Clarifications Requests

Rev 0.9
21/06/12

Overview of Changes

No	Date	Description	Author
1	06/10/11	First version	Thomas Lefort
2	11/10/11	Added clarifications requests on LDAP federation and anew topic on sharing of data via the common services	Thomas Lefort
3	13/10/11	Addition on SEM and SEA	Thomas Lefort
4	17/10/11	Added new requirements following some clarifications	Thomas Lefort
5	20/10/11	Added new discussion and requirements regarding the DDP and the use of the DDP for SEA	Thomas Lefort
6	22/11/11	Added requirements regarding Web GIS and language support, changed certificate requirement to CA signed	Thomas Lefort
7	27/01/12	Included conclusions from the December 2011 Rome meeting and discussions that followed.	Thomas Lefort
8	16/03/12	Included conclusions from the Madrid meeting and discussions that followed.	Thomas Lefort
9	21/06/12	Added some clarifications and a chapter 2 for possible improvements and next iterations for the BMM network.	Thomas Lefort

The purpose of this document is, first, to provide clarifications on the BMM System View Requirements wherever they are deemed to be incomplete or inaccurate, and based on experimentation and community driven discussions. Second, the document opens up to improvements to the existing specifications and new ideas for future iterations of the BMM pilot project.

Submitted to all PN TR, industry PoC and TWG leader

1. Clarifications on the BMM System View Requirements

1. Types of Secondary Nodes and Users

There are two types of SN, BMM and dependant SNs:

- BMM SN are computers directly connected to the BMM network and hence the public internet. These SN can in effect connect to any other PN directly. The https is a one way SSL. The only access control is via user name/password provided through the PN web portal.
- Dependant SN are computers physically located on the local national network and do not have access to the BMM network other than through their National PN. These dependent SN cannot connect to other PNs directly because they are not on the public Internet by definition.

Users are not strictly assigned to an SN and as such can use any computer to access the BMM network through any SN and the PN it is connected to.

User privileges – ie the BMM functionality a User will have access to – will depend on the SN and the PN it is connected to, as discussed further down in this document.

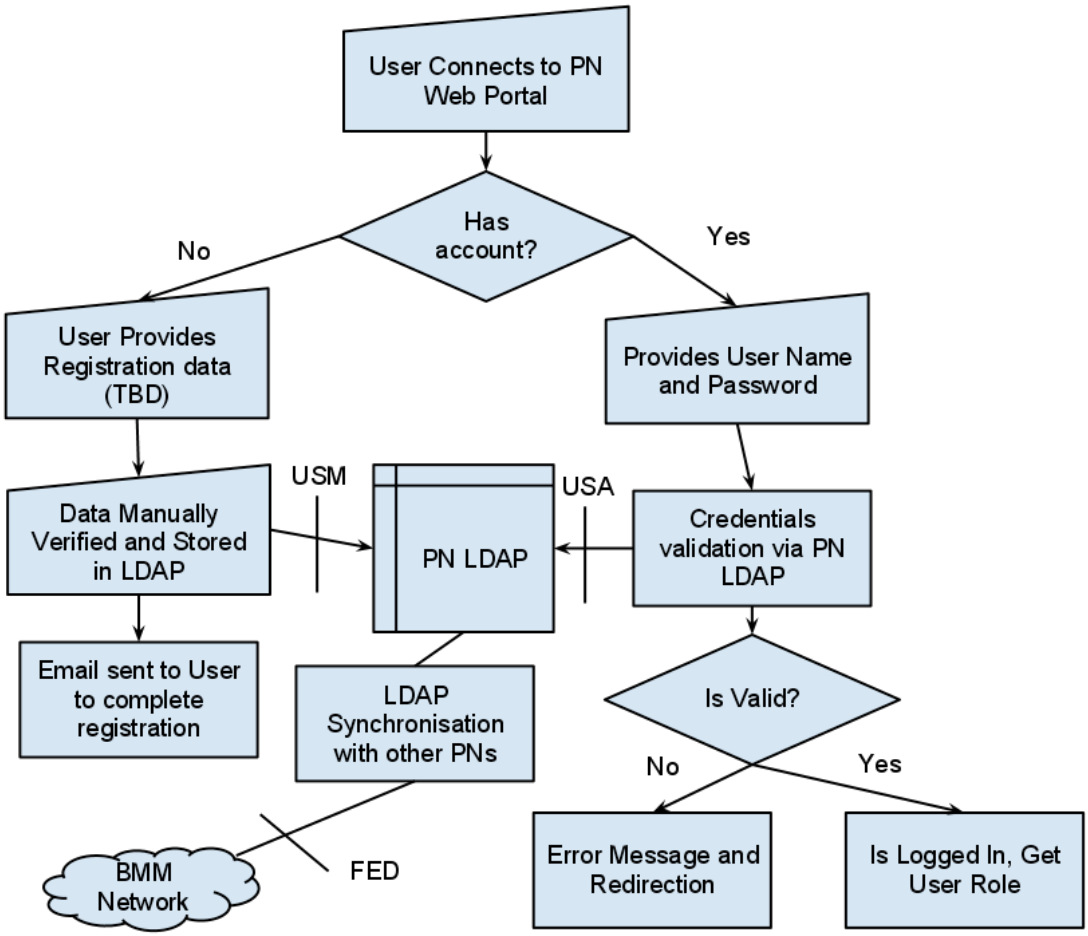
2. Connectivity and Security

Communication security is ensured by means of https.
From SN to PN, security is ensured by a one way ssl connection, which guarantees at least that the communication is encrypted. The BMM data and functionality is available through a dedicated web portal, managed by the PN the user is connected to. To access the BMM network data and functionality through the web portal the user needs to be authenticated. Authentication is ensured by means of a user/password token, requested by the web portal's sign in page. The user token is valid for all the BMM's web portals.
From PN to PN, security is ensured by a two way ssl connection, which guarantees at least that the communication is encrypted and the PNs are mutually authenticated. Two-way SSL authentication also known as mutual SSL authentication allows SSL client to confirm an identity of SSL server and SSL server can also confirm an identity of the SSL client. This type of authentication is called client authentication because SSL client shows its identity to SSL server with a use of the client certificate.

REQ.8.1	PN to SN shall communicate over a one way SSL HTTPS connection.
REQ.8.2	PN to PN shall communicate over a two way SSL authenticated HTTPS connection.
REQ.8.3	PN certificates shall be signed by the PN CA. This CA will be trusted (level 1) by the other PNs. Additional security can be implemented by checking the certificate's CN.

3. User Management and User Authentication Flow

The USM and USA is not very explicit in the BMM SV. Here is a simple diagram in an attempt to be more descriptive.



It is a rather standard way of proceeding.
Replication/synchronisation is performed via LDAP mechanisms (FED in the diagram) and authentication is done at PN level. All PNs have exactly the same User Data.
User Management (USM in the diagram) and User Authentication services, referenced in BMM SV at page 26/27, are only accessed internally, ie by the web portal, and should only be seen as an internal service for accessing the LDAP content. They are not meant to be used by another PN.

LPAD replication strategy is still TBD. There are many alternatives, as described in http://www.openldap.org/doc/admin24/replication.html. The current solution is to go for replication using a third party solution as there is no real interoperable standard for LDAP replication to date.

An alternative to the above diagram is to use referrals instead of duplications. In referral, each PN will have its own domain and their “natural” set of users. For users that have no natural PN,

such as EU agencies or MT or GR, they could either provide access to their own LDAP over HTTPS or be "hosted" by one of the PN's LDAP.

The solution selected for federating User Data should not have any impact on the Integration Tests as it is functionally equivalent and should be transparent from a usability point of view.

This part of the specifications is still open. Further study the best LDAP replication mechanism to be implemented and decide on one common interoperable solution.

The following requirements have been added.

REQ.8.4	A User shall be assigned one and only one Parent PN. The choice of a Parent PN will be the most natural choice (country, dependent PN).
REQ.8.5	Each PN shall be responsible for validating their User information at creation and also when modified.
REQ.8.6	A User shall only be allowed to modify their User Settings from their Parent PN.
REQ.8.7	A simple registration interface shall be provided by the web portal to enable a new user to create an account.

In addition the current definition of User Roles need clarifications.

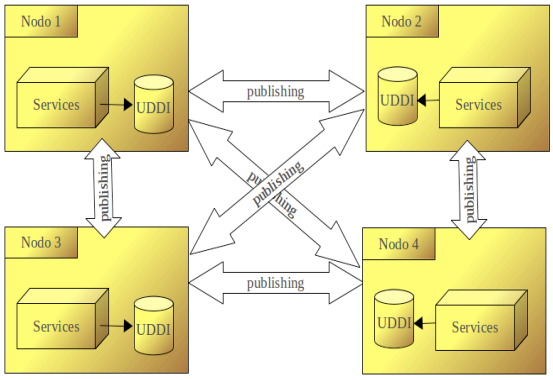
It was decided in the December 2011 Rome meeting to adopt a two step approach to handling User Management and federation. First step is to build a static User Data table to be shared with all PNs and manually entered in each PN's directory. The LDAP structure to adopted using LDIF:

dn: uid=mail,dc=bmm,dc=org
ou: ou = organisation/agency, ou = nation, ou = pn_code
uid: user normal work email adress (eg pedro.inacio@knowledgeworks.pt)
cn: email with @ replaced by .at.
givenName:
lastname:
jobTitle:
userPassword: xxx (provided as an MD5 hash)
telephoneNumber: xxx

REQ.8.8	Each PN shall create and maintain its Data Distribution Plan, a table giving correspondence between a user's credentials and its access rights to the PN's services operations and data access.

4. UDDI, Service Management and Service Authorisation

Each PN exposes its Services via publishing to its own UDDI. However the UDDIs are also federated. This means that all PNs UDDI contain the same information on services. If a new service is added or a service definition changes in one of the PN UDDI, the other UDDIs are automatically updated. The procedure used for UDDI update is the one proposed by the TWG, in the IT BMM PN TA document.



It is based on the standard publishing mechanism. Therefore each node is in charge of publishing to the other nodes any OF ITS OWN service changes.

The full description of the process to implement is available at
http://bmm.bluemassmed.net/opengoo/index.php?c=files&a=file_details&id=371

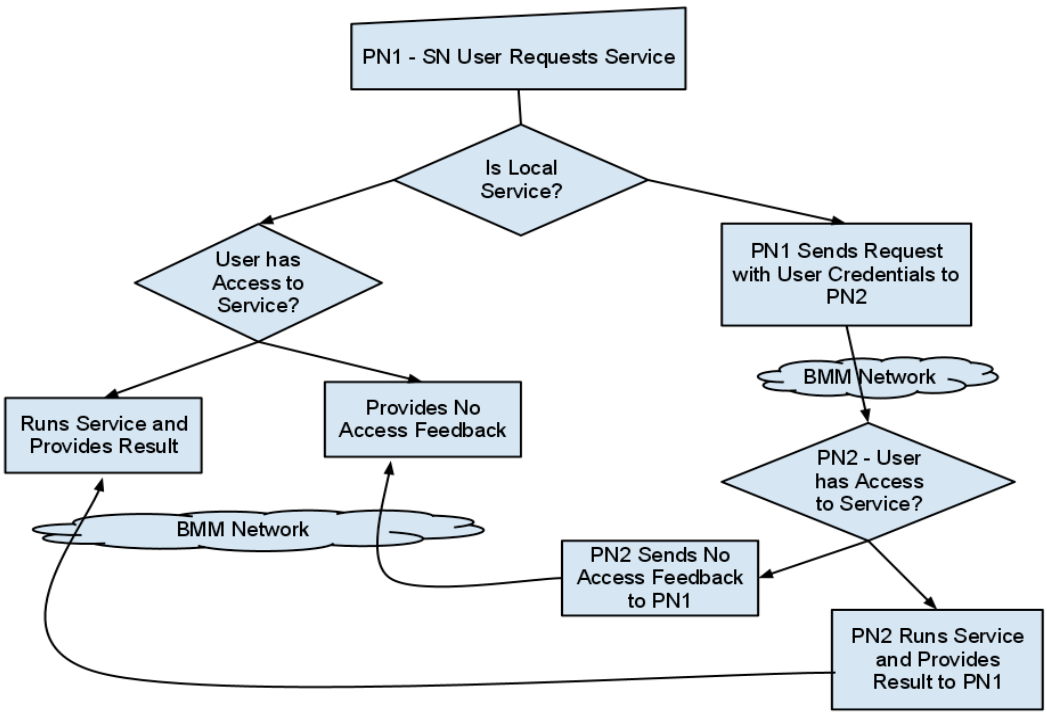
SEM and SEA mechanisms are not fully defined yet, at least not on paper. This is a first attempt to draft a common behaviour for SEM in an operational context.

The web service calls can be subdivided into the following topologies:

1. PN to PN. A PN requests a service from another PN without User involvement. This is typically the case with background data collecting, be it on subscription or polling, such as data collected to build the SBCMP.
2. SN to connected PN. The SN requests a “local” service via the web portal, that is to say a service implemented by its own PN.
3. SN to remote PN. The SN requests a “remote” service, that is to say a service implemented by a PN that is not the PN it is connected to.

In case 1, PN to PN connection is authenticated and secured thanks to the two ways SSL with each PN’s certificates. Although slightly redundant, a user password could also be used to improve authentication. In this case each PN will need a user/password defined.
Cases 2 and 3 are represented by the following diagram.

Assuming this work flow is correct, the external interfaces involved, ie PN1 to PN2, are not clear. The main question is how does PN1 sends the service request to PN2 on behalf of its SN User in a secure way. The BMM SV mentions the use of XACML and SAML to exchange authentication and manage authorisation. This web page provides a simple overview of the process http://www.cse.wustl.edu/~jain/cse571-09/ftp/soa/index.html#sec4.2.



Some thoughts:

- Whilst SAML provides an additional level of security when exchanging the authentication data between PNs, is it really necessary? The credentials were initially sent over the public Internet and over https (SN to PN when logging in the web portal), in effect there is not much difference between the two (PN to PN and SN to PN). One could also argue that in a trusted community, PN2 could rely on PN1 for the authentication of the User. Therefore authentication could be skipped
- An alternative solution would be to provide authentication data via the services SOAP Headers. The web service handler at PN2 level could check user credentials and user roles and authorise or deny access.

The latter has been adopted at the Madrid Meeting on 09/02/2012. The UserToken profile of Web Services Security has been adopted. User name and MD5 password as passed in clear between the calling PN and the receiving PN.

In addition it has been suggested to only use WSS UserToken profile when necessary, ie when a call requires User Authentication and hence a DDP check. The other service calls can be made without User credentials.

The following requirements have been added.

REQ.8.9	Each PN shall publish to all other PN's UDDI registries any changes made to their own UDDI registry when and only when it is one of their own services.

REQ.8.10	Naming conventions shall follow the document produced by IT "Italian Primary Node Service Registry Service_Rev_2.doc".
REQ.8.11	User Authentication for Service Authorisation shall be done using the UserToken profile of WSS.
REQ.8.12	User Authentication and hence the UserToken profile should only be used for services that require User Authentication. In other words a call to service not requiring user authentication does not need the user token in its message.

5. Collaboration tools at BMM levels

The SV does clearly specify which collaboration tools should be available on the BMM network. A number of out of the box tools are available in standard web portals solutions such as LifeRay, these include local chat, rss, blog, calendar, document sharing and opensearch. **However these solutions are local to the web portal and do not come federated across several nodes.** Following the December 2011 Rome meeting actions, all participants agreed to the need of at least a federated chat and a federated forum. PT proposed a way forward making use of XMPP for the chat, iCal for calendars and RSS feeds for the blog/forum, please refer to http://bmm.bluemassmed.net/opengoo/index.php?c=files&a=file_details&id=396.

The following requirements have been added.

REQ.8.13	The collaboration tools, chat and RSS feeds/blogs, of a Primary Node shall be BMM federated to all primary node and SN nodes connected to them.
REQ.8.14	Chat federation shall be based on the XMPP protocol and an XMPP server needs to be installed on each PN to this effect.
REQ.8.15	Chat federation client shall provide the ability to create, find and use chat rooms on all nodes and from all nodes. Chat rooms may be password protected.
REQ.8.16	Chat federation client shall provide the ability to define a user nickname and this nickname shall be used for the chat.
REQ.8.17	Chat federation client shall provide the ability to store the chat sessions on a local database for further retrieval.

Experimentation has shown that Chat and Forum federation is possible with free and OS third party solutions and taking advantage of the User Data federation.
Further experimentations are required to consolidate the specifications of federated Forum and Calendars.

6. GIS Server authenticated access

There are two possible topologies for GIS Server access: SN to connected PN or SN-PN1-PN2 when for instance invoking Rapid Mapping Services (RMS). In both cases all data are served over htttps.

Both access need to be authenticated, meaning a non logged in user cannot access any of the

PN GIS Server features. For SN to PN the authentication and authorisation can be based on the browser session with the right filter access implementation. For SN-PN1-PN2 services things get trickier as PN1 will have to proxy the requests to PN2 together with the user credentials. For this reason it seems to me that it would make more sense to access RMS resources or any other PN2 GIS data via the web service request and not via WMS/WFS requests. This however implies that a custom client be developed to handle these services and the resulting data. Raster data could be projected (assuming all clients use the same projection) and tiled and served as PNG images. Vector data could also be served using a common standard, eg GML 3.1.1 as proposed in IT BMM SV.

From a usability point of view, if a user wants to be able to view data from other PNs, he needs to be aware of the resources available on those nodes. This implies that each Map portlet includes a UI for retrieving each Web GIS Server's resources, viewing the list of resources and selecting a resource for display.

Being able to access WMS/WFS capability on any remote GIS server is an essential condition for the implementation of the Rapid Area Mapping capability, ie to display the satellite imagery tiles on top of the map client and to access the processing results such as ship detection reports (TBC).

The following requirements have been added.

REQ.8.18	An authenticated SN User shall be able to access any GIS Server resources on the BMM network through the web portal. Some GIS Server resources can have restricted access and not be available to a non authorised User.
REQ.8.19	The Web GIS Server shall be included in the SEA and resource access shall be specified in the DDP.
REQ.8.20	The map client shall display a list of all WMS and WFS resources available to the user across the BMM network. Resources available might be filtered based on the User's access right.
REQ.8.21	A User shall be able to select a WMS or WFS layer from the list of available resources and add it to their map as a layer or as a base map.
REQ.8.22	A PN should proxy WMS and WFS authenticated SN requests to the other PNs. Proxying is necessary to circumvent SOP issues, ensure full encryption and authenticated access to resources, and to provide support to dependant SN (not directly connected to the internet).

A technical note is available in Annex 1 to explain how the proxying can be implemented.

7. User Groups

User groups are shared between PNs. They should provide Users with different privileges and web portal functionality across the BMM network.

The SV states:

· BMM Super Users, users of Primary Nodes
They will be able to:
- request / provide BMM common services through their legacy systems.
- manage BMM Network (core services) through the Primary Node
- administrate services and users (core services) through the Primary Node
· BMM Full Access Users, will be able to:
- Provide data & information to the BMM network through specific adapters (SOA / P2P) to their legacy systems, implemented by the Primary Node
- Access BMM network through Primary Node web portal (with basic functions for data ex change like AoI, track data & track features entry, etc.)
· BMM Users, will be able to access BMM network only through web portal of a Primary Node

Those groups are local and BMM wide groups. Extra groups needed *locally* by the PN for let say additional maintenance, etc… exist too but are different and only visible to the PN, and should only concern their own subset of users.

The entitlements are specified but may be not so clear wrt different possible use cases. In particular it doesn't describe the entitlements for the User Group when connected to another node or requesting a service from another node.

These are the potential cases for a User:
1) User connected to its own PN
1.1) web portal functionality
1.2) calls to "local" services
1.3) calls to "remote" services
2) User connected to a remote PN
2.1) web portal functionality
2.2) calls to "local" services
2.3) calls to "remote" services
2.4) calls to "remote" own PN services

For each cases the user rights for each group of users needs to be defined. This drills down to a table with a list of permissions/functionality for each combination. For instance a FullUser should be allowed to use the track injection portlet functionality on any node it connects to. A SuperUser should have access to administrative tools locally and be able to publish in the other UDDI and LDAP registries via its own PN.

Each PN can grant any more privileges to the users at their sole discretion.

8. Service Authentication and DDP

Whilst the System View recommends the use of SAML and XACML for service Service authentication and authorisation, given that we are in trusted environment, it was finally decided

to use the UserToken profile of WS Security, without password encryption.

A static and predefined Data Distribution Plan (DDP) is to be defined to enable authenticated and authorised access to a PN Node services. This DDP needs to be defined by **each PN** based on the User Data available in the shared LDAP structure, which is shared at BMM level.

The implementation of the DDP is free and each PN should be able to do it the way they want.

Access to data shall be filtered at service level. Therefore restricted data should only be sent if the service call is user authenticated and if the user is authorised according to the node's DDP. If a service call is not authenticated, only BMM wide data should be sent.

REQ.8.23	Service Authentication shall be optional. If a service call is not authenticated, only data available to all BMM users should be sent.
REQ.8.24	Service Authentication shall be performed by means of the WS Security UserToken profile with no password.

9. Fine(r) grain DDP implementation

As mentioned at the Rome meeting there are cases where DDP should be dynamic and filter at the data item level, that is to say for each piece of data and not each category/type of data. In addition this data access rule shall be modifiable over time. A good use case is that of an organisation injecting new data, let's say some information on the captain of a vessel, that at first they only want to share with a selected subset of users, then a month later, release the information to everyone. **This functionality is currently not available.**

It was agreed that this new finer grain control over the DDP is far more complex and to adopt a two steps approach, ie keep on with the current implementation in a first phase whilst investigating on possible solutions to satisfy the above mentioned scenario. A DG DIGIT project called eTrustEx has been cited as a possible solution and should be further investigated.

10. Data Sharing with Common Services

This topic is being covered by the IT SBCMP proposal, please check the following file at http://bmm.bluemassmed.net/opengoo/index.php?c=files&a=file_details&id=451.

REQ.8.25	A PN shall only send its own raw data to other PNs. Raw data should be understood as data that does not result or include other PNs' data. This is to avoid any reinjection of information.
REQ.8.26	Common rules for the establishment of an SBCMP shall be implemented as per TWG proposal "SBCMP v1 Procedure".

11. Time Synchronisation and time stamping

PNs need to be time synchronised to provide accurate time stamping. The easiest solution is to use available Time Servers (any level) synchronised on a GPS clock for instance.

In addition it is recommended to keep a traceability of all data exchanged, for this purpose messages should be timestamped.

REQ.8.27	Each PN should use an NTP Time Server to ensure a synchronised clock at BMM level.

12. Common Data Model and Common Services definition

It has been agreed during the September 2011 Core Group Paris meeting to create a group for defining a common data model. This data model should be used by all PN Common Services implementation.

Whilst service definition does not have to follow a common model, it is recommended to start from the reference set of service definitions (PT proposal) as provided by the same working group, in an effort of standardisation and to avoid growing software development costs.

At the very least each TA document should precisely reflect on the services implemented and provide adequate documentation for other PNs to understand the way the services are running.

The PT proposal for Common Services has been adopted by 4 out of the 5 PNs, and whilst IT has different wsdls, the services definitions are converging.

REQ.8.28	All PN Common Services should use the common BMM Data Model.
REQ.8.29	All PN should update their TA document with their Common Services implementation and provide adequate documentation on their functioning.

The data model and the PT and IT CS definitions have required a few points of clarifications. The PT proposal CS and the data model definition files (wsdls and xsds) have been upgraded with inline documentation. Please refer directly to these files for CS and data model clarifications.

13. Display and injection of alerts

The choice of how to display alerts should be left entirely to the PN. However it is assumed that alerts will be at the very least visible on the map client using an appropriate symbology.

It is also expected to be able to inject new alerts, based on the user group, through a widget or a specific portlet.

14. Language Support

There is no requirement regarding the language and language support of the web portal.

The risk is that we quickly run into a usability issue if each PN provides the interface in its own language which is not necessarily spoken by SN users. The problem will occur with Users wanting to connect to the BMM network with another PN than their country's one(s) or for users without a PN, such as Greece and Malta or EU institutions.

We need to add a requirement there. There are two alternatives:
(1) all English
(2) multi (at least local and English languages) support

(2) is obviously more appealing but can get rather complicated. (1) is simple but assumes all users have a reasonable command of English.

The problem extends to documents and any data exchanged too and not just the User Interface.

At the December 2011 Rome meeting it was decided to have all PN UI in UK English language.

REQ.8.30	The PN web portal interfaces, including portlets, should all be in UK English language.

2. Suggestions for future iterations of the BMM project

1. Creation of scenarios

This is a proposal from PT and completed by FR. The idea is to tag items in the SBCMP (alerts, tracks) with an identifier which would help the operator tailor its current view to a maritime situation (or scenario) of choice.

Scenario tagging, would open up a whole new range of possibilities, such as:

- filtering the viewing of data in the SBCMP by scenario
- opening one view for each scenario
- automatic creation of collaboration assets (federated chat room, federated forum), dedicated to the scenario
- automatic generation of report for a scenario
- automatic replay of a scenario for auditing or training purposes

For further details please refer to the original document provided by PT.

http://bmm.bluemassmed.net/opengoo/index.php?c=files&a=file_details&id=450

2. Chat improvements and other collaboration tools

The current solution with jwChat provides a poor user experience and adds friction to the process. The following are suggestions to improve the chat experience:

- auto loggin and assignment of a meaningful nickname
- possibility to share also images via chat
- minimize the number of opened windows
- improve integration of chat within the operational window, eg not as a separate page. For instance, a side bar could be available with the list of available and active chat rooms on the BMM network.

Also as mentioned in chapter 1, much more needs to be done to have a full set of collaborative tools. Whilst the exact needs of operators need to be defined, it is widely accepted that at least a federated forum and a federated document management system that can be browsed and searched across the BMM network are needed.

3. Attaching and sharing documents to Tracks

This is a feature actually implemented by the FR node, but that could benefit the overall BMM community if it was supported by the CS. The basic idea is to be able to link documents to a track. On the French portal, when the user displays track information, it has access to all documents that have been added to the track. Common Services could be enhanced to support

the exchange of this type of information between nodes by, for instance, adding a list of urls element to the trackNotification type.

4. Existing Common Services and Data Model improvements

The idea is to converge to a common and "standardised" set of services and data model. This means a shared set of wsdls and xsds. There are currently two (very similar) CS definitions and one data model. The two CS definitions need to merge. We can use the PT proposal as the baseline and enrich with the IT proposal. Here are a few suggestions:

1. Use a shipId structure wherever a ship needs identifying, in requests and in responses.
2. Improve the definition of alerts by adding a generic alert structure from which other alerts can derive and add to this structure a time of validity (more elements to add TBC).
3. Use standards wherever suitable instead of redefining new structures. For instance the area/polygon could be based on gml.
4. Add a field to trackNotification to identify if the track is a regular track or one that has been inserted manually. This would enable different rendering in the SBCMP.

Some issues remain and could be solved by further improvements of the wsdls:

1. How do we update/cancel/delete an alert? The use case is that of an alert that has been raised but is no longer actual. The operator that created the alert needs to be able to remove it and all nodes should be notified that the alert is no longer valid and that it needs removing from the SBCMP.
2. Similar to 1, it should also be possible to remove manual tracks from the SBCMP, by invoking a removeTrackNotification.
3. How do we make WAM work for future imagery? At present it is not possible to have support for asynchronous ordering feedback. Also how do we trigger analysis of Satellite Imagery, or should it be automatic?

In addition, it has also been suggested to use DAS only for exchange of notifications. This needs debating as it has many impacts at system level.

It has also been suggested to leave the use of getAreaInfo in favor of WFS requests, which implies a shared an secured access to the different PNs' web GIS servers. Also the choice of xml, via soap messages, has been highlighted as costly and could be improved by more compact interfaces such as a RESTFul API with json data format. As this would be a major architectural change, a thorough investigation of the proposal needs to be done.

A similar suggestion with regards the use of WFS and WMS has been suggested for the Rapid Area Mapping services. Any solution considered should reflect, if not adopt, on the EC INSPIRE directive.

5. Community maintained Open Source Software project

Whilst it should be possible for each joining node to implement the BMM specifications the way they see best, there is much to gain by providing a basic implementation of the SV under the form of a free and Open Source software project. This would significantly speed up the integration time and cost for any new comer. By reducing the amount of friction to join the network, more nations and organisations should be willing to (at least) "give it a try". In addition, being open source, any modifications can be made to the solution. It can therefore be further tailored to an organisation's operational needs and specificities. Improvements to the software made by participating organisations, based on experimentation and actual operational needs, can be re-injected into the project. This would start a virtuous circle, with participants benefiting from and sharing each others work and contributions.

The choice of Open Source license is to be debated and will have impact on the solutions used and further developments.

The exact content of the software package provided is to be defined. However it should provide sufficient functionality to, after some configuration and a small amount of programming (essentially to connect to the user's back end systems), be connected to the BMM network and use its main functionality.

A part of the project would be a software testbed facility to validate the implemented Common Services in a semi automatic way. The testbed would enable automatic validation of the BMM services implementation of a PN prior to it joining the network, therefore minimising the integration risks and costs.

6. Selective sharing of information at service and data level

The current implementation and specifications does allow selective (user based) sharing at service level, through the use of the WSS UserToken profile. However, little experimentation (if any) has been done on this essential feature. The current approach is to share all data between nodes regardless of the users. The SBCMP is generated by each PN for all users. This does allow selective sharing and selective display of sensitive data, based on user access rights. A new mechanism needs to be implemented to allow selective insertion of information in the SBCMP.

Let's take a simple use case: the French Customs inject a track (or a document, an alert, voyage notification, etc...) and this track should only be visible to users from the Italian Customs.

There are two sides to the issue of selective sharing of data. The first side is the insertion of the data with the ability to define its access rules. How can we provide a simple interface for quick and efficient configuration of access rules, in particular in the case of manual injections through a user interface? The second side is the handling of the data and the enforcement of the access rules in the final SBCMP rendering in the user's web client. First of all there is the issue of the sensitive data being handed over from the remote node to the local node. In the use case taken, assuming the IT Custom user is requesting the sensitive information through the IT PN client, French Custom sensitive information is leaving the FR PN to go to the IT PN. From the FR Customs point of view, there is no real guarantee that the information injected into the FR PN and then dispatched to other PNs will never be disclosed to unauthorised recipients.

A first measure is to have organisation level PNs and user access agreements limited to organisation - organisation topology. This limits the dispatch of sensitive information to the authorised nodes only.

A second measure is to implement an encrypting mechanism for each sensitive data exchanged. This mechanism will make sure that only authorised user, ie with the right key, can read the information it contains. This significantly complicates the handling of data and the computation required. The implications on the generation of the SBCMP need to be evaluated too.

In all cases we need to perform user based SBCMP generation to take into account the different level of data access for each users. This can be a rather computationally intensive process. To simplify, a basic SBCMP can be generated for all users, which can then be further enriched based on the user rights. This "layer 0" of the SBCMP can be generated by data collected using non user authenticated Common Services calls. Any additional layer is User specific, and based on additional data collected by the PN through User authenticated calls to the Common Services.

To conclude, a system of data traffic auditing should be mandatory to be able to trace which, to who, and how data has been exchanged.

7. SV requirements non completed within the BMM project

Last but not least, remains the work that was not completed within the framework of the BMM project and as identified in the Integration Test report in particular.
Here is a summary of the different items:

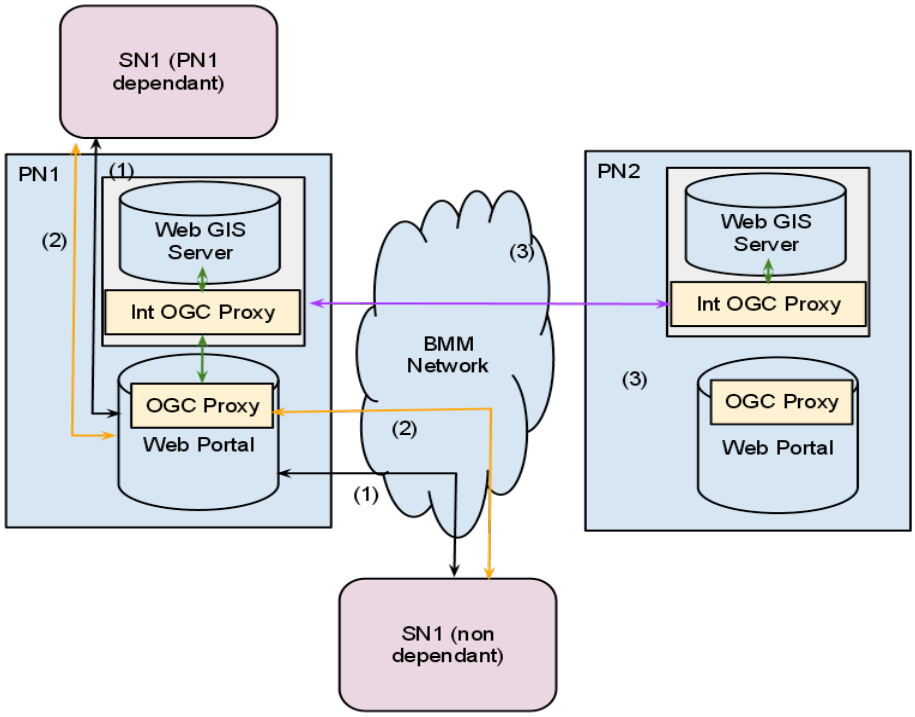
1. Service Authorisation - whilst the solution (WSS UserToken) was agreed, there was no concrete example of implementation made and therefore no real testing of the functionality. Service Authorisation based on User rights and the node's DDP need to be finished.
2. User Federation - no agreement could be reached on how to perform federated user management. User tables were statically exchanged between partners each time one node's user table was updated. The main issue is that there is currently no commonly accepted LDAP exchange standard. One solution would be to send the updated tables in LDIF format to all nodes for update. This would entail the creation of a new service for exchanging the file between nodes and updating the directories accordingly.
3. Two way ssl and User Access protected Web GIS resources - currently the web GIS are not all two way ssl, also GIS resources are all available to any user, ie there is no DDP applying to the Web GIS server. Finally remote Web GIS servers that are two way ssl protected are not remotely accessed, which is a problem for WAM in particular. Therefore we need, as explained in this document a mechanism for two way ssl User Authenticated and remote access to all Web GIS servers on the BMM network. Having BMM wide access to all Web GIS servers would also open up a number of possibilities beyond the sharing of projected Satellite Imagery. This would facilitate the sharing of layers of information between nodes, such as specific maps owned by one node and made available to other nodes' users.
4. Vessel Detection System integration of EC – JRC and integration of service providers at

large. This could not be done due to lack of budget and time. The initial idea was to enable the EC - JRC BlueHub to inject an on demand Vessel Detection Service capability in the BMM network. This work could provide grounds for a larger framework for "plugging in" external service provider capability into the BMM network.

5. Implement more alerts. There are more alert types than the "Other" type of alert, eg POLREP or SITREP. Due to the complexity and length of integrating one type of alert and the limitation of the demo scenarios to the "Other" type of alert, only the "Other" type of alert was actually integrated and tested. More alert types need to be included and the schemas need to be finalised. This job has been partially done by some nodes but there is still a large amount of experimentation required.
6. WAM - rapid area mapping was very partially tested and only for a few nodes. Amongst possible improvements are 1) exchange remote WMS Urls for map client rendering, 2) support for future acquisitions (which is more complex due to the delay in the ordering process and the acquisition delays too, and requires modification to the existing Common Services definition).

Annex 1

The following graph shows a possible implementation for the use of WMS and WFS across the BMM network.



Web GIS Servers are located in the two way ssl zone, the web portals in the one way ssl.

The flow of data goes as follows:

(1) SN1 requests web portal access and map portlet. SN1 is identified, SN1 receives data from the web portal.

(2) map portlet javascript running on SN1 requests a WMS or WFS GetCapability to either the PN1 or PN2 web gis server via the PN1 map portlet.

(3) The map portlet forwards the requests to its OGC proxy. The OGC proxy can validate the user using the web portal session. If the request is for the local web gis server, it is forwarded and the response is sent back to the map portlet.

(4) If the request is for PN2, the proxy passes the requests to a second proxy able to reroute the requests over two way ssl to the PN2 Web GIS Server proxy. The request is forwarded with the user credentials.

Because the two PN proxies exchange data over https two way ssl, the connection is authenticated and secured. It is not possible for a user to tamper unauthenticated into PN2, because over one way ssl, the only access is via the OGC proxy which uses the web portal session to identify the user, ie the user has to be authenticated via the web portal first.