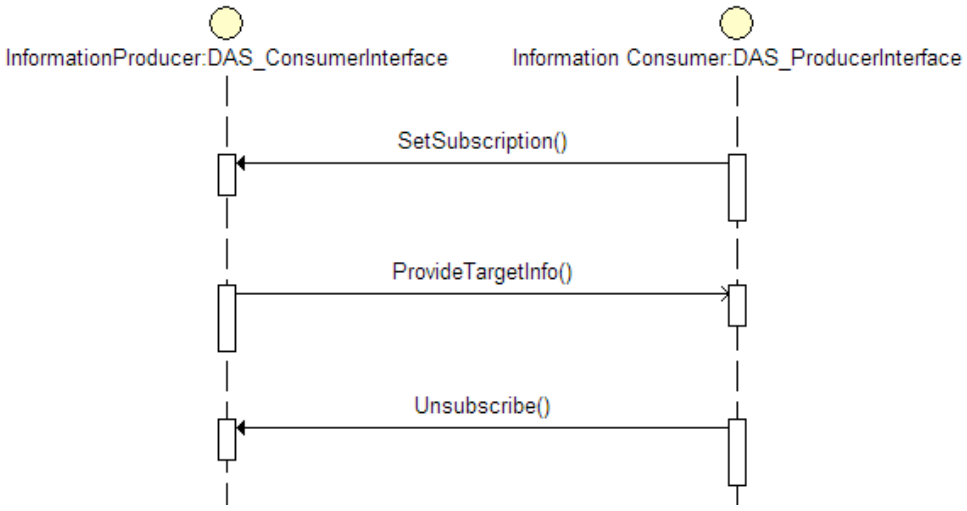


Fig. 6 – Common Services – Asynchronous Operations

Beyond the basic set of harmonized common services, required to implement the interoperable machine independent PN to PN interface, the Service Oriented Architecture allows every Primary Node to publish **other added value services** based on the capabilities and resources available in the respective back-ends.

The following categories of additional Common Services have been designed in the frame of the BMM proejct:

- ✓ WIDE AREA MAPPING SERVICE
- ✓ INTELLIGENCE INFORMATION EXCHANGE SERVICE
- ✓ REGIONAL TRACK CORRELATION SERVICE

For details about the definition of such services please refer to the BMM CCTP document and to the BMM System View document.

The Common Services Harmonization

Thanks to the adoption of the standard WS SOA paradigm, the implementation of the Common Services at each PN level can be autonomous and independent. The detailed interface is in fact discovered by the requesting node directly at run-time. However, in order to ensure the maximum interoperability, a harmonization mechanism has been foreseen, limited to the following:

- Minimum set of Semantic Rules

The data types, classes and structures be used within web-services specifications, xml schemas in order to ensure interoperability within the network:

- ✓ Positional Data
- ✓ Basic Current Voyage Data
- ✓ Basic ID Data
- ✓ Historical Data
- ✓ Other Ship Related Data

- ✓ Time Data
- ✓ Area Data
- ✓ Image Data

- WSDL specification
  - ✓ Operations Mandatory Input Parameters
  - ✓ Operations Mandatory Output Parameters

The Service-Based Data Segregation Approach

In the BMM solution, data segregation is **performed at Service Level**. Any specific service operation is allowed or not to any specific User based on the level of restrictions/limitations associated to the user credentials.

A specific Data Access and Distribution Plan, adopted by operational and legal considerations, will be exploited to define the service authorization logic to be implemented at each Node level.

In the figure below a basic representation of how this principle works is presented. In the first case, the DDP requires that some Users cannot access to *BasicIdData* of exchanges ship tracks, while all users can access *PositionalData*.

Consequently, different sub-operations are implemented in the GetShipInfo operation providing access to different subset of data, and the Data segregation is performed at service level by granting different authorization level to the two operations depending on User credentials.

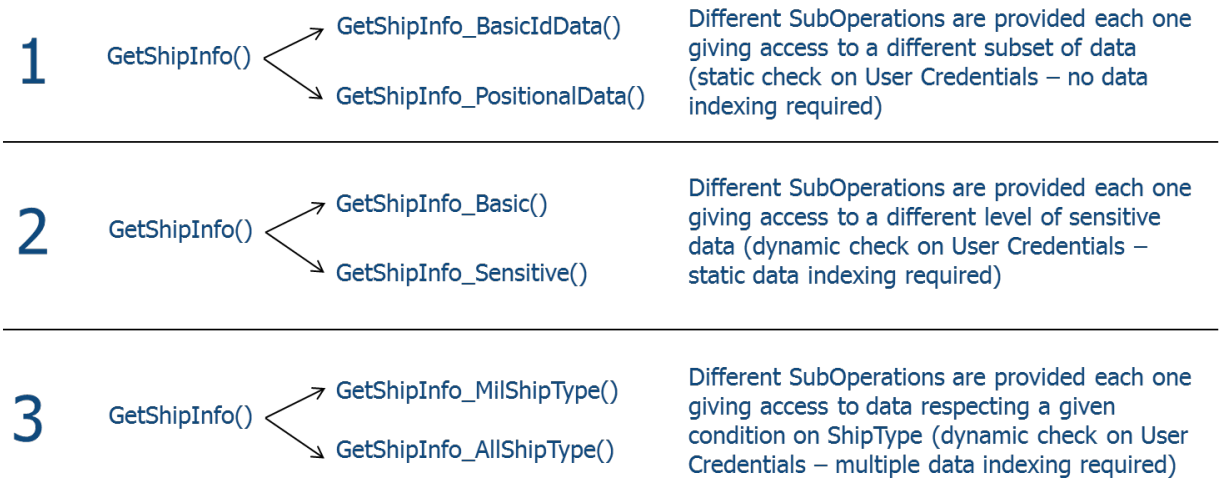


Fig. 7 – Examples of Managing Data Access and Distribution Plan through the Service Authorization Logic

In the second case, the DA&DP requires that some Users cannot access to information tagged as “sensitive” while all Users can access to information tagged as “basic”.

Consequently, different sub-operations are implemented in the GetShipInfo operation providing access to different groups of data records, and the Data segregation is performed at service level by granting different authorization level to the two operations depending on User credentials. Depending on how data

are stored and indexed in the back-end, data re-indexing according to the key "sensitive/basic" could be required as part of the back-end component developments in order to make such process effective.

Finally in the third and more complex case, the DA&DP requires that some Users cannot access to track information meeting certain criteria, e.g. the ship type is "military". In this case, the same solution as in the second case applies, but dynamic data re-indexing according to the key "ship type" would be required as part of the back-end component developments in order to make such process effective.

2.4 The Procedure for the SBCMP compilation

Primary Nodes in the BMM network, participating to the establishment of the SBCMP, shall implement the basic procedure depicted in Fig. 8 and shall respect the following implementation requirements.

- Own Tracks Processing Rules

Tracks received by a PN from its back-end shall be promoted to the status of "SBCMP tracks" through the following rules:

- ✓ assignment of an unique SBCMP identifier of the form PN_nnnn (IT_000001, PT_000001, SPA_000001, SPG_000001, etc.)
- ✓ assignment of a track origin indicator (0-Unknown, 1-Other ShipRep, 2-AIS, 3- LRIT 4-SAR, 5-Radar, 6-Intel, 7-Visual)
- ✓ Assignment of a Data Provider indicator (= the full domain name of the agency owning the data)
- ✓ a data classification level (0 – Basic, 1 –9 Sensitivity Level 1..9 TBC)

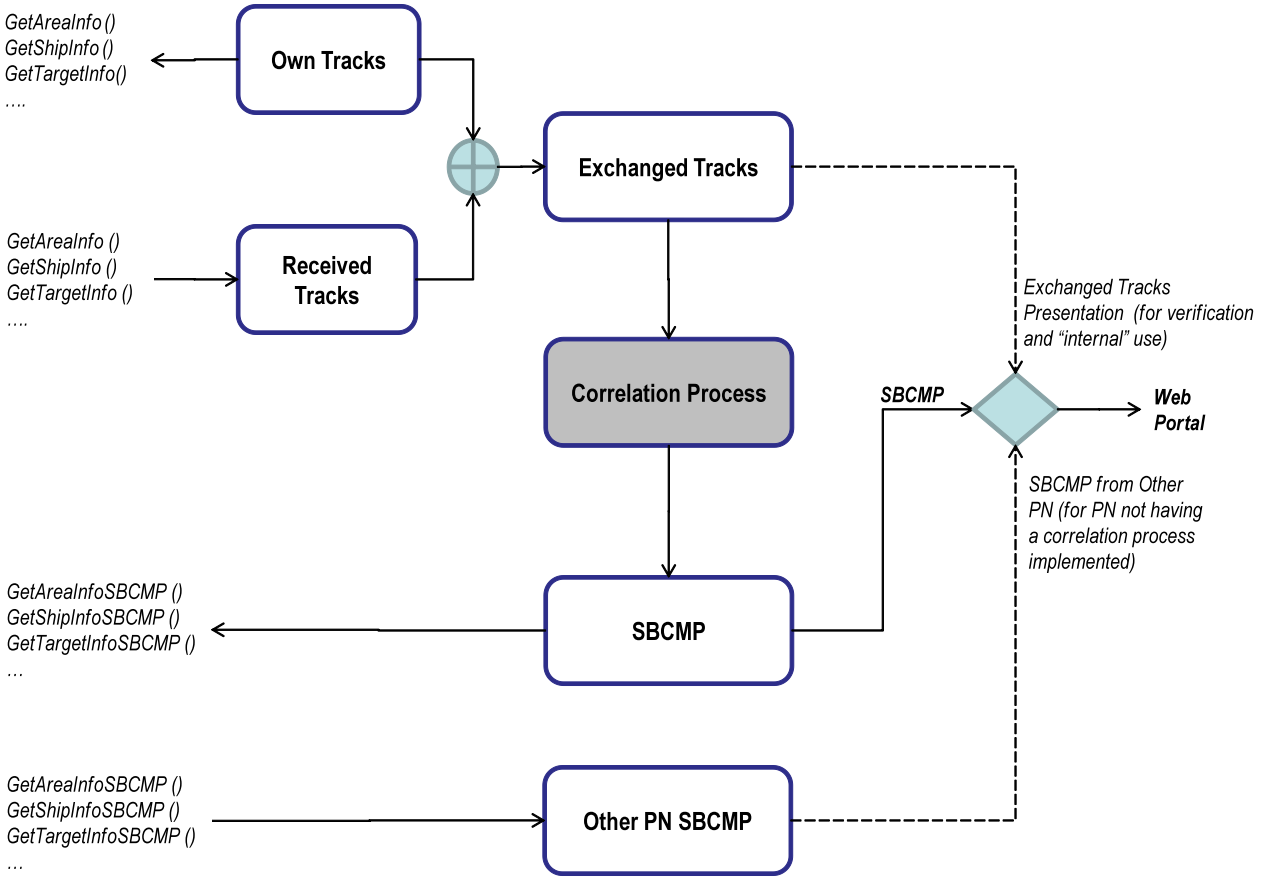


Fig. 8 – The BMM SBCMP procedure

Note: the Data Classification level assigned to each single track shall apply to all the "non-basic" data fields contained in the track (according to the BMM OV)

- ✓ a confidence indicator:
  1 = very high confidence, verified data,
  2 = high confidence (cooperative / non cooperative correlation),
  3 = confident (non coop / non coop correlation or coop/coop correlation)
  4 = low confidence (unsure source of verification, low confidence correlation)
  5 = very low confidence (no verification, co-operative target TBC)

- Correlation Process

All exchanged tracks are processed at regular intervals, variables according to the operational needs (e.g. from 1 to 10 min) by each PN in order to establish the potential association/ correlation. For any group of tracks having the same SBCMP identifier, only one correlation processing shall be performed using the track with the most recent time of validity.

Tracks that are not associated nor correlated (based on space-time and/or basic_Id criteria) are only processed by time normalisation for visualisation purposes, and are not modified throughout the Correlation process and keep their original identifier.

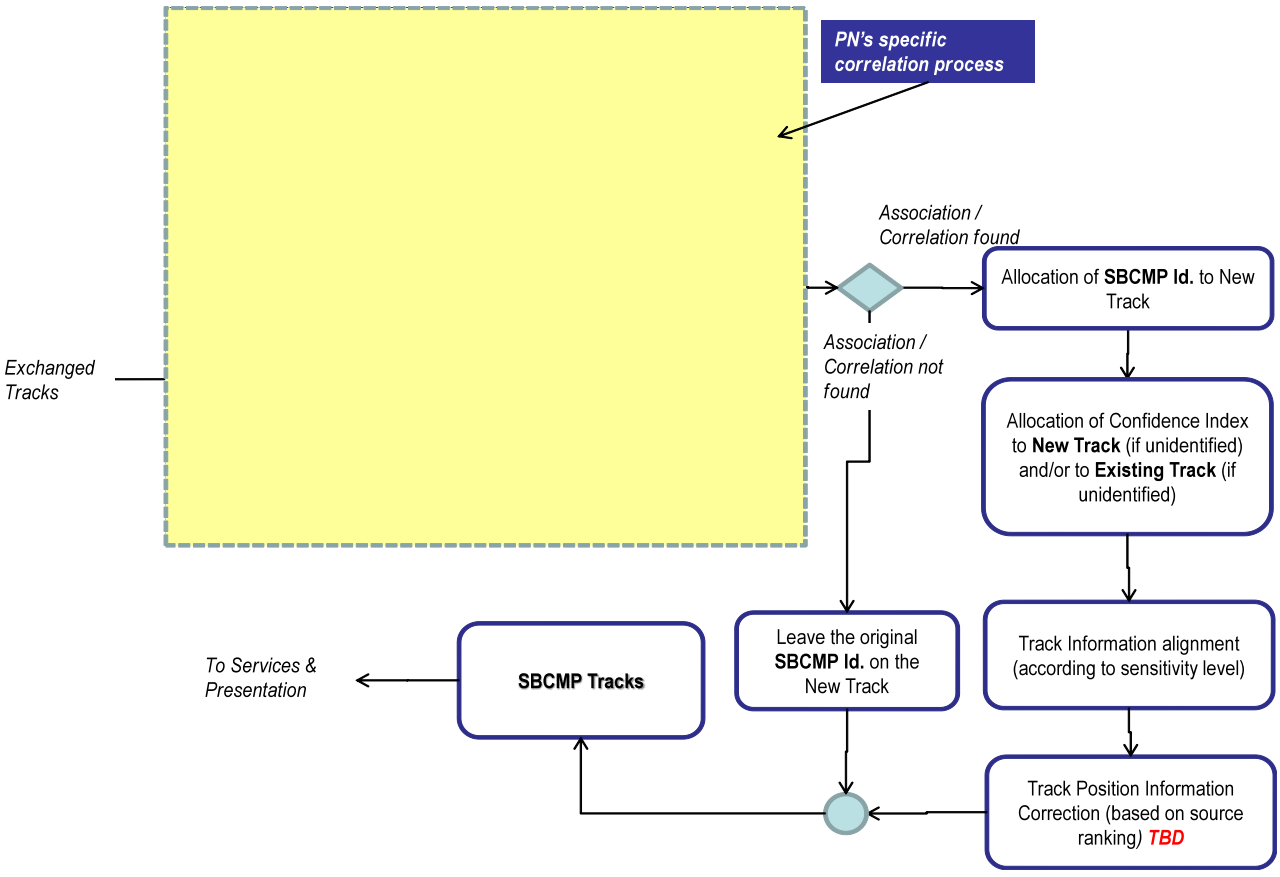


Fig. 9 – The BMM SBCMP procedure – Business Logic and algorithms

Tracks showing association of *Basic_Id* parameters and/or time-space correlation of relevant positional data and/or motion parameters beyond a defined threshold, shall be processed according to the following steps:

- The SBCMP identifier of the track with the older validity time shall be assigned to all correlated/associated tracks
- All data fields that are void in one track (except positional data) shall be updated with data fields present in the associated/correlated tracks having lower classification level
- The positional data missing in each of the tracks (if any) is updated using the known positional data of the associated / correlated tracks (regardless classification level)
- In case the times of validity of the correlated / associated tracks are closer than *30* seconds, the positional data and time of validity of all those tracks shall be aligned using the positional data and time of validity of the track with higher *track_source* indicator, and in case of ambiguity, the most recent time of validity

Correlation Process – Track Confidence Improvement

The confidence indicator of the associated /correlated tracks is modified according to the following rules:

Confidence before correlation	Confidence after association with a very high confidence track	Confidence after association/correlation with a track from an alternate source (cooperative / non cooperative)	Confidence after association/correlation with a track from the same source (cooperative / non cooperative)
1	1	1	1
2	1	2	2
3	1	2	3
4	1	2	3
5	1	4	4

Table 2 – SBCMP. Evaluation of the Correlation Confidence

The basic SBCMP procedure has been demonstrated during the experimentation phase by the 5 running Primary Nodes, and the need for further enhancing the harmonizing such deployment has been put in evidence during the demonstration phase.