

Request for Services

SC14/EMSA/OP/08/2011

SSN software updates for the second production release of SSN in 2015 (code name "SSN v3.1") including the implementation of an interface between SafeSeaNet and the Common Emergency Communication and Information System (CECIS)

Objectives and technical specifications

Table of Contents

1. Background	4
1.1 Tentative release and deployment plan for SSNv3 in 2015	4
1.2 SSN CECIS interface.....	4
2. Objective of the contract.....	5
3. High-level business requirements for the SSN CECIS interface	5
4. Assessment of changes required and impacts to Central SSN due to the implementation of the SSN CECIS interface	6
5. Contract phases and deliverables.....	6
5.1 Kick-off (tele-conference).....	7
5.2 Design	7
5.3 Development and tests	7
6. Conditions of execution	8
6.1 Schedule.....	8
6.2 Tests by the contractor	9
6.3 Scope of tests by the contractor:	10
6.4 Test environment for software pre-view	12
6.5 Acceptance procedure.....	12
7. Service requirements	13
7.1 Functional requirements for SSN CECIS interface	13
7.1.1 Message format.....	13
7.1.2 Access	14
7.1.3 Push of POLREP compliant with the IR protocol	14
7.1.4 Push of POLREP compliant with the "Alert" V1 protocol.....	15
7.1.5 Central SSN web interface	16
7.1.6 Avoiding double distribution to CECIS	17
7.1.7 SSN User Management console	18
7.2 Non-functional requirements for SSN CECIS interface	18
7.3 Other requirements concerning SSN updates	18
7.3.1 Central Ship Database.....	18
7.3.2 Amendment of EIS application logs.....	22
7.3.3 Improvement on SSN web interfaces	22
7.3.4 Improvement of the user management console.....	24
7.3.5 SSN GI –vessel position visualisation	25
8. List of appendices	26

Definitions and acronyms

CECIS: Common Emergency Communication and Information System

ERCC: Emergency Response Coordination Centre

EU: European Union

IdM: EMSA Identity Manager System

MARPOL: International Convention for the Prevention of Pollution from Ships

MS: Member State

NCA: National Competent Authority

POLFAC: POLLution FACilities

POLINF: POLLution INFORMATION

POLREP: POLLution REPORT

POLWARN: POLLution WARNING

SSN: SafeSeaNet

1. Background

1.1 Tentative release and deployment plan for SSNv3 in 2015

This Request for Services is related to the SSN software updates for the second production release of SSN in 2015 (code name "SSNv3.1") including the implementation of an interface between SafeSeaNet and the Common Emergency Communication and Information System (CECIS)

The tentative planning of SSN releases and their deployment in 2015 foresees the following releases:

1. Release identified as "SSNv3.0" [Tentative production date: Week 15 (April 2015)]:
 - Already covered by SC#9 and SC#10 under EMSA/OP/08/2011
2. Release identified as "SSNv3.1" [Tentative production date: Week 31 (July 2015)]:
 - Compliant with this RFS and including the hotfixes for the resolution of the non –critical bugs which are to be still unresolved until the 15th of May 2015
3. Release identified as "SSNv3.2" [Tentative production date: Week 40 (October 2015)]:
 - Compliant with the STMID RFS (SC#13) plus other RFS.

1.2 SSN CECIS interface

In accordance with Directive 2002/59/EC as amended, Coastal Stations are obliged to distribute information about incident and accident posing a potential hazard to shipping or a threat to maritime safety, the safety of individuals or the environment. Such Incident Reports shall be distributed via SSN to the potentially affected Member States (art. 16, 17 and 21).

The pollution incident report (POLREP) is a widely employed form to exchange information with other interested parties whenever the environment is affected or is likely to be affected after a confirmed or possible spill or an illegal discharge. POLREP is composed of 3 sub-messages named POLWARN (aiming at warning recipients), POLINF (in order to inform by providing additional information) and POLFAC (for requesting international assistance). Note: Refer to the "SafeSeaNet - Incident Report Guidelines" available at: <http://www.emsa.europa.eu/ssn-main/documents/technical-documentation.html> for more information.

The SSN High Level Steering Group (HLSG) agreed that:

- SSN will be used for reporting POLWARN and POLINF messages.
- The Common Emergency Communication and Information System (CECIS), managed by DG ECHO, will be used to report POLFAC messages.
- To avoid double reporting, POLWARN and POLINF should be provided from SSN to CECIS through a link between both systems.

The overall objective is to:

- Establish one single reporting mechanism for avoiding multiple reporting to SSN and CECIS, minimising the administrative burden for the reporting parties for matters related to pollution.
- Support the EU/MS emergency response services to provide effective response to maritime incidents.

The link to CECIS should serve the needs of:

- Reporting parties (e.g. MRCC, VTs etc.) responsible for the completeness and accuracy of the POLWARN and POLINF information transmitted to SSN,

- Relevant MS authorities (such as SSN NCAs) responsible for receiving, validating and processing the POLWARN and POLINF information transmitted by the reporting parties,
- CECIS National users responsible for providing effective response to maritime pollution,
- ERCC users supporting the response to maritime disasters coordinating the resources from the countries participating in the Union Civil Protection Mechanism,
- EMSA services responsible for validating the data quality of the information exchanged between MS through SSN.

Note: CECIS users may also, in parallel, receive POLWARN and POLINF information from emails through the existing Incident Report (IR) distribution tool of SSN (if they are identified as email recipients in the SSN management console).

2. Objective of the contract

The objective is to design, implement and test an upgrade of SSN which will feature all the software updates foreseen for release SSNv3.1 (including the SSN CECIS interface as introduced above).

The upgrades will comply with the specific requirements provided below in this document in the chapter 7. More over the software to be delivered shall include bug fixes of all the defect artifacts affecting SSN v3.0 production release. Exclusion of some artifacts could be proposed by the contractors and agreed with EMSA if the justification for the exclusion is deemed sufficient.

The cost of resolution of the defect artefacts bugs (those not under warranty) will be covered by the on-going SC#12.

3. High-level business requirements for the SSN CECIS interface

At its meeting of 23 June and 2 December 2014, the HLSG agreed on the following technical options:

- SSN will automatically “push” all the POLWARN and POLINF Incident Report messages to CECIS when notified to SSN. This will apply regardless if the data provider requested that the Incident Report is distributed and not.
- Any update or feedback to the original POLREP Incident Report message reported in SSN will be automatically “pushed” to CECIS. The data from SSN will be processed by CECIS and made available to its users.
- The message will be sent to CECIS whatever interface (web or machine to machine) or protocol is used for notifying the POLWARN and POLINF Incident Report message. In this regard, POLREPs can be provided to SSN using two different protocols (refer to SSN XMLRG version 3.01):
 - Incident Report messages (MS2SSN_IncidentDetail_Not and related messages) compliant to V2/V3 protocol, and;
 - Alert messages (MS2SSN_Alert_Not and related messages) compliant to V1 protocol.

4. Assessment of changes required and impacts to Central SSN due to the implementation of the SSN CECIS interface

The SSN2CECIS interface shall be implemented utilising the following messages (already foreseen and implemented in SSN)

1. SSN2MS_IncidentDetail_Tx.xml message (used for pushing Incident notifications that SSN has previously received from a data provider)
2. SSN Receipt (used by CECIS to report back to SSN the successful reception of a Polrep notification distributed to CECIS)

Subject to further contractor analysis and confirmation and considering the detailed requirements presented in the chapter 7, the following observations are made:

1. The implementation of the automatic distribution of all the POLREPS to CECIS implies that the IR distribution instructions provided by the original provider shall be "overruled" to ensure that (according the wording in the REQ_3) CECIS (*configured as an POLREP incident recipient under "European Commission"*), will receive the notifications pushed by SSN.
2. With reference to the requirements in chapter 7, the business logic and software of the SSN EIS application need to be amended to comply with the business rules introduced in the **SSN2CECIS_REQ_3** and **REQ_4**. In this respect:
 - a. Incident notifications delivered to SSN via the v2 end point should be delivered to incident reports recipients:
 - using the v2 end-point and a v2 compliant SSN2MS_IncidentDetail_Tx.xml message
 - using the v3 end-point and a v2 compliant SSN2MS_IncidentDetail_Tx.xml message
 - b. The requirement SSN2CECIS_REQ_4 requires a change in the way the SSN processes POLREP incidents received via v1 Alert protocol. The requirement refers to the processes to:
 - Retrieve the content of POLREP notifications provided by MS to SSN using the v1 Alert protocol
 - Based on the data mapping proposed in Appendix A, marshal the SSN2MS_IncidentDetail_Tx.xml message and distribute it to POLREP incident recipients under "European Bodies" through the end-point they use and in the proper format. It is important to note in this respect that CECIS shall be configured as an Authority utilising the v3 end-point.
 - c. The textual interface shall be also amended for incident report submission and distribution in line with the requirements SSN2CECIS_REQ_3 and REQ_4.

5. Contract phases and deliverables

The software updates required for the SSNv3.1 will be based upon the software code delivered for SSNv3.0 which shall be appropriately modified to address the SSNv3.1 requirement here-in. In order to meet this deadline the software for SSNv3.1 should be received in as early as possible (beginning of June) to be able to be deployed in production in July 2015 following a full SAT cycle including regression, eventual corrections for the issues to be detected during the SAT and

verification by EMSA during a second SAT run. Due to this tight deadline the contractor is invited to clearly indicate in the offer the requirements that cannot be implemented in the required timeframe (refer to chapter 6.1 below) taking into account that the implementation of the requirements marked as Priority 1 (which include those related to the SSN CECIS link and Central Ship Database) cannot be delayed.

5.1 Kick-off (tele-conference)

Before the kick-off meeting the contractor will deliver a detailed execution plan for the contract (including a planning and update of the SSN EIS Project Quality Plan).

The meeting should take place within one working day after the contract's signature.

5.2 Design

The purpose of this phase is to design the software, including functionalities, business rules, data model, user interface, system interfaces, architecture, and database model.

The design documentation to be delivered by the contractor will include as a minimum:

- a. An updated version of the Software Requirement Specification (SRS) of SSN,
- b. An updated version of the Software Design Specification (SDS) of SSN, including the system architecture, use cases and business rules, database model, web interface design including mock-ups, etc.
- c. An updated version of the Software Test Plan (STP) of SSN, covering both the system-to-system and web interfaces for all new or changed components

The SRS should be delivered at the kick-off meeting.

EMSA will review the design documentation delivered by the contractor and provide the contractor with its comments and/or reservations within 5 working days from the date of delivery of the design documents. The contractor will be required to revise the design documentation to address EMSA's comments and/or reservations. The revised design documentation shall be submitted to EMSA within a timeframe established by EMSA.

The design phase will be considered concluded when the contractor and EMSA reach an agreement on the design documentation and finalised versions have been delivered to the Agency. However it is well understood that due to timing constraints the formal finalisation of the design will take place in parallel with the software implementation.

5.3 Development and tests

The purpose of this phase is to develop the new version of SSN according to the design documentation as well as undertaking the necessary testing and correction to ensure that the deliverables meet the requirements and are in line with the design documentation.

The documentation to be delivered by the contractor includes as a minimum:

- a. Software source code,
- b. Software binary,
- c. On request from EMSA: Virtual machine containing the software,
- d. Factory Acceptance Test (FAT) reports and any updates of the Software Test Plan (STP),
- e. Updated version of the SSN Installation and Configuration Manual (ICM) including installation sequence, configurations, etc.,

f. Applicable scripts:

- Database scripts,
- Configuration and deployment scripts to perform the weblogic server installation. These should use WLST and properties files that can be edited by EMSA depending on the installation environment. JDBC data source configurations should be delivered in a separate script,
- Scripts for data migration,

g. Update of the User Interface Manuals (UIM-Central SSN and UIM-MSS guide),

h. Release and Deployment Plan. This document should follow EMSA Release and deployment template.

A draft of documents (d) shall be delivered for review at least 1 week before the delivery date of the software.

The final version of the Software Test Plan (STP) and the FAT report must be delivered with the first software delivery.

For each software delivery, the items (a), (b), (d), (e) and (f) must be delivered.

The delivery must be driven by release and not by contracts. This means that all the functionalities and bug corrections that go to production in the same release must be delivered at the same time and independently of the contracts that they are bound for.

Delivery is considered concluded when a successful installation of the software has been executed on EMSA's acceptance environments using the software source code delivered by the contractor.

6. Conditions of execution

6.1 Schedule

The schedule is to be provided by the contractor in the offer and agreed with EMSA at the kick-off meeting. The schedule in the offer must at least meet the maximum dates as indicated in the table 1 below.

Milestone	Date	Tentative calendar date	
Signature of the contract	T0	12/05/2015	Contract milestone
Kick-off meeting (as introduced in chapter 5.1)	T1 = T0+1 day	13/05/2015	
Delivery of design documentation (as introduced in chapter 5.2) and the amended test plan	T1=T0+1 week	20/05/2015	Contract milestone

Milestone	Date	Tentative calendar date	
Delivery of development and tests phase (as introduced in chapter 5.3). New version of SSN tested by the contractor (2 runs of FATs minimum) and running on EMSA environments.	T2=T0+4 weeks	10/06/2015	Contract milestone
Positive acceptance by EMSA	T3=T0+7 weeks	01/07/2015	A full SAT cycle will be executed. It will include regression, followed by the eventual corrections for the issues to be detected during the SAT and another verification by EMSA during a second SAT run

Table 1: Project's schedule and contract milestones

6.2 Tests by the contractor

Keeping in mind the provisions for the FAT as described in the contract Project Quality Plan (PQP), the following specific requirements are applicable:

1. Before the contractor formally delivers software to EMSA for the acceptance procedure, it shall ensure that all tests required by the development cycle have been successfully completed.

For this purpose, the Contractor:

- a) Should conduct internally a Test Readiness Review¹ (TRR);
- b) Shall conduct a Factory Acceptance Test (FAT)²;

¹ Test Readiness Review I (TRR I) is a formal review, conducted by the Program Manager (PM) appointed by the contractor, signifying the Component Validation and Integration portion of the system or system component under development is complete and recommends that the system/component shall move into the Factory Acceptance Testing. The results of the TRR will demonstrate that each individual component and the system where the components belong are developed or configured in accordance with the approved design and function properly to meet specified requirements.

- c) Shall provide EMSA with access to a software "preview" site to track that all the changes made in the SSN web interface meet the agreed specifications (see chapter 6.4).
2. EMSA staff can be present at the FAT to obtain evidence of the successful completion of the activity. Only after EMSA has accepted the results of the FAT (based on the FAT report) is the contractor allowed to deliver the software for pre-SAT³ and SAT.
3. The FAT shall be executed in accordance with the Software Test Plan (STP – see section 3.2) and as agreed with EMSA. In this respect the STP should be delivered to EMSA at the planned finish of the design phase (as stated in section 5.2) and an update be delivered at least three weeks before the delivery of the software (as stated in section 5.3).
4. During the FAT, the contractor shall perform all the installation steps as detailed in the ICM for the release(s) being delivered.
5. The FAT report shall:
 - a) Describe, and justify the suitability of, the characteristics and scale of the FAT environment.
 - b) Describe all the issues found and reported by EMSA during the preview of the software and indicate if they have been corrected.
 - c) Include proofs that full regression tests of SSN components affected by the delivery have been conducted.
 - d) Describe all the aspects of the delivery that are major or blocking (refer to the definitions in chapter 6.5).
6. With the FAT reports, the contractor will provide all the tests scripts used to automate test cases along with instructions enabling EMSA to re-use the scripts.

6.3 Scope of tests by the contractor:

During the FAT, the system should be sufficiently tested (proper implementation of business rules / functional requirements, performance, security of transactions, load, etc.) before being delivered to EMSA for the acceptance tests.

The goals related to testing of system functions are:

1. Conformance with business rules/functional requirements,
2. Completeness,
3. Correctness,
4. Avoidance of regression errors (impacts to functions of the application that should not be affected by the contracted work).

² The main objective of the FAT is to confirm that the software implemented meet the agreed design specification (functional/ non-functional) and contract requirements, so it could be delivered for installation at EMSA.

³ Refer to the Annex D of the FWC – "Work procedures service level Evolutive Maintenance"

The non-functional goals of the overall testing procedure are the average response time of the system to a request for information and the security of transactions.

The STP should make clear references to the test cases/scenarios that will be executed during the FAT. In this respect the following table provides the minimum requirements with respect to the test goals mentioned above.

Table 2: Minimum requirements regarding the Factory Acceptance Test by the Contractor

Quality Requirement	Quality Criterion	Metric Threshold	Threshold
Completeness	Coverage of requirements	Percentage of requirements listed in chapter 7 below covered by the STP (at minimum one test case, as well as additional test cases if necessary for fully testing the applicability of the requirement)	100%
Completeness	Coverage of business rules	Percentage of business rules, as defined during the design phase, covered by the STP (at minimum one test case, or more)	100%
Completeness	Test Coverage for database tier	Percentage of statements covered in unit or integration test for database tier	>65%
Completeness	Test Coverage for business logic presentation tier	Percentage of statements covered in unit or integration test for business logic and presentation tier	>65%
Correctness	Blocking Issues/FAT	Blocking issues identified in FAT cycle 1	Less than 3
		Blocking issues identified in FAT cycle 2	No blocking issues No regression impacts
Correctness	FAT cycles	Number of attempts to pass FAT criteria	As many as required to eliminate all blocking issues (Min 2 attempts)
Performance	Response Time	Average response time	As per SSN IFCD or agreed with EMSA during the design phase

Referring to the thresholds related to the first four rows of the table above, the percentages mentioned in the "Threshold" column represent the amount of statements covered for each distinct module of the SSN system during the Unit and Integration tests. The Unit or Integration tests to be conducted (of functional or non-functional nature) shall be included in the test plan. The software approval work-flow at contractor site could envision the following three steps (steps a and c below are mandatory, step b optional):

- Unit and integration tests during software development,
- Unit and integration tests during the Test Readiness Review (TRR),
- Unit and integration tests during the Factory acceptance test (FAT).

The values in the table above show the rate of completeness of tests before the start of the FAT. The amount of tests and their nature has to be approved by EMSA and will be described within the test plan document.

6.4 Test environment for software pre-view

For the purpose of the software preview as introduced in the previous chapter , the contractor shall provide EMSA with access to a test environment set up and maintained by the contractor which includes:

- All the software components of the SSN upgraded or altered during the course of this contract; as well as
- The components and system interfaces that shall be integrated and used for pilot projects (e.g. BlueBelt), ancillary modules (e.g. Accident module) or for interfacing SSN with other EMSA applications.

This test environment shall be maintained in operation, as detailed in the FWC between the date scheduled for the start of FATs until the acceptance of the delivery by EMSA. The system will be initially used for executing the FATs and subsequently for testing patches and hotfixes that are to be delivered against bug reports of EMSA during the pre-SAT, the SATs and the 12-month warranty period of the software.

The system configuration will allow testing of the SSN System Interface using the message examples provided in the STP. Furthermore the system will emulate realistically "external" systems interacting with SSN i.e. IMDATE, THETIS, LRITDC, CSN, IdM, MAP (Liferay) and MS NCA applications.

The test environment and the way of "simulating" external systems should be described in the offer in broad lines. The specifications and configuration should be further detailed during the design phase of the system.

6.5 Acceptance procedure

For each delivery, EMSA will provide a formal indication of the acceptance, conditional acceptance or rejection of the delivery to the contractor.

The acceptance procedure will start when the software is available and running in EMSA's test & quality environments.

EMSA will verify that:

- All issues detected in any previous acceptance procedures have been corrected,
- The software conforms with the requirements and with the design specifications,
- The existing components which are not impacted by this contract still conform to their specifications (no regression impacts),
- Implementation best practices have been followed,
- The binaries resulting from the software build in-house are correct and can be used for installing the application in EMSA environments (pre-production and production) and once installed achieve the desired results.

EMSA will classify any issues identified in three different categories reflecting their impact and severity:

1. Blocking issues:

Structural problems or serious issues (functional or technical) considered as limitations of the implementation with very high probability of interfering with the expected result. The contractor will be obliged to correct/execute all issues considered in this category,

2. Major issues:

Problems or issues that do not conform to the requirements or specifications or best practices or considered to be the wrong approach to obtain the result, but for each one of them a workaround or a correction is available. The contractor will be obliged to correct/execute all issues considered in this category,

3. Minor issues:

Changes considered to be a better solution but without a deep impact on the quality of the system. The correction/execution of the issues under this category will be decided on a case by case basis.

Each issue will be identified and described by EMSA and sent to the contractor. All issues will be registered in TeamForge. Appropriate access to TeamForge will be established for the contractor. The contractor is requested to track and monitor the treatment of each issue sent by EMSA. The acceptance tests and the classification of the issues will be determined in collaboration between EMSA and the contractor.

The outcome of the acceptance procedure is positive if no issue is found by EMSA. If issues are found by EMSA during the acceptance procedure, the contractor is requested to immediately correct them and the acceptance procedure restarts from the date of the delivery of the corrected deliverable.

EMSA can decide to conditionally accept the deliverable when some issues remain uncorrected and are not blocking. The condition for that acceptance is that a date for the correction of the remaining issues is defined by the contractor and agreed with EMSA. EMSA will take the decision to conditionally accept the product after evaluation of each remaining issue.

7. Service requirements

In this document, each requirement is given a reference number and identified as "Mandatory" or "Desirable".

Each requirement is given a priority: higher priority "P1", lower priority "P2". The contractor is requested to indicate which requirements with priority P2 can be included in the software to be delivered considering the required schedule (refer to chapter 6.1 above)

7.1 Functional requirements for SSN CECIS interface

7.1.1 Message format

Ref: SSN2CECIS_REQ_1	Priority: P1 Nature: M RFC ref: artfartf13645
The POLREP information will be pushed to CECIS in the form of SSN2MS_IncidentDetail_Tx message as defined in the SSN XML RG v3. This will be done either using the XML or the SOAP interfaces (to be decided by EMSA).	

7.1.2 Access

Ref: SSN2CECIS_REQ_2	Priority: P1 Nature: M RFC ref: artf13645
CECIS will be configured as a SSN user (for receiving PORLEPS) through the SSN user management console. The user account will have location code = EUCOM, and will have an e-mail address.	

7.1.3 Push of POLREP compliant with the IR protocol

Ref: SSN2CECIS_REQ_3	Priority: P1 Nature: M RFC ref: artf13645
<p>The Central SSN will prepare and send a message to POLREP incident report recipients configured under "European Commission" (therefore including CECIS) each time it receives an Incident Report notification (MS2SSN_IncidentDetail_Not) quoting incident type=POLREP through the SSN web interface or the SSN system interface.</p> <p>Note1:</p> <p style="padding-left: 40px;">This will apply regardless if the data provider requested that the Incident Report is distributed and not.</p> <p>Note2:</p> <p style="padding-left: 40px;">This will apply to any kind of Incident Report type POLREP (Update Status=N, U or D, Incident or Feedback)</p> <p>Note3:</p> <p style="padding-left: 40px;">This will apply to any kind of POLREP message, including POLWARN, POLINF and POLFAC (in the case where a MS still sends a POLFAC to SSN).</p> <p>Note4:</p> <p style="padding-left: 40px;">All the organisations/persons created under location code = EUCOM and granted access to receive POLREPs will automatically receive the message "pushed" from SSN via XML/SOAP or email depending on their access rights configuration.</p> <p>The message to CECIS will be considered by SSN in a similar manner as any other SSN2MS_IncidentDetail_Tx message. The distribution status (success or failure) will therefore be reported to the provider in an acknowledgment message (SSN2MS_IncidentDetail_Tx_Ack and via the IR monitoring tool of the SSN Web Interface).</p> <p>In case of a failure in the distribution to CECIS, SSN will activate the ordinary failure management procedure. Therefore, a warning email will be sent to: (i) the dedicated recipient, (ii) an email recipient acting as NCA24/7; and (iii) EMSA MSS (in cc).</p> <p>The data flow is the following:</p> <ol style="list-style-type: none">1. The data provider notifies the POLREP Incident Report either through the Central SSN web interface or via the SSN national system through the SSN system interface (in XML or SOAP).2. The notification is accepted by Central SSN which sends back a positive receipt.3. The Central SSN prepares and sends the SSN2MS_IncidentDetail_Tx to CECIS.	

4. CECIS sends back a SSN_Receipt message to Central SSN.
5. Central SSN presents to the data provider the consolidated distribution results through the SSN2MS_IncidentDetail_Tx_Ack (for XML/SOAP data providers) or via the IR monitoring tool of SSN (for web data providers, as developed in SSN V3).

The transaction is depicted in the figure below.

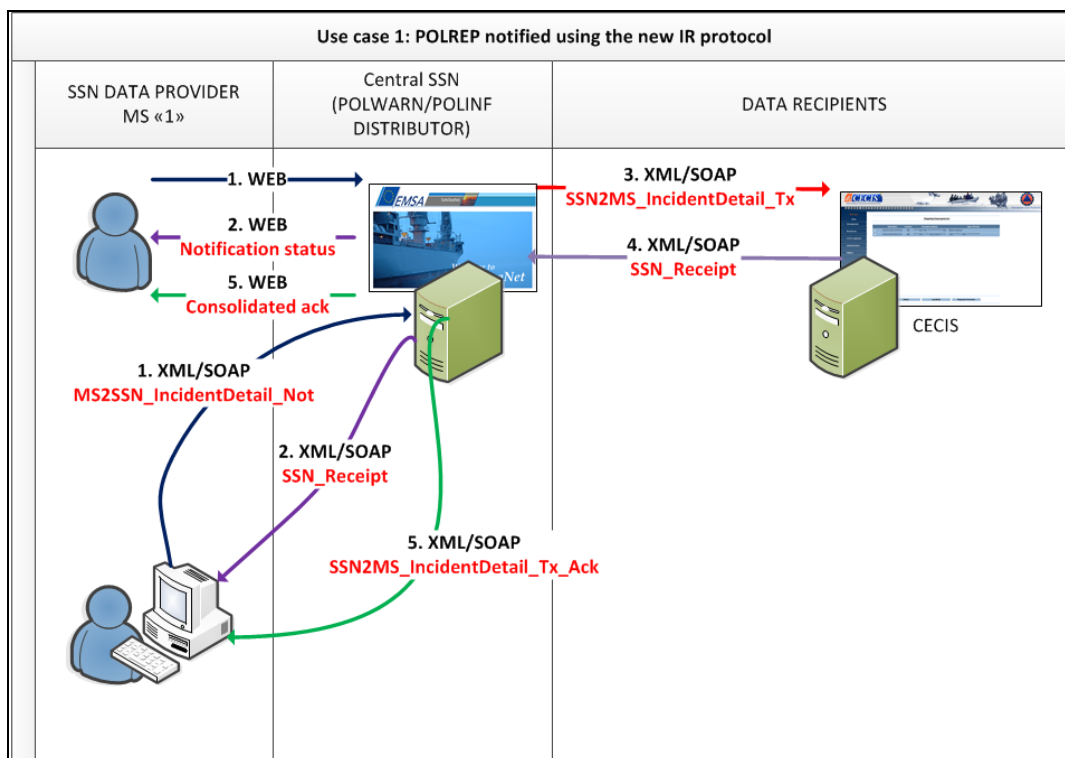


Figure 1: Notification and distribution process using the new protocol

7.1.4 Push of POLREP compliant with the "Alert" V1 protocol

Ref: SSN2CECIS_REQ_4	Priority: P1 Nature: M RFC ref: artf13645
<p>The Central SSN will prepare and send a message to CECIS each time it receives an Alert notification (MS2SSN_Alert_Not) quoting incident type=POLREP through the SSN system interface.</p> <p>Note: only the information available in the MS2SSN_Alert_Not (type POLREP) will be mapped in the SSN2MS_IncidentDetail_Tx to CECIS. A detailed data mapping for the preparation of the SSN2MS_IncidentDetail_Tx, included the relevant business rules, is provided in Appendix A.</p> <p>Note: all the organisations/persons created under location code = EUCOM and granted access to receive POLREPs will automatically receive the message "pushed" from SSN.</p> <p>The message to CECIS will be considered by SSN in a similar manner as any other SSN2MS_IncidentDetail_Tx message. The distribution status (success or failure) will therefore be available via the IR monitoring tool of the SSN web interface). The original data provider, using the "Alert" V1 protocol is not expected to receive the acknowledgment from SSN.</p> <p>Note: in case of a failure in the distribution to CECIS, SSN will activate the ordinary failure management procedure. Therefore, a warning email will be sent to the dedicated recipient</p>	

configured via the SSN user management console

Note: The "Alert" V1 protocol does not allow updating an existing Alert. Therefore, if the data provider wants to report additional information, a new Alert needs to be send to SSN. As a consequence, the Central SSN will send to CECIS a new SSN2MS_IncidentDetail_Tx message quoting a new IncidentID.

The data flow is the following:

1. The data provider notifies the POLREP MS2SSN_Alert_Not via the SSN national system.
2. The notification is accepted by Central SSN which sends back a positive receipt.
3. The Central SSN prepares and sends the SSN2MS_IncidentDetail_Tx to CECIS using the information available in the MS2SSN_Alert_Not (for the mapping refers to the Appendix A).

Note: SSN will not request any detail to the "Alert" data provider.

4. CECIS system sends a SSN_Receipt to Central SSN.

The transactions are depicted in the figure below:

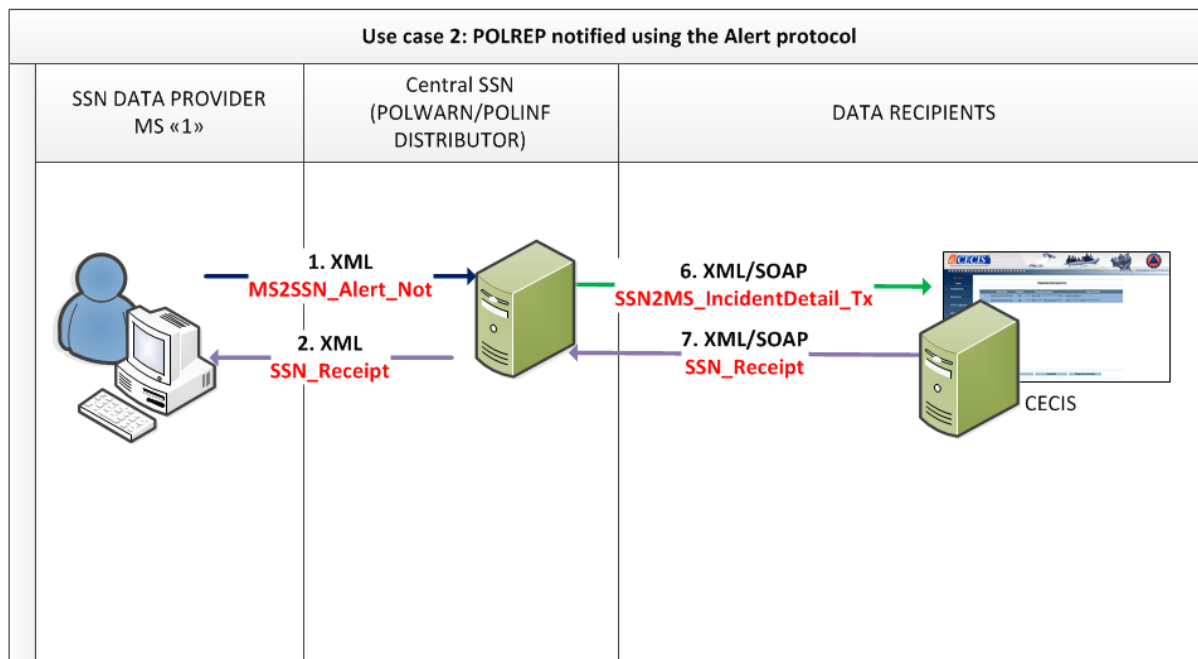


Figure 2: Notification and distribution process using the "Alert" V1 protocol

7.1.5 Central SSN web interface

Ref: SSN2CECIS_REQ_5	Priority: P1 Nature: M RFC ref: artf13645
In the SSN TI, the checkbox "European Union" in the IR distribution list will be renamed to "European Bodies". This applies to all incident report types.	
Ref: SSN2CECIS_REQ_6	Priority: P1 Nature: M RFC ref: artf13645

In the pages of the SSN web interface for submitting POLREP Incident Reports (*Send notification>Incident report>Create <Incident Type>=POLREP*), the "POLFAC" section will be amended with the following:

1. All the relevant "POLFAC" fields will be read-only (background colour: dark grey colour). The purpose is twofold: on the one hand preventing the accidental provision of POLFAC via the web SSN; on the other hand, avoiding losing information in case of a wrong injection of POLFAC information in SSN via XML.
2. A banner, including a hyperlink pointing to the CECIS web application, will be added to warn the web user not to send POLFAC information via SSN. The Central SSN administrator should have the possibility to amend the text box (including the above URL).
3. The check box "European Bodies" will be flagged by default and will not be modifiable by the user whenever a POLREP will be notified to SSN. The aim is to inform a web user that the information is automatically pushed to CECIS. The user will not have the possibility to unflag the checkbox.

A mock-up is provided below.

Figure 3: Mock up for the SSN web interface – Send notification

7.1.6 Avoiding double distribution to CECIS

Ref: SSN2CECIS_REQ_7	Priority: P1 Nature: M RFC ref: artf13645
When the data provider, providing a POLREP to SSN via XML/ SOAP interface, requests that the Incident Report is distributed to recipient country "EU", Central SSN will prevent that a SSN2MS_IncidentDetail_Tx message is sent twice to CECIS, and will therefore send to CECIS only	

one SSN2MS_IncidentDetail_Tx.

7.1.7 SSN User Management console

Ref: SSN2CECIS_REQ_8	Priority: P1 Nature: M RFC ref: artf13645
<p>The SSN application management console will include:</p> <ol style="list-style-type: none">1. Configuration to activate/deactivate the automatic "push" of POLREPs to CECIS.2. Configuration of the text and URL pointing to the CECIS web application (as introduced in section 7.1.5 above).	

7.2 Non-functional requirements for SSN CECIS interface

Ref: SSN2CECIS_REQ_9	Priority: P1 Nature: M RFC ref: artf13645
<p>It is expected that SSN will provide to CECIS at least 10,000 messages (including amendments and feedback) per year.</p>	

7.3 Other requirements concerning SSN updates

7.3.1 Central Ship Database

7.3.1.1 Improve the usability of the CSD

Ref: SSNv3.1_REQ_OTHER_1	Priority: P1 Nature: M RFC ref: artf14098, artf12986
<ol style="list-style-type: none">1. Currently a single page exists for "search or update vessel" which is used by CSD administrators to either update or consult vessel ship particulars. This is not suitable to cover the needs of users with "READER"-only access to the CSD. To ensure better usability, the system shall be changed to the following:<ol style="list-style-type: none">a. From the list of ships in the page "Search or Update Vessel", when clicking on a ship, the user will get the page "Vessel details", which will display in a similar manner as the current "Update Vessel Panel" the details of the ship. All the fields in this panel will be "read-only" (not-editable). For each field, in addition to its value, the source of the information will be displayed, e.g.<ul style="list-style-type: none">• "SSN" (for code "SSN"),• "LRITDB" (for code "LRITDB"),• "THETIS" (for code "THETIS"),	

- "SSN_MS" (for code "SSN_MS").

b. If the user has the CSD MANAGER right, a "Edit ship details" button will be provided in the "Vessel details" page. This button will bring the user to the current page "Update Vessel Panel". This page should be renamed to "Edit Vessel Details".

2. The current design of the "Update Vessel Panel" should be properly modified to ensure that the CSD MANAGER accessing the panel, if properly authorised, may edit, in addition to the ship particulars also ship identifiers (namely MMSI, Call Sign and Ship name).

3. A "source" and "reason for update" should be automatically recorded for all the changes performed to specific ship particulars via the "Edit Vessel Details" page.

Changes performed by users created under an Authority belonging to "European Bodies" shall be recorded with source "SSN" and reason for update "UP_MSSO". Changes made by administrators created under Authorities of any country (other than "European Bodies") shall be recorded with source SSN_MS and reason for update UP_MS_VERIFIED. Changes made via the CSD web interface will be considered as having a level of confidence "1" and shall be process taking into consideration the prioritisation rules in the SIG (Business rule 10).

4. In case an administrator performs a change that will not result in an update of the CSD (due to business rule 10), a warning should be produced with a message as follows:

QUOTE

[Field name] could not be updated because the information already stored in the system has a higher priority.

UNQUOTE

5. All the users that are to be granted access to the web interface of the CSD as "MANAGER" will get access and be able to create/update all ships (the permission at level of restriction "None").

6. All the users that are to be granted access to the web interface of the CSD as "READERS" will get access to all ships (the permission at level of restriction "None").

7. To allow uploading MARS data in the CSD, the current structure of the MARS schema in the SSN database should be changed following the format as the example file attached in the Teamforge artefact artf12986). The following data will be extracted from the CSV file and registered in the MARS schema in the database

Field content	Position in the MARS_Vessels.csv
MMSI	Column 1-9 (9 chars maximum)
Vessel Name	Column 11-58 (48 chars maximum)

	Vessel Call Sign	Column 60-66 (7 chars maximum)	
	Country	Column 68-70 (3 chars maximum)	
	Geographic Area	Column 72-74 (3 chars maximum)	
	MARS Ship Type	Column 76-77 (2 chars maximum)	
	Last Date (DD/MM/YYYY)	Column 79-88 (10 chars maximum)	
	Last Action (A – Added; M – Modified)	Column 90 (1 chars maximum)	
<p>8. The IMO column in the current MARS schema in the SSN DB shall not be deprecated but “null” entries will be allowed.</p> <p>9. The MARS information regularly uploaded in the schema with status A or M shall be considered for Verification/ validation process following the rules listed in the table included in the section 2.1.5 of the SIG for ship particulars.</p> <p>10. The business rule 9 will be modified as below: “When requesting information via the ship particulars service or consulting via SSN GI or TI, users will receive / visualise ship particulars with the source listed as “SSN” or “LRITDB” or “THETIS” or “SSN_MS” .The visualisation of the data in the CSD web pages providing ship information source shall be amended to identify also “LRITDB” and “SSN_MS”.</p> <p>11. Ship data (those either modified or consulted via the web interface of the CSD) for a specific ship could be printed or exported (in pdf or excel format).</p>			

7.3.1.2 Alignment of the CSD SIG and the web interface

Ref: SSNv3.1_REQ_OTHER_2	Priority: P1 Nature: M RFC ref: artf13790
<p>The “Vessel details” and “Edit Vessel details” pages should present (properly labelled) only the fields corresponding to the ship particular elements (and/ or attributes) defined in the current version of the SIG for ship particulars. Any other field should not be visible.</p> <p>During the design phase, the contractor will provide to EMSA mock-ups of the pages for agreement on their layouts.</p>	

7.3.1.3 Additional data source for ship particulars

Ref: SSNv3.1_REQ_OTHER_3	Priority: P1 Nature: M RFC ref: artf13683
<p>In the present SSN DB design the table PORTPLUS_SHIP_PARTICULARS holds the ship particulars reported in a PortPlus Notification. The ship particulars data stored in this table present another valuable source for information for ships with valid ship identity stored in the CSD. In order to enable the use of the information currently stored in the PORTPLUS_SHIP_PARTICULARS for CSD updates, the following changes should be implemented.</p> <ol style="list-style-type: none">The application implementation shall be revised to be in line with amended business rule 1 in the SIG as below: QUOTE revised text <i>The process of validation of ship identity is performed during ship particulars exchange and relates only to the key vessel particulars, which are: the IMO number, MMSI number, Call Sign, ship name, flag, and IR number (for fishing vessels).</i> <i>Additional ship particulars may be provided to the CSD:</i> <i>a. Those notified to SSN by THETIS,(according to the XML schema specified in the SIG), including the PSC ship type (refer to Annex E) .</i> <i>b. Those notified to SSN by MS via PortPlus notifications. E.g.: In the VesselDetails element: GrossTonnage, ShipType, Inmarsat, CompanyName, IMOCompanyNr.</i> <i>c. Those notified to SSN by MS via ship AIS notifications received via the streaming interface: Length (A+B from AIS message 5)/Breadth(C+D from AIS message 5)/ and the AIS ship type transmitted by the ship's transponder – (refer to Annex D)</i> <i>The data exchange mechanism to be used for a, b and c above is the web service defined in the SIG.</i> <i>d. e. The Lloyds (LLI) ship type (refer to Annex C) , if available</i> <i>f. The UNECE ship type (refer to Annex B), if available</i> <i>The information provided in the incoming notification for additional ship particulars from the sources specified above shall be stored in the SSN OSD. For vessels which identity is successfully verified, the information shall also be stored in the CSD. The storage of the additional ship particular in the CSD will depend on the "level of confidence" (refer to the table in the section 2.1.5) of the source providing the data according to business rule 10.</i> <ol style="list-style-type: none">Upon receipt of a PortPlus notification which includes ship particulars, the SSN EIS application will:<ol style="list-style-type: none">Store the information in the PORTPLUS_SHIP_PARTICULARS table.Should more than one INMARSAT number is received through PortPlus notification (up to 5), this information will be stored in the PORTPLUS_SHIP_PARTICULARS table. All (up to 5) INMARSAT numbers will be displayed through the CSD web console. Only the first number appearing in the PortPlus notification will be exchanged through the CSD web service.Consider that the ship particulars reported in the PortPlus notification have a level of confidence "2".Perform a check to verify the identity of the vessel<ol style="list-style-type: none">For vessels whose identity has a "temporary" status, store the additional	

<p>ship particulars in the OSD and record the source and reason for the update.</p> <p>ii. For vessels with valid identity, initiate the procedure foreseen in the business rule 10 to identify whether the additional ship particulars reported in the incoming notification can be used for an update of the CSD record for the ship.</p> <p>3. Upon receipt of a ship AIS notification from the streaming interface which includes ship particulars, the SSN application will:</p> <p>a. Store the information in the AIS_NOTIFICATIONS</p> <p>b. Consider that the additional ship particulars reported in the AIS notification have a level of confidence "3"</p> <p>c. Perform a check to verify the identity of the vessel</p> <p>i. For vessels whose identity has a "temporary" status store the additional ship particulars in the OSD recording source and reason for update</p> <p>ii. For valid vessels, initiate the procedure foreseen in the business rule 10 to identify whether, the additional ship particulars reported in the incoming notification can be used for an update of the CSD record for the ship.</p>
--

7.3.2 Amendment of EIS application logs

Ref: SSNv3.1_REQ_OTHER_4	Priority: P2 Nature: M RFC ref: artf14177
The search logs functionality should show not only the HTTP Status Code 202 and 200 but also any other status code that is returned by the MS servers (e.g. 500 code).	

7.3.3 Improvement on SSN web interfaces

Ref: SSNv3.1_REQ_OTHER_5	Priority: P2 Nature: M RFC ref: artf14150
In the SSN TI the coded elements should be displayed decoded including the full description to facilitate the reading of the user. The following elements should be modified:	
<p><u>In Voyage details:</u></p> <ul style="list-style-type: none"> Activity: Description of ship-to-ship activity performed defined using the EDIFACT codes (8 025) Anchorage: Y: Ship at anchorage / N: Ship not at anchorage PossibleAnchorage Y: Ship expected at anchorage / N: Ship not expected at anchorage AuthorityType: NCA: National Competent Authority / POR: Port Authority / OTH: Other CallPurposeCode: Description of the primary purpose of the call as defined by EDIFACT cod 	

e 8025

- Flag: Country name in addition to two-digits flag code. Example: "France (FR)"
- INFShipClass: INF1: Class INF 1 / INF2: Class INF 2 / INF3: Class INF 3
- IssuerType : GVT: Contracting Government / RSO: Recognized Security Organization
- PackageType: Description of the outer package using annex VI of UNECE R21. EDIFACT codes (7065)
- PortOfCall / LastPort / NextPort / PortOfDischarge / PortOfLoading / PortDeliveryRemaining Waste / Port / LoCode / LastPortDelivered / PortOfRegistry / Route-Port : Port name in addition to Locode. Example: "Le Havre (FRLEH)"
- ShipConfiguration: SHT: single hull tanker (SHT) / SHT-SBT: single hull with segregated ballast tanks (SBT) / DHT: double hull tanker
- ShipType: ship type description according to UNECE R28 codes
- Exemption - Country: Country name in addition to (two-digits flag code)
- Exemption - AuthorityType: NCA: National Competent Authority / POR: port authority / OTH: Other
- WasteCode: label as provided in Annex B of XMLRG, column "Description"

In Incidents/Alert details:

- Flag: Country name in addition to two-digits flag code
- P1_ReportType: A: Loss (ship having lost a or several containers/package goods) / B: Observation (ship noting the presence of containers/packages goods drifting at sea)
- PortOfDestinationQuotedInIR / PortOfDestination / PortOfDepartureQuotedInIR / PortOfDeparture / NextPort /
- WasteDeliveryDuePort: Port name in addition to Locode
- RecipientCountry: Country name in addition to two-digits flag code

In AIS/MRS details:

- AnyDG Y: declares that dangerous or polluting goods are on board / N: declares that there is no dangerous nor polluting goods on board / X: the information on the presence of dangerous and polluting goods is not available
- HazardousCargoType DG: Dangerous goods / HS: Hazardous substances / MP: Marine pollutants
- NextPortOfCall / LoCode: Port name in addition to Locode
- ShipType: ship type description according to UNECE R28 code
- NavigationalStatus:
 - 0 (under way using engine)
 - 1 (at anchor)
 - 2 (not under command)
 - 3 (restricted manoeuvrability)
 - 4 (constrained by her draught)
 - 5 (moored)
 - 6 (aground)
 - 7 (engaged in fishing)

<ul style="list-style-type: none">- 8 (under way sailing)- 9 till 14 (reserved -> should not be used)- 15 (not defined)	
Ref: SSNv3.1_REQ_OTHER_6	Priority: P2 Nature: M RFC ref: artf14150
The changes required above in SSNv3.1_REQ_OTHER_5 will also be applied in SSN-GI.	

Ref: SSNv3.1_REQ_OTHER_7	Priority: P2 Nature: M RFC ref: artf10920
On "Statistics Console > Notification Analysis > Count number of notifications", the field labelled "User id" currently requires the insertion of the UNIQUE_ID of a PARTY of type PERSON. This particular search criterion should be modified to allow the insertion of UNIQUE_ID of a PARTY of both types (PERSON or AUTHORITY).	

7.3.4 Improvement of the user management console

Ref: SSNv3.1_REQ_OTHER_8	Priority: P2 Nature: M RFC ref: artf8504
<p>The current work-flow for creating or updating a user account requires that the administrator, once having created a user in IdM, has to search and identify the user account (s) that should be fully configured in SSN and define the user (s) (their) access permissions. In this respect is currently used the menu option labelled as "Search/ Update IdM users" . The title of the menu option might confuse national administrators. Therefore, the menu item under user management console currently labelled as "Search/ Update IdM users" should be renamed to "Users lacking SSN access permissions".</p> <p>Apart from renaming the menu option the following improvements in the workflow should be made:</p> <ol style="list-style-type: none">1. Upon an administrator clicks on the menu option "Users lacking SSN access permissions" the application should automatically execute a query to detect those user accounts (one or more) that have been provisioned in IdM but not in SSN. The query shall pick only those accounts the administrator is authorised to provision. The results of the query shall be presented to the user accessing the page "Users lacking SSN access permissions"2. Upon selecting a user from the list, the administrator will:<ol style="list-style-type: none">a. First select the type of SSN user account (Person or Authority)b. Then, the administrator should be directed to the relevant user update page to complete the provisioning (assign group, tasks and permissions to users).	

7.3.5 SSN GI –vessel position visualisation

Ref: SSNv3.1_REQ_OTHER_9a	Priority: P2 Nature: M RFC ref: artf11699, artf11698
<p>The visualisation of vessel positions in SSN GI should be improved in order to properly enforce access rights on the historical track presented to users. For drawing the "history" line, the system should only retrieve tracks from sources that the user is authorised to access to (currently the system retrieves positions from sources that the user is not authorised to and it should not).</p>	

Ref: SSNv3.1_REQ_OTHER_9b	Priority: P2 Nature: M RFC ref: artf11699, artf11698
<p>The visualisation of vessel positions in SSN GI should be improved in order to ensure that the system always displays the last position from the sources that the user is authorised to access to. Currently if the last vessel position (based on time-stamp) known to the system is derived from sources that the user is not authorised to (e.g. S-AIS or LRIT), the vessel "disappears" from the map window. Instead, and for the example given, the system should be able to display, within the visibility window set for the SSN GI, the latest position received from T-AIS.</p> <p>The contractor will propose in his offer a design solution which does not impact to the current performance of the system.</p>	

8. List of appendices

The table below summarises the applicable appendices that shall be considered an integral part of this specifications

Appendix	Title
A	Data mapping and business rules for aligning Alert information (type POLREP) with SSN2MS_Incident_Detail_Tx

Appendix A: Data mapping and business rules for aligning Alert information with SSN2MS_Incident_Detail_Tx

See Attached Excel file