MARSEC EWG

Security Message – Business Rules

Version: 1.10

Date: 20 July 2012

Table of Contents

Background

On 20 October 2010 the Commission published the Directive 2010/65/EU on reporting formalities for ships arriving in and/or departing from ports of the Member States (known as the FAL Directive) which repealed the Directive 2002/6/EC. The purpose of the Directive is to "simplify and harmonise the administrative procedures applied to maritime transport by making the electronic transmission of information standard by rationalising reporting formalities."

According to the provisions of Article 5, MSs shall accept the fulfilment of reporting formalities in **electronic format** and their transmission via a National **Single Window (SW)** no later than **1st June 2015**. The Annex of the Directive lists the 14 reports which are to be submitted through a National SW in accordance with the reporting formalities.

Among reporting formalities resulting from legal acts of the Union, the **notification of security information** (Article 6 of Regulation (EC) No 725/2004 on enhancing ship and port facility security) will be exchanged through SSN. In the Appendix of the Annex of the Directive is presented the form to be used for the transmission of the information.

The security message shall be submitted electronically only once (via a National SW) and made available to various competent authorities. The SW concept at national level is introduced in order to gather the information more effectively. In defining the business rules of the security message the MARSEC EWG considered the following principles:

a. The inclusion of the security information into SSN should not only facilitate the legal obligations enabling the transmission of the reporting formalities but should primarily satisfy the user requirements.

b. The National SW has to meet the requirements of the Directive 2010/65/EU including the international recommendations and national policies.

c. The principles of the existing SSN should be fulfilled to the possible extend in order to build on what already exists avoiding major changes and taking benefit of the investments made by the Members States.

d. Similar tasks have to be executed for all the other messages composing the National SW as prescribed in the Directive. As soon as the business rules of the security message will be defined, the results shall be harmonised with the rules of all the other messages being part of the National SW. Then, the technical work for the entire SW will be launched to determine the technical specifications meeting the requirements of the defined users and functionalities.

The inclusion of the security message into SSN was discussed at the MARSEC Committee (Brussels 7 February 2011) which decided to set up a MARSEC Experts Working Group (EWG) for the development of the business rules. 10 Member States have volunteered to participate: Cyprus, Denmark, France, Germany, Ireland, Latvia, Spain, Poland, the Netherlands and the UK.

This report presents the business rules proposed by the EWG to the MARSEC committee for the integration of the security message in the single window and in SafeSeaNet.

Business Rules

1. Type of ships

The legal framework is provided by Art. 3.1, 3.2 and 3.3 of Regulation (EC) No 725/2004:

a) Vessels falling under the Chapter XI-2 SOLAS Convention. These are ships engaged in international voyages (passenger ship regardless of tonnage and cargo ships ≥ 500 GT and mobile offshore drilling units);

b) Class A passenger ships (as defined by Art. 4 of Directive 98/18/EC), engaged in domestic voyages; and

c) Other categories of ships, (as defined by Art.3.3 of Regulation (EC) No 725/2004), engaged in domestic services (hereinafter "other categories").

Recital 10 of Directive 2010/65/EU on reporting formalities from ships specifies that reporting formalities regarding information for solely national purposes should not need to be introduced in the SafeSeaNet system.

Following a consultation by the Commission, the MARSEC Committee has agreed at its 40th meeting that the pre-arrival ship security message will be only applied to vessels falling under SOLAS Convention.

Business Rule 1: The security notifications of the ships falling under type (a) above shall be provided for all calls in EU ports and exchanged through SSN. There is no need to submit the security notifications for ships engaged in domestic voyages (b, c) through the National SW, unless otherwise provided. The security messages will be exchanged between the MSs on request.

2. Definition of «primary key»

According the form in the Appendix of Directive 2010/65/EU, ships are identified by: *IMO number, Name of ship or Call sign and Flag State*. The MMSI is not included in the form. This definition differs from the one currently applied in SSN, where the ship is always identified through the IMO number and/or the MMSI number.

Considering that the security notification to be exchanged among MSs via SSN is not an individual message, but a fragment of the National SW (broader set of messages where MMSI is requested), the EWG considers this is a non-issue because in practice it will not happen a security notification to be submitted individually.

The Commission has underlined the fact that the matter at hand regards only SOLAS ships.

Business Rule 2: The IMO number shall be considered as "primary key". The Ship MMSI is not mandatory for the pre-arrival ship security message, however MMSI can be used as a "primary key" if available.

3. Voyage related information

Business Rule 3: UN/LOCODEs should be used to identify the ports and the IMO Port Facility Number (GISIS database) codes to identify the port-facilities.

The UN/LOCODEs list and IMO Port Facility Numbers are managed and maintained by the UNECE and with the active contributions of the national governments and commercial bodies. The list needs to be "cleaned" by each national government in order to remove LOCODEs that are no longer valid as port location. In addition, the shipping industry must be informed of the proper use of the UN/LOCODEs list and the IMO Port Facility list.

The possibility of re-using information already existing in SSN (to automatically pre-fill the previous ports) shall be considered by the SSN technical experts.

4. Classification of the security message

Business Rule 4: The information included in the security message does not require special security measures to be taken (it is not classified information). The information contained in the security message is unclassified and shall be considered as sensitive information that shall be protected from unauthorised access or disclosure. Some parts include personal data, which shall be protected in compliance with the rules on personal data protection. The information is of similar nature to the existing SSN information.

5. Cargo, crew and passenger lists related information

Business Rule 5: All the information already provided once shall be reused; therefore the dangerous cargo manifest, the ship's crew list and the ship's passenger list (all these items are part of the ship pre-arrival message should not be required to attach to the security message), if already provided to the National SW.

6. Information on ship's agent

6.1 Ship's agent name and contact details

The question of the information related to the credentials (name and contact details) of the person providing the security notification have to be provided within the notification was assessed. The main argument was that this type of information is already available to the NCA managing the users (therefore the credentials are known).

The Ship's agent is among the persons authorised to provide the security information and the field in the Security form for the details of the ship's agent have to be included in the security message.

Business Rule 6: Ship's agent is only one of the profiles of users authorised to provide the security information. The relevant field in the Security form for the details of the ship's agent have to be included in the security message.

6.2 Signature

Business Rule 7: There is no need for a formal sign (digital signature). The NCA has already the user's credentials (User ID and password) of the data provider. The information could be submitted to SafeSeaNet.

7. User Profiles

The National Competent Authority (NCA) for SafeSeaNet in close cooperation with the competent authority for maritime security has to identify the users of the ship security message.

After the identification of the users of the ship security message, the National Competent Authority (NCA) for SafeSeaNet grants them access rights.

The role of EMSA is to apply the rights granted by the National Competent Authority (NCA) for SafeSeaNet, by the technical implementation of the central SSN system.

Business Rule 8:

- The SSN NCA is responsible for providing the security information to the central SafeSeaNet system.
- The "Competent Authority for maritime security", as defined in Art. 2.7 of Regulation (EC) No 725/2004, shall be entitled to get access to the security-related information stored in the SSN.
- There should be two Security profiles: at national level and local level. The Security profile at local level will be restricted to vessels departing from or bounding to their port. There will be no restriction to access security information at national level (access to all security messages). If a security user has additional SSN profiles, it shall be possible to combine the profiles in a single access.
- PSO-PFSO will have access to the security information through the National Single Window.
- The management of the security user's credentials shall be made by the SSN NCA in cooperation with the competent authority for maritime security.

8. Data Providing Process

Business Rule 9:

- The MSs shall develop the appropriate data entry tools to allow the user to enter data to the National SW. Both EDIFACT and XML can be used to provide data to the National SW at the discretion of the MS. The communication between the national SSN applications and the central SSN will be based in XML. The SSN XML message format shall be defined by the SSN group.
- The ship pre-arrival security information may be originated by different agents at national level. The agent should have access to the relevant information previously provided by another user so that the information is provided only once and re-used for the notifications to follow.

- The MSs shall develop mechanisms to ensure the non-repudiation and traceability of actions performed by users accessing the National SW.
- The single window concept will prevent the same information required by the different message (as defined in the Annex of Directive 2010/65/EU) to be provided more than once.
- Updates on previously provided information may be accepted after the first message in order to correct some parts of the information. The cancelation of the full ship call may also be foreseen. It is essential for the system to link the whole information flow to a single ship call.
- The security notification shall be part of the pre-arrival notification already set in SSN (as part of the PortPlus message).
- Common data quality checking rules shall be applied in all systems that are linked. This is of particular importance to the SW system (national or port) that is the entry point for all the information. However, the information shall always be accepted at central level, even if some parts needs to be checked/corrected before being submitted to SSN.

9. Exemptions

Business Rule 10: The management of exemptions must be established in compliance with Art. 7 of Regulation (EC) No 725/2004. Member States shall draw up a list of companies and ships granted exemption under this Article, and shall update that list. They shall communicate the list and updates thereof to the Commission and any Member State concerned. The lists of exempted companies and ships shall be kept in each national SSN and in the central SSN. The central SSN will provide upon request, the contact details of the authority granting the exemption and the lists of exempted companies and ships to the concerned State

The distribution of the information on granted exemptions for security notifications could be done either by submitting the exemption information according to an agreed template directly to central SSN system or by including in the national system the scheduled services and generating automatic notifications according to the schedule. Both solutions are accepted, provided that the information on exemptions is available in the National SW and through SafeSeaNet to other MS on request.

10. Functionalities

The main purpose of implementing the security message (and the other reporting formalities) in electronic format is to facilitate the **clearance process**.The types of functionalities that may be defined for the data processing include several warning functionalities for the national authority on:

- the validity of the ISS certificate;
- the security level higher than 1;
- checks for specific security measures in place.

More experience is needed to define the functionalities (e.g. filtering, correlation, monitoring, alerting, data quality checks and statistics). Member States should decide which functionalities to develop at national level. The EWG is not in favour of harmonising the functionalities.

Business Rule 11: The data processing at central level should facilitate the exchange of information. The SSN group should consider to what extend functionalities may be developed to make use of the security information among MSs.

11. Data Storage and Data Availability

Business Rule 12: To maintain coherence with SSN, the same data storage requirements shall be applicable.
Open issue: The issue of cost of the data storage was raised. To maintain coherence, the minimum time for data storage needs to be agreed. This question was subject to a written procedure to the MARSEC committee completed on 14 October 2011. Following this consultation, the MARSEC Committee has agreed that, taking into account legal provisions and operational needs, the minimum period for data storage should remain in accordance with the period currently in place in SSN:

- 5 years minimum for data related to incidents or accidents
- 2 months minimum for data related to port (from ship departure) and ship notifications.

Business Rule 13: The system shall maintain the same availability requirements as SSN (minimum of 99% over a period of one year, with the maximum permissible period of interruption being 12h).

12. Personal Data Protection

Business Rule 14: The protection of personal data at national level shall be in line with national legislation for data protection and with Directive 95/46/EC.The protection of personal data at central level shall be in line with Regulation (EC) No 45/2001 on protection of data by the Community Institutions and bodies.

NCAs have to verify the compliance of the measures implemented for the protection of personal data in their national SafeSeaNet with the EU and their national legislations.

EMSA has to verify the compliance of the measures implemented for the protection of personal data in the central SafeSeaNet with the EU legislation.