ANNEX III
Security Guidelines

Document Approval

	Name	Date
Prepared by:	EMSA	DD-MM-YYYY
Checked by:	SSN DCG	
Quality control by:	EMSA	
Approved by:	SSN group	

Change Control History

Version	Date	Description	For Info / Approval
0.01	16-11-2003	First Draft	Revision
1.00	25-02-2004	Release 1.0	Approved
1.10	02-04-2004	Incorporated feedback from Y.Hardy	
1.11	16-02-2005	Additional information about SSL	
1.12	30-03-2005	Incorporated feedback from EMSA	
1.13	12-04-2005	Incorporated feedback from EMSA	
1.14	27-04-2005	Page 48: changed E-Trust URL	
1.15	22-08-2011	Incorporated Internet Access, updates in sTESTA, SSN architecture modifications and interfaces, EMSA PKI services and annexes	
1.16	21-03-2012	Updates made to incorporate MS comments and HLSG 6 outcome.	
1.16	14-09-2012	• Document formatting; • Internet and STESTA Network accesses included in Security Enforcements chapter. Chapter 2 "Network access" removed as the document is not a "Network and Security guidelines" anymore (feedback from Italy); • Type of data description moved away from Introduction (feedback from Italy); • Addition of Traceability and Accountability measures at central SSN system (feedback from Italy).	

Version	Date	Description	For Info / Approval
1.16	15-11-2012	• Document structure updated to follow the IFCD chapter 7 (feedback from the UK); • Addition of Training and Audit (feedback from the UK); • Addition of technical background information in annex (feedback from Italy and the UK); • Distinction between the recommendations for the national SSN systems and their connections with Central SSN system and the requirements within central SSN system (feedback from Italy and the UK).	
1.16	10-01-2013	Draft to be submitted to the DCG (Jan 2013)	Revision

Document information

Filename	SSN Security Guidelines v1.16
Location	http://www.emsa.europa.eu/documents/technical-documentation.html
Number of pages	59

Cover photo credits: Flickr Creative Commons, Hair-Flick

Table of Contents

1. Introduction

This document describes the security requirements making part of the security policy defined in the IFCD chapter 7 which objectives are:

- To protect against the potential breaches of confidentiality, integrity or availability of an information/service;
- To ensure that all SSN information assets and computing and network facilities are protected against damage, loss or misuse;
- To ensure that all SSN Users are aware of and comply with rules which apply to the processing of information;
- To increase awareness and understanding of the requirements of information security and the direct responsibilities of users for protecting the confidentiality, availability and integrity of the data.

As stated in the IFCD, these requirements are to be enforced by the central SSN system and its interfaces with the National SSN systems and be referred to as optional at national/local level. The SSN authorities may assign similar or higher security measures on the system components they manage due their specific needs and policies as long as these additional measures do not limit the ability of duly authorised SSN users to access relevant information.

Each national administration should appoint individual(s) which are directly responsible of the security policy implementation within their area and which are in charge to ensure the security measures on the system components they manage (see IFCD section 7.2.1).

Future developments might lead to the identification of additional requirements to be met by the system. As soon as identified, further developments will require additional security measures aiming at keeping the objectives of the SSN security policy described above. These future additional requirements will become part of the SSN security guidelines.

The central SSN system has different interfaces available to facilitate different mechanisms of transmission. This document will also help understand the central SafeSeaNet system security features implemented by each interface to enable the secure exchange of information among the Member States.

The security requirements and implementations described here are based on the ISO/IEC 27001:2005 and ISO/IEC 27002:2007 international standards for information security.

The information contained in this document is not intended for general distribution. Only the appointed individual(s) by the each national administration in charge of the security policy implementation and their senior management should be aware of the contents of the document as the responsibility rest with them to ensure that the guidelines contained in it are followed.

2. Security Enforcements

2.1 SafeSeaNet Security Requirements

2.1.1 Introduction

This chapter is intended to provide the SSN Authorities in charge of implementing the SSN system in form of hardware and software and/or with responsibilities in terms of provision of access rights to the SSN system with the necessary information about the security features recommended[1] to be used to exchange data between Member States using SSN.

The SSN Authorities should clearly assign to specific responsible individuals the following minimum security related functions (which shall be adjusted to the needs and the organisation of each Member State):

a. Functions related to security management:

- Evaluation of requests to become a SSN user, against the user management rules described in the IFCD Chapter 3 and any other specific rule on access rights;
- Association of user roles and sets of user access rights;
- Ensuring, facilitating and carrying regular system security audits;
- Carrying out of training courses on security matters;
- Proposing review and update of the security policy of the authority; and of the security requirements deriving from the IFCD and the SSN documentation to the SSN group.

b. Functions related to security implementation:

- Technical implementation and monitoring of the security measures deriving from the IFCD and the SSN documentation;
- Technical implementation and monitoring of the security policy of the authority.

2.1.2 Access Control

a. All authorities implementing the SSN system in form of hardware and software residing at their premises should keep record of individuals gaining physical access to it

Each visitor should be recorded in a specific logbook containing at least the following information:

- To be filled by the security personnel:
  - name;

[1] Following the general security measures stated in the IFCD Chapter 7. They are reproduced in this section in bold.

  - reference to a personal document (identity card which must be checked by the security personnel);
  - organizations (name of the company for which work);
  - visit reason;
  - date;
  - arrival and departure time of the visitor;
  - contact person at premises;
- To be filled by the person:
  - signature.

The visitor should receive a temporary badge which should be used and visible during the whole visit.

b. Tailoring of privileges granted to a SSN user by the NCA administrator shall be performed as per access rights policy defined in the IFCD Chapter 3:

- The NCAs (via their individual(s) in charge of the security management functions) will be granted the right to manage their own SSN users for their own Member State using the SSN management console. Such user management includes adding, editing and deactivating of SSN users, along with setting their groups, roles and access rights (see IFCD Chapter 3 for further information);
- Each SSN user should be assigned to a role, which includes the access rights associated to a given profile in line with the applicable access rights distribution policy adopted by the SSN community. Each role should define a set of maximum privileges to be assigned to the user. However, these privileges could be further customised by the individual(s) in charge of the security management functions, at central or national level, creating the user profile, in order to meet the proper need to know of the User;
- Each user profile should be characterised within a group representing the user's category who want to gain access to SSN. SSN provides the NCA with a basic list of groups that are characterised within the system with a proper maximum set of privileges. However, in case a new group is required, the NCA should inform individual(s) in charge of the security management functions at central SSN system, who should act accordingly for the revision or the creation of groups;
- Each user should belong to one group. Each group should be characterised by a set of maximum privileges for each message, data type or feature available within the system. The NCA authority should modify these privileges in order to better tune the accesses to the system and not to compromise confidentiality of the system and of its data;
- All users accessing the SSN system (either at central or national level) should have access solely to the sensitive information they have been authorized/cleared to, based on the role assigned by the individual(s) in charge of the security management functions;

- Only needed access rights should be assigned to a user.

2.1.3 Authentication

c. A reliable authentication mechanism shall be implemented to uniquely identify the SSN users

A SSN user is a person (i.e. an SSN Web user using a browser-based web interface at central, national or local level) or a system (at national level the national SSN system, and at local level the SSN LCAs systems) accessing SSN by means of both automated systems (message based and streaming mechanism) and/ or the web interface (web-browser based mechanism). Authentication of a SafeSeaNet user depends on the interface chosen to connect to the central SafeSeaNet system:

- Authentication for SSN users accessing the system via an automated process is carried out at transport layer (i.e. by means of the client digital certificate) to authenticate the communication endpoint (for both XML messages and AIS streaming data interfaces) and carried out at business level by embedding the user credentials and the identification of the distinguished name information contained in the digital certificate installed at Member State application level (as per applicable xsd/ wsdl files) in the Header element of the XML messages;
- Authentication for SSN users accessing the system via the web browsing mechanism is carried out by user credentials (User ID and strong password).

d. Passwords should be compliant with the SSN password policy

Passwords should be compliant with the SSN password policy defined in Annex C: SSN Password Policy.Annex C: SSN Password Policy

e. **The creation of User IDs should follow the naming convention**

The creation of User IDs should follow the naming convention defined in Annex B: Common naming convention for human and system users.

f. **SSN Authorities implementing a web interface shall guarantee the authenticity of the web interface by appropriate means based on industrial best practices. For the central SSN web interface 1-way SSL will be implemented** (using certificates issued by a globally trusted CA)

Central SSN web interface uses SSL in combination with PKI to provide authentication of the server to the client (see Annex E: Technical background Annex E: Technical background

for more information on PKI services and 1-way SSL).

g. **SSN Authorities implementing a machine-to-machine interface shall guarantee the authenticity by appropriate means based on industrial best practices. For interfaces with the central SSN system 2-way SSL will be implemented** (using certificates issued by the EMSA CA)

SSL in combination with EMSA PKI (see EMSA PKI Services) has been adopted for incoming and outgoing communications with the central SSN system, providing authentication of the server to the client and of the client to the server (see Annex E: Technical background for more information on 2-way SSL).

For outgoing XML messages (sent by the central SafeSeaNet system to the national SSN system) the central SSN system is identified by its client digital certificate plus the credentials stored within the Header of the XML message. The national SSN system is identified by its server digital certificate.

In case of file download, e.g. Incident notification details available as PDF file on a Member State's file server, 2-way SSL should also be configured at Member State level. The Member State URLs are masked at central SSN system level and the file is made available without disclosing the exact location of data. The central SSN system will be in charge of downloading those files.

h. **A User ID should only be used by the appointed SSN user or users. Authorities in charge of providing access to the SSN system should keep a record of all accesses per User ID at their system level**

In case a User ID needs to be shared for operational reasons, a trace of the user accessing the system with the given credentials should be recorded by the system itself or by means of record on a logbook maintained at central and/or national level**.**

i. **A review of the credentials (e.g. password modification, user account revocation) used to access the SSN system should be performed at each system level regularly (at least each year) or whenever there is an upgrade of the SSN security policy affecting the authentication mechanism (e.g. SSN password policy):**

- A proper user account review procedure should be put in place by each authority part of the SSN system, to guarantee that all present users are still active and their credentials are still valid. Special attention should be taken after any user status change (promotion, downgrading, transfer, termination).
- User accounts should never be disabled (not physically removed) in order to prevent unwanted and uncontrolled accesses to the SSN system;

- Secure methods for creating and distributing temporary, initial-use passwords (in accordance with the SSN password policy defined in Annex C: SSN Password Policy.

  Forcing users to change any temporary/initial-use password and periodically change passwords and to use strong passwords at each change (in accordance with the SSN password policy defined in Annex C: SSN Password Policy.

  Prohibiting storage of passwords on computer systems in unprotected form. Passwords should be encrypted or hashed stored. Hashed with salt is recommended.

2.1.4 Authorization

j. Authorisation of the NCA by EMSA, or of the LCA (implementing a local system) by the NCA should be subject to the identification of the individuals in their organization responsible for the security management and security implementation:

- The National Competent Authority with administrator role willing to be authorised to gain initial access to SafeSeaNet will be contacting the MSS which administers the SSN User Accounts and Authorities. The authorities' details will be declared in the "Welcome on Board" document provided by EMSA for the access to the browser-based web and for the XML message-based interfaces. The "Conditions of Use for SafeSeaNet Data exchange through the STIRES interface" will be the equivalent for accessing the SSN streaming interface;
- The National Competent Authority with administrator role can create any SSN users under its responsibility. Authorisation of these users accessing the National SSN system should be subject to a security agreement (equivalent to the ones described aforementioned) between the NCA and the user.

k. SSN Authorities should grant access only to users in accordance with the rules in the IFCD Chapter 3

Authorization is made at business layer and depends on the user access rights linked to each SSN user. The definition of the SSN functional groups, roles and associated permissions (access rights) can be found in the IFCD - Chapter 3. The adoption of 2-way SSL (with EMSA CA) for incoming and outgoing communications provides mutual authentication. To protect users' attempts to masquerade other users from a different Member State during the message exchange protocol, an authorization process has been introduced in combination with authentication: the identification of the distinguished name information contained in the digital certificate installed at Member State application level has been made accessible to the central SSN system.

The central SSN system processes this information in order to authorize users to access the resources for which privileges have been granted.

l. A review of the authorisation (access rights) should be performed at each system level at least each year or whenever there is an upgrade of the SSN security policy affecting the authorisation protocol (e.g. change in the access right policy):

- review the user access rights at regular intervals (at least each year), and after any user status change (promotion, downgrading, transfer, termination) and change in the SSN access right policy;
- more frequent review of privileged ("super user") access rights.

2.1.5 Traceability and Accountability

m. Central SSN system allows the verification of the history, location, or application of the information from the mandatory system functionalities (as per IFCD – chapter 2.3) by means of documented recorded identification. **NCAs are responsible for collecting this security data at national level**.

n. The following actions shall be traced and the records shall be available to the data provider of the information upon request:

- **Receipt of the information.**
- **Modification of the information.**
- **Requests for the information.**

o. The information recorded shall be as follows:

- **User identification[2].**
- **Time stamp.**
- **Description of action.**

At central SSN system, all this information and user actions are stored at central SSN database level and available to all NCAs through the central SSN browser-based web interface (from the Search Logs section available in the Management Console).

p. Each SSN system (national and central) shall ensure the non-repudiation and traceability of actions performed by SSN users accessing the system by means of both automated systems (message based and streaming mechanism) or the web interface (web-browser based mechanism). An administration providing the information can request the identity of the data requestor, without delaying the response

As mentioned in Authorization section (bullet k), the central SSN system cross-checks the user ID transmitted in the FROM field in each message sent to central SSN system against the distinguished name information contained in the client digital certificate installed at Member State application level. Based on this control, the

[2] In case a user account is shared by a group of people sharing the same functions, the identity of all the persons that make use of the account shall be available.

central SSN system is protected against traceability of actions at MS application level. Central SSN system is able to block an attacker who is trying to abuse the XML interface of a MS (A) attempting to masquerade a user belonging to a MS (B).

2.1.6 Confidentiality

q. SSN authorities implementing the SafeSeaNet system in form of hardware and software and/or with responsibilities in terms of provision of access rights shall ensure that the confidentiality of the data stored within or exchanged by the system is not compromised. Data protection procedures shall be put in place

- To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorized entities. This implies that messages transmitted over the SSN network should be secure protected in terms of confidentiality, authentication and integrity. The messages transmitted over the network between national SSN systems and the central SSN system will be encrypted at transport level using SSL and PKI combined with HTTP and TCP/IP (see Annex E: Technical background). Other equivalent methods that could be implemented at national SSN systems could be the use of VPN(s) plus secure VPN protocols;
- Confidentiality or non-disclosure agreements reflecting the protection of the SSN system classified information and related information (e.g. user credentials) should be identified and regularly reviewed. These agreements should comply with all applicable laws and regulations for the jurisdiction it applies. As an example of confidentiality agreement, here follows the one used by the central SSN system:

  "Dear SSN user, please note that an account has been created by the system administrators in the SafeSeaNet (SSN) central system in order to administer your access. This account contains certain personal information (e.g. you name/surname, email address, telephone/fax number, etc.). The personal data of SSN users is processed in accordance with Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. It shall be processed solely for purposes relating to the SSN system. SSN users have the right to see their personal data and to request their national administrators (or in the case of users employed in a European Institution/Body, the EMSA administrators) to amend their personal information if it is inaccurate or incomplete. Should a user have any queries concerning the processing of his/her personal data, he/she should address them to his/her NCA administrator (or to the Maritime Support Services at EMSA if he (she) is employed in a European Institution/ Body). SSN users have right of recourse to the European Data Protection Supervisor at all times."
- Networks controls are to be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks to protect the exchange of information. E.g. using defense-in-depth layers as firewalls, reverse proxies, DMZ, VLANs, etc.

r. The SSN system shall manage data according to their confidentiality level for both data exchanged and data stored. According to Commission Decision

2001/844/EC amending its internal Rules of Procedure by annexing Commission Provisions on Security, the SSN system is classified as an "unclassified system". SSN nevertheless includes some commercial sensitive data, system security related information and personal data as follows:

- **"Commercial Sensitive" : all Hazmat, incidents and port call information;**
- **"System Security related" : user authentication password, security tokens and certificates;**
- **"Personal data": users' credentials and contact details of the person to provide details of certain information types.**

s. **Data storage shall be performed in accordance with the following rules:**

- **System Security related data shall be stored encrypted;**
- **Commercial Sensitive data shall be protected according to the access rights policy;**
- **Personal data should be stored in accordance with bullet w below.**

Classified (commercial, security and personal) information shall be protected during collection, processing and storage:

- The storage is located outside any public accessible environment (e.g.: restricted area, behind DMZ 2, etc.);
- Passwords for each environment (production and training) shall be stored in each environment (production and training) database;
- Classified information on paper or electronic storage media should be locked away;
- Back-ups should be protected by means of encryption where data is classified.

t. **Users shall not provide information to any unauthorised persons or systems**

- Contractors and third parties should not have access to operational (production) data nor to the operational facilities (production environment) except for supporting application/infrastructure monitoring or issue solving purposes. Contractors should only work with test data and test facilities (test environment):
  - The test system environment should emulate the operational system environment as closely as possible;
  - Development, test and operational software should run on different systems and in different domains (different VLANs);
  - Sensitive data (commercial, system security and personal) should not be copied into the test system environment;
  - Users should use different log-in credentials for the different environments.
  - Application and system documentation storage and distribution shall be protected against unauthorised access (e.g.: documents distributed via extranet with login credentials access).

u. Users shall not disclose their log-in credentials to unauthorised persons

- At core, national and local system level, passwords should be security sensitive classified. Password hashing should be used during message exchanged and database storage;
- The confidentiality of the system should be enforced also by physical users of the SSN system, who should not disclose their log-in credentials to anyone. To better enforce this mechanism, user workstations should not permit to save log-in credentials to the SSN system.

v. Users shall not provide to the SSN system classified information as defined by Commission Decision 2001/844/EC

See Commission Decision 2001/844/EC Appendix 2: Practical classification guide.

w. The principles of personal data protection as defined in Directive 95/46/EC shall be applicable to any information concerning an identified or identifiable person exchanged through SSN system. In addition, the central SSN system shall comply with Regulation (EC) 45/2001 on protection of data by the Community Institutions and bodies and in accordance with Directive 2001/45/EC for EMSA

The following principles shall be applicable:

- subjects whose data is being collected shall receive notice of such collection;
- data collected shall be used only for stated purpose(s) and for no other purposes;
- personal data shall not be disclosed or shared with third parties without consent from its subject(s);
- once collected, personal data shall be kept safe and secure from potential abuse, theft, or loss;
- subjects whose personal data is being collected shall be informed as to the party or parties collecting such data;
- subjects shall have access to their personal data and shall be allowed to review and correct any inaccuracies;
- subjects shall be able to hold personal data collectors accountable for adhering to all seven of these principles.

2.1.7 Integrity

x. SSN shall ensure that the information is authentic and complete. The information transmitted via in the central SSN system shall only be modified by:

- **the data provider;**
- **the NCA covering the data provider, or;**
- **the central SSN system (in accordance with the rules/procedure defined in the SSN documentation).**

Integrity is the way to protect the accuracy and completeness of information. Integrity of data exchanged through the public Internet or STesta (more detailed information available in Annex E: Technical background

Annex E: Technical background) between the national/local SSN system and the central SSN system should be assured by the use of 2-way SSL encryption algorithm for both data requests and response in case of machine2machine interface. The SSL protocol with PKI will be used to guarantee that data is not been altered during the communication.

y. The management of data provision shall ensure all reasonable steps have been taken to prevent denial of service attacks, the introduction of `malware', or other malicious events with the potential of compromising SSN functionalities

- In order to prevent downtimes and to try to limit possible malicious attacks, the whole SSN network should be controlled by means of proper monitoring tools (e.g. IDS (intrusion detention systems), IPS (intrusion prevention systems), data loggers, etc.), in order to keep under control both the status of the network and the data exchanged;
- Each authority taking part in the SSN system should foresee the continuous availability of the SSN system as per agreed SLAs and security enforcing functions like:
    - Access control mechanisms and data;
    - Authentication mechanisms and data;
    - Authorisation mechanisms and data;
    - Confidentiality mechanisms;
- In order to meet the availability requirement, replication or backup of critical security mechanisms should be taken into account;
- A proper business recovery plan should be put in place for such devices, in order to restore them in the shorter time as possible in case of failure or service disruption;
- Enhanced protection measures (such as installation of the equipment in a restricted area, Business Continuity Facilities, forbidden access for normal users etc.) should be applied to critical WAN/LAN components (e.g., servers, routers, communications);
- Servers hosting the application at national, local or central level should be made redundant in order to prevent service failures. System Administrators should foresee a proper check and update synchronisation between the two servers. This process should be performed every night;
- A proper business recovery plan should be prepared for the involved devices in order to foresee procedures for fast switch over in case of failure. In the same way the business recovery plan should take into account the recovery of the failure on the affected system so that the replication is assured.

z. The list of hardware and software, used to implement the SSN system or used within the authority to interface with it, shall be recorded in a register. This register shall be maintained during the whole system lifecycle

- An inventory of the software configuration of the system should be maintained by the individual(s) in charge of the security implementation functions and should be shared with the individual(s) in charge of the security management functions in case of audit. The following items describe the information which is to be kept in the inventory for every S/W delivery and installation of SSN application releases:
  - Software package and version;
  - Which version(s) is(are) active;
  - Release date;
  - Release notes;
  - Installation notes;
  - Installation date;
  - Installation location;
  - Store location (source code);
  - Created by.
- An inventory of the hardware configuration of the system should be maintained by the individual(s) in charge of the ICT infrastructure and should be shared with the individual(s) in charge of the security management functions in case of audit. The following items describe the information which is to be kept in the inventory:
  - Machine name, IP, number of CPUs allocated, memory allocated/used;
  - Environment;
  - Created by;
  - Created on;
  - Technology used;
  - Software installed.
- Both inventories should be maintained, and retained for all the life of the system in secure places that are only accessible by authorised staff. This information should be properly backed-up.

2.1.8 Training

aa. Each authority shall ensure that all system users within its jurisdiction are aware of the security requirements of the system and have the knowledge and competencies to fully discharge their obligations

- Each authority shall foresee security awareness campaigns to all system users, contractors and third party users, in order to increase their knowledge about their responsibilities and their duties while using the system. Awareness sessions should include an introduction of the SSN security guidelines, be suitable and relevant to the person's role, responsibilities and skills and include information on who to contact for further security advice and the proper channels for reporting information security incidents (the individual(s) in charge of the security management functions at national and central SSN level);

- The individual(s) in charge of the security management functions shall plan a periodic training update sessions within their general training plan. These sessions should be paired with training level evaluation sessions;
- Training sessions shall be attended by all personnel involved in SSN operations and they should be focused on both operational and security aspects;
- In case of system modification or adoption of new security measures, a specific training update session should be carried out by the individual(s) in charge of the security management functions involving all the relevant staff dealing with the system;
- Operative sessions should include aspects about the correct use of information processing facilities such as, for example, log-on procedure, sessions time outs, password management systems, etc.;
- The individual(s) in charge of the security management functions should be in charge of managing periodic training meetings within the organisation. During this activity, personnel should be informed about:
  - The information that every user is allowed to access to in accordance with their role;
  - The security measures to be adopted to preserve the availability, confidentiality and the integrity of the system;
  - The business continuity plan;
  - Back-up procedures established by system administrators, addressing the frequency of back-ups, the storage requirements on-site and off-site and the control of authorized access to back-up copies;
  - Procedures to report hardware and software failures as soon as possible.
- In order to evaluate the level of personnel training, the individual(s) in charge of the security management functions should foresee training and security awareness assessment sessions. They could be carried out by means of questionnaires and submitted to all the users. Filled questionnaires should be returned to the individual(s) in charge of the security management functions who will be in charge of evaluating answers and, eventually, foresee specific sessions to fill the identified gaps.

2.1.9 Audit

bb. Security audits on the SSN system implementation and usage should be carried out on a regular basis or in case of events defined within the SSN Technical and Operational Documentation. Whenever possible, existing auditing arrangement will be accepted as the fulfilment of this requirement

- A secure audit trail should be created and maintained by the system, by means of internal logging of activities and anomalies. These logs should be protected from unauthorized deletion and/or modification. They should be available for access only to the individual(s) in charge of the security management and implementation functions. The audit trail should be presented to the individual(s) in charge of the security management functions in human-readable format either directly (e.g. storing the audit trail in human-readable format such as a pdf) or indirectly (e.g. using audit reduction tools) or both.
- Areas that should be audited from a security point of view are: SSN hardware and software system, the security policy and the trainings;
- The audit is used to monitor the progress and the effectiveness of the new system implementation. Central SSN system passes a security audit every time a major release is implemented.

cc. Following a security breach there should be an investigation to identify the cause and any remedial actions required

- The logical implementation of SafeSeaNet should provide automated means to analyse and review system activity and audit data, in order to look for possible or real security violations. This facility should enable the generation of automatic audit information in case of:
  - successful log-on;
  - unsuccessful log-on;
  - tentative of violation of security measures;
  - accesses to documentation stored within the system.
- Appropriate privacy protection measures should be taken (e.g. passwords in plain text should not be appearing in the logs). Logging facilities and log information should be protected against tampering and unauthorised access (only the individual(s) in charge of the security management and implementation functions should have access);
- By analysing the traffic over the network it will be possible to identify patterns that lead to malicious or unwanted events;
- (ITIL) Problem Management process, focused on implementing the appropriate corrective actions to address problems is recommended.

2.2 Central SafeSeaNet system Security Implementations

2.2.1 Introduction

This section gives an overview of the SafeSeaNet security requirements implemented within the central SSN system.

2.2.2 Central SafeSeaNet system architecture

As explained in the SSN XML Messaging Reference Guide, the heart of the SafeSeaNet architecture consists of the SafeSeaNet XML Messaging System acting as a secure and reliable yellow pages index system and as a "hub & spoke" system (including authentication, validation, data transformation, logging, auditing,…), for sending requests to and receive notifications and responses from the right Member States (and corresponding NCAs).

The system is using:

- standard Internet protocols (XML, HTTPS,…);
- PKI infrastructure (EMSA PKI services);
- Internet network or S-TESTA network[3];
- 2-way SSL communication between the central SSN system and the MS systems.

SafeSeaNet system provides three different interfaces mechanisms to help the Member States communicate with the central SafeSeaNet system:

- A browser-based web interface
- An XML message-based interface made available in two forms:
  - A SOAP-based web-services one (refer to the applicable .wsdl file in the SSN domains, both for Production and Training environments);
  - A bare XML messages one (refer to the applicable .xsd file in the EMSA extranet – protected area).
- A streaming interface to enable constant flow of AIS data.

2.2.3 SafeSeaNet Digital Certificates and EMSA PKI Services

This section describes the EMSA PKI services and the procedures that the Member States should follow to request or revoke a digital certificate.

More detailed information is available in Annex E: Technical background for general information on digital certificates and PKI services.

[3] The use of sTESTA or Internet is a question of choice and EMSA will support both type of connections. The connection method shall provide guaranteed service levels for network availability, performance and security (see IFCD- Chapter 4 for SafeSeaNet performance and Chapter 7 for System Security).
Refer to Annex E: Technical background for general information on how to set up an Internet or a sTESTA connection.

2.2.3.1 EMSA PKI Services

The EMSA PKI is a particular infrastructure devoted to the EMSA maritime application user communities and provides the following services:

- A set of trusted procedures and of associated services to create, renew and revoke public key certificates;
- Availability of the public keys associated with each user, under the form of Public Key Certificates (PKC) guaranteed by the EMSA Certification Authority (CA);
- Availability of Certification Revocation List (CRL), allowing the user to check the validity of a given certificate.

Compared to the general organisation of a PKI (see Annex E "Components of a PKI"), the EMSA PKI adds the following concepts:

- **Closed User Group** (CUG): the creation of a CUG means that the stringent requirements imposed by the CA on public Registration Authorities can be relaxed towards the needs of the CUG. The CA will only sign EMSA-CUG certificates for the users who have been approved by the relevant RA, which goal is to verify the identity of the users requesting the certificate, and approving or rejecting the certificate request. In the frame of central SSN system and its interfaces with the national SSN systems , there will be a single RA played by the EMSA Maritime Support Service (see SafeSeaNet PKI CUG below);
- **Suspension and Revocation Authority** (SRA): the SRA's goal is to handle all revocation requests of the CUG users. The SafeSeaNet SRA will represented by the EMSA Maritime Support Services.

2.2.3.2 EMSA PKI Technical aspects

The generic EMSA PKI architecture is based on the market standards:

- Certificates follow the X.509 V3 standard and CVC certificates according to EAC 1.11 (BSI TR-03110);
- Compatible with the PKIX standard.

The PKI infrastructure that will be used is the the EJBCA Open Source PKI.

2.2.3.3 Type of certificates

Server and client certificates will be issued for the national SafeSeaNet systems.

Such type of certificates may be requested remotely via the individual(s) in charge of the security management functions at national level (at NCA level) which shall submit proof of fact that this person is duly authorized to sign for the Member State legal representative. These digital certificates will be RSA certificates with a 1024-2048 bit key length valid for two years.

2.2.3.4 SafeSeaNet PKI CUG

A dedicated SafeSeaNet PKI CUG has been defined and managed by EMSA.

The SafeSeaNet CUG requires a "SafeSeaNet Registration Authority Officer" and a SafeSeaNet "Member State Certificate Officer" for every Member State.

2.2.3.4.1 SafeSeaNet Registration Authority Officer

EMSA will be the SafeSeaNet Registration Authority and represented by EMSA Maritime Support Services. The EMSA designated SafeSeaNet Registration Authority Officer is the Maritime Support Services Officer.

Its role is to be single point of contact for the Member States to issue the digital certificates. He/She will receive the requests/revocations for digital certificates, verify them, generate the digital certificates and send them back to the corresponding Member State.

2.2.3.4.2 SafeSeaNet "Member State Certificate Officer"

Every Member State, via their individual(s) in charge of the security implementation functions, should designate an administrator that will be in charge of requesting, installing and managing the server certificate at National level.

The role of this administrator is to be the single point of contact between a Member State and the SafeSeaNet Registration Authority Officer. He/She will send the request for digital certificates (see "How can a Member State apply for a digital certificate?" for more details on an e-mail. He/She will receive back (via e-mail) the requested digital certificate for installation.

2.2.3.5 Certificates Management

The management of SSN Digital Certificates will be done in accordance with the following rules:

- A unique PKI Service will be established for SafeSeaNet (at central and national SSN systems);
- SSN PKI Service will be managed by EMSA. The certificates will be issued by EMSA CA using the intermediate CA. Creating certificates directly from the CA root certificate increases the risk of EMSA CA root certificate compromise (if the private key is being stolen, the entire infrastructure will be affected). The usage of intermediate certificates for issuing end-entity certificates provides an added level of security.
- NCAs shall request and revoke SSN Digital Certificates using the EMSA PKI Services;
- LCA, after NCAs authorisation and in accordance with the Security Agreement between NCA and LCA, shall request and revoke SSN Digital Certificates using Commercial PKI Services.

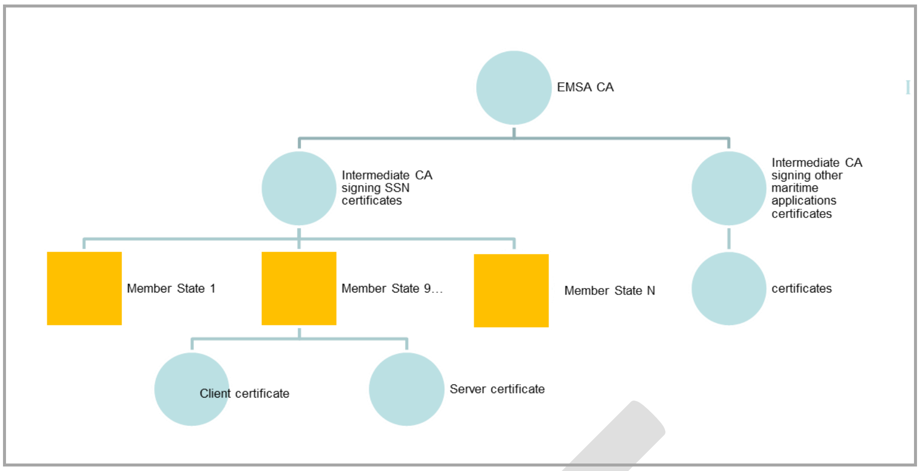

EMSA CA
Intermediate CA signing SSN certificates
Intermediate CA signing other maritime applications certificates
Member State 1
Member State 9…
Member State N
certificates
Client certificate
Server certificate

Figure 1 –Certificates management

2.2.3.6 PKI needs for SafeSeaNet

Every national SafeSeaNet user will be assigned the required digital certificates to guarantee confidentiality and authentication when exchanging messages. The table below describes the different types of SafeSeaNet users for which the PKI has been established (LCAs are not to be connected to central SSN system and as such can make use of commercial PKI services) and their corresponding type of certificate:

SafeSeaNet User Type	Description
National SafeSeaNet system	A *national SSN system* (developed by Member States for exchanging XML messages or AIS data streaming with the central SSN system) will make use of the SafeSeaNet services and is therefore considered for SafeSeaNet as a single user. Consequently, digital certificates will be assigned to every *national SSN system*: • Client certificates must be installed on the application servers sending SSN data; • Server certificates must be installed on the web/application servers receiving SSN data.
Central SafeSeaNet system	The central *SafeSeaNet* system stands for the core system that will offer the services for exchanging XML messages (notifications, requests, and responses) between the *national SSN systems*. Therefore, two digital certificates (client and server) will be assigned to the single central SafeSeaNet system (to be installed on the application server receiving and sending the XML messages).

2.2.3.7 How can a Member State apply for a digital certificate?

The procedure for requesting a digital certificate is described below. This procedure is the same for the renewal of the certificates (every 2 years after expiration). In case of renewal, the Maritime Support Services reminds the concerned party, before the expiration date on the renewal request.

2.2.3.7.1 Prerequisites

Prior to applying for a digital server certificate, every Member State must set up the corresponding application servers (for sending and/or receiving SafeSeaNet XML messages or send AIS streaming data) at their local (National) site. EMSA CA delivers client and server certificates for any server compatible with the X509 v3 standard digital certificates and that are able to make a PKCS # 10 (PEM encoded) electronic certificate request. This covers most of the recent web application servers available nowadays.

The application server must then be compatible with the X509 v3 protocol that enables secure end-to-end electronic data exchange.

The application server should also have a DNS domain name registered in its configuration file. During the generation of the certificate request, you will be prompted to enter some specific information about your server. This information is very important since it will be the one that will be certified by EMSA CA. The most important part to enter correctly is the name of your server (CN). It must correspond to the registered Web site server name you will protect when requesting server certificate. Indeed, if the real server name does not match the name in the certificate, you will never be able to start your SSL Server sessions. When requesting a client certificate, the CN can be the machine's name, the requester's email, etc.

For the Member States connected through the Internet, you have to make sure your DNS domain name is well registered and recognized officially by an Internet Service Provider

In the framework of the SafeSeaNet project, for the Member States connected through sTESTA backbone, the full DNS domain name should be registered as follows on the web server of every Member State: SSNxxx<Country_Code>[4]TESTA.EU

2.2.3.7.2 Stakeholders

The following stakeholders will intervene in the workflow for requesting a digital certificate:

- The EMSA Certificate Authority;
- The SafeSeaNet Registration Authority Officer (Maritime Support Services Officer);
- The SafeSeaNet "Member State Certificate Officer".

2.2.3.7.3 Procedure

The procedure to follow depends on the mechanism chosen by the Member State to connect to the central SSN system:

- In the case of XML message based mechanism, procedure for the Messaging Interface is the applicable;

[4] <Country_Code> is composed of two characters of your country (i.e. Ireland:IE, Greece:GR,…)

- In the case of AIS data stream mechanism, procedure for Streaming Interface is the applicable.

Both procedures (Annex A: SSN certificates procedure) request to generate a CSR per digital certificate.
In order to create a CSR, first a private key shall be generated, that shall remain in the application server key store. The CSR is created using this private key and contains the public key of the application server with some metadata.

This public key and metadata is the CSR that will be sent to the Maritime Support Services. This public key will be included in the certificates.

The certificate created with a particular CSR will only work with the private key that was generated with it.

2.2.3.8 How can a Member State revoke a digital certificate?

Revoking a digital certificate might occur when the private key is lost or accidentally shared. A presumption of hacking is also an urgent reason for revocation.

2.2.3.8.1 Prerequisites

The revocation code shall be the same as the one used for the certificate signing request creation.

2.2.3.8.2 Stakeholders

The following stakeholders will intervene in the workflow for requesting a digital certificate:

- The SafeSeaNet Registration Authority Officer (Maritime Support Services Officer);
- The SafeSeaNet "Member State Certificate Officer".

2.2.3.8.3 Procedure

The procedure is the following:

Step	Action	Actor
1	Call, email or fax immediately the SafeSeaNet Registration Authority Officer (Maritime Support Services Officer) at: ▪ Tel: + 351 21 1209 415, ▪ Fax: +351 21 1209 480, ▪ Email: MaritimeSupportServices@emsa.europa.eu	The SSN "Member State Certificate Officer"
2	As soon as the revocation is being acted, apply for a new digital certificate.	The SSN "Member State Certificate Officer"

2.2.4 SSN data exchange protocols

In order to ensure authentication, confidentiality and integrity around the exchange of SSN data between the national SafeSeaNet systems and the central SafeSeaNet system, HTTPS and SSL over TCP/IP must be used along with the supplied digital certificates for the different interfaces mechanisms provided by the central SafeSeaNet system.

More detailed information is available in Annex E: Technical background for a description of the SSL protocol and the SSL handshake.

2.2.4.1 HTTPS with Server Certificate

1-way SSL (with commercial CA) is implemented at SSN web interface level. When SSN Web users access the SSN web interfaces (for both Production and Training environments) they will be presented with the Commercial Global Sign server certificate issued specifically for those interfaces. The digital certificate installed at server level fulfils that the information exchanged within the SSN web interface keeps its integrity and confidentiality (through SSL encryption). It also allows the authentication of the central SafeSeaNet system via the SSN Web user browser.

The central SSN web interface, apart from user identification and authentication and password management controls has implemented session time-out as access control mechanism to prevent unauthorized access to operating systems.

2.2.4.2 HTTPS and SSL over TCP/IP with Client & Server Certificates

2-way SSL (with EMSA CA) will be used to exchange XML messages and AIS data stream between the central SafeSeaNet system and national SafeSeaNet systems (including Regional and National Proxy servers). The first recipient of any sent SSN data is always the application server of the target recipient. Once received at application level, and after the exchange of the digital certificates for authentication of the sender and the recipient servers, the SSN data is in clear (setting up the SSL session is carried out behind the scenes).

Additionally, when detailed information of notifications are made available for download as files on a national SafeSeaNet system’s web server, HTTPS (2-way SSL) should also be used to let the central SSN system download these files. The central SSN system shall be the only SSN user to be able to download files from national SafeSeaNet systems servers.

Such a solution fulfils data integrity, confidentiality (through SSL encryption) and authentication of both client and server applications (through the usage of the national SSN systems certificates and the central SafeSeaNet system server’s certificates).

This solution requires:

- In case of using the messaging interface, both the central SafeSeaNet system and every national SafeSeaNet system should supply a single address (URL to a single page on the web server) for receiving XML messages (requests or responses). HTTPS (by default on port 443) must be configured on these application servers for accessing their single page receiving the incoming XML messages (requests or responses). Firewalls and/or proxies should also be configured to allow HTTPS from/to these application servers.

- In case of using the streaming interface, both the central SafeSeaNet system and every national SafeSeaNet system should assign a unique TCP/IP port to each data stream application instance (Ref. NPR User-Manual for a more complete description).
- Generation of client and server digital certificates by EMSA CA.
- The installation of the EMSA root CA and client digital certificates on the central SafeSeaNet system server and on the national SafeSeaNet system servers providing XML messages or AIS data stream (acting as client). The client only needs the root CA to be stored in its key store which will use to verify the authenticity of the intermediate certificate presented by the server when the client connects to it (the server will send the chain intermediate certificate + server certificate).
- The installation of the EMSA root CA (if the application server is different from the application client), the EMSA intermediate and server digital certificates on the central SafeSeaNet system server and on national SafeSeaNet system servers receiving incoming XML messages (acting as servers). These application servers need also to be configured to require HTTPS and client certificates for accessing their single page receiving the incoming XML messages (requests or responses).
- For both connections, central SSN system to Member State and Member State to central SSN system, access should be granted only to application servers (acting as SSL server and/or SSL client) signed by EMSA CA

Annex A: SSN certificates procedure

1. Confidentiality and 2-way SSL

Member States have adopted the 2-way SSL method (Secure Socket Layer) to ensure SSN data security. Digital certificates should be installed both at the system server hosted by EMSA as well as the site where the SSN-EIS National System, hosted by the National Authorities, will be installed.

EMSA has created its own Certification Authority (CA) to issue the digital certificates used in the SSN communication process. To provide your Administration with the certificates you are kindly requested:

- To complete and send the "Appointment of the Officer Responsible for the Server" and the Certificate Registration Form (included in Appendix I and Appendix II)
- To generate the Certificate Signing Requests (CSR) for both client and server certificates (refer to http://www.openssl.org/ for general instructions or to https://www.geotrust.com/support/generate-csr/ for specific instructions depending on the server type)

2. Digital certification procedure

The following procedure should be applied by your Administration for getting the SSN-EIS 2-way SSL server and client certificates:

1. Open a call to the Maritime Support Services of EMSA (Tel: + 351 21 1209 415, Fax: +351 21 1209 480, Email: MaritimeSupportServices@emsa.europa.eu) requesting for the digital certificates for SSN-EIS.
2. The MSS will request your Administration to complete the "Appointment of the Officer Responsible for the Server" (see appendix I), the Certificate Registration Form (see appendix II) and to send the Certificate Signing Request (CSR).
3. Your Administration will send back to the MSS, by e-mail (signed documents have to be scanned into PDF files) the following documents, for both client and server certificates:
   a. The Certificate Registration Form;
   b. The Appointment of the Officer Responsible for the Server;
   c. The CSR file;
   d. A legible photocopy of a valid identity card of the Officer signatory to the Registration in a) above (and appointed under b) above).
4. After verification, the MSS will inform your Administration about the status of the application.
5. EMSA will send to the e-mail address of the Officer Responsible (that appears in the Registration Form) the digital certificates. MSS will be available to support your Administration if discovered any errors or defects in the certificate.

6. Your Administration will install the digital certificates issued by EMSA only on the server corresponding to the domain indicated on the said certificates (in the Common Name field).

7. If problems occur during the procedure, your Administration may contact the MSS.

8. Your Administration will inform the MSS about the completion of the task.

9. Your Administration should follow the above mentioned procedure when the certificate's renewal becomes due.

Appendix I – Appointment of Officer Responsible for the Server

The undersigned, _ , in his/her capacity as representative of the Organization/Authority named _ designates Mr./Ms. _ , as specified in the *Certificate Registration Form* application, as designated Officer Responsible for the Server in observance of the requirements related to the digital certification procedure.

Place and date _

Signature of representative and stamp of the Organization

_ _

Appendix II – Certificate Registration Form

(ATTENTION: to be filled-in per Certificate Request)

System	Choose an item. Click here to enter text. ☐ EMSA internal
Environment	Choose an item.
Type of certificate	Choose an item.
Information about the Officer Responsible for the Server[1]	**Value**
First Name	Click here to enter text.
Last Name	Click here to enter text.
E-mail [2]	Click here to enter text.
Company Name	Click here to enter text.
Registered Office Address	Click here to enter text.
City/Town	Click here to enter text.
Postal code	Click here to enter text.
Province	Click here to enter text.
Telephone	Click here to enter text.
Fax	Click here to enter text.
First Name of the Representative of the Organization [4]	Click here to enter text.
Last Name of the Representative of the Organization	Click here to enter text.
E-mail of the Representative of the Organization [5]	Click here to enter text.
Certificate Request (.csr) Information This info needs to match the corresponding values in the .csr file	**Value**
Common Name (**CN**) [6]	Click here to enter text.
Organization Name (**O**)	Click here to enter text.
Organization Unit (**OU**) [3]	Click here to enter text.
City (**L**)	Click here to enter text.
Province (**ST**) (server certificates only)	Click here to enter text.
Country (**C**)	Click here to enter text.

Additional Information	Value
Revocation code [7]	Click here to enter text.
End-point [8]	Click here to enter text.
Type of webserver	Choose an item. Click here to enter text.

[1] The Officer Responsible for the Server is the operational reference person, authorized by the Representative of the Organization.

[2] The electronic mailbox to which the Registration Form and the issued certificate are sent.

[3] The Organization Unit of the web server is that which appears in the *Organisational Unit* (OU) in the *subject* field of the certificate.

[4] The representative of the Organization is the person indicated by the appointment signed by the Legal Representative, or equivalent.

[5] The electronic mailbox to which the Registration, which must be signed by the representative of the Organization or equivalent; the Appointment of the Officer Responsible for the Server and the issued certificate are sent.

[6] The Fully Qualified Domain Name (FQDN) in case you are requesting a server certificate.

[7] The revocation code is used to verify telephone requests. It consists of 9 numbers uniquely associated to the certificate requested. This code cannot be repeated on other forms.

[8] The end-point is only needed for EU LRIT DC certificates (*e.g.: https://es-evtest.member-state.eu/lrit2es, using SSL*)

Place and date ________________________________

Signature of the Officer Responsible for the Server

____

Annex B: Common naming convention for human and system users

It is proposed that the following common user naming convention should be enforced in SafeSeaNet. To enhance clarity, and to avoid confusion, two separate schemas are presented below, with one being for “human users” and the other for “system users.” A common set of rules applicable to both schemas is also introduced below.

1. General rules applicable to the common naming convention

The following general rules should apply commonly, either for human or system userIDs:

a) The following notations are used in defining the user naming schemas in this document:

<*chars*> : means mandatory; [*chars*] : means optional;

italics : indicates a type of field; **bold**: indicates literal text to be used

b) The notation *ISO-country-code* corresponds to the alpha-2 (two characters) country code in the ISO 3166-1:2006 standard. This should be used to indicate the names of countries and their subdivisions.

The following special rules should be taken into account:

i. If values other than the officially assigned “A-to-Z” ISO codes are to be used, these must be indicative of the relevant organization.

The ISO 3166-1 standard already foresees room for user assigned values (e.g. XA=Bonn Agreement; XB=Black Sea Commission; XM=MAOC-N; XN=NATO; XI=IMO; XP=Paris MOU on PSC; etc.).

A dedicated mapping table should be developed to map “X-type” specific cases when the user cannot be associated to a specific country or to only one country (e.g. specific missions, regional agreements, etc.).

ii. the value ‘EU’ is used to indicate that the user belongs to an EU institution or agency.

c) The following ASCII characters are **allowed** (regex character set): [a-zA-Z0-9._-]

d) User names **cannot** contain the following characters:

backslash (\)	greater than sign (>)	apostrophe (')	caret (^)
slash mark (/)	less than sign (<)	parentheses (())	at sign (@)
colon (:)	question mark (?)	vertical bar (|)	braces ({})
semi-colon (;)	exclamation point (!)	ampersand (&)	tilde (~)
comma (,)	number sign (#)	quotation mark (")	percent (%)
asterisk (*)	dollar sign ($)	whitespace (‘ ’)	

e) it cannot contain empty spaces and special characters (e.g. "van de Rompuy" becomes *vanderom*, "arnviðrd" becomes *arnviord*, "agmær" *agmaer*; "björn" or "bjørn" becomes *bjorn*, etc.);

f) userID can **contain,** but **not begin** with, a period (.), an underscore (_) or a hyphen (-). Characters such as2 +*-0032 period (.), underscore (_) and hyphen (-) are allowed as separators.

g) UserIDs are **NOT** case sensitive.

2. Recommendations

The following **recommendations** are common to both human and system userID's:

a) If the user belongs to an EU agency or other institution, this should be indicated within the user name with a dedicated value. The same principle should be applied to users in regional, national or local authorities (e.g. port, coastal, flag state etc.). A list of possible values is shown in Table 1.

b) The userID should **not** be **less** than 7 characters, and **not more** than 17 characters, including separators (this is a recommended value as, technically, the maximum length is set to 75 characters).

c) The use of separators is recommended, especially to separate and distinguish the different parts (whenever necessary).

3. Common naming convention for "human users"

The following schema[5] is proposed for the creation of userIDs for human users, along with a short description of the basic rules to be applied. Existing users' IDs should be migrated to the new schema in accordance with an agreed "migration plan."

<ISO-country-code_>[**CN_**]*<chars>*

Examples: IT_FIAMMLO (or) it_fiammlo

(Nat.: '*Italian'*; String indicating the user ID (chars): '*fiammlo*')

It_CN_FiammLo

(Nat.: '*Italian*', Special ind."_CN_", String indicating the user ID (chars): '*fiammlo*')

The same user can be named differently, but only once

a. The <*ISO-country-code*> is a mandatory part and shall respect the general rules in 1.b above. It is used to indicate that specific human users are linked to an organisation/authority in a certain country. It shall be followed by a '_' (underscore).

EMSA users are exempted from having the ISO-country-code placed before their user names (a specific rule will be enforced at EMSA infrastructure level).

b. [**CN_**] is an optional notation that can be used to indicate that the user belongs to a contractor.

[5] Underscore signs ("_") shall be used to divide the sections of the user name.

For example, a user working for a contractor engaged by a national administration may have a username such as "***FR_CN_1***", while for a contractor engaged by EMSA, it could be "***EU_CN_04***" (the section after the "CN_" is only an example - it could be a number or an alpha-numerical string).

c. The <*chars*> attribute is a mandatory part for human users. The *chars* notation should represent the name of the actual user and should respect the following rules:

- It should have a minimum length of 3 characters and a maximum of 10.
- It is recommended that 7 characters are used, and it should respect one of the following structures:
    - **<5-chars-lastname><2-chars-firstname>**
    - **<first-char-firstname><lastname>**
    - **<firstname><.><lastname>**

Where necessary, the following may be applied:

- In the combination <5-chars-lastname><2-chars-firstname>, or in <first-char-firstname><lastname>, if the family name is less than 5 characters (e.g. Sa, Cau, Bono, Mils), the chars notation is built by adding the last name plus a portion of the first name, up to the completion of the 7 chars:

– Matilde Sa	*samatil*
– Paolo Bono	*bonopao*
– Mike Blue	bluemik

- If the combination firstname.lastname is less than 7 characters in total, the chars notation is built by adding the first name plus the last name followed by a portion of the first name, up to the completion of the 7 chars:

– Fil Pa	*fil.paf*
– Joe Sa	*joe.saj*

d. The user name can be used to indicate that a user belongs to a specific category of institution or authority. To this end, it is recommended that a special value of 3 characters should be included. The envisaged values are shown in Table 1 (the list is to be considered to be indicative only, and not exhaustive).

Value	Description	Value	Description
POR	Port	NCA	National Authority
CST	Coastal	BCL	Border Control
FLG	Flag	LWE	Law Enforcement
POL	Pollution	NDE	Navy/ Defense
REM	Regional/Mission	CUS	Customs
PLC	Police	PSC	Port State Control
ADM	Administrator	SEC	Security

Value	Description	Value	Description
ENT	DG Enterprise	EFC	EFCA
EMS	EMSA	COM	EU Commission
MOV	DG MOVE	JRC	EU Joint Research Centre
TAX	DG TAXUD	FRX	Frontex

Table 1 - List of special values to be included in the user name <chars>

4. Common naming convention for "system users"

The following schema[6] is proposed for the creation of userIDs for system-users,' together with a short description of the basic rules to be enforced.

<**sys_**>[*alpha-3-function_*]<*ISO-country-code_*>[*alpha-3-location-code_*][**CN_**][*chars*]

Example: sys_ncaesmad1

(Function: 'NCA'; Nationality: 'Spain'; Location: 'Madrid', Interface: 1)

sys_ES_MAD

(Type of user: '*system'*; Nationality: '*Spain'*; Location: "Madrid"*)*

sys_ES

(User type: 'system'; Nationality: 'Spain')

sys_ES_CN_1

(Type of user: '*system'*; Nationality: '*Spain'*; Contractor; Interface: 1)

The same user can be named differently, but only once

e. The <**sys_**> prefix is **mandatory** for all system users.

f. The [*alpha-3-function_*] is an **optional** acronym which can be used to identify the service to which the interface belongs (e.g. POR for a port, NCA for a national authority).

g. The <*ISO-country-code_*> is **mandatory** and follows the rules in 1.b above.

h. The [*alpha-3-location-code_*] is an **optional** acronym which can be used to identify the location where the system interface is placed. It should form a valid LOCODE by combining it with the ISO_country_code above.

i. The [**CN_**] part is **optional** and follows the same rules as per 2.b above.

j. The [*chars*] part is **optional** and could be used to identify a system user that corresponds to a department/division/sector, etc. of an organisation/authority.

[6] Underscore signs ("_") shall be used to divide the sections of the user name.

Annex C: SSN Password Policy

Policy Configuration	
Parameter	**Value**
Password Minimum Length	9
Password Maximum Length	30
Minimum Number of Uppercase Characters	1
Minimum Number of Lowercase Characters	1
Minimum Number of Nonalphanumeric Characters	0
Minimum Number of Numeric Characters	1
Password Validity Period	90
Password Expiry Notice Period	10 (days)
Mode of Conveying the Expiry Notice	At login
Password minimum age	0
Change on reset	Yes
Password history	3
Number of login tries allowed	5
Lockout Duration	An account can be unlocked after a new password is set by the MSS or the NCA administrators. *NOTE: At a later stage an automatic lockout capability will be provided. The maximum locked period will be 3 hours (according to EMSA's strong password policy).*
Login tries reset	• *After a successful login;* *or* • *Manually by the MSS at password reset.* *NOTE: At a later stage 1 day (according to EMSA's strong password policy).*

Annex D: SSN Security Vocabulary

1. Overview

This Security Vocabulary, as part of the SSN Security Study, has been prepared with the aim of providing SSN involved stakeholders with a useful instrument to share a basic terminology on security.

The annex has been divided into three main sections:

- A list of acronyms including the most frequent technical terms used in SSN context.
- A definition of security related terms available in SSN documentation, SOLAS normative and EU directives.
- A definition of security related terms not present in current evaluated documentation but that could be used for the security of the SSN system.

2. List of acronyms

Definition	Description
BCF	Business Continuity Facility
BMP	Bean-Managed Persistence
CA	Certification Authority
CMP	Container-Managed Persistence
CN	Common Name
CSR	Certificate Signing Request
DAO	Data Transfer Objects
DB	Database
DC	Data Centre
DHTML	Dynamic HTML
DMZ	Demilitarized zone
DNS	Domain Name System
EIS	Enterprise Information System
EJB	Enterprise JavaBean
EMSA	European Maritime Safety Agency
ESB	Enterprise Service Bus
EU	European Union
FTP	File Transfer Protocol
GIS	Geographic Information System
GUI	Graphical user interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IPSEC	Internet Protocol Security
ISP	Internet Service Provider
JDBC	Java Database Connectivity
JEE	Java Enterprise Edition

Definition	Description
JMS	Java Message Service
JSF	Java Server Faces
JSP	Java Server Pages
LDAP	Lightweight Directory Access Protocol
Mbps	Megabit per second
MOM	Message Oriented Middleware
NAT	Network Address Translation
NPR	National Proxy
OS	Operating System
OSB	Oracle Service Bus
OWASP	Open Web Application Security Project
POJO	Plain Old Java Objects
R. Proxy	Reverse Proxy
RAC	Real Application Clusters
RIA	Rich Internet Applications
RMI	Remote Method of Invocation
SAN	Storage Area Network
SANS	SysAdmin, Audit, Network, Security Institute
sFTP	Secure File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SRM	Site Recovery Manager
SOAP	Service Oriented Architecture Protocol
SOLAS	International Convention for the Safety Of Life At Sea
SSL	Secure Socket Layer
SSN	SafeSeaNet
RFC	Request for Comments (Internet Standards)
RSA	Rivest, Shamir and Adleman who first publicly described an algorithm for public-key cryptography
TB	Tera Bytes (i.e. 1012 bytes or 1 million mega bytes)
VLAN	Virtual Local Area Network
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language
XWS	WS Security implementation from Sun Microsystems

3. SSN Security Related Terminology

3.1. Introduction

The methodology used to define a common Security Terminology to be adopted in SafeSeaNet takes into account both worldwide security standards and SSN documents.

The first step of the methodology is focused on the analysis of the terminology already used in the SSN documentation. This analysis already provides a preliminary vocabulary; however the identified security terms do not fully cover the expected evolution and upgrading of the system.

Therefore, in order to provide an exhaustive terminology to be shared among the SSN stakeholders without ambiguity, information security standards have been taken into account. A further step aims at completing and tailoring the list of terms, taking into account possible future needs in terms of security of the SSN improvements. The results of this analysis are presented in the next 3.4 section.

3.2. Methodology

The evaluated terminology has been selected from the SSN documents (also taking into account EU directives), with the objective of covering all the main security aspects needed for the development and operation of SSN.

The identified terms have been properly defined in order to be easily understood and adopted by every involved player in the SSN implementation and usage, including those with no prior experience in the field of security.

In order to provide shared definitions of the security terms, the following criteria have been used:

- If the evaluated term is already defined in the SSN documents and the definition is compliant with security best practices, this definition is used for the SSN Study vocabulary.
- If the evaluated term is not defined in the SSN documents or the definition is not compliant with security best practices, international standard are used to provide the definition.
- If the definition for the term is not available or is ambiguous in the different standards used as reference, a customised definition is provided, taking into account the contractor experience and know how.

3.2.1. Analysis of Standard-derived terminology

Three main worldwide security standards have been used as source of concepts and definitions for their intrinsic quality, widespread use and applicability to the SSN environment:

- ISO 27001:2005;
- NIST[7] SP800-47;
- NIST SP800-53A.

The use of multiple standards helped in addressing different aspects of SSN. The ISO 27001 standard has been used for terms focused on the management and procedural concepts; while the NIST standards have been adopted for terms focusing on the technical and operational part.

The definitions adopted or derived from the identified standards have been tailored on SSN needs and provide a clear knowledge base to be shared in the common development and operational environment.

[7] The National Institute of Standards and Technology is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. More information can be found in www.nist.gov .

If none of the definitions available resulted in a clear expression of the meaning other best practices or standards have been used as provided in the references (e.g. SANS documents) or a new customised definition has been identified.

3.3. SSN Security related Terms Definitions

Access Control - The process that ensures that resources are only granted to those users who have a need for the information and own the proper access rights.

Accountability - The process that ensures that the actions within the system of an entity may be traced uniquely to the entity.

Access Rights - The set of privileges granted to a user allowing them to have access to certain kinds of information or services.

Authentication - The process of determining whether someone or something is who or what it is declared to be.

Authorisation - The process of granting access rights to a user.

Authority (SSN authority) - These are authorities defined as NCAs, LCAs and EMSA, on behalf of the European Commission for the central SSN system. This covers both “Competent authorities” and “Port authorities” as defined in Article 3 of 2002/59/EC as amended.

Availability - A characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorized entity. In the SSN context, assets include information, systems, facilities, networks and computers. All of these assets must be available to authorized entities when they need to access or use them.

Classified Information - Any information and material, an unauthorised disclosure of which could cause varying degrees of prejudice to EU interests, or to one or more of its Member States, whether such information originates within the EU or is received from Member States, third States or international organisations (in accordance with Commission Decision 2001/844/EC amending its internal Rules of Procedure by annexing Commission Provisions on Security).

Confidentiality - The process that ensures that information is not made available or disclosed to unauthorized entities.

Digital Certificate - A digitally signed statement that certifies the binding between the owner’s identity information and his/her electronic public key.

Encryption - The Cryptographic transformation of data into a form that conceals the data's original meaning to prevent it from being known or used by unauthorized entities.

Group - Common functions that SSN users need to perform are collected together creating a group in SSN.

HTTPS - A communication protocol based on the combination between HTTP and SSL/TLS, in order to provide a web server with encrypted communications and security identification capabilities. Aim of HTTPS is the creation of a secure communication channel between the generator and requester of the information.

Integrity - The process that ensures the accuracy and completeness of information.

Local Competent Authorities (LCA) - These are authorities or organisations designated by MSs to receive and transmit information pursuant to the SSN legal framework (e.g. port authorities, coastal stations, Vessel Traffic Services, shore-based installations responsible for a mandatory ship's routing system or a mandatory ship reporting system approved by the IMO and bodies responsible for coordinating search and rescue operations).

National Competent Authority (NCA) - The body which assumes responsibility for a national SSN system and its management on behalf of a MS. It is responsible for the operation, verification and maintenance of the national SSN system, and for ensuring that the standards and procedures comply with the requirements described within the IFCD and with the agreed technical and operational documentation. The NCA responsibilities are defined in Annex III of the Directive 2002/59/EC (as amended).

Non-repudiation - The process that ensures that the entities involved in a communication cannot deny having participated (e.g. sending entity cannot deny having sent a message).

Password - A string of characters used to authenticate the identity of a user. The format of passwords used in SSN is given in the SSN Technical and Operational Documents.

Person - A physical human being, accessing SSN local/ national sites and central site (hosted at EMSA premises).

Personal Data - Any information relating to an identified or identifiable natural living person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number.

Privilege - A permission or right granted to a Person or User (Authority or user).

Role – A set of information that defines the functions and position of a user within the organisation/group.

Security Incident - An event which results in a breach of the organisation and application Security safeguards.

Security Level - The quantification of the probability of a threat being executed and it is measured in escalating categories. This term is synonym of the term Occurrence.

Security Manager - The individual(s) in charge of the security management functions is (are) responsible for carrying out the risk assessment of the SSN System and to manage the whole system security. Each Authority can have its own Security Manager(s).

sTESTA - A private network that gives public administrations access to modern telecommunications services for daily dealings with other public sector bodies across Europe. Its purpose is to provide European institutions and agencies, as well as administrations in the member States, with a network infrastructure that ensures the easy, reliable exchange of data.

Task - The set of tasks assigned to a user defines the permissions of that user. The permissions give them access to the corresponding functionality of the SSN application. The tasks are predefined. For some tasks a geographical restriction applies.

Traceability - The possibility to verify the history, location, or application of the information by means of documented recorded identification.

User (SSN user) - This refers to a person or persons performing the same function, e.g. MRCC duty officer (i.e. an SSN Web user using a browser-based web interface at central, national or local level) or a system (at national level the national SSN system, and at local level the LCA systems).

User Account - A unique set of information in the SSN System identifying a SSN User and their access rights.

User ID - The unique identification code assigned to a SSN User in the SSN System.

3.4. General Security Terminology

Accreditation - The official management decision given by the individual(s) in charge of the security management functions to authorize operation of SSN System and to explicitly accept the risk to SSN operations, assets or individuals, based on the implementation of an agreed-upon set of security controls.

Alert - A formal notification that an incident has occurred which may develop into a Business Continuity Management or Crisis Management invocation.

Antivirus Software - A program that monitors a computer or the entire network with the aim to identify all major types of malware and virus, and to prevent or contain malware or virus incidents.

Asset - Anything that has value to SSN. It could be a system composing SSN or a set of information involved in the SSN provided services.

Asymmetric Keys - Asymmetric keys are a pair of keys, namely a public key and a private key, used to perform complementary operations, such as encryption and decryption or signature generation and signature verification [8]

Audit - An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures and to recommend necessary changes in controls, policies or procedures.

Audit Data - A chronological record of the SSN System activities to enable the evaluation of the sequence of specific events and anomaly changes in the occurrence of each event.

Audit Trail - A record showing who has accessed SSN System and what operations the user has performed during a given period.

Authentication Mechanism - Hardware or software-based mechanism that forces users to prove their identity before accessing a system.

Authentication Protocol - A well-specified message exchange, to verify the possession of specific characteristics by a claimant and to allow its remote authentication. Some authentication protocols also generate cryptographic keys that are used to protect an entire session.

Authentication Token - Authentication information conveyed during an authentication exchange.

[8] William Stallings, Cryptography and Network Security: Principles and Practice.

Authenticity - The property of being genuine and being able to be verified and trusted; authenticity improves confidence in the validity of a transmission, a message, or message originator.

Automated Password Generator - An algorithm which creates random passwords that have no association with a particular user.

Backup - A method, by which data, electronic or paper based, is copied in some form so as to be available and used if the original data from which it originated is lost, destroyed or corrupted.

Basic Authentication - The simplest authentication scheme that works by sending the username and password with each request.

Biometric - A measurable physical or behavioural characteristic belonging to a human being which is used to recognise the identity of a claimant.

Boundary Protection - The monitoring and control of communications at the external boundary between information systems, which are completely under the management and control of the organization, and external information systems, which are not. The boundary also includes the key internal boundaries between information systems, completely under the management and control of the organization, to prevent and detect malicious and other unauthorized communication, employing controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels).

Brute Force Password Attack - A method of accessing a password protected device or service, through attempting multiple combinations of numeric and/or alphanumeric passwords. It can be applied to SSN System and sub-systems as well as normal SSN workstations.

Business Continuity Plan – It represents the management policy and procedures designed to maintain SSN operations, in the event of emergencies, system failures or disaster.

Business Continuity Facility - An alternate facility geographically separated from the main facility that has the necessary infrastructure and utilities to recover SSN operations and systems.

Business Recovery Plan - It represents the management policy and procedures designed to restore SSN operations, possibly at an alternate location, upon occurrence of emergencies, system failures or disaster.

Certificate - A binding of a person, user or organisation to a public key which is guaranteed by a trusted person, user or organisation.

Certificate Based Authentication - The use of SSL and certificates to authenticate and encrypt HTTP traffic.

Certificate Authority - An organization that issues and manages security credentials and public keys for message encryption and decryption. This is an essential part of a public key infrastructure (PKI) because it manages the process of issuing and verifying the certificates used to grant people and systems access to other systems. These certificates include keys that help to strengthen authentication, privacy and non-repudiation.

Certification - A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Certification and Accreditation – A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by the individual(s) in charge of the security management functions to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Challenge-Response Protocol - An authentication protocol where one party sends a random number to the other, who then transforms it in a special way and then returns the result to the sender[9] Authentication is based on the principle that both parties know how to process the received random number.

Change Control - The set of procedures to ensure that all changes are controlled, including the submission, recording, analysis, decision making, approval, implementation and post-implementation review of the change.

Cipher text – It represents a string of characters in its encrypted form.

Claimant - An entity whose identity has to be verified by SSN using an authentication mechanism.

Client - A system entity that requests and uses a service provided by another system entity, called a "server." In some cases, the server may itself be a client of some other server.

Compromise - The disclosure of information to unauthorized entities, or a violation of the security policy of SSN system in which unauthorized disclosure (either intentional or unintentional), modification, destruction or loss of an asset may have occurred.

Contingency Plan – It describes emergency organisation, roles and responsibilities of the involved personnel and the necessary emergency training requirements in order to respond timely and efficiently to notifications of maritime emergency cases.

Control - Any administrative, management, technical, or legal method that is used to manage risk. Controls are safeguards or countermeasures. Controls include things like practices, policies, procedures, programs, techniques, technologies, guidelines, and organizational structures.

Corrective Actions - Steps that are taken to address existing nonconformities and make improvements. Corrective actions deal with actual nonconformities (problems), ones that have already occurred. They solve existing problems by removing their causes.

[9] A. S. Tanenbaum, Computer Networks

Countermeasure – It identifies actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Its synonymous is security control or safeguard.

Credential - The combination of User ID and Password uniquely identifying a user account.

Cryptographic Key - A value used to perform operations, such as decryption, encryption, signature generation or verification.

Cryptography – A discipline which transforms data or messages to prevent their intelligibility by unwanted receivers.

Crypto-period - The validity period of the key during which it can be used to encrypt data.

Data Confidentiality - Any information and material, an unauthorized disclosure of which could cause varying degrees of prejudice to EU interest, or to one of more of its Member States, whether such information originates within the EU or is received from Member States, third States or international organizations (in accordance with Commission Decision 2001/844/EC amending its internal Rules of Procedure by annexing Commision Provisions on Security).

Data Integrity - Please refer to definition of Integrity.

Data Protection - The process of guaranteeing the confidentiality of data is preserved during the whole data lifecycle.

Data Recovery - The process of restoration of computer files from backup media to restore programs and production data to the state that existed at the time of the last safe backup.

Decryption - The process of transforming an encrypted message (cipher-text) into its original form (plaintext).

Demilitarised Zone (DMZ) - A physical or logical sub-network enabling Internet users to access a company's public servers, including Web and File Transfer Protocol (FTP) servers, while maintaining security for the company's private LAN.[10]

***Denial-of-Service Attack* (DoS attack)** - An IT attack which goal is the achievement of the unavailability of a computer resource to its foreseen users.

Digital Envelope - An encrypted message with the encrypted session key.

Digital Signature - A hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission.

Disaster - A sudden, unplanned catastrophic event causing unacceptable damage or loss.

Disaster Recovery Plan - An IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency (see Business Continuity Plan).

[10] www.cisco.com

Disruption - An unplanned event causing the whole SSN System, or part of it, to be inoperable or inaccessible for an unacceptable period of time

Downtime - The total period that a service or component is not operational within an agreed service time. Measured from when a service or component fails to when normal operations recommence.

Due Diligence - The requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

Encapsulation - The process of including one data structure within another structure so that the first data structure is hidden for the time being.

Error Detection Code - A code designed only to detect, but not correct, unintentional changes in the data exchanged by SSN entities. These codes are usually computed on the original data before transmission and the result of the computation is added as additional information to the existing data.

Failover - The capability to switch over automatically to a redundant or standby computer server, system, or network upon the failure or abnormal termination of the previously active server, system, or network. Failover happens without human intervention and generally without warning, unlike switchover.

Firewall - A system or group of systems that enforces an access control policy between two networks.

Form Based Authentication - Authentication carried out by means of input of User ID and password on a form on a webpage.

Gateway - A network node acting as an entrance to another network.

Group – It is used to represent a collection of Users within an IT system. Groups are usually created to reflect the organisation structure.

Hash Function - A mathematical function that starting from a string of arbitrary, but pre-determined, length generates a fixed length string. It is used to produce checksum codes which are called hash values.

Identification - The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to information or services of the SSN System.

Identity - The set of physical and behavioural characteristics by which an individual is uniquely recognizable. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information to make the complete name unique.

Identity Verification - The process of confirming or denying that a claimant's identity is correct by comparing the credentials of a claimant with those previously verified and stored in SSN System. The stored credentials are in fact associated with the identity being claimed.

Impact - The level of harm, measured on an escalating basis, generated by the occurrence of an attack threatening the SSN System.

Information Security - The process of preserving confidentiality, integrity and availability of information.

Information Security Awareness - The process which seeks to focus an individual's attention on an information security issue or set of issues.

Information Security Management System - The set of all of the policies, procedures, plans, processes, practices, roles, responsibilities, resources, and structures that are used to protect and preserve information. It includes all of the elements that organizations use to manage and control their information security risks.

Information Security Policy – A statement which expresses management's commitment to the implementation, maintenance, and improvement of its information security management system.

Intellectual Property - Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Intrusion Detection System (IDS) - Software that looks for suspicious activity and alerts administrators.

Intrusion Prevention System - A system aimed at detecting intrusive activities and attempting to stop them before they reach the target. Targets could be represented by SSN System and sub-systems or SSN treated information.

IT Security Architecture - A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments.

Key – See Cryptographic Key.

Key Exchange - The process of exchanging public keys in order to establish secure communications.

Key Pair - A pair of mathematically related keys characterised as follows:

1. a message encrypted with one key can only be decrypted by the other;
2. the discovery of the other key in a pair is computationally unfeasible even knowing the other one.

Lightweight Directory Access Protocol (LDAP) - A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet.

Malicious Code - Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Malicious Code is often used as a general term to identify a virus, worm, Trojan horse or other code-based entity that infects a host.

Malware - A program whose target is to compromise the confidentiality, integrity or availability of system data, applications. Malware are usually covertly inserted in the system.

Mandatory Access Control - A mean of restricting access to data based on different degrees of security requirements for information and the corresponding security clearance of users or programs.[11]

Masquerade - A type of attack where the attacker pretends to penetrate the systems by using the identity of legitimate users and their logon credentials[12]

Mutual Authentication - Achieved when parties at both ends of a communication activity authenticate each other.

Occurrence - The quantification of the probability that a threat exploits a vulnerability of the system. It is estimated using escalating categories.

One-way Encryption - The irreversible transformation of plaintext to cipher text, such that the plaintext cannot be recovered from the cipher text by other than exhaustive procedures even if the cryptographic key is known.

Owner - A person or entity that has been given formal responsibility for the security of an asset or asset category. Asset owners are formally responsible to assure that assets are secure while they are being developed, produced, maintained, and used.

Password Protected - The ability to protect a file using a password access control, protecting the data contents from being viewed with the appropriate viewer unless the proper password is entered.

Penetration Testing - A method of evaluating the security of the SSN System by simulating an attack from a malicious source. The process involves an analysis of the system for any potential vulnerabilities or operational weaknesses in countermeasures. This analysis is carried out as if it was performed by a potential attacker.

Personal Identification Number (PIN) - A password consisting only of decimal digits. It is a secret that a claimant memorizes and uses to authenticate his or her identity.

Potential Impact - The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect; a serious adverse effect, or a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Private Key - The secret part of an asymmetric key pair. The Private Key is typically used to sign or decrypt data.

Proxy - An application that filters the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it permitting or denying the flow towards it. Proxy is used to physically separate internal and external networks, making more difficult for an attacker to obtain internal addresses and other details of the organization’s internal network.

Public Key - The public part of an asymmetric key pair. Public Key is typically used to verify signatures or encrypt data.

Redundancy - The replication of a system or parts of it, with the aim to reduce the number of failures and service interruption.

[11] ISACA, CISM Glossary

[12] ISACA, CISM Glossary

Risk - The level of impact on operations, assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Acceptance - Part of the risk treatment decision making process. Risk acceptance means the individual(s) in charge of the security management functions is (are) aware of a certain risk and accepts to cope with it.

Risk Analysis - The use of information to identify possible sources of risk. It uses information to identify threats or events that could have a harmful impact. It then estimates the risk by defining, for each threat or event, their probability and their impact on the analysed asset.

Risk Assessment - The process of identifying and evaluating the risk, it is composed by two phases: risk analysis and risk evaluation.

Risk Communication - The process of sharing risk information to the involved people, in order to increase awareness about a certain risk and the related decisions (identified countermeasures, acceptance of the risk or procedures definition).

Risk Evaluation - The process of comparison of the estimated risk with a set of risk criteria. This is done in order to determine how significant the risk really is.

Risk Management - A process that includes four activities: risk assessment, risk acceptance, risk treatment, and risk communication. Risk management includes all of the activities that an organization carries out in order to manage and control risk.

Risk Treatment - The process of choosing, for each risk, amongst at least four options: accept the risk, avoid the risk, transfer the risk, or reduce the risk. In general, risks are treated by selecting and implementing measures designed to modify risk.

Security - The process which takes into account all aspects relating to defining, achieving and maintaining data confidentiality, integrity, and availability.

Security Baseline - The set of minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection.

Security Label - The explicit or implicit marking of a data structure or output media associated with an information system representing the security category, or distribution limitations or handling caveats of the information contained therein.

Security Log - Security Log is a report on all events relevant to security occurred to a system. Security Log can be implemented via Software or by means of procedural processes.

Security Policy – See Information Security Policy.

Security Requirements - Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Single Sign-on - The process guaranteed by software packages allowing users to get access to multiple computers and applications without learning many different passwords. Single sign-on tools generally do not change the underlying applications, but hide their differences through a layer of software.

Spyware - Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge

Secure Socket Layer (SSL) – A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

Symmetric Key - A key used to perform cryptographic operations such as encryption, decryption and signature of data. However, to be effective, it has to be shared among the entities taking part to the process of data exchange in their encrypted form.

System Interconnection - This term refers to the direct connection of two or more IT systems for the purpose of sharing data and other information resources.

System Security Information - Information which requires protection as its public or unauthorised disclosure would reveal privileged or confidential information related to persons, systems, operations and/or facilities.

Strong Password - A password characterised by enough complexity to prevent its disclosure through guessing and making computationally unfeasible its discovery by means of Brute Force Attack.

Threat - Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Transport Layer Security (TLS) - An authentication and security protocol widely implemented in browsers and web servers.

Unauthorised Access - Used to define an entity gaining logical or physical access without permission to the SSN network, system, services, data, or other resources.

Unauthorised Disclosure - An event involving the exposure of information to entities not authorized access to the information.

Unclassified information - Information that can be released to individuals without a clearance except when it is deemed personal or sensitive.

User Account Management – The process that represents the functional flow composed by: 1) the process of requesting, establishing, issuing, and closing user accounts, 2) tracking users and their respective access authorizations and 3) managing these functions.

Validation - The process of proofing that all specifications of a system are satisfied after its implementation. If referred to data validation, it is the process of ensuring that a program operates on clean, correct and useful data.

Virtual Private Network (VPN) - A logical network that is established over an existing physical network and typically does not include every node present on the physical network. All information flowing through this channel is encrypted.

Virus - A software program, with self-replicating capabilities, that runs and spreads by affecting programs or files.

Vulnerability - The term vulnerability is used to identify a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment - A formal description and evaluation of the vulnerabilities in an information system.

Web Services - The W3C defines a "Web service" as "a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically Web Services Description Language WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards."

Worm - A self-propagating software program that exploits networking mechanisms to spread itself.

Annex E: Technical background

1. Network access

1.1. Internet Access

Getting access to SafeSeaNet through the Internet means that the Member States will have to set up an Internet connection (with back-up connection) with the ISP of their choice. The ISP selected by each Member State will determine the most effective connection(s) based on location, scope and the data to transmit.

The connection metrics that need to be taken in account are:

- Bandwidth
- Latency
- Number and type of accesses (remote/local)
- SLAs
- Data (payload)

Bandwidth in computer networking refers to the data rate supported by a network connection or interface. In networking, bandwidth represents the overall capacity of the connection. The greater the capacity, the more likely that better performance will result. Bandwidth is the amount of data that passes through a network connection over time as measured in bps. High values are recommended.

Latency is another element that contributes to network speed. It refers to any of several kinds of delays typically incurred in processing of network data. A so-called low latency network connection is one that generally experiences small delay times; therefore low values are desirable for this parameter.

Network tools like ping tests and traceroute measure latency by determining the time it takes a given network packet to travel from source to destination and back, the so-called round-trip time. Round-trip time is not the only way to specify latency, but it is the most common.

Optical fibre with path redundancy is the recommended connection method through Internet for SafeSeaNet.

1.2. sTESTA network service

sTESTA is the natural successor to the initial TESTA and TESTA II networks developed under the IDA and IDABC Community programmes and is managed by the European Commission’s Directorate-General for Informatics (DG DIGIT). The sTESTA network infrastructure interconnects all EU institutions, EU agencies, Member States’ administrations and European Economic Area (EEA) countries.

Getting access to SafeSeaNet through sTESTA means the Member States will have to set up a sTESTA connection.

The objective of sTESTA is to offer a managed, reliable and secure pan-European communication platform on top of which European and National administrations can build pan-European eGovernment services irrespective of the policy area in which they are involved. sTESTA users can achieve great synergies, compared to the situation where each sector would have to set up and manage its own communication network infrastructure. One single network control and operation centre can manage the (virtual) networks used by the sectors and, where possible, physical network connections can be shared.

Because of the nature of some of these pan-European eGovernment services, this infrastructure must be able to transport classified information. The European Commission has four official security classifications[13] which are now invariable in all linguistic versions (i.e. not translated) and always appear in capital letters in quotes in the following form:

- "EU RESTRICTED",
- "EU CONFIDENTIAL",
- "EU SECRET",
- "EU TOP SECRET".

The sTESTA infrastructure is subject to a security accreditation process to allow the exchange of EU classified information up to the "EU RESTRICTED"[14]level.

General information and technical 'How-To' can be found at the following sTESTA Web Portals:

- https://portal.testa.eu/jetspeed/portal (portal is only visible on all the networks outside the EC that have access to sTESTA);
- http://ec.europa.eu/isa/actions/02-interoperability-architecture/2-4action_en.htm (internet portal)

2. Digital certificates and PKI Services

2.1. Introduction to Digital Certificates

Security solutions using digital certificates rely on public key cryptography in which each user has a pair of cryptographic keys: one private key that is kept private by the user, and one related public key widely made public.

A **Digital Certificate** is a digitally signed statement that certifies the binding between the owner's identity information and his/her electronic public key.

This certified public key can be used to encrypt confidential information to the certificate owner and/or to verify digital signatures generated by the certificate owner.

[13] Under Article 2 of Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations, as last amended by Commission Decision 2005/952/EC.

[14] "EU RESTRICTED": this classification shall be applied to information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of its Member States.

The certified public key is linked to the private key of the certificate owner in such a way that:

- A digital signature is computed from the message and the private key of the signer. It is a small size coded file appended to the signed message. Verification of a digital signature involves the certified public key of the signer. If the check succeeds, the recipient is convinced about its origin and has the guarantee that nothing has been modified in the message since the signature process.
- Confidentiality is obtained from the ciphering of the message with the certified public key of the recipient. The only way to decrypt a ciphered message is to use the corresponding private key that is supposed to be known only to the certificate owner.

Digital certificates provide thus solid assurance that a public key actually belongs to the right entity whose identity has been certified by a **Certification Authority**, a known trusted third party, which controls and confirms the accuracy of the binding between a public key and its legitimate owner.

Digital certificates are the Internet passports that prevent to disclose confidential information to unauthorised persons, and/or to accept an imposter's digital signature as authorisation for a critical electronic business transaction.

2.2. Introduction to PKI

2.2.1. What's a PKI?

PKI stands for Public Key Infrastructure. The PKIX Working Group defines a PKI as "The set of hardware, software, people and procedures needed to create, manage, store, distribute and revoke certificates based on public-key cryptography".

Public-key cryptography meets the major requirements of confidentiality, integrity, authenticity and non-repudiation.

2.2.2. Components of a PKI

A PKI comprises the following components:

Components	Functions
Certificate Authorities (CAs)	issuing and revoking certificates
Registration Authorities (RAs)	verify the binding between public keys and the identities of their holders
Certificate holders (or subjects)	people, machines, software agents that have been issued with certificates and can use them to sign digital documents
Clients	validate digital signatures and certification paths from a trusted CA's public key
Repositories	store and make available certificates and certificate revocation list (CRLs)
Security policy	sets out and defines the organization's top-level direction on information security, as well as the processes and principles for the use of cryptography. It is described in the Certificate Practice Statement (CPS)

2.2.3. Functions of a PKI

Here below is a summary of the major functions performed within a PKI:

Function	Description
Registration	Process in which a prospective certificate holder presents itself to the CA in order to request a certificate.
Certification	The CA issues a certificate (with the subject's public key), delivers it to the subject and publishes it in a suitable public repository.
Key generation	If the CA is responsible for generating the key pair, it does so and supplies them to the subject as an encrypted file or physical token (e.g. smart card).
Key update	All key pairs (and associated certificates) should be updated at regular intervals in case the date of a certificate reaches its expiration date or a private key is compromised.
Cross-certification	Process allowing users from one administrative domain to trust certificates issued by a CA operating in a different administrative domain.
Revocation	Some events necessitate the early revocation of a certificate's validity (subject changes of name, employee leaves the company, compromise of a private key...). The revoked certificates are listed in a certificate revocation list (CRL) published, at regular intervals, by the CA into the same repository as the certificates themselves.

3. SSL protocol

3.1. Introduction

Secure Sockets Layer (SSL) provides secure connections by allowing two applications connecting over a network connection to authenticate the other's identity and by encrypting the data exchanged between the applications. Authentication allows a server and optionally a client to verify the identity of the application on the other end of a network connection. Encryption makes data transmitted over the network intelligible only to the intended recipient.

3.2. Private Keys, Digital Certificates and Trusted Certificate Authorities

Private keys, digital certificates, and trusted certificate authorities establish and verify server identity.

SSL uses public key encryption technology for authentication. With public key encryption, a public key and a **private key** are generated for a server. The keys are related such that data encrypted with the public key can only be decrypted using the corresponding private key and vice versa. The private key is carefully protected so that only the owner can decrypt messages that were encrypted using the public key.

The public key is embedded into a **digital certificate** with additional information describing the owner of the public key, such as name, street address, and e-mail address. A private key and digital certificate provide **identity** for the server.

The data embedded in a digital certificate is verified by a certificate authority (also referred to as trusted certificate authority) and digitally signed with the certificate authority's digital certificate. A trusted certificate authority establishes **trust** for a server. An application participating in an SSL connection is authenticated when the other party evaluates and accepts their digital certificate. Web browsers, servers, and other SSL-enabled applications generally accept as genuine any digital certificate that is signed by a trusted certificate authority and is otherwise valid. For example, a digital certificate can be invalidated because it has expired or the digital certificate of the certificate authority used to sign it expired. A server certificate can be invalidated if the host name in the digital certificate of the server does not match the host name specified by the client. Additional checks are also applied following the relevant RFCs.

3.3. HTTPS and SSL over TCP/IP

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer or HTTP over SSL) is a protocol that provides encrypted communication and secure identification of the communication participants. HTTPS uses default port 443 instead of HTTP default port 80 in its interactions with the lower layer, TCP/IP.

The Transmission Control Protocol/Internet Protocol (TCP/IP) governs the transport and routing of data over the Internet.

The SSL protocol runs above TCP/IP and below higher-level protocols such as HTTP. It uses TCP/IP on behalf of the higher-level protocols, and in the process allows an SSL-enabled server to authenticate itself to an SSL-enabled client, allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection.

SSL is an integral part of most Web browsers (clients) and Web application servers. SSL is an open, non-proprietary protocol that Netscape developed for transmitting private documents via the Internet.

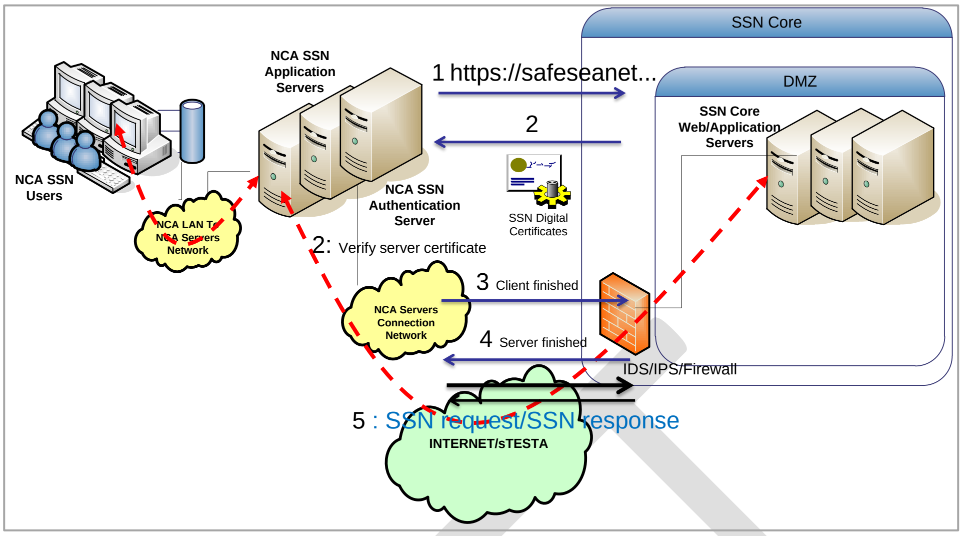
3.4. One-Way and Two-Way SSL

SSL can be configured one-way or two-way:

- With one-way SSL, the server is required to present a certificate to the client but the client is not required to present a certificate to the server. To successfully negotiate an SSL connection, the client must authenticate the server, by checking the signature of the server certificate (root and intermediate certificate) and that the CN value of the certificate corresponds to the name of the site the client is connecting to, but the server will accept any client into the connection. One-way SSL is common on the Internet where customers want to create secure connections before they share personal data.
- With two-way SSL, the client also presents a certificate to the server. In this case, the server shall check the signature of the client certificate received and that the CN value of the certificate corresponds to the name of the application client.

3.5. SSL concept and Handshake

3.5.1. 1-way SSL


SSN Core
DMZ
NCA SSN Application Servers
1 https://safeseanet...
2
SSN Core Web/Application Servers
NCA SSN Users
NCA SSN Authentication Server
SSN Digital Certificates
NCA LAN To NCA Servers Network
2: Verify server certificate
3 Client finished
NCA Servers Connection Network
4 Server finished
IDS/IPS/Firewall
5 : SSN request/SSN response
INTERNET/sTESTA

1. The client starts the connection and sends the version of the highest SSL/TLS protocol supported, client random (used in the calculation of the master secret from which the encryption keys are derived) and cipher suite.

2. The server sends the highest version of the SSL/TLS protocol that is supported by both sides, the server random, which along with the client random is used to generate the master secret, its digital certificate (public key) and chooses the strongest cypher that both the client and server support (if not, the handshake fails).

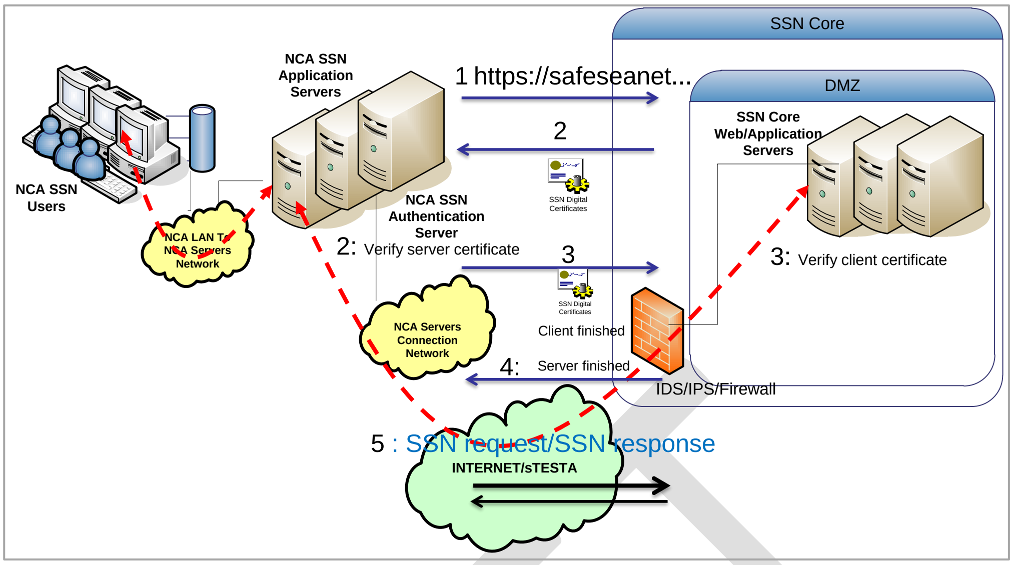
   The client uses the server’s public key to authenticate the server and to encrypt the pre master secret. It also verifies the digital signature on the server's digital certificate, the CN value of the certificate which needs to correspond to the name of the site the client is connected, that the certificate is not expired and the date of emission is previous to the current date.

3. The client computes the premaster secret using the client random and the server random. This premaster secret is encrypted by the public key of the server’s certificate. Both parties compute the master secret locally. It finally sends the client protocol version (the same as in step 1 to be verified by the server) and the premaster key. The client notifies the server that all future messages including the “finish” are encrypted using the keys and algorithm negotiated. At this point, the server is authenticated and the client has sent the premaster secret. Both the client and server have calculated the master secret. Up until now, however, any encryption has used the server’s private/public keys. This message tells the server that the client is ready to use the master key for all further encryption. Finally, it sends a "finished” message to the server indicating that the client part of the handshake is complete.

4. The server notifies the client that the server will begin encrypting messages with the keys that were just negotiated and sends the client a "finished" message indicating that the server part of the handshake is complete.

5. For the duration of the SSL session, the server and client can now exchange messages in a secure way.

3.5.2. 2-way SSL


SSN Core
DMZ
NCA SSN Application Servers
1 https://safeseanet...
SSN Core Web/Application Servers
2
SSN Digital Certificates
NCA SSN Users
NCA LAN To NCA Servers Network
NCA SSN Authentication Server
2: Verify server certificate
3
SSN Digital Certificates
3: Verify client certificate
Client finished
NCA Servers Connection Network
4: Server finished
IDS/IPS/Firewall
5 : SSN request/SSN response
INTERNET/sTESTA

1. The client starts the connection and sends the version of the highest SSL/TLS protocol supported, client random (used in the calculation of the master secret from which the encryption keys are derived) and cipher suite.

2. The server sends the highest version of the SSL/TLS protocol that is supported by both sides, the server random, which along with the client random is used to generate the master secret, its digital certificate (public key), chooses the strongest cypher that both the client and server support (if not, the handshake fails) and requests the certificate to the client.

   The client uses the server's public key to authenticate the server and to encrypt the pre master secret. It also verifies the digital signature on the server's digital certificate, the CN value of the certificate which needs to correspond to the name of the site the client is connected, that the certificate is not expired and the date of emission is previous to the current date.

3. The client sends the client's digital certificate for client authentication (public key) It computes the premaster secret using the client random and the server random. This premaster secret is encrypted by the public key of the server's certificate. Both parties compute the master secret locally. It finally sends the client protocol version (the same as in step 1 to be verified by the server) and the premaster key.

   The server verifies the signature on the client certificate (with the public key of the client, that ensures that it was signed with the client's private key), the CN value of the certificate which need to correspond to the name of the application client, that the certificate is not expired and the date of emission is previous to the current date

   The client notifies the server that all future messages including the "finish" are encrypted using the keys and algorithm negotiated. At this point, client and server are authenticated and the client has sent the premaster secret. Both the client and server have calculated the master secret. Up until now, however, any encryption has used the client's or server's private/public keys. This message tells the server that the client is ready to use the master key for all further encryption. Finally, it sends a "finished” message to the server indicating that the client part of the handshake is complete.

4. The SSL server notifies the client that the server will begin encrypting messages with the keys that were just negotiated and sends the SSL client a "finished" message indicating that the server part of the handshake is complete.

5. For the duration of the SSL session, the SSL server and SSL client can now exchange messages in a secure way.