Annex A
to Tender Specifications

SafeSeaNet overview

EMSA

TABLE OF CONTENTS

Introduction

SafeSeaNet (SSN) is an EU vessel traffic information exchange system between designated participants. This annex to the tender specifications provides the objectives of SSN, a system overview and the main flows of information, system functionalities and actors. Technical specifications are developed in separate technical documents adopted by the SSN group.

Objectives of SSN and its network organisation

The objective of the SSN system is to support EU and MS activities with respect to maritime safety, port and maritime security, marine environment protection and the efficiency of maritime traffic and maritime transport.

The operation of SSN involves a number of entities or users at regional, national and local level. These can vary from those in the shipping industry (ships' masters, agents or operators) to national administrations (such as port authorities and coastal stations, Port State Control officers, SAR centres, VTS, ship reporting systems, pollution response bodies, etc.).
Through sharing and distributing maritime related information, the SSN system supports users at EU and MS level in achieving the objectives set out in the Article 1 of Directive 2002/59 (as amended). SSN facilitates the exchange of information in electronic format between MS and to provide the Commission with the relevant information.

It is composed of a network of national SSN systems in Member States and a central SSN system acting as a nodal point (see figure 1 below). The central SSN system has a number of interfaces available thereby allowing optional/alternative means of information exchange with Local Competent Authorities (LCA) and National Competent Authority (NCA) at MS level (see figure 1 below)

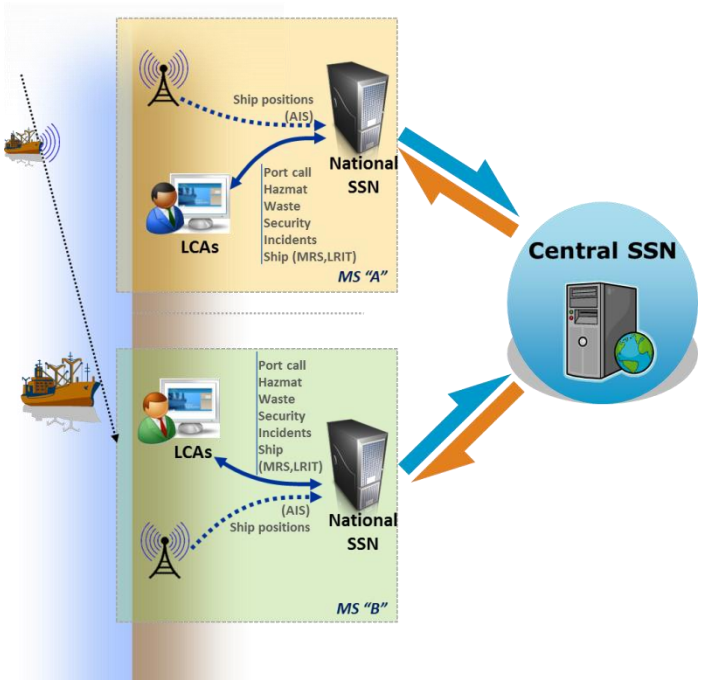

Figure 1 SafeSeaNet system

- LCAs may be data providers as well as data users at local level.
- National SSN systems and/ or National Single Window (NSW) systems established in accordance with Directive 2010_65_EU provide information to the central SSN system in the form of notifications. Authorised users within the SSN Community can retrieve information related to these notifications. The central SSN system locates and retrieves this information and provides it to the data user.
- While the central SSN system stores some information which enables rapid, effective response to users' requests, detailed information may be stored at national level. When the notifiable information is changed by the data provider, a notification is provided to the central SSN system, and information is updated accordingly.

Mandatory system functionalities

SSN, at its national and central levels, is built upon mandatory system functionalities which are essential to the normal operation of the system. The mandatory system functionalities are the sending, receipt, storage, retrieval and exchange of information required by the SSN legal framework. SSN shall support the exchange of the following information:

- Port call information:
  - ✓ Pre-arrival information sent to ports 72 and 24 hours in advance from estimated arrival to the Port of Call
  - ✓ Actual arrival and departure notification
  - ✓ Notifications on carriage of dangerous or polluting goods (sent or pre-arrival and departure stages)
  - ✓ Notifications on waste/ security (sent at pre-arrival stage of the call, at least 24h prior to the estimated arrival.;
- Incident information:
  - ✓ Information on accidents and incidents which have occurred at sea;
- Position information: AIS, MRS and LRIT flag state information;

The information collected and exchanged through SSN must comply with the quality and performance standards defined in the Interface Control and Functionalities document (IFCD) agreed with the MS and in the relevant technical and operational documentation.

Additional system functionalities

SSN provides for additional functionalities in support of its main operations. These functionalities are not considered mandatory, therefore their unavailability would not affect the overall service level of the SSN system.

The additional system functionalities are related but not limited to:

- statistics;
- graphical display of information;
- SAT-AIS position information;
- background information display (nautical charts, etc.);
- system monitoring tools;
- secondary or reference data sources (Location codes, SSN users contact details, ship particulars, special lists of ships).

Subject to approval by the SSN group, further functionalities may be incorporated in the SSN system.

Information exchange mechanisms

The central SSN system provides different alternative mechanisms to the national SSN systems in order to enable the mandatory exchange of information. These are:

- Message-based mechanism: A mechanism which allows individual messages to be exchanged between the national and central SSN applications. The messages (in XML format) fulfil the needs of both data users and data providers (e.g. proprietary protocol, web-services, etc.). This mechanism supports the notification, request and response functions for all types of SSN information.
- Streaming mechanism: A mechanism which enables the constant flow of AIS data (based on predefined criteria) from the national systems to the central SSN system (either directly or via an AIS regional server). This mechanism is currently only available for the provision of AIS information and is an alternative to the message-based mechanism.
- Central SSN Web browser-based mechanism: This mechanism is available for requesting information and providing Incident Reports, and may be used to provide other information as a back-up solution in the case of failure of the national or local SSN systems. It is also available for system administration. The central SSN Web browser-based mechanism offers two interfaces:
    - Textual interface: This provides direct access to the central SSN system using a textual layout;
    - Graphical interface: This uses geographical information system technology to provide access to ship positions enriched with the data in the central SSN system (information on pre-arrival, arrival, Hazmat cargo, incidents, etc.), thus creating a vessel traffic image showing movements in near-real time.

The table 1 below lists the mechanisms available for exchanging information via the central SSN system.

Table 1 SSN mechanisms for information exchange

SSN Mechanisms for information exchange		Message-Based	Streaming	Web Browser-Based	
				Textual interface	Graphical interface
Available for:	**Data Providing**	All information	Ship AIS positions	Incident, exemptions information and In case of failure as a backup mechanism for 72 hours pre-arrival, ATA and ATD	N.A.
	Data Request	All information		All information	All information
	Data Distribution	Incident reports	Ship AIS positions enriched with SSN data	Incident reports	N.A.

Message based mechanism

Notification:

- The data provider gathers the necessary information to be reported.
- This information is sent to the national SSN system.
- The national SSN system compiles the message in the SSN compliant format and forwards it to the central SSN.
- On receipt the central SSN determines whether the notification is well formed:
    - If well formed, the notification is indexed in the server.
    - If not well formed, the notification is rejected by the central SSN system and the national SSN system should resend the corrected message.

Request and response:

- The data user requests information from the national SSN system.
- When the information cannot be provided nationally, the national SSN system forwards the request to the central SSN system.
- The central SSN system verifies the access rights of the user, and subject to acceptance, proceeds as follows:
- In the case of information stored at central SSN level, the information is sent back to the requester (via national SSN system).
- In the case of information is available in MS national servers through document download, the central SSN system retrieves directly the document and forwards it to the requester (via the national SSN system).
- In the case of information is available upon request only, the central SSN system forwards the request to the national SSN system where the information is located, which, may, in turn, forward it to the data provider that owns the information. The data provider that owns the information then responds with detailed information which is transmitted (via the national SSN system) back to the central SSN system for forwarding to the data user.

A sequence diagram describing the above mechanisms is provided in the figure below.

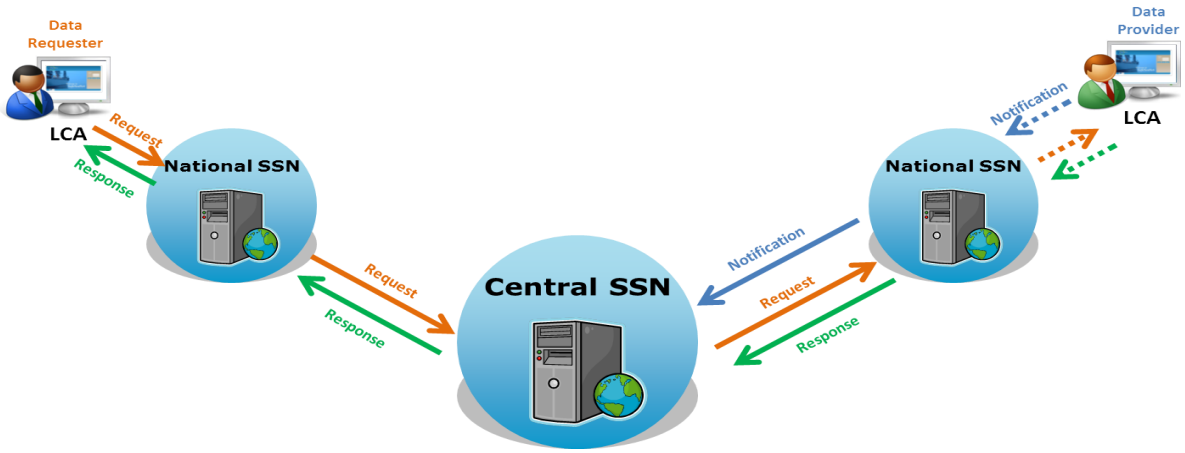

Figure 2 Sequence diagram of notification, request and response mechanisms

Distribution for Incident Reports

- The *data provider* can define the list of recipients for distributing Incident Reports via the national SSN system (in XML) or via the central SSN web interface.
- The central SSN system verifies the access rights of the user and distributes the Incident Reports in accordance with the distribution list.
- Incident Reports can be distributed via XML, emails or both depending on the user configuration as follows;
  - If the user is an XML recipient, the central SSN forwards the full information to the national SSN system;
  - If the user is an email recipient, the central SSN distributes emails including basic information about the incident. The full details can be retrieved by the user through the central SSN web interface.
- The central SSN logs the distribution status and activates a failure management procedure in case of a failure in the distribution.

Streaming mechanism:

- Provision of AIS data
  - SSN is equipped with a streaming mechanism which enables the near-real-time exchange of ship positions obtained via the AIS network. This exists at the regional and national levels in order to enable national SSN systems to provide AIS information to regional servers and/or the central SSN system.

- Distribution for Ship AIS position enriched with SSN data
  - The streaming mechanism supports the distributing of AIS information enriched with SSN data in accordance with the access rights of the user.

Cooperation with Other EU Systems

Information exchanged between the central SSN system and other EU systems must respect the access rights policy defined in Chapter 3 of the SSN IFCD (refer to Appendix C of this annex).

The cooperation between the central SSN system and the other EU systems described above can be summarised as follows.

- **SSN/THETIS:** The central SSN system provides to the THETIS system information received from national SSN systems on the port call (pre-arrival 24 hours, arrival, and departure), waste and security information for ships calling at EU ports and anchorages.
- **SSN/CSN:** The central SSN system provides ship positions and identifiers (transmitted by national AIS networks) to the CSN system in order to assist in the identification of vessels and possible polluters (within a limited timeframe and area).
- **SSN/EU LRIT CDC** [1]
- **SSN/EU LRIT Ship Database:** The EU LRIT ship database provides the central SSN system with ship information in order to validate the ship information held in the SSN system
- **SSN/CECIS:** The central SSN system provides incident reports of type POLWARN and POLINF to CECIS

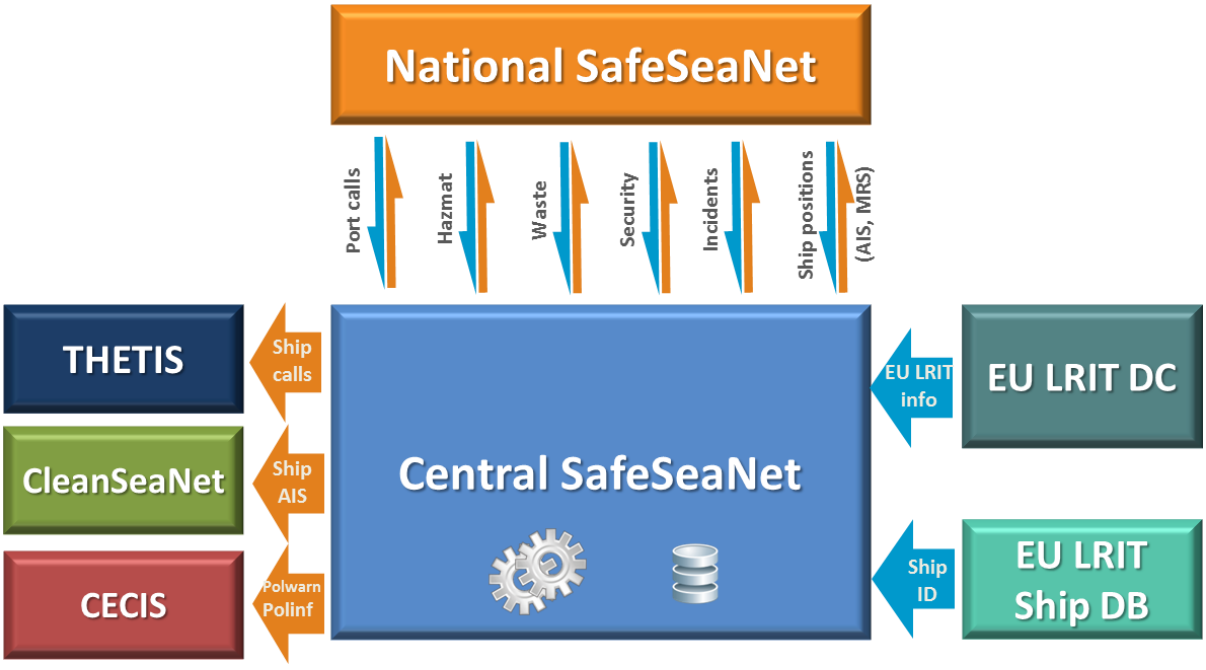

Figure 3 Interfaces of the central SSN system with other EU systems

[1] The technical implementation to allow for the full distribution of LRIT data to MSs through SSN is under development.

SSN Applications

The architecture of the Central SSN system at the time of launching this procurement includes several applications (either already in operation/production or under development). The applications are designed/implemented with Service Oriented Architecture logic.

The SSN applications are:

- **The European Index Server (EIS)**

  Through this application certain core services are implemented e.g.
  - ✓ **The SSN textual interface, t**
  - ✓ **The XML/ SOAP messages interface,**
  - ✓ **The Central Ship database (CSD)** containing reference data for ship identifiers and ship particulars
  - ✓ **The Central Organisation Database** containing reference information for maritime Authorities
  - ✓ **The Central Location Database containing reference location (e.g. ports) information.**
- **The SSN Tracking Information and Real Time Exchange System (STIRES) module**

  Through this application certain core services are implemented e.g. the SSN Graphical Interface (SSN GI) and SSN Streaming Interface – SSN SI)

  Important note:
  This applications shall be deprecated within 2016 and replaced by STAR (refer to the Annex G of the tender specifications for the anticipated evolution of EMSA maritime applications architecture
- **The SSN accident module**

SSN uses the single sign on platform of EMSA (**Oracle Identity Management** suite) for user access authentication. The EIS application comprises several **SSN management utilities** (made available as distinct deployables) enabling provisioning of user access rights and management of the reference and operational data in the SSN system. User are accessing SSN via the **Maritime Application Portal** a LifeRay-based application used by all the critical operational services currently managed by EMSA.

The GIS capabilities for SSN GI mentioned above are currently based on the ESRI ArcGIS platform. The visualisation of Electronic nautical charts (ENCs) is implemented as an horizontal web map service fetching ENCs from the Agency's chart database (licenced by Jeppesen). For the verification and validation process of ship particulars, a link to the Agency's MARINFO database has been implemented (utilising store procedures).
The reference databases are exposed tapplications external to SSN via XML/ SOAP-based web services. At the time of the procurement the CSD is exposed to MS in the framework of a pilot project while COD and CLD are exposed only to other EMSA applications.

SSN release in production at the time of launching the procurement (SSNv3.0)

At the time of launching the procurement the release of SSN available in production is the one identified as "SSNv3.0"". The release complies with the data exchange specifications listed in the XML Reference Guide v3.02 and meets the legal requirements of Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system as amended by the Directives 2009/17/EC as well as the legal requirements of the Directive 2010/65/EU (on reporting formalities for ships arriving in and/or departing from ports of the Member States

The following new features of SSN v3 are supported:

1. Creation of additional user profiles: Enables SSN and national administrators to create the National Single Window Authority and assign to users permissions associated with the provision/request of waste and security information,
2. Option to notify SSN using the revised PortPlus[2] notification that includes Waste, Security and Hazmat information,
3. Option to notify SSN of exemptions using the new exemption notification,
4. Option to query SSN using the new ShipCall request / response mechanism[3],
5. The new MRS protocol including:
    a. A revised Ship MRS notification;
    b. A revised Ship request/response mechanism;
6. A mechanism to support a transition period from SSN v2 to SSN v3 protocol (refer to SSN Group paper SSN 22.4.2):
    a. PortPlus notifications and ShipCall request / response
    b. Ship notifications and Ship request / response
7. Improvement of the SSN Textual Interface and Graphical Interface in relation to the changes mentioned above and the Incident Reports function.
8. Central Ship Database

Detailed design information concerning this release is available in the Appendices of this Annex A .

SSN baseline version for the procurement (SSNv3.2)

Bidders should note that at the time of signature of an FWC based on this tender the baseline SSN version in production shall be **SSNv3.2**. Below is outlined the context of the two releases anticipated to enter into production during the time this tender shall be still in the evaluation stage:

SSNv3.1 (target GO LIVE – July 2015)

- The release shall include:
    a. SSN CECIS interface
    b. Improvements on the IR protocol for the SSNv2 –SSNv3 transitional period[1]

SSNv3.2 [target GO LIVE – October 2015)]:

- The release shall include:
    a. Upgrades enabling the integration of Shore-based traffic monitoring infrastructure database (STMID) in the COD.
    b. Implementation of a WFS that COD shall expose to SEG enabling the visualisation of the STMID data in SEG..
    c. Implementation of a WFS that the Central Geographical Database (CGD) will expose for enabling registering a reference descriptor for geographical areas in the COD (for STMID purposes).
    d. Improvements in the web interface of the CSD (for improved usability and alignment with the System Interface Guide agreed for the MS CSD pilot).

[2] The Portplus message was initially introduced in SSN v2 back in 2011 and is used as well for the notification of pre-arrival notices (72h/ 24h) and actual arrival/ departure notices.
[3] This mechanism is utilised in SSN for the exchange of voyage/ shipcall information notified to SSN using Portplus. It was initially introduced to the system with SSNv2.

e. Amendment of the CSD business logic enabling registration of ship particulars delivered via PortPlus and AIS messages into the CSD.
f. Amendment of EIS application logs to register all types of http errors.
g. Improvement of labelling the fields in the SSN web interface forms concerning ship voyage details, MRS and incident details.
h. Implementation of data archiving for SSN EIS data (voyage/ ShipCall, Incident, MRS) including changes in the SSN EIS business logic for accepting shipcall updated where data was registered in the system more than a year in the past.

(For the following items the Release version (SSNv3.2 OR ssnV3.3) is to be confirmed)

i. Improvement of the SSN user management console to streamline the user provisioning workflow[1].
j. Removing access rights-related data visualisation inconsistencies in SSN GI.
k. Fine-tuning and improvement of EIS and reference registries infrastructure for better performance and scalability.
l. The segregation from the STIRES application of all the functionality re-used in SSNv3 and currently implemented using its "front-end. The features to be migrated concern:
    i. Accident module input tool.
    ii. Accident module database.
m. Other minor-scale improvements in SSN EIS, SSN textual interface, COD/CSD/CLD web consoles stemming from requests from users.
n. Hotfixes for the resolution of non –critical bugs affecting SSNv3.1 which are to be still unresolved until the 28th of August 2015.
o. Changes in the COD/CLD/CSD web services taking into consideration the results of the CSD pilot with MS as well as the requirements of the CMC project
p. The correction of messages 5, 24 – generated inconsistencies in timing referencing position tracks in SSN GI.3

Bidders may refer to Appendices G and H which contain information on the RFS launched by EMSA on SSNv3.1 and the main change in SSNv3.2 concerning the integration of STMID information into COD.

System performance requirements

The following performance requirements apply to the processing of messages and system information. Note that Member State authorities may assign more specific performance standards in accordance with their national requirements.

Timeframes for data availability

The national SSN systems connected to the central SSN system should be supported by data communication links and networks that allow them to transfer information within 1 minute between the two systems.

SSN data requesters should receive the desired information from SSN within an average of 30 seconds (central SSN system will not process responses received after 4 minutes) of making a request. In the case of phone, fax or email, data requesters should receive the requested information within 60 minutes. This is not applicable to archived information. . The timeframes above should be respected for 95% of the information exchanged during a 24h period and for 99% of the cases during a one year period.

The NCAs should respond to requests for archived data as per point below within 5 working days.

Timeframes for data storage[4]

The data shall be available "live" through the SSN system:

a) Minimum of five (5) years for information related to incidents and accidents; and

b) Minimum of two (2) months from the departure of the ship for information related to port calls and hazmat and from the reporting date for ship messages.

In any case, the data indicated above should be archived (off-line) for at least five (5) years, down-sampled when necessary. The archived data should be made available following a request by another NCA or EMSA. The requestor must provide adequate reasoning as to why the information is required. This type of data may be used for purposes such as statistical analysis or studies on traffic flows.

System availability requirements

System availability refers to the availability of the hardware and software necessary for the performance of the mandatory functionalities of the SSN system.

The SSN system shall be maintained in operation twenty-four hours a day, seven days a week to satisfy the mandatory functionalities of the system.

Availability of the SSN system shall be maintained at 99% minimum over a period of one year, with a maximum permissible period of interruption being 12 hours per incident.

The same availability requirements apply independently/individually to each national SSN system (including the communication links to the central SSN and local systems) and to the central SSN system (and communication links to the national SSN systems).

Backup procedures

Backup procedures should be implemented for each SSN system component in the event of a failure or a scheduled interruption as provided in the "Common Operational Procedures ".

The NCA shall ensure that SSN messages are stored and transmitted to the central SSN system when communications and/or systems have recovered. The national and central SSN systems should be able to resend messages for up to 2 weeks.

The body responsible for the affected SSN system component must inform the other SSN system participants, in accordance with the operational procedures, whenever a failure or scheduled interruption occurs.

Additional system performance requirements

All participants should aim to prevent invalid messages (those not compliant with standards set in the SSN interface reference guide) from being sent. Nevertheless, invalid messages should be less than 0.1% of the total number of messages sent.

When the central SSN system receives an invalid message, an error message shall be produced and forwarded to the national SSN system. When central SSN system transmits an invalid message, the national SSN system should inform the MSS of the reasons for the invalid message as soon as possible.

[4] This requirement at the time of drafting this document is still to be implemented. Some of the relevant actions are planned for SSNv3.2

Data quality

MSs should ensure that the automatic data quality rules agreed by the SSN group are applied prior to notifications being sent to central SSN.

Missing information (that should have been provided in accordance with the SSN legal requirements) should be less than 0.1% per type of notification (PortPlus, incident reports etc.).

MSs should put in place, in cooperation with EMSA, the appropriate control mechanisms to investigate data quality issues that affect more than 0.1% of the reports per country and type (as per chapter **Error! Reference source not ound.**) per month.

Network coordination

Each NCA and EMSA should maintain a 24/7 contact point available to manage SSN related requests relating to daily operations or reporting issues from any other NCA or EMSA.

EMSA Maritime Support Services (MSS) provides 24/7 monitoring of notification requirements and network coordination as well as a helpdesk for the SSN system.

Other pertinent information concerning SSN data quality

The SSN system complies with the following requirements with respect to all information provided by the NCA or LCA..

Reliability - SSN system shall ensure that the information is available, accessible and usable under the defined conditions.

Confidentiality - SSN shall ensure that information is shared only among authorised persons or organisations (e.g. the information can be accessed only by the data provider or by accepted users). The level of confidentiality is defined for each type of information. Where information is requested via a national SSN system, the national SSN system is responsible for ensuring that information is only provided to authorised persons.

Integrity - SSN system shall ensure that the information is authentic and complete.
The information transmitted via the central SSN system is not modified unless by:

- its data provider;
- the NCA covering the data provider;
- the central SSN system, according to rule or procedure defined in the SSN documentation.

Traceability - SSN system allows the verification of the history, location, or application of the information by means of documented recorded identification.
The following actions are traced by the central SSN system and are available to the data provider at all times:

- Receipt of the information;
- Modification of the information;
- Request of the information through request/response mechanism;
- Communication of the information by any other mean.

The information recorded is:

- user identification
- time stamp
- description of action

The requirements above are translated into measures applied to the whole SSN system.

Appendices to Annex A (SSN technical/ Operational references)

Appendix A	SSN EIS System Design Document applicable to SSNv3.0
Appendix B	SSN SDDB applicable to SSNv3.0
Appendix C	SSN IFCD applicable to SSNv3.0
Appendix D	SSN XML Reference Guide v3.02 (version applicable to SSNv3.0)
Appendix E	CSD System Interface Guide applicable to the on-going MS pilot project
Appendix F	SSN Design Documents that could be made available to bidders on request
Appendix G	EMSA RFS for the implementation of the SSNv3.1 release
Appendix H	EMSA RFS for “Upgrades to the Central Organisation Registry of EIS for the implementation of a Shore-based Traffic Monitoring and Information Database (STMID)”