Test Plan & Procedures for the BMM Integration Tests

Rev 0.9
22/06/12

Overview of Changes

No	Date	Description	Author
1	06/10/11	First draft version	Thomas Lefort
2	07/10/11	Added OpenSSL tests for Connectivity	Thomas Lefort
3	10/10/11	Modifications following remarks	Thomas Lefort
4	25/10/11	Changes in CT, WUG and UDL Test Procedures following discussions and first tests	Thomas Lefort
5	27/10/11	Small updates to WUG and UDL Test Procedures	Thomas Lefort
6	25/11/11	Various and small updates to Test Procedures	Thomas Lefort
7	16/03/12	Multiple modifications on existing tests. Added Collaborative tools tests, vignettes validation, time synchronisation and time stamping, and a first try at Track Information and Data Exchange testing.	Thomas Lefort
8	24/04/12	Added tests regarding notifications, alerts, rapid area mapping	Thomas Lefort
9	22/06/12	Further updates to testing and finalisation of traceability table.	Thomas Lefort

This document describes the BMM Test Plan and Test Procedures for the BMM XMSN Integration Tests.

Table of Contents

I. Approach Taken....3
II. Tests....5
(1) Connectivity Test....6
a) Purpose....6
b) Test Readiness....6
c) Test Procedures....7
(2) Basic – Web Portal User Management, Map Client Portlet and Web GIS access over HTTPS10
a) Purpose....10
b) Test Readiness....10
c) Test Procedures....11
(3) Basic – UDDI and LDAP federation....14
a) Purpose....14

b) Test Readiness....14
c) Test Procedures....15
(4) Basic – SEM and SEA....17
a) Purpose....17
b) Test Readiness....17
c) Test Procedures....18
(5) Federated Collaborative Tools....19
a) Purpose....19
b) Test Readiness....19
c) Test Procedures....19
(6) Common – Time Synchronisation, Time Stamping and Geo Reference....21
a) Purpose....21
b) Test Readiness....21
c) Test Procedures....22
(7) Regular Tracks Exchange, Display, Ship Information and Voyage....23
a) Purpose....23
b) Test Readiness....23
c) Test Procedures....24
(8) Common – Injection, Exchange and Visualisation of Alerts....26
b) Test Readiness....26
c) Test Procedures....27
(9) Common - Wide Area Rapid Mapping Service....29
b) Test Readiness....29
c) Test Procedures....29
(10) Basic – DDP implementation on Ship Voyage Information....31
a) Purpose....31
b) Test Readiness....31
c) Test Procedures....32
Annex 1 – Requirements Traceability....33
Annex 2 – HelloWorld WSDL....44
Annex 3 – Track template for Common Services Testing....45
Ship Information....45
Annex 4 – List of contacts for Testing....46

I. Approach Taken

BMM XMSN remains an experimental project, as such the proposed testing approach is made of short end to end functional tests. It does not pretend to be complete but rather focuses on validating a working prototype for the BMM Vignettes demonstrations.

BMM XSMN is composed of 5 Primary Nodes and 27 Secondary Nodes communicating and exchanging NRT data using SOA principles. PN are the nuts and bolts of the system, SN are simple client computers connected to the BMM XSMN through a browser.
The 5 PN are developed by 5 different industry consortia. Although their implementations are made using the same set of requirements - the BMM System View Document Requirements - incremental integration testing will be of paramount importance to ensure that all nodes communicate with each others in the intended way and that the overall requirements of the BMM XSMN are met. Upon completion of the integration tests contained in this document, the BMM XSMN stakeholders shall be able to execute the User Vignettes contained in the BMM Demo Plan with the assurance that the underlying technology is functional.

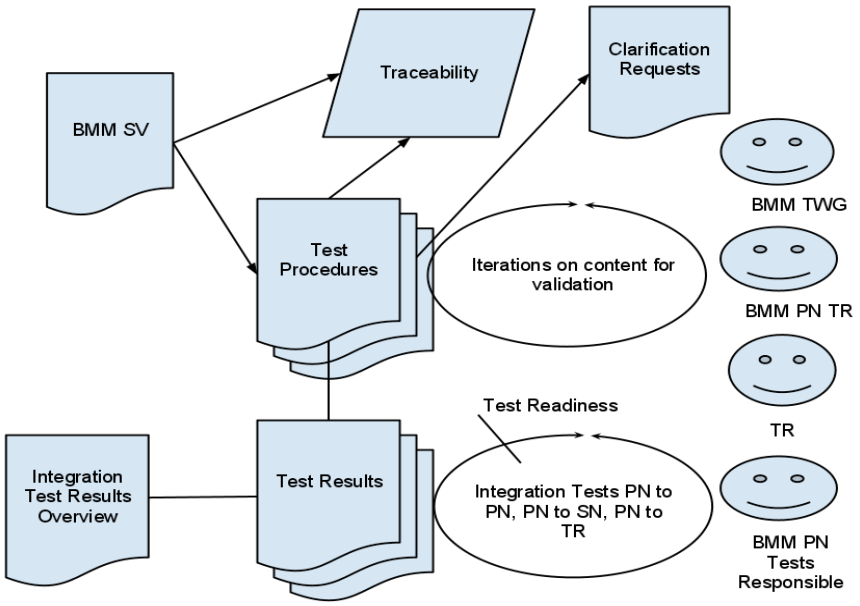
The Integration Tests are not designed to be a substitute to the PN's own validation & verification tests. They are designed to verify and guarantee that PNs and SNs are able to work together as specified in the BMM SV. It is assumed that each PN will have performed some basic (unit) testing to validate their implementation at the node level before any corresponding Integration Test Procedure is carried out. This will ensure that the Integration Tests procedures are effectively dealing with integration issues.

The full integration test set will be divided into test steps. Each step will reflect on an incrementation of the functionality of the PN, so as to say on a possible implementation milestone. Therefore, for each step, the minimum set of required implemented features is specified, as well as any dependence to (successful completion of) other test steps. Each test procedures will specify the network topology used. The topology of the tests can be threefold, PN to PN, PN to local SN and PN to external SN. Finally, each test step will require a Test Environment set-up to be Test Ready. A PN shall signal when it becomes Test Ready or not. When PNs and SNs are Test Ready they can carry out the test procedures according to the topology of the test. A spreadsheet is maintained to follow testing progress for each PN. This spreadsheet is also a good indicator of the overall BMM XMSN implementation progress and a possible tool for external reporting.

The elaboration of the Test Procedures themselves is an iterative development. They are initially proposed by the TR to the PN managers and industry team for feedback. Once the test procedures for a test are approved by all parties, they can be used for testing. It could be that some adjustments are necessary – debugging of the test procedures themselves – in which case an update is proposed. Add ons to the existing SV will be suggested, when it is felt that the initial specifications are incomplete or not accurate enough for testing. These will be listed in a table together with the actual SV requirements covered.

To facilitate coordination of tests, the web portal's chat widgets should be used between people during the testing, ie the PNs, SNs and the Technical Reviewer. Alternatively the https://bmm.covam.es/sparkweb/history.htm conference application available on the Spanish Armada node can be used. It allows for multi users conference talk instead of one to one chat sessions. The TR will start the test session. All people involved in the Testing Sessions should have their names and contacts, telephone number made available in Annex 4 of this document. Planning and organisation of testing sessions will be handled by the Technical Reviewer, essentially by email. On completion of the tests, the test spreadsheet will be updated with the test results.

Here is a simplified overview of the process:



Although initially drafted by the TR, the TWG Responsible and all PN TR are also involved in elaborating the test procedures steps.
Any issue regarding the existing specifications will be formalised in a Clarification Requests document for discussion.
Assumptions, directives or new requirements will be added in the test document with traceability to the Clarification Requests and System View documents.
Once a step of test procedures has been agreed and validated, it is proposed for test runs. When the participants for a test step are Test Ready, the test can take place with the BMM PN Tests Responsible, according to the test topology, and under the supervision of the TR.
The results of the tests are formalised in a central document which also provides an overview of the progresses made on integration.

II. Tests

The following sections contain the integration test procedures. Test procedures are grouped into steps to provide for incremental functionality testing. Tests steps start with basic PN connectivity tests and end with the full XSMN functionality test with all PN involved.

The following structure is used for each step:

1. Purpose – explains the overall objectives of the tests and the SV Requirements covered by the tests
2. Test Readiness – lists all requirements in terms of implementation and test environment such as tools and data, necessary to carry out the tests
3. Test Procedures – the actual test procedures to be run and the criteria for success

Test results are to be completed directly in the corresponding Test Step Sheet of the Integration Test Follow-up Spreadsheet called BMM Integration Test Follow-up.xls.

The Integration Test Follow-up Spreadsheet contains the following sheets:

- an Overview sheet showing for each Test Step the progress made by each PN
- two separate sheet for each Test Step with the following
  - Test Environment set-up sheet
    - Test Readiness, the planned date for being system ready to run the tests
    - Platform, description of the platform tested with software versions
    - A line for each Test Data required, if data is required to be provided, such as IP address, it should be mentioned there
  - Test Procedures Results sheet
    - Date of the Test
    - A line for each Test Procedure to be run with the Test Results to be completed as specified in the Test Procedure itself
    - Test Result, overall result for all test procedures. If not fully completed a test coverage indicator is provided, ie in the form of a percentage of tests covered

(1) Connectivity Test

a) Purpose

i. Objectives

- Test and characterise the IP connection between nodes
- Check HTTPS communication one way SSL SN-PN and two ways SSL between PNs
- Validate the Web Portal and SOAP server access over HTTPS

ii. SV requirements covered:

- Req 1.4, 1.5, 1.6 and 1.7

iii. Additional requirements and assumptions made

- One way SSL for PN-SN and two way SSL for PN-PN as agreed during the PN Design review meeting
- PN SSL client certificates are CA signed. Each PN CA used for signing certificates has been made available to other PN for configuration. When requested CN and DN of certificates also.

b) Test Readiness

i. Implementation requirements

This test assumes the PN machine server is available and running and that the web portal and the soap server have been installed and configured to run on HTTPS. It also assumes that the User Authentication and Service Authorisation services are NOT running, so that the web portal and the basic SOAP service can be accessed without user credentials.

List of Requirements:

- The PN server is available, connected to a public WAN and has a public static IP, optionally a (sub) domain name, ICMP is not blocked by the PN firewall
- The PN server is connected to a screen and has a web browser installed
- Each PN will have provided its connection bandwidth (uplink and downlink) measured using, for instance, the following online tool http://www.ip-adress.com/speedtest/
- HTTP port 80 and HTTPS port 443 are opened, or if any other port is used instead it needs to be specified, for instance if SOAP is configured to be used on another port.
- LoadUI & SoapUI installed, requires a JVM 1.5 or more
- The PN self signed SSL certificate has been made available to the other PN and installed on their server's keystore and vice versa
- The web portal and soap server are installed and configured to run with HTTPS access on the specified port
- The web portal is accessible with a one way SSL authentication. The URL needs to be provided.
- The SOAP server is accessible with a two way SSL authentication. A simple web service for testing has been implemented and the WSDL should be provided. The HelloWorld WSDL

could be used, available in Annex 2, in which case the implementation should return a greeting message using the input parameter firstName.

- Each PN will provide a name for the PN IT administrator, in charge of certificates, network configuration, etc...

ii. Test environment

1. Tools
    1. Ping
    2. Openssl
    3. A web browser for the SNs
    4. SoapUI from http://www.eviware.com/ in its free version
2. Input Data
    1. The other PNs IP addresses and (sub) domains if available
    2. The other PNs SSL certificates
    3. The other PNs web portal URL
    4. The other PNs simple SOAP service (HelloWorld service) URL or the full WSDL of the one to be used
    5. The other PNs firewall's configuration if relevant

c) Test Procedures

For the Connectivity Tests, we have 3 types of topologies to cover:

1. PN to PN tests. This means we have the following combinations: PT-SP1, PT-SP2, PT-IT, PT-FR, SP1-SP2, SP1-IT, SP1-FR, SP2-IT, SP2-FR, IT-FR. Tests are perform both ways for each combination.
2. PN to external SN tests. Any laptop situated on a different network can represent an external SN. The Technical Reviewer will perform the tests with his own laptop.
3. PN to local SN. This a second “breed” of SN which are located in the National LAN and do not have direct access to the BMM Network, other than through their own PN. These SN cannot in effect connect to the other PNs but only to their own PN.

1. PN to external SN tests

ID	Description	Criteria	Comment
CT_1	**Visibility. (IF PING IS ALLOWED BY PN)** The TR laptop performs a PING command to the other PN IP address and (sub) domain if available. Ping -c 10 Ipaddress_or_domain.	All ten messages were sent and round trip was below 200ms.	
CT_2	**One way SSL connection.** TR laptop enters openssl s_client -connect PNAddress:portNumber	Check connection is made and certificate delivered	
CT_3	**One way SSL connection Performance.** TR laptop enters openssl s_time -connect PNAddress:portNumber -ssl3	Write down performances, ie connections/s	Wait 30s for tests to complete

CT_4	**One way SSL HTTPS access to web portal for external SN.** The TR connects via their laptop to the other PN web portal using a standard web browser and the HTTPS URL provided for the web portal home page. The TR also tries with HTTP only.	Web Portal Front Page available with HTTPS but not available with HTTP.	Warning about the certificate.
CT_5	**One way SSL HTTPS access to web service not working.** The TR tries to access the wsdl file using its URL over https or over HTTP.	No access to web service due to client certificate missing.	Warning about the certificate.

2. PN to PN tests

ID	Description	Criteria	Comment
CT_6	**Visibility. (IF PING IS ALLOWED BY PN)** PN performs a PING command to the other PN IP address and (sub) domain if available. Ping -c 10 Ipaddress_or_domain.	All ten messages were sent and round trip was below 200ms.	
CT_7	**Two ways SSL HTTPS Certificate Check.** PN opens their web browser and adds their p12 certificate to the list of certificates. PN opens the wsdl link for the other PN HelloWorld Service in the browser.	WSDL is displayed in the web browser.	
CT_8	**Two ways SSL Performance.** Each PN enters openssl `s_time` -connect PNAddress:portNumber -key yourkey -cert yourCert -www HelloWorldService_WSDL_URL	Write down performances, ie connections/s	Wait 30s for tests to complete. The URL should be a relative path to PNAddress.
CT_9	**Two way SSL HTTPS for SOAP.** Each PN performs this step. Open SoapUI. Open the preferences page of SoapUI. Select the SSL tab and specify your keystore location and password. Create a new project and use the WSDL URL of the simple service provided by the other PN. Expand the service binding and double click on the request. Fill in the missing parameters (firstName in the HelloWorld example), send the request (using the green arrow on the top) and check the reply is as expected.	The service replied and the reply is as expected.	

3. PN to local SN

ID	Description	Criteria	Comment
CT_10	**Visibility.** All National SN located on the National LAN only, performs a PING command to the PN local machine address. Ping -c 10 machine_address.	All ten messages were sent and round trip was below 200ms.	

CT_11	**One way SSL HTTPS.** All National SN located on the National LAN only, connects to the PN web portal using a standard web browser and the machine local address provided.	Web Portal Front Page available	Warning about the certificate.

(2) Basic – Web Portal User Management, Map Client Portlet and Web GIS access over HTTPS

a) Purpose

Building on the connectivity tests we check the web portal User Management UI is available with a local test user (no federation for now) as well as authenticated access to the Web GIS Server through a web portal portlet. Web GIS Server is (optionally) tested together with USA and USM to demonstrate User access to Map resources based on the DDP.

i. Objectives

This is an intermediary test step to show the implementation of two essential web portal components:

- User Management UI through the web portal and connection to USM and USA services
- Authenticated access to the Web GIS server through a simple portlet of the web portal, with access to map data via WMS and WFS over https one way SSL.
- Authenticated access to another PN's Web GIS server through the same portlet of the web portal

ii. SV requirements covered:

- *Req.1.9, Req.1.10, Req.1.11, Req. 3.3, Req. 3.4, Req.4.1, Req.4.2, Req.4.3, Req.4.4, Req. 4.8, Req. 4.9, Req.4.18, Req.4.19, Req.4.20, Req.4.21, Req.4.22, Req.4.23, Req.4.24, Req.4.25 (all), Req.4.26, Req.4.27, Req.4.28, Req.4.29, Req.4.31*

iii. Additional requirements and assumptions

Add requirements from Clarifications Requests document.

b) Test Readiness

i. Implementation requirements

These tests assume the connectivity tests have been run successfully. In addition, the following is required:

- Web Portal is set-up and has a sign-in User Interface
- USM and USA services have been implemented for the local LDAP
- trUser@spa.bmm.org account has been created across all nodes
- The DDP has been set up and at least the Map data access has been configured
- The Web GIS server is running and available to an authenticated user. Data is transmitted over HTTPS.
- A portlet gives access to a map environment with means to query and display WMS and WFS data from the PN's Web GIS server AND a remote PN's Web GIS Server (at least for the getCapabilities request). Test data should be stored in the GIS server to this effect, preferably a raster file and a vector file.
- Test specific requirements
  - Two rasters and two vector files have been added to the Web GIS Server. The first ones are called “test1_raster” and “test1_vector”. The second ones are called test2_raster and

test2_vector

- The DDP is set up so that the TR (trSuperUser@spa.bmm.org) has access to test1 data and not to test2 data. The Web GIS Server has been configured accordingly.

ii. Test environment

This is a SN to PN test only

1. Tools
    1. a browser on SN
2. Input Data
    1. The web portal URL
    2. The PN Web GIS server URL

c) Test Procedures

These Test procedures are to be carried out by the TR with each PN using a simple laptop over the public Internet. Test procedures relating to the Web Client access should also be performed by at least one dependent SN. The Remote PN Web GIS Server access requires a special topology for testing, as it implies to test that all other PNs Web GIS Server are available and that User Authentication and Authorisation is implemented at that level too.

ID	Description	Criteria	Comment
WUG_1	**User Management.** TR connects to the PN web portal using the web portal URL in a web browser.	Home Web Portal page is displayed and a portlet is available for User Sign-In. It is not possible to register, either the link is not available or an error is raised.	
WUG_2	**User Management.** TR clicks on the Sign-In and enters the user/password trUser@spa.bmm.org/wrong password	A message is provided stating access denied, wrong credentials.	
WUG_3	**User Management.** TR clicks on the Sign-In and enters the user/password trUser@spa.bmm.org/correct password	TrUser has access to the web portal functionality.	
WUG_4	**User Management.** TR accesses his own profile page on the web portal.	Profile information is displayed including the User contact details as provided by TR. User Name, email addresses, nation and organisation are not changeable. Telephone number can be changed.	
WUG_5	**User Management.** TR edits the phone number.	Phone number is changed.	
WUG	**English language:** TR navigates through	All text is displayed in	To have the pages

_6	the different web pages available and verifies that they are available in English language	english.	displayed in English it is possible that a user settings need configuring via the User Interface.
WUG_7	**GIS Portlet.** TR tests the following features of the GIS portlet: map display, navigation controls, layer control.	The GIS portlet displays a 2D or 3D map. There are zoom and pan controls available to help navigate in the map. A control is available that enables the user to switch between different background maps.	

For this special test procedure we will need to test access with all other PNs. This implies that other PNs have also set up their DDP and Web GIS Server access according to the test requirements. The TR – PN set up can be reused.

WUG_8	**Remote Web GIS Server Access.** The portlet displays a lists of resources available from the remote Web GIS Servers for display. TR requests display of raster and vector data.	Test2 data is not visible or accessible for TR. Test1 data is added to the map and displayed.	

This test procedure covers the optional requirement of a User, with adequate rights, to be able to publish manually GIS data from a SN to the BMM network via the Primary Node it is connected to. Only PNs implementing this optional requirement should perform the test. The implementation of this feature is opened and each PN should explicitly explain how publishing is to be performed.

WUG_9 (optional)	**SN Publishing Data.** TR is granted enough User privileges by PN. TR checks if UI is available for inserting User web GIS data.	Links or UI elements are available. Publishing of data is available. A UI is available with data access level control specification.	Explicitly report the types of publishing available (Web GIS and/or information database) and if data access control is provided.
WUG_10 (optional)	**SN Publishing and retrieving Data.** TR publishes data on PN. TR checks availability of data in the web portal map client.	Data is available	

(3) Basic – UDDI and LDAP federation

a) Purpose

These tests cover the UDDI and LDAP set-up for federation over all PNs. User data include user name and password and a number of attributes some which will help define their access rights to services (roles for authorisation). In practical terms, this means that if a new user is registered, removed or information is changed, in one of the PNs LDAP, the changes will be reflected in due time to all other PNs. The same way if a PN updates its services it should register the changes in its own UDDI registry and all PNs UDDI registry will be updated accordingly.

The User Services, USM and USA, provide a service layer on top of the local LDAP service. They are an internal service used for instance by the Web Portal to check a user's credentials or for managing users and user data. USM and USA are tested in (2) and are deemed to be working for the LDAP federation tests procedures.

i. Objectives

- Verify that PNs UDDI Registries replication mechanism are in place and working over https two ways SSL
- Verify that PNs LDAP are able to exchange credentials and authenticate users over https two ways SSL

ii. SV requirements covered:

- *Req.3.2, Req.3.3, Req.3.4, Req.4.6, Req.4.7, Req.4.11, Req.4.12, Req.4.13, Req.4.14, Req.4.15*

iii. Additional requirements and assumptions

Refer to the Clarification Requests document for additional requirements and discussions on LDAP federation and UDDI replication strategies.

b) Test Readiness

i. Implementation requirements

These tests assume:

- the LDAP service to be up and running as well as the UDDI registry
- both services are configured for replication with the other PNs registries
- UDDI publishing to and from the other PNs UDDIs is enabled and configured
- LDAP federation mechanisms between PNs have been enabled over HTTPS
- The PN's UDDI inquiry, publish and security URL has been given to all other PNs an user/password have been set-up for access to the UDDI
- UDDI automatic publishing for new services has been implemented
- The Service Management has been implemented and Super Users can manage their registry through it.

These tests assume the following test cases were successful:

- (1) Connectivity
- (2) USA and USM

ii. Test environment

1. Tools
    1. Web browser
    2. UDDI browser
2. Input Data
    1. The other PNs IP addresses and (sub) domains if available
    2. The PN's UDDI inquiry, publishing and security URL
    3. The PN's LDAP URLs and credentials

c) Test Procedures

For these Tests, we perform SN to PN tests with two PNs involved to test PN to PN exchange of data.

ID	Description	Criteria	Comment
UDL_1	**LDAP Federation.** TR requests creation to PN1 of a new User Account as per PN1 procedures. Upon account creation, TR connects to PN2 with the new Account credentials.	TR succeeds in connecting to PN2.	
UDL_2	**LDAP Federation.** TR accesses profile information on PN2.	Information is visible but not editable.	
UDL_3	**LDAP Federation.** TR logs out from PN2 and logs in to PN1 with the same user credentials. TR accesses profile information.	Information is visible and editable.	
UDL_4	**LDAP Federation.** TR changes phone number, save profile information, logs out of PN1 and logs in PN2, checks new profile information.	Phone number has been updated.	

This test is PN to PN to test UDDI federation. It is not used to verify that all services have been published. This will be done in each Service Tests Procedures.

ID	Description	Criteria	Comment
UDL_5	**UDDI Federation.** PN1 Super User adds the HelloWorld service to its UDDI registry using the Service Management interface. PN2 Super User checks the new dummy service is visible in its own UDDI registry.	New HelloWorld service is visible and the Business Service Name is according to specifications which is PN1_code.bmm::Hello World. PN nation	

		codes are: pt, spa, spg, it, fr.	
UDL_6	**UDDI Federation.** PN1 Super User changes its HelloWorld endpoint value using the Service Management interface. PN2 Super User checks the PN1 HelloWorld service information has been updated from its own UDDI registry.	Service has been updated.	
UDL_7	**UDDI Federation.** PN1 Super User removes its own HelloWorld service from its UDDI registry using the Service Management interface. PN2 Super User checks the PN1 HelloWorld service has been removed from its own UDDI registry.	Service has been removed.	
UDL_8	**(to be performed when all services are available) UDDI URLs.** All PNs check that they have all required URLs registered in their UDDI from all nodes of the BMM network. These include Web Server GIS access URL, all Common Services URLs, all UDDI access URLs.	Services are registered in all nodes according to the naming conventions.	

(4) Basic – SEM and SEA

a) Purpose

These tests will test the authentication and authorisation to a PN services for the following cases:

- a User behind a SN
- a PN to PN service request without User involvement

i. Objectives

- Verify that an authenticated user
  - has access to the connected PN web service when authorised by the PN DDP
  - does not have access to the connected PN web service when not authorised
- Verify that an authenticated user
  - has access to a remote PN web service when authorised by the remote PN DDP
  - does not have access to a remote PN web service when not authorised by the remote PN DDP

ii. SV requirements covered:

- Req.4.4, Req.4.5, Req.4.10, Req.4.11, Req.4.12, Req.4.13, Req.4.14, Req.4.15, Req.4.16, Req.4.17

iii. Additional requirements and assumptions

b) Test Readiness

i. Implementation requirements

These tests assume:

1. User Data is federated at BMM level
2. A DDP is available on the PN and configured, for TR User and Full User accounts, for the HelloWorld service and for the IES getShipInfo service (or any other more suitable service as agreed with the nodes prior to testing. Full User should have higher data access privileges than User.
3. The helloworld service is available

These tests assume the following test cases were successful:

- (1) Connectivity

ii. Test environment

1. Tools
   1. no specific tool required

2. Input Data
    1. Helloworld service wsdls

c) Test Procedures

For these Tests, we perform SN to PN tests.

ID	Description	Criteria	Comment
SES_1	TR uses SoapUi to send two calls to the HelloWorld service, one with the WSS UserToken profile set to trUser@spa.bmm.org account and the other one with trFullUser@spa.bmm.org.	trFullUser@spa.bmm.org gets a hello world response whilst trUser@spa.bmm.org doesn't	This is a local only call, which intends to simulate the server to server call with the user Token set. It is not a full validation per se.
SES_2	**Remote**: (assumes CS testing has been done for IES) TR requests a ship info from the remote node using the available UI.	trFullUser@spa.bmm.org has access to more information than the trUser@spa.bmm.org	Test can be adapted to other services if the remote node does not filter on IES getShipInfo service.

(5) Federated Collaborative Tools

a) Purpose

These tests will test capability of three SN connected to three different PNs to exchange information via a chat room and via a forum.

i. Objectives

- Validate the availability of federated chat and federated forums, at least to the level required by the vignettes, which implies more or less a chat room for the chat part.

ii. SV requirements covered:

- Additional requirements from the Clarifications Requests, Req8.11 and Req8.12

iii. Additional requirements and assumptions

b) Test Readiness

i. Implementation requirements

These tests assume:

1. User Data is federated at BMM level
2. The web portals are up and running with Chat and Forum functionality enabled

These tests assume the following test cases were successful:

- (1) Connectivity
- (2) Basic

ii. Test environment

3. Tools
    1. no specific tool required
4. Input Data
    1. No specific input data required

c) Test Procedures

For these Tests, we perform SN to PN to PN to SN tests. This requires TR and at least two more PN SN to be available and coordinated, all logged to a different PN.

We need a test service for testing SEA.

FT_1	**Chat log in**: All users log in their chat (if not already logged in) in their respective PNs.	Chat portlet available, a chat popup or new window opens. In there other users can be found, other users can be invited, other users can join, chat rooms can be searched or and chat rooms can be created.	
FT_2	**Chat room creation**: All users create a chat room in their respective PN. The chat room is called “BMM Test”, the chat room needs to be publicly visible.	Chat rooms are created and listed in the chat client.	
FT_3	**Chat room discovery:** All users look for the newly created chat rooms in their respective chat servers.	Rooms can be found.	
FT_4	**Chat room use:** All users enter the newly created chat rooms and post the message “Hello World from User xxx” in each chat room.	Messages appear in all the chat rooms, from all users.	
FT_5	**Forum (optional)**: All users logged in. TR starts a forum topic through the web portal. TR invites the other users to join the forum discussion. All other users join. All users send a “hello world from ” and their name.	Forum portlet available, new forum topic visible, new forum entries visible.	

(6) Common – Time Synchronisation, Time Stamping and Geo Reference

a) Purpose

These tests will test the PN time stamping capability and geographical referencing of all data being exchanged on the BMM network. This implies having a common Time Reference, using an NTP time server, and using the same Geo Referencing system, WGS-84.

i. Objectives

- Check the time synchronisation between PNs
- Check the ability of nodes to send time stamped messages and store the time stamped messages received
- Check the geographical referencing of data

ii. SV requirements covered:

- Req.4.30, Req.4.31

iii. Additional requirements and assumptions

b) Test Readiness

i. Implementation requirements

These tests assume:

- Maritime Surveillance Data is being exchanged between PNs
- PNs have set up their NTP Time Server

These tests assume the following test cases were successful:

- (1) Connectivity
- (2) CS with time stamping available

ii. Test environment

1. Tools
    1. no specific tool required
2. Input Data
    1.

c) Test Procedures

These Tests are performed by the TR to evaluate the implementation of an NTP service by each PN to synchronise the time reference across the BMM network, the ability to keep a time stamped

reference of data exchanged between nodes and the correct use of the WGS-84 as the geodetic datum for exchange of positions in the data models used.

ID	Description	Criteria	Comment
TSW_1	Check the use of an NTP time server in the Target Architecture Document.	An NTP Time Server should be used to synchronise the clock of the PN.	
TSW_2	Check the PN CS systematically include a time stamp in their messages. Receiving PNs check that each node is sending messages with a filled in time stamp and message id and that the time stamp is correct and with a time zone.	Message time stamp should be set to within a few seconds of the time the message was received.	

(7) Regular Tracks Exchange, Display, Ship Information and Voyage

a) Purpose

These tests aim at validating the PN to PN exchange of regular track data between the nodes to compose an SBCMP. Track data should be exchanged on a regular basis via polling (synchronous). Indeed, it has been commonly agreed to use getAreaInfo with tracks to retrieve regular tracks and NOT to use the asynchronous DataAugmentation service for this purpose. The DataAugmentation service will be limited to exchange of alerts and manually injected tracks.

A sufficient refresh rate for polling and response should be implemented for operational purposes. Whilst there is no reference time defined per se in the system views, 10mns could be used as a maximum delay for access to track information.

It should be possible to access Ship information and Voyage information on any ship available in the operational picture, be it a local ship or a ship provided by a remote node. The information fields available and their content has to follow the rules defined in the data model and the common rules of the SBCMP.

The test procedures are focusing on the high level functionality rather than the actual service implementation as each PN can implement the service with the wsdl of their choice. For this reason we base our tests on the PN's web portals directly both for injecting tracks and for viewing them.

Because there is no guidance or strict specifications on the client User Interface, tests procedures are very loose. It is clearly up to the TR to adapt the testing procedures to each PN web portal.

i. Objectives

- Check that the PN have implemented the minimum set of services to exchange regular tracks and ship information between nodes.
- Check that the PN web portals provide the right User Interface to view regular tracks and ship information

ii. SV requirements covered:

- Req.4.32, Req.4.33

iii. Additional requirements and assumptions

b) Test Readiness

i. Implementation requirements

These tests assume:

- PN portal up and running with Map Client available
- CS IES implemented
- CS services configured, areas set for information request, display set to display all tracks available

These tests assume the following test cases were successful:

- (1) Connectivity
- (2) Service Management
- (3) Map Client

ii. Test environment

1. Tools
    1. no specific tool required
2. Input Data
    1. Regular backend feeds of tracks from the national systems or simulators

c) Test Procedures

These Tests are performed with a TR - PN to (multi) PN topology, one being the client and calling the service and rendering the result in the Map Client, the other one(s) being the server(s) and sending the messages based on the client PN requests.

ID	Description	Criteria	Comment
TM_1	**General regular tracks exchange between nodes**: TR logs in all PN web portals and access the operational map client.	The map portlet displays tracks in all areas covered by the nodes. There is no hole in the “tracks” display.	Additional portlets can also be available to view tracks using a different layout such as in a table.
TM_2	**Ship information accessibility, availability and consistency**: TR uses the UI available to query the ship basic information from the available tracks in the map client, in each PN's portal and for each PN. TR uses the available UI Retrieve extended information on that ship.	The basic information should at least include the name, position and speed of the ship and (a link to) the ship's photo. The full information on the ship from the track should include all fields defined in Annex 3 and following the rules laid out for each field.	Use the table to compile the results of the tests. This is a N (map clients) x N (PN tracks) check, N being the number of PNs involved.
TM_3	**Voyage information accessibility and content**: TR uses the UI available to query the ship voyage information, in each PN's portal and for one track of each PN.	Track history is displayed in the map according to the period of time requested. The textual information available includes all fields as defined in Annex 3.	Use the table to compile the results of the tests. This is a N (map clients) x N (PN tracks) check, N being the number of PNs involved.
TM_4	**General check up of tracks and performances**: TR compares for each PN's	Ship tracks are generally consistent from one node to the other.	

	areas of data that the displayed tracks across the different map clients is roughly equivalent, ie that there is no large differences due to refresh delays of information.		
TM_5	**SBCMP rules**: TR requests randomly ship information on each PN web portal to verify the SBCMP rules have been applied.	The following should be implemented: common shipGuid and prefixed by a PN code followed by a unique identifier, origin of the track should be clearly visible, type of sensor should be clearly indicated (Unknown, Other ShipRep, AIS, LRIT, SAR, Radar, Intel, Visual) and a confidence indicator should be available.	

(8) Common – Injection, Exchange and Visualisation of Alerts

These tests aim at validating the PN implementation of the creation, exchange and rendering of alerts and manual tracks. Alerts and manual tracks can be received asynchronously, based on subscriptions, or synchronously using regular polling.

Due to the urgency of an alert and of a manual injected track (generally done in collaborative context of a maritime situation), it is expected that the information be sent immediately after their creation by a user and sent asynchronously to all subscribed nodes, so they can be visualised within 30 seconds of their creation time.

There is no specification related to the creation and rendering of alerts and manual tracks, and it is up to the different nodes to implement it the way they see fit. However to ensure a minimum of consistency between nodes, and facilitate the user experience, it has been suggested to provide:

- Rendering: map based and/or list based visualisation of the alerts. Map based should use specific color schemes for alerts and if possible decorate the incriminated ship or area with an alert icon.
- Creation: a form based, tailored to the alert type, widget, portlet or dialog should be displayed to create an alert and a manual track.

There are many types of alerts defined. Due to timing constraint, the current tests will only be based on the "other" type of alert.

i. Objectives

- Check that the PN have implemented alert creation and rendering and that alerts are exchanged between nodes.

ii. SV requirements covered:

-

iii. Additional requirements and assumptions

b) Test Readiness

i. Implementation requirements

These tests assume:

- PN portal up and running with Map Client available
- CS IES and DAS implemented
- CS services configured, areas set for information request, display set to display all tracks available, service subscriptions set to receive asynchronous alerts via the Data Augmentation Service from all other nodes

These tests assume the following test cases were successful:

- (1) Connectivity

- (2) Service Management
- (3) Map Client
- (4) Tracks exchange

ii. Test environment

1. Tools
    1. no specific tool required
2. Input Data
    1. Sample ship track record
    2. Sample alert notification

c) Test Procedures

These Tests are performed with a TR - PN to (multi) PN topology, one being the client and calling the service and rendering the result in the Map Client, the other one(s) being the server(s) and sending the messages based on the client PN requests.

ID	Description	Criteria	Comment
EAL_1	**Tracks injection and visualisation**: TR injects a ship track record with meaningful data according to Annex 3, through the different PNs web portals. TR accesses each one of the PN Client Map Portlet and looks for the local and the remote PN fictional ships on the map. TR requests the basic track info on the tracks and compares with the injected data.	All ships are present in the expected areas, with the expected positions at the time of request and their basic track data is displayed according to the injected data. The track is visible within 30s of injection (map refresh rate). The origin country and entity are set to the TR country and organisation.	
EAL_2	**Alerts injection and visualisation**: TR logs in as trSuperUser on all PNs involved in the test procedure. TR creates an “Other” alert notification on an existing ship through each node's web portal, using the available user interfaces. The Other alert should include a “Alert from “ with the PN node name in the “details” field of the alert creation form. TR requests more information on each alert created using each web portal's interfaces.	Each alert created is displayed and rendered within 30s in each remote web portal and immediately in the local one to ensure good feedback to the user. The alert is located on the selected ship. The details message is displayed correctly, the origin of the alert is displayed correctly in particular the origin country and	

		organisation.	
EAL_3	**Tracks injection and visualisation – no ship**: TR logs in as trSuperUser on all PNs involved in the test procedure. TR creates an “Other” alert notification without a ship through each node's web portal, using the available user interfaces. TR requests more information on each alert created using each web portal's interfaces.	Each alert created is displayed and rendered within 30s in each remote web portal and immediately in the local one to ensure good feedback to the user. The details message is displayed correctly, the origin of the alert is displayed correctly in particular the origin country and organisation.	

(9) Common - Wide Area Rapid Mapping Service

These tests aim at validating the PN implementation of the exchange of wide area mapping services, ie the Satellite Imagery based services.

This is an optional service and not all nodes have implemented it or integrated it.

i. Objectives

- Check that the PN have implemented principles laid out in the SBCMP proposal.

ii. SV requirements covered:

-

iii. Additional requirements and assumptions

b) Test Readiness

i. Implementation requirements

These tests assume:

- PN portal up and running with Map Client available

These tests assume the following test cases were successful:

- (1) Connectivity
- (2) Service Management
- (3) Map Client

ii. Test environment

3. Tools
    1. no specific tool required
4. Input Data
    1. The areas and time availability of satellite imagery for each nodes

c) Test Procedures

These Tests are performed with a TR - PN to (multi) PN topology, one being the client and calling the service and rendering the result in the Map Client, the other one(s) being the server(s) and sending the messages based on the client PN requests.

ID	Description	Criteria	Comment
WAS_1	**Requesting and visualising existing imagery**: TR logs in as trSuperUser on all PNs involved in the test procedure.	A processing request feedback message is displayed. After a little	

	Using the web portals interfaces, TR requests Satellite Imagery from the PNs providing the service for a specific zone and a specific time period, as agreed with the different PNs beforehand and mentioned in the test input data section.	while the available imagery is displayed in the web portal's interface, either projected in the main map client or in a map in a separate portlet.	
WAS_2	**Requesting future acquisitions**: TBD	TBD	

(10) Basic – DDP implementation on Ship Voyage Information

a) Purpose

These tests will test the authentication and authorisation to a PN services for the case of a common service, ie the ship voyage information service. Different amount of information should be visible to two different categories of users.

This is a repeat of Test (4), with a test case which allows for User (SN) to PN to PN service authorisation testing.

i. Objectives

- Verify that an authenticated user
  - has access to the connected PN web service when authorised by the PN DDP
  - does not have access to the connected PN web service when not authorised
- Verify that an authenticated user
  - has access to a remote PN web service when authorised by the remote PN DDP
  - does not have access to a remote PN web service when not authorised by the remote PN DDP

ii. SV requirements covered:

- Req.4.4, Req.4.5, Req.4.10, Req.4.11, Req.4.12, Req.4.13, Req.4.14, Req.4.15, Req.4.16, Req.4.17

iii. Additional requirements and assumptions

b) Test Readiness

i. Implementation requirements

These tests assume:

1. User Data is federated at BMM level
2. A DDP is available on both the PNs and setup for less access rights on the ship voyage information service for trUser than for trSuperUser. Ideally one PN will be less restrictive than the other PN on data filtered, so that the comparison between two different DDP is also possible.
3. The voyage information service is implemented and integrated

These tests assume the following test cases were successful:

- (1) Connectivity
- (2) Track data and information exchange

ii. Test environment

2. Tools
   1. no specific tool required

3. Input Data
    1. none

c) Test Procedures

For these Tests, we perform SN to PN tests.

ID	Description	Criteria	Comment
DDP_1	**Filtered access to data, locally:** trUser and trSuperUser are logged in. trUser requests voyage information on a ship belonging to the PN they are connected to.	trFullUser@spa.bmm.org gets more voyage information than trUser@spa.bmm.org does.	
SES_2	**Filtered access to data, remotely:** trUser and trSuperUser are logged in. trUser requests voyage information on a ship belonging to the remote PN they are connected to.	trFullUser@spa.bmm.org gets more voyage information than trUser@spa.bmm.org does.	

Annex 1 – Requirements Traceability

Requirement	Covered By
[Req.1.1] The BMM XMSN Demonstrator shall consist of the following Primary Nodes (see Annex 1 for the census of all the BMM Nodes): *1. Italian Primary Node : Interagency* *2. French Primary Node : Interagency (Navy, Customs, Maritime Affairs)* *3. Spanish Primary Node 1 : Armada* *4. Spanish Primary Node 2 : Guardia Civil* *5. Portuguese Primary Node (double instance) : Marinha & Guarda Nacional Republicana* *6. Maltese Primary Node : Armed Forces*	By Design
[Req.1.2] The BMM XMSN shall comprise the following Secondary Nodes. A secondary node shall be connected either to its national Primary Node through a Local Area Network or directly to other (foreign) Primary Nodes through the BMM Network, as indicated in Annex 1.	CT and design
[Req.1.3] Primary nodes shall be able to assure services to Secondary Nodes, granting access to available web portal adapted to BMM requirements, and providing access to BMM SBCMP and related services to authorized BMM Secondary Nodes.	CT/More
[Req.1.4] The BMM XMSN Network shall be a broadband TCP/IP network implemented through https/ssl protocol over the Public Internet.	CT
[Req.1.5] The BMM XMSN Network shall take into account the source data rates expressed in the census of the Primary Nodes and Secondary Nodes (Annex 1).	CT
[Req.1.6] The BMM XMSN Network shall provide basic information security measures based on https/ssl. One BMM Partner shall be designed to ensure the delivery of the required certificates.	CT
[Req.1.7] Each Primary Node has to assign one skilled technical administrator to ensure Network Administration (@IP, certificates, ...) in order to allow maximum flexibility of the network configuration and scenarios execution	CT – specified in Test Data Set-up
*[Req.1.8] Within the scope of BMM XMSN demonstration, BMM primary nodes should provide the following reduced set of **services,** responding to the broad definition of the BMM Service Categories defined in the BMM CCTP:* • ***Common Services*** *S1. Track data / information exchange (COP service, implementation of CS2 defined in the CCTP);* *S2. Regional correlation (COP service, implementation of CS2 defined in the CCTP);* *S3. Wide Area Rapid Mapping (Satellite service, implementation of CS5 defined in the CCTP);* *S4. Data Augmentation Service (Limited implementation of CS1 defined in the CCTP).*	

Requirement	Covered By
• ***Core Services*** *S4. Web Portal and WebGIS (Community services);* *S5. Identity & Access Management (Information Assurance Services);* *S6. Service Registry Management (Service Management & Control services);*	
[Req.1.9] The Web Portal will provide BMM users with a secure and user-friendly Web Based front-end application, which enables them to dynamically and interactively access to a wide range information and application services provided within BMM Network.	WUG
[Req.1.10] The WebGIS Service will provide support for accessing and exploiting raster, vector and satellite maps within BMM Network, according to the (WMS 1.1.1 or better) and WFS standards.	WUG
[Req.1.11] The Identity & Access Management will assure the respect of BMM Authentication and Authorization policy, maintaining a federated database of identity, where username, password and role are assigned to each user.	WUG/More
[Req.1.11b] The Service Registry Management will ensure a standard and common definition of BMM web services and will verify that BMM users are able to invoke services and to access data according to a pre-defined BMM Data Distribution Policy.	
[Req.1.12] The Track Data & Information Exchange Service will assure the capability to provide BMM Users (both local and remote) with current-time and/or historical track information available from connected National Systems and associated to targets already identified by the requesting entities (by IMO number, Ship Name, MMSI) in an area of interest.	TM
[Req.1.13] The Regional Track Correlation Service will assure the capability to provide BMM Users (both local and remote) with current-time and/or historical track information correlating to track information held by requesting entities on the base of the available data from connected National Systems and of pre-defined levels of confidence and integrity.	NA
[Re.1.14] The Wide Area Rapid Mapping service will provide BMM Node Users with the capability to exchange Satellite Geospatial Products (including SAR images) available from their respective National Systems, over an Area of Interest or a Track of Interest.	WAS
[Req.2.1] The BMM demonstrator (XMSN), shall be composed of the following main standards components: • *Identity Access Management, implementing standards like SAML / XACML procedures and a shared Directory according to the LDAP standard;* • *Service Management with simple services publish and discovery logic based on a UDDI Standard Service Registry* • *System Portal with Web Interface according to commonly adopted standards like JSR168, JBR268 and WSRP* • *WebGIS embedded in the Portal at Web Interface Level and*	CT/WUG/More

Requirement	Covered By
implementing WGS84 coordinate system, as well as the most commonly adopted standards for maritime data visualisation (eg. AIS visualisation standard) • *Map and images management, according to OGC standards* • *Standard SOA architecture based on web-services technology operated according to a synchronous (request-reply pattern for instance) and asynchronous (publish and subscribe pattern for instance) through a SOAP over HTTP / HTTPS protocol stack* • *Application Server environment J2EE/JEE or compatible hosting a reduced set of common services:* o *Track data & information exchange* o *Regional track correlation* o *Wide area mapping* • *Temporary DB for BMM tracks storage, based on COTS Relational Spatial Enabled Databases like PostGIS, MySQL, Postgre SQL or Oracle*	
[Req.2.2] With reference to the reference architecture of the XMSN, reported in Figure 2 and described in Req. 2.1, the INT_01 Interface (from Primary Node to Primary Node) shall be implemented through: • *interface between other Primary nodes and the Service Registry component (UDDI interface)* • *interface between the Primary nodes and the Map Server (at least for Satellite images exchange)* *The INT_01 Interface shall be mandatorily implemented by all the Primary Nodes participating in the XMSN demonstrator*	Design
[Req.2.3] With reference to the reference architecture of the XMSN, reported in Figure 2.1 and described in Req. 2.1, the INT_02 Interface (from Secondary Node to Primary Node) shall be implemented through: • *Direct interface between external users and the Web Portal of the Primary Node (Browser Interface)* *All BMM Primary Nodes shall implement the INT_02 interface for the sake of local users connections to the Node. However, when they give a service access to dependant Secondary Nodes as listed in Annex 1, the BMM Primary Nodes shall implement the INT_02:*	Design
[Req.2.4] The BMM nodes involved in the XMSN demonstrator as Primary Nodes, shall implement nation-specific interfaces (based on SOA interfaces or Point-to-Point interfaces) towards the following available national systems and assets: • *Italian Primary Node :*	Design

Requirement	Covered By
○ *National Coastal Surveillance System;* ○ *National VTMIS* ○ *National AIS network;* ○ *ARES reporting system (Italian commercial cargo ship reports)* ○ *VMS, (Italian fishing vessel reports)* ○ *COSMO Sky-Med Ground Station (Satellite SAR Images)* • *French Primary Node:* ○ *National Maritime Surveillance and State Action at Sea Coordination System - SPATIONAV through OCEAN system interface ((correlated radar & AIS tracks).* • *Spanish Primary Node 1 (Armada):* ○ *National MSA System (SIVICEMAR).* • *Spanish Primary Node 2 (Guardia Civil):* ○ *SIVE (Maritime Border Surveillance and Protection System);* ○ *National AIS network.* • *Portuguese Primary Node (two instances : Marinha & Guarda Nacional Republicana):* ○ *Coastal and Açores Surveillance System – COSMOS (Marinha);* ○ *Coastal Surveillance System – SIVICC (Guarda Nacional Republicana).* • *Maltese Primary Node (Armed Forces):* ○ *National VTS*	
[Req.2.5] With reference to services to implement in the BMM XMSN demonstrator (see Req.2.1), the Primary Nodes shall be subject to the following exclusions and limitations: • *Italian Primary Node:* ○ *No exclusions and limitations* • *French Primary Node :* ○ *No exclusions and limitations*	Design

Requirement	Covered By

• *Spanish Primary Node 1 (Armada):*
  ○ *No exclusions and limitations*
• *Spanish Primary Node 2 (Guardia Civil):*
  ○ *One limitation : the vessel tracks of the SIVE system are classified and during the demonstration therefore the SIVE tracks will be fake tracks*
• *Portuguese Primary Node (Marinha & Guarda Nacional Republicana):*
  ○ *Exclusions : to be confirmed (NLT May 20th)*
  ○ *Limitations : Satellite images availability is under analysis, to be confirmed (NLT May 20th)*
• *Maltese Primary Node:*
To be defined	

[Req.3.1] The following table defines the specifications of communication requirements for BMM nodes that will be involved in the BMM XMSN demonstration.	Design
[Req.3.2] The XMSN demonstrator shall be capable to implement federated Identity & Access Management based on synchronised User Credential and BMM Primary Node available list of Service Registry according to LDAP and UDDI standards. *Thus, in the XMSN environment, BMM Primary Nodes shall be able to handle a static and pre-defined Data Distribution Plan resulting from the above mentioned registries.*	UDL
[Req. 3.3] Each BMM partner shall be identified on the XMSN network by a unique username, password and role. Username, password and roles will be set in a pre-defined and static table.	WUG
[Req.3.4] At each BMM Primary Node, when a BMM user requests access to the BMM network, a User Authentication procedure shall control that username and password are compliant with the value set in the pre-defined user credentials.	WUG
[Req.3.5] At each BMM Primary Node, when an authenticated BMM user asks to invoke a BMM service, a Service Authorization procedure shall look-up the DDP to find the restrictions and / or limitations to the access of the requesting User to services and data, as option, according to its credentials.	SES
[Req. 3.6] The restrictions and limitations of access to the BMM services and data shall consist of:	SES

1

Requirement	Covered By
• *Denied access to one specific BMM service (S1,….S6);* • *Denied access to the different groups of Data Packages (Basic / Sensitive[1]);* • *Denied access to specific types or classes of tracks (by query on BASIC_ID_DATA)* • *[**Optional**] Limitations in access on specific track data fields (Basic_ID_Data, Basic_Voyage_Data, Historic_Data, Other_Data).*	
[Req. 3.7] BMM XMSN User Credentials will be in accordance to the following definition: • ***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 exchange 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* *With reference to the BMM XMSN demonstrator, the following table provides the User Credentials of involved partners*	Design
[Req.4.1] The User management shall assure the creation and maintenance of a BMM User Register.	WUG
[Req.4.2] The User management shall be able to add new users, delete existing users and modify users attributes.	WUG
[Req.4.3] At each BMM User shall be at least assigned a unique username and password and a BMM role.	WUG
[Req.4.4] BMM roles shall be set in accordance to a pre-defined ~~Data~~ Service Distribution Policy	WUG
[Req.4.5] BMM user role shall assign BMM services and level of data that the user may access.	

Requirement	Covered By
[Req.4.6] User management shall be based on a federated approach, assuring that BMM nodes share the same BMM User Register data.	UDL
[Req.4.7] XMSN User Register shall comply with LDAP standard	Design
[Req.4.8] BMM XMSN users credentials shall be set on a pre-defined and static table that will be implemented in the BMM XMSN nodes.	WUG/More
[Req.4.9] When a BMM user is logging to a BMM node, a user authentication function shall validate the username and password, and shall permit / refuse the access to the BMM network, in accordance to the user data included in the User Register.	WUG
[Req.4.10] Exchanging of authentication data shall be based on SAML/XACML standard.	NA, was changed to WS Security UserToken profile
[Req.4.11] The service management shall enable the discovery, publication, addressing and invocation of BMM services, ensuring their location and access to the relevant meta-data (tokens, wsdl and xsd) by the internal and external users.	UDL
[Req.4.12] The service management shall be able to add new services, delete existing services and modify service attributes.	UDL
[Req.4.13] The service management shall implement a server registry. The implementation shall be compliant with UDDI standard.	UDL
[Req.4.14] Being BMM based on a federated service management approach, BMM service registry shall consist of several UDDI nodes deployed on the different BMM primary nodes.	UDL
[Req.4.15] The service management shall support the implementation of simple methods coordinating Service discovery and location, Identity & Access Management and actual service provision over the BMM network.	UDL
[Req.4.16] Service authorization shall be based on SAML / XACML request-response language.	NA, was changed to WS Security UserToken profile
[Req.4.17] The SEA function shall process requests from authenticated users applying the limitations and restrictions applicable to the User according to the established DDP and the user credentials / role.	SES
[Req.4.18] Web Portal shall implement access control procedures on https.	WUG
[Req.4.19] Web Portal shall validate user credentials (username and password) of BMM users accessing the portal.	WUG
[Req.4.20] When a BMM user is authenticated, a web portal session shall be assigned to the user.	WUG
[Req.4.21] Exploiting the WebGIS capabilities, the Web Portal shall assure the visualization of raster, vector and satellite Maps.	WUG

Requirement	Covered By
[Req.4.22] BMM web portal users shall be able to select the layers that can be presented on maps.	WUG
[Req.4.23] BMM web portal users shall be able to select an object on maps and visualize a table representing main object attributes.	WUG
[Req.4.24] BMM web portal users shall be able to perform pan and zoom actions.	WUG
[Req.4.25] BMM Nodes shall access the web portal via web browser Explorer 7 (or newer) or Firefox 3.5 (or newer).	WUG
[Req.4.25 bis] BMM Secondary Nodes, accessing BMM Network via a web portal exposed by a BMM Primary Node, should be able to manually insert data on the BMM scenario (optional)	WUG
[Req.4.25 ter] BMM Primary Node shall be able to publish the data inserted by a BMM Secondary Node via web portal (optional)	WUG
[Req.4.26] Web Portal, WebGIS and Map manager shall be able to support, import, manage and display standard maritime charts, represented in common GIS file format as Geo Tiff 6.0, Geo Tiff + tfv, etc.	WUG
[Req.4.27] Map requests shall be implemented according to the OGC Web Map Service 1.1.1 (or better) standard protocol.	WUG
[Req.4.28] Requests for geographical features shall be implemented according to the Web Feature Service Interface Standard (WFS).	WUG
[Req.4.29] BMM tracks shall be displayed on BMM maps that use WGS84 standard.	WUG/More
[Req.4.30] BMM Nodes shall be able to time stamp all exchanged data among nodes, using Coordinated Universal Time (UTC).	TSW
[Req.4.31] BMM Nodes shall be able to geographically reference on a global scale all exchanged data among nodes, using the World Geodetic System 1984 (WGS-84).	WUG/TSW
[Req.4.32] The TM function shall exchange track data over point-to-point (or local SOA) interfaces with Nation-specific legacy systems, and shall adapt the exchanged data to the BMM data model.	Design
[Req.4.33] – [Optional] - The TM function shall provide the Node operators with basic operations like the visualisation, assignment or modification of a track number, the analysis, modification or deletion of an existing track attributes.	TM
[Req.4.33a] The TEX function shall perform the basic operations supporting the exchange of track data among BMM nodes: • *Receive and handle the Local or Remote Users requests of services concerning track exchange*	TM

Requirement	Covered By
• *Follow-up on-going services requests* • *Process received BMM tracks from other nodes and extract the track data according to the BMM data model, storing the track data into the Node Track Temporary Data Base* • *Execute the necessary functions according to the requesting services and involving the TS and TAC functions (see §5.5)* • *Prepare BMM tracks for transmission to requesting nodes, according to the BMM data model, retrieving the track data from the Node Track Temporary Data Base*	
[Req.4.34] The TSAC function shall perform the basic operations supporting: • *synchronisation of tracks known different time of validity* • *association of tracks (i.e. based on static or semi-static parameters matching)* • *correlation of tracks, meaning the association of partially unknown tracks on the base of dynamic (kinematic) parameters matching.*	TM
[Req.4.34a] The TSAC Synchronisation function shall be capable to align the input track data to a common reference time instant, implementing standard prediction algorithms or, if necessary to recover large synchronisation gaps, back propagation and forward propagation algorithms	Not tested as such only result visualised
[Req.4.34b] The TSAC Association function shall be capable to associate input and own tracks presenting a firm matching in static or semistatic parameters like MMSI, IMO Number, Ship Name and Call Sign, etc. • *The association function shall mark associated tracks as such, and merge them if requested.* • *A suitable logic shall be applied to handle discrepancies in associated tracks data, based on the trustworthiness and accuracy of the respective origin.*	Not tested as such only result visualised
[Req.4.34c] The TSAC Correlation function shall be able to correlate input tracks with own tracks matching in dynamic parameters like position / course / speed and their expected predictions / propagations, defining and assessing a confidence index of the correlation that will be used to indicate the usability of the correlation results. *The correlation can be based on a mix of deterministic, statistical methods as well as on adaptive tracking techniques, taking into account the specific characterisation of the different targets and a maximum time span among the tracks to be correlated up to several hours.*	Not tested as such only result visualised
[Req.4.35] The RMM function shall perform the basic operations supporting the exchange of satellite mapping products,(represented in common GIS file format as Geo Tiff 6.0, Geo Tiff + tfv, etc), among BMM	WAS

<table>
<tr><th>Requirement</th><th>Covered By</th></tr>
<tr><td>nodes:
Receive and handle the Local or Remote Users requests of services concerning rapid mapping
Follow-up on-going services requests until the requested products are transmitted to the requesting entities</td><td></td></tr>
<tr><td>[Req. 5.1] In order to demonstrate the target level of interoperability within XMSN, each Node shall define and implement the appropriate service meta-data (in terms of WSDL and XSD) according to the established requirement and the Data Model defined in §6.</td><td>Design</td></tr>
<tr><td>[Req. 5.2] Track Data & Information Exchange Service – Web Services Definitions</td><td>TM, EAL</td></tr>
<tr><td>[Req.6.1] The BMM XMSN Demonstrator shall implement the following reduced Data Structure.</td><td>Design</td></tr>
<tr><td>[Req.7.1] The following table correlates the measure of success of XMSN Common Services with the Quality Requirements that apply to the BMM XMSN demonstrator environment.

<table><tr><th>Service</th><th>Measure of Success</th></tr><tr><td>Regional track correlation service</td><td>Maximum number of tracks

Timing for data availability (time period from the service request to the service provision)

Source data type (AIS, LRIT, VMS, etc.)

Track streaming update time

Detection and Classification Capabilities</td></tr><tr><td>Wide Area Rapid Mapping service</td><td>Covered Area

Timing for data availability (time period from the service request to the service provision)

<s>Satellite Scheduling Capabilities</s>

Type of Satellite Imagery</td></tr></table></td><td>TM, EAL</td></tr>
</table>

Annex 2 – HelloWorld WSDL

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions name="HelloService"
  targetNamespace="http://www.ecerami.com/wsdl/HelloService.wsdl"
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:tns="http://www.ecerami.com/wsdl/HelloService.wsdl"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">

  <message name="SayHelloRequest">
    <part name="firstName" type="xsd:string"/>
  </message>
  <message name="SayHelloResponse">
    <part name="greeting" type="xsd:string"/>
  </message>

  <portType name="Hello_PortType">
    <operation name="sayHello">
      <input message="tns:SayHelloRequest"/>
      <output message="tns:SayHelloResponse"/>
    </operation>
  </portType>

  <binding name="Hello_Binding" type="tns:Hello_PortType">
    <soap:binding style="document"
      transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="sayHello">
      <soap:operation soapAction="sayHello"/>
      <input>
        <soap:body
          encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
          namespace="urn:examples:helloservice"
          use="encoded"/>
      </input>
      <output>
        <soap:body
          encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
          namespace="urn:examples:helloservice"
          use="encoded"/>
      </output>
    </operation>
  </binding>

  <service name="Hello_Service">
    <documentation>WSDL File for HelloService</documentation>
    <port binding="tns:Hello_Binding" name="Hello_Port">
      <soap:address
        location="SPECIFY YOUR PN URL BINDING"/>
    </port>
  </service>
</definitions>
```

Annex 3 – Track template for Common Services Testing

mmsiNumber: following MMSI standard, starting with 2 (Europe MID) and remaining 8 digits, make sure there is no collision with existing ship
shipName: ***PN*_TEST_SHIP**
imoNumber: random 6 digits and 7th digit set to the corresponding check digit, as per IMO standard

navigationalStatus: vary the value amongst the different statuses defined
sensor:
position: in the PN's area and in the sea
reliability: **1 = very high confidence, verified data, 2 = high confidence, 3 = confident, 4 = low confidence, 5 = very low confidence**
receivedAt: generated by the PN
timeOfContact: generated by the PN

originCountry: generated by the PN, should be the user country in case of manual track injection
originEntity: generated by the PN, should be the user organisation in case of manual track injection
originId: TBD

shipType: should follow the ship type AIS standard
courseOverGound: any sensible value
rateOfTurn: any sensible value
speedOverGround: any sensible value

trueHeading: any sensible value

Ship Information

The following information should be available:
beam
country
mmsiNumber
imoNumber
callSign
name
hullMainColor
ispsCode
length
width
maximumSpeed
numberOfEngines
numberOfMasts
shipPhoto
flag
shipType
shipCrew
shipCrewMember

Annex 4 – List of contacts for Testing

Title	Name	email
PT PN TR	Fernando Sérgio Bryton Dias Marques	dias.marques@marinha.pt
PT PN Industry	KnowledgeWorks team	bmm@knowledgeworks.pt
SP1 (Armada) PN TR	Antonio Jesús Garcia MELGAR	agmelgar@fn.mde.es
SP1 PN Industry	Rosa Fuentes	rfuentes@indra.es
SP2 (Guardia Civil) PN TR	Conrado Ávila Alexandre	conradoa@guardiacivil.es
SP2 PN Industry	Juan Caja	aswmovilidadjc@amper.es
FR PN TR	Fabrice LESAINE	fabrice.lesaine@dga.defense.gouv.fr
FR PN Industry	Patrick Leroy	plr@eurocis.fr
IT PN TR	Nicola FRACCASCIA	nicola.fraccascia@marina.difesa.it
IT PN TR	Sergio Ciannamea	sergio.ciannamea@marina.difesa.it
IT PN Industry	Eng. Domenico RECCHIA	drecchia@selex-si.com
TWG Lead	Osvaldo Broggi	osvaldo.brogi@marina.difesa.it
TWG Technical Lead	Stefano Sorge	s.sorge@alice.it
Technical Reviewer	Thomas Lefort	leforthomas@gmail.com

Not directly concerned but kept in copy:

Laurent Michoux laurent.michoux@dga.defense.gouv.fr

Olivier Plessiet olivier.plessiet@dga.defense.gouv.fr

Caprian Borg caprian.borg@gov.mt

Dyonissios CHRISTOFILIS sbc@yen.gr