

# European Maritime Safety Agency (EMSA)

## Security and Interoperability Solutions Study for SafeSeaNet

Specific Contract N°1 implementing Framework Contract DI/07624 (ABC IV Lot 3)

D3-6-1

Interim Report for Task 3



**Funded by the European Union –  
European Maritime and Fisheries Fund**



# Table of Contents

<b>1 EXECUTIVE SUMMARY .....</b>	<b>5</b>
<b>2 INTRODUCTION.....</b>	<b>6</b>
2.1 BACKGROUND ON SAFESEANET (SSN) .....	6
2.2 OBJECTIVES OF THE STUDY.....	6
2.3 PURPOSE OF THIS REPORT .....	7
2.4 OVERVIEW OF THE METHODOLOGY .....	7
2.5 STRUCTURE OF THIS REPORT.....	8
<b>3 STRUCTURE AND ORGANISATION OF SSN USERS.....</b>	<b>9</b>
<b>4 INFORMATION SECURITY MANAGEMENT SYSTEM FOR SSN.....</b>	<b>11</b>
4.1 STATEMENT OF APPLICABILITY .....	11
4.2 SECURITY CONTROLS .....	11
<b>5 SECURITY, DATA PROTECTION AND INTEROPERABILITY CRITERIA FOR SSN .....</b>	<b>16</b>
<b>6 ASSESSMENT OF CEF BUILDING BLOCKS.....</b>	<b>17</b>
6.1 OVERVIEW OF CEF BUILDING BLOCKS SELECTED FOR ANALYSIS IN THE SSN CONTEXT.....	17
6.2 ASSESSMENT OF RELEVANT CEF BUILDING BLOCKS.....	18
6.2.1 Assessment of eID suitability in the context of SSN .....	19
6.2.2 Assessment of eDelivery suitability in the context of SSN .....	22
6.2.3 Assessment of eSignature suitability in the context of SSN.....	24
6.2.4 Assessment of eArchiving suitability in the context of SSN .....	26
<b>7 ASSESSMENT OF TECHNICAL OPTIONS FOR SSN .....</b>	<b>30</b>
7.1 OVERVIEW .....	30
7.2 IDENTITY AND ACCESS MANAGEMENT - DESCRIPTION AND ASSESSMENT OF SUITABILITY IN THE SSN CONTEXT	33
7.2.1 Identity and Access Management – description of the technical options.....	33
7.2.2 Identity and Access Management – assessment of the technical options.....	37
7.2.3 Identity and Access Management – conclusion on technical options assessment.....	38
7.3 DATA STORAGE - DESCRIPTION AND ASSESSMENT OF SUITABILITY IN THE SSN CONTEXT .....	39
7.3.1 Data Storage – description of the technical options .....	39
7.3.2 Data Storage – assessment of the technical options .....	40
7.3.3 Data Storage – conclusion on technical options assessment.....	41
7.4 ARCHIVING - DESCRIPTION AND ASSESSMENT OF SUITABILITY IN THE SSN CONTEXT .....	42
7.4.1 Archiving – description of the technical options .....	42
7.4.2 Archiving – assessment of the technical options.....	42
7.4.3 Archiving – conclusion on technical options assessment .....	43
7.5 PRIVACY ENHANCING TECHNOLOGIES AND ARCHITECTURE - DESCRIPTION AND ASSESSMENT OF SUITABILITY IN THE SSN CONTEXT.....	44
7.5.1 Privacy Enhancing Technologies and Architecture – description of the technical options ....	44
7.5.2 Privacy Enhancing Technologies and Architecture – assessment of the technical options ...	45
7.6 NETWORK SECURITY - DESCRIPTION AND ASSESSMENT OF SUITABILITY IN THE SSN CONTEXT .....	46
7.6.1 Network Security – description of the technical options.....	46
7.6.2 Network Security – assessment of the technical options.....	47
7.6.3 Network Security – conclusion on technical options assessment .....	48
7.7 PROPOSED TARGET ARCHITECTURE FOR SSN.....	49
<b>8 ROADMAP OF ACTIONS FOR IMPLEMENTATION OF SSN SECURITY, DATA PROTECTION AND INTEROPERABILITY MEASURES.....</b>	<b>50</b>
8.1 ROADMAP FOR SSN.....	50
8.2 OVERVIEW OF THE ROADMAP ACTIVITIES .....	51
<b>9 CONCLUSIONS.....</b>	<b>53</b>
9.1 ON DATA PROTECTION ASPECTS .....	53
9.1.1 Data Protection Impact Assessment (DPIA) [Attention point #1] .....	53
9.1.2 Roles and responsibilities [Attention point #2] .....	53
9.2 ON INTEROPERABILITY ASPECTS .....	53

9.2.1	Compliance with relevant network and information security standards [Interoperability gap #1]	53
9.2.2	Degree of support from different interest groups [Interoperability gap #2]	53
9.2.3	Transparency [Attention point #1]	54
9.3	ON SECURITY ASPECTS	54
9.3.1	Information security policies [Security gap #1]	54
9.3.2	Access control [Security gap #2]	54
9.3.3	Compliance with security policies and standards [SSN Security gap #3]	54
9.3.4	Complementary security recommendations	54
9.4	ON STRUCTURE AND ORGANISATION OF SSN USERS	55
9.5	ON CEF BUILDING BLOCKS	55
9.5.1	eID suitability	55
9.5.2	eDelivery	55
9.5.3	eSignature	56
9.5.4	eArchiving	56
9.6	ON TARGET ARCHITECTURE	56
<b>GLOSSARY AND ACRONYMS</b>		<b>58</b>

## List of Figures

FIGURE 1	OVERVIEW OF THE METHODOLOGY FOR TASK 3	7
FIGURE 2	RELEVANT CEF BUILDING BLOCKS	18
FIGURE 3	ARCHITECTURAL AREAS	30
FIGURE 4	BASIC FUNCTIONAL ELEMENTS OF IAM SOLUTIONS (TECHNICAL OPTIONS)	33
FIGURE 5:	IAM_1 - DELEGATED AUTHENTICATION FOR CENTRAL SSN	34
FIGURE 6:	IAM_2 - DELEGATED IDENTITY FOR CENTRAL SSN	34
FIGURE 7:	IAM_3 - FEDERATED IAM ADOPTING THIRD PARTY AUTHENTICATION	35
FIGURE 8:	IAM_4 - FEDERATED IAM ADOPTING eIDAS	36
FIGURE 9	DATA STORAGE INVOLVING SEGREGATED DATABASES	39
FIGURE 10	ROADMAP OF ARCHITECTURAL OPTIONS FOR SSN	50

## List of Tables

TABLE 1	NEW SSN ROLES	9
TABLE 2	NEW DATA PROTECTION AND SECURITY SSN ROLES	9
TABLE 3	ISMS ACTIVITIES FOR INFORMATION SECURITY POLICIES	11
TABLE 4	ISMS ACTIVITIES FOR ORGANIZATION OF INFORMATION SECURITY (INTERNAL ORGANIZATION)	11
TABLE 5	ISMS ACTIVITIES FOR ASSET MANAGEMENT	12
TABLE 6	ISMS ACTIVITIES FOR INFORMATION CLASSIFICATION	12
TABLE 7	ISMS ACTIVITIES FOR ACCESS CONTROL	12
TABLE 8	ISMS ACTIVITIES FOR OPERATIONS SECURITY	12
TABLE 9	ISMS ACTIVITIES FOR INFORMATION SYSTEMS AUDIT CONSIDERATIONS	13
TABLE 10	ISMS ACTIVITIES FOR COMMUNICATIONS SECURITY	13
TABLE 11	ISMS ACTIVITIES FOR INFORMATION TRANSFER	13
TABLE 12	ISMS ACTIVITIES FOR SECURITY IN DEVELOPMENT AND SUPPORT PROCESS	13
TABLE 13	ISMS ACTIVITIES FOR INFORMATION SECURITY INCIDENT MANAGEMENT	14
TABLE 14	ISMS ACTIVITIES FOR INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	14
TABLE 15	ISMS ACTIVITIES FOR COMPLIANCE	14
TABLE 16	SECURITY, DATA PROTECTION AND INTEROPERABILITY CRITERIA FOR SSN	16
TABLE 17	OVERVIEW OF SELECTED CEF BUILDING BLOCKS	17
TABLE 18	SECURITY ASSESSMENT OF eID FOR SSN	20
TABLE 19	DATA PROTECTION ASSESSMENT OF eID FOR SSN	20
TABLE 20	INTEROPERABILITY ASSESSMENT OF eID FOR SSN	21
TABLE 21	SECURITY ASSESSMENT OF eDELIVERY FOR SSN	22
TABLE 22	DATA PROTECTION ASSESSMENT OF eDELIVERY FOR SSN	23
TABLE 23	INTEROPERABILITY ASSESSMENT OF eDELIVERY FOR SSN	23
TABLE 24	SECURITY ASSESSMENT OF eSIGNATURE FOR SSN	25
TABLE 25	DATA PROTECTION ASSESSMENT OF eSIGNATURE FOR SSN	25

TABLE 26 INTEROPERABILITY ASSESSMENT OF eSIGNATURE FOR SSN .....	26
TABLE 27 SECURITY ASSESSMENT OF eARCHIVING FOR SSN.....	27
TABLE 28 DATA PROTECTION ASSESSMENT OF eARCHIVING FOR SSN .....	27
TABLE 29 INTEROPERABILITY ASSESSMENT OF eARCHIVING FOR SSN .....	28
TABLE 30 SECURITY ASSESSMENT OF IAM OPTIONS FOR SSN .....	37
TABLE 31 DATA PROTECTION ASSESSMENT OF IAM OPTIONS FOR SSN.....	37
TABLE 32 INTEROPERABILITY ASSESSMENT OF IAM OPTIONS FOR SSN.....	38
TABLE 33 ALTERNATIVE DEPLOYMENT MODELS FOR DATA STORAGE .....	39
TABLE 34 SECURITY ASSESSMENT OF DATA STORAGE OPTIONS FOR SSN .....	40
TABLE 35 DATA PROTECTION ASSESSMENT OF DATA STORAGE OPTIONS FOR SSN.....	41
TABLE 36 INTEROPERABILITY ASSESSMENT OF DATA STORAGE OPTIONS FOR SSN.....	41
TABLE 37 SECURITY ASSESSMENT OF ARCHIVING OPTIONS FOR SSN .....	42
TABLE 38 DATA PROTECTION ASSESSMENT OF DATA STORAGE OPTIONS FOR SSN.....	43
TABLE 39 INTEROPERABILITY ASSESSMENT OF ARCHIVING OPTIONS FOR SSN.....	43
TABLE 40 COMPARISON OF PHYSICAL NETWORK AND SDN/NFV SOLUTIONS.....	46
TABLE 41 EXAMPLES OF ACTIVITIES FOR SCOPING AND DESIGNING NETWORK SEGMENTATION ALTERNATIVES.....	47
TABLE 42 SECURITY ASSESSMENT OF NETWORK SECURITY OPTIONS FOR SSN .....	47
TABLE 43 DATA PROTECTION ASSESSMENT OF NETWORK SECURITY OPTIONS FOR SSN .....	48
TABLE 44 INTEROPERABILITY ASSESSMENT OF NETWORK SECURITY OPTIONS FOR SSN.....	48
TABLE 45 PROPOSED TARGET ARCHITECTURES .....	49
TABLE 46 ROADMAP ACTIVITIES FOR ISMS .....	51
TABLE 47 ROADMAP ACTIVITIES FOR IAM .....	51
TABLE 48 ROADMAP ACTIVITIES FOR DATA STORAGE.....	51
TABLE 49 ROADMAP ACTIVITIES FOR ARCHIVING .....	51
TABLE 50 ROADMAP ACTIVITIES FOR PRIVACY ENHANCING TECHNOLOGIES AND ARCHITECTURE .....	52
TABLE 51 ROADMAP ACTIVITIES FOR PRIVACY ENHANCING TECHNOLOGIES AND ARCHITECTURE .....	52
TABLE 52 OTHER ROADMAP ACTIVITIES .....	52

# 1 Executive Summary

The objective of the contract is to elaborate a comprehensive study on security and interoperability solutions for SSN under the CISE context and in the perspective of the additional foreseen SafeSeaNet developments (these include the Regulation (EU) 2019/1239 establishing the EMSWe and the Directive 2017/2109 on the registration of persons sailing on board passenger ships).

The study focuses on the security measures to be implemented in the Central SSN system, in National SSN systems and in the interfaces between the Central SSN system and National SSN systems and covers the following tasks:

- ✓ Task 1 - Identification and definition of security measures to be applied in SSN.
- ✓ Task 2 - Technical analysis of the existing SSN system.
- ✓ Task 3 - Assessment of implementation options for SSN.
- ✓ Task 4 - Elaboration of the technical specifications for the implementation in the Central SSN system.

This report deals with Task 3 which aims at defining of the options for implementing and applying the security and interoperability measures identified in Task 1 in SSN so as to correct the gaps identified in Task 2 of the study.

This report provides a detailed account of the users' organization and structure in order to simplify and harmonize the access right policy, the procedures necessary for establishing an information security management system for SSN, the assessment the suitability of relevant Connecting Europe Facility (CEF) Building Blocks, the definition of technical options for SSN, and the actions that need to be taken regarding SSN to apply the security and interoperability measures.

## 2 Introduction

### 2.1 Background on SafeSeaNet (SSN)

SafeSeaNet (SSN) is a system for the exchange of vessel and voyage related information between designated participants within European Union (EU).

The objective of SSN is to support EU and Member States (MSs) activities and enable the receipt, storage, retrieval and exchange of information for the purpose of maritime safety, port and maritime security, marine environment protection, and the efficiency of maritime traffic and maritime transport.

The operation of SSN involves a number of entities or users at regional, national and local level. The majority of these are in the shipping industry (ships' masters, agents, and operators) and National Administrations (Port Authorities and coastal stations, Port State Control (PSC) Officers, Search and Rescue (SAR) centres, vessel traffic services (VTSs), ship reporting systems, pollution response bodies, etc.). By enabling the exchange of vessel and voyage related information, the SSN system supports users at EU and MS levels in:

- ✓ The efficient and timely response to incidents or pollution at sea in progress including search and rescue operations;
- ✓ The monitoring of ships that pose a potential risk to the safety of shipping and the environment, including those involved in incidents, thus allowing for earlier precautionary actions and risk mitigation at sea by coastal states;
- ✓ The effective collection of information in support of the PSC inspection regime;
- ✓ The effective collection of the required information on port calls, the carriage of dangerous and polluting goods, security and waste for ships calling into a port of a MS;
- ✓ The management of flag State responsibilities, including the follow up of ships involved in incidents/accidents;
- ✓ The efficiency of port calls;
- ✓ The facilitation of maritime transport; and
- ✓ The gathering and comparison of objective and reliable information on maritime safety and on pollution by ships, thus enabling users to take the necessary steps to improve maritime safety and the prevention of ship generated pollution, and to evaluate the effectiveness of existing measures.

SSN is a specialised system established to: enable the exchange of information in an electronic format between MSs; provide the European Commission (EC) with the relevant information in accordance with Community legislation and; support MSs in satisfying their operational information needs. SSN is a network of National systems in MSs which are linked to a Central SSN system at EMSA that acts as a nodal point. The Central SSN system has different interfaces available to facilitate different means of transmission.

### 2.2 Objectives of the study

The **Security and Interoperability Solutions Study for SafeSeaNet** delivers a comprehensive study on security and interoperability solutions for SSN under the Common Information Sharing Environment (CISE) context and in perspective of additional foreseen developments. The solution will be implemented in the Central SSN system, in National SSN systems, and in the interfaces between the Central SSN system and National SSN systems.

The results of the study will define the measures and implementation options to ensure that within SSN:

- ✓ Data will be genuine and from bona fide sources (**authenticity**);
- ✓ Data will be accessible and usable upon request by an authorised entity (**availability**);
- ✓ Data will not be disclosed to unauthorized recipients (**confidentiality**);
- ✓ Data exchanged during the transactions will not be altered (**integrity**);
- ✓ All transactions will take place and will be attributable to identifiable individuals (**non-repudiation**);
- ✓ Access will only be granted to those who are authorized to (**authorization**);
- ✓ Exchanging data will require prior authentication of the parties (**authentication**);
- ✓ Information will be exchanged between all information systems involved (**interoperability**).

## 2.3 Purpose of this report

This report provides a detailed account of the proposed architectural options for future development of the Central SSN system and of the interfaces with the National SSN Systems.

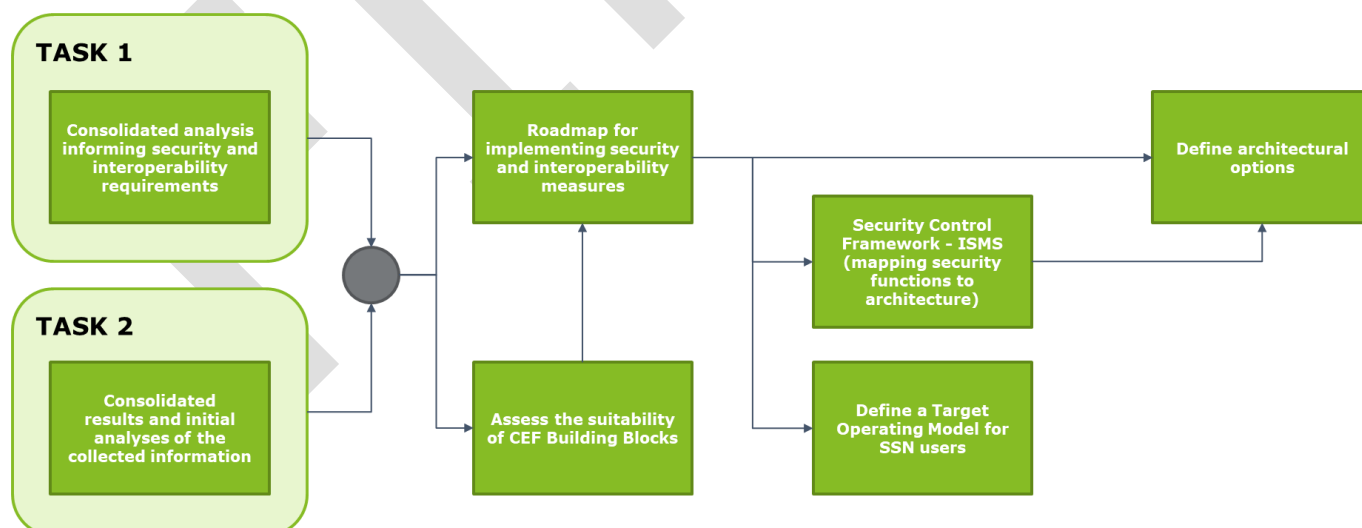
Taking into account the results of the Task 1 and of the Task 2, this report provides a structure and organisation of SSN users for the design of adequate role-based access control policies and measures. It provides a high-level Information Security Management System (ISMS) tailored for SSN. Specifically, as identified in Task 2, the scope of the ISMS takes into account the following elements:

1. The Central SSN System (CSSN)
  - ✓ European Index Server (EIS), which is the core of the CSSN architecture. It provides a secure and reliable index system (including authentication, validation, data transformation and logging) within a network, which sends requests to, and receives notifications and responses from, approved users. Users can provide and/or request data. The EIS is able to locate and retrieve information on vessels related to one Member State in response to a query or request made by another.
2. The National SSN systems (NSSN).
  - ✓ Only interfaces interacting with EIS are in scope.
3. The external systems: i.e. THETIS, EO DC, Sat-AIS, MS Specific, EU LRIT CDC, EU LRIT Ship DB, CECIS, Reference DB, MetOcean, and other EU systems (e.g. VMS, EUROSUR).
4. Only the interfaces and interactions with external systems interacting with EIS are in scope.

The proposed architectural options addressing security, data protection and interoperability gaps (identified by Task 2) provide alternative solutions in relevant areas of developments. This report provides also an assessment of the suitability of selected CEF Building Blocks, which offer basic capabilities that can be reused in any European project to facilitate the delivery of digital public services across borders and sectors. The tailored ISMS together with the identified architectural options form a roadmap of actions for future developments of SSN.

## 2.4 Overview of the methodology

Figure 1 provides an overview of the methodology for Task 3 (Assessment of implementation options for SSN) in alignment with the PM3-1 Project Plan. The methodology highlights also the relationships with the executed Task 1 and Task 2.



**Figure 1 Overview of the methodology for Task 3**

## 2.5 Structure of this report

The remainder of this report is structured as follows:

- ✓ **Section 3 Structure and organisation of SSN users** proposes a design for the structure and organisation of SSN users starting from the current situation, as mapped in the previous tasks. It is important to mention that this section takes into account the SSN users identified by previous tasks.
- ✓ **Section 4 Information security management system for SSN** defines a high-level Information Security Management System (ISMS) for SSN. This provides a high-level management framework, which should be further tailored for its implementation to the governance and operational environment of EMSA.
- ✓ **Section 5 Security, data protection and interoperability criteria for SSN** defines security, data protection and interoperability criteria for the assessment of architectural options. The security, data protection and interoperability criteria guide the assessment of the suitability of CEF Building Blocks as well as of the proposed alternative architectural options.
- ✓ **Section 6 Assessment of CEF Building Blocks** provides an overview and an assessment of the suitability of selected Connecting Europe Facility (CEF) Building Blocks with regards to the security, data protection and interoperability criteria for SSN.
- ✓ **Section 7 Assessment of technical options for SSN** describes the identified technical options for relevant architectural areas (i.e. Identity and Access Management, Data Storage, Archiving, Privacy Enhancing Technologies and Architecture, and Network Security) and provides an assessment according to the security, data protection and interoperability criteria for SSN.
- ✓ **Section 8 Roadmap of actions for implementation of SSN security, data protection and interoperability measures** provides a roadmap of actions for the implementation of the identified and selected architectural options for SSN.
- ✓ **Section 9 Conclusions** highlights key conclusions based on the analyses of the options for implementing and applying the security and interoperability measures and gaps identified.



### 3 Structure and organisation of SSN users

Taking into account the results of Task 1 and Task 2 reports, this section proposes a design for the structure and organisation of SSN users starting from the current situation, as mapped in the previous tasks. Furthermore, it presents a comprehensive design of all relevant categories and classes of SSN users and of the organisational attributes associated to the users. This supports the analysis of existing and planned access right policies for SSN. The analysis of the SSN roles shall support the implementation of the operational model and its consistency with the identified roles and responsibilities.

There are two key elements relating to SSN user access:

- 1. Current User Management in SSN.** A key aspect of a secure SSN is the organisation of user access management and access and control policies. The analysis conducted in Task 2 of SSN user profiles, roles, responsibilities, and access rights policies highlighted that there is a lack of a coherent operational end-to-end strategy on identity and access management in the SSN (Security gap #2). Currently, the Central SSN System and the National SSN systems (operated by Member States) rely on different decentralised authorisation mechanisms operated locally. The SSN documentation provides a limited account of standards or operational instructions considered as guidelines. Although this solution is sufficient in order to support information exchanges between the Central SSN System and the National SSN Systems, it provides limited support in order to implement end-to-end authorisation mechanisms, resulting in a reduced traceability and accountability. Implementing a centralised solution for identity and authorisation would enhance the overall security of the data exchanged between the different systems, because it will support defining detailed relevant authorisation mechanisms (including access control policies) guaranteeing security of data exchanged via SSN systems.
- 2. Current SSN Cyber Security Landscape.** The analysis conducted in Task 2 provides an overview of the cyber-security threat landscape for the transport maritime sector. The analysis highlights adversary types, threats, threat scenarios and risks tailored to SSN. Given the complex environment for SSN interoperability, user access and access management could be an entry point for many attack vectors resulting from the threat scenarios described.

In order to address the Security gaps identified in Task 2 report (in particular, the security gap concerned with Access Control), it is necessary to take into account all relevant SSN users, including users of the CSSN system as well as users of the NSSN systems). This is to develop a comprehensive Identify and Access Management (IAM) solution, which would support security requirements of CSSN system and NSSN systems. In order to achieve such objective, it is necessary to identify all SSN users and cluster them in groups related to their roles and responsibilities (hence, corresponding to different security rights).

At the operation level, different types of user profiles have been implemented in SSN by EMSA. The current version of the Access Right Matrix identifies 35 profiles (of which 15 profiles relate to SSN EIS) – 6 profiles for EMSA of which 1 with admin responsibilities, and 29 profiles for MS of which 1 with admin responsibilities. According to the EMSWe Regulation, an additional user role must be added (Table 1).

**Table 1 New SSN roles**

New SSN roles	SSN users organisational attributes
<b>MNSW Declarant</b>	Any natural or legal person who is subject to reporting obligations or any duly authorised natural or legal person acting on that person's behalf within the limits of the relevant reporting obligation. The declarants report information to the Maritime National Single Windows.

In addition to the current SSN roles, it is necessary to identify additional data protection and security roles drawn from relevant regulatory frameworks (in particular, EU DPR, GDPR and Commission Decision 2017/46). In order to integrate the identified data protection and security roles among the SSN roles, the roles presented in Table 2 **Error! Reference source not found.** below shall be created and integrated in the access policies of SSN.

**Table 2 New data protection and security SSN roles**

New data protection and security SSN roles	Description	Source
<b>Data Protection Officer</b>	As required by Regulation 2018/1725 EU DPR: Each Union institution or body shall designate a data protection officer in accordance with Article 43, Section 6 in Regulation 2018/1725.	Regulation 2018/1725 (EU DPR)
<b>Data Protection third party</b>	As required by Regulation 2018/1725 EU DPR: A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of	Regulation 2018/1725 (EU DPR)

New data protection and security SSN roles	Description	Source
	the controller or processor, are authorised to process personal data. This natural or legal will be authorised by the controller or processor.	
<b>Local Informatics Security Officer (LISO)</b>	As required by Commission Decision 2017/46: The officer who is responsible for IT security liaison for a Commission department.	Commission Decision 2017/46
<b>Data owner</b>	As required by Commission Decision 2017/46: The individual responsible for ensuring the protection and use of a specific data set handled by a Communication and information system (CIS).	Commission Decision 2017/46
<b>System owner</b>	As required by Commission Decision 2017/46: The individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of a Communication and information system (CIS).  Although the system owner might not require access to SSN, it is necessary to formalise the ownership and if necessary to provide access to SSN and its data following need-to-know principle, that is, accessing the system and data (only in the modes for which access is needed and only during the time frame when access is needed) in order to fulfil relevant security responsibilities.	Commission Decision 2017/46

The System owner would require access to operational data, conversely other roles would access operational data based on their profile that would define the 'need to know'. Note that in order to maintain segregation of duties, the new data protection and security SSN roles shall be distinct from the SSN\_ADMIN role. In case of personal data, the Data Protection Officer and the Data Owner cannot be combined.

It is necessary to map the roles above with specific SSN access right policies in order to reflect the different responsibilities and types of users. These access rights shall be reflected in the design of architectural options, for example implementing a federated identity management solution for Central SSN and National SSN systems.

## 4 Information security management system for SSN

According to ISO/IEC 27001/2, the development of an **Information security management system for SSN**, (ISMS) is a strategic decision an organisation makes in order to preserve the confidentiality, integrity, and availability of information by applying a risk management process, with the ultimate goal of giving confidence to interested parties that risks are adequately managed. This section defines a high-level Information Security Management System (ISMS) for SSN. The detailed definition of the applicable controls of the ISMS for SSN and their implementations are out of scope for this study.

### 4.1 Statement of Applicability

A Statement of Applicability (SoA) is developed to document which controls are applicable, and whether each applicable control is implemented or not, and how. The ISMS for SSN involves controls of ISO/IEC 27001/2 in order to comply with the requirements of Commission Decision 2017/46 rather than to achieve certification. As a result of **Task 1: Identification and definition of security measures to be applied in SSN** and **Task 2: Technical analysis of the existing SSN system** below is a list of applicable controls which are in scope of the study:

- ✓ Information security policies.
- ✓ Organization of information security.
- ✓ Asset management – Information classification.
- ✓ Access control.
- ✓ Operations security.
- ✓ Information systems audit considerations.
- ✓ Communications security.
- ✓ Information security incident management.
- ✓ Information security aspects of business continuity management.
- ✓ Compliance.

### 4.2 Security Controls

The tables below present a systematic high-level view per control, as they may apply in the context of the SSN ISMS. A total of 10 sections out of 14 sections in Annex A of ISO/IEC 27001/2 are considered as applicable. The activities in each applicable section are briefly described as they relate to the security controls. Each table defines for the identified activities their implementation status based on activities that EMSA has conducted. EMSA shall reassess the status of these activities on a regular basis and for implementing the ISMS for SSN.

**Table 3 ISMS activities for Information security policies**

ID	Activity	ISMS Activities Description	Status
SP_1	Policies for information security	Create a set of policies for information security to be defined, approved by management, published and communicated to employees and relevant external parties.	Implemented
SP_2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur.	Implemented

**Table 4 ISMS activities for Organization of information security (Internal organization)**

ID	Activity	ISMS Activities Description	Status
IS_1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Implemented
IS_2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Implemented
IS_3	Contact with authorities	Considering the interactions with national authorities responsible for National SSN system, review and maintain appropriate contacts with the relevant authorities.	Implemented

**Table 5 ISMS activities for Asset management**

ID	Activity	ISMS Activities Description	Status
AM_1	Inventory of assets	Identification and inventory of assets associated with information and information processing facilities.	Implemented
AM_2	Ownership of assets	Assign ownership of the inventoried assets.	Implemented
AM_3	Acceptable use of assets	Define rules for the acceptable use of information and of assets associated with information and information processing facilities.	Implemented

**Table 6 ISMS activities for Information classification**

ID	Activity	ISMS Activities Description	Status
IC_1	Classification of information	Define and maintain an information classification system, which takes into account the different type of data processed by the Central SSN system.	Implemented
IC_2	Labelling of information	Define and maintain an information labelling procedures according to the information classification scheme.	To be implemented

**Table 7 ISMS activities for Access control**

ID	Activity	ISMS Activities Description	Status
AC_1	Access control policy	Create an access control policy and review it based on business and information security requirements.	Implemented
AC_2	Access to networks and network services	Implement access controls based on the principles of 'need-to-know' and 'least privilege' to ensure that users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Implemented
AC_3	User access management	Establish processes to manage user access to ensure authorized user access and to prevent unauthorized access to systems and services.	Implemented
AC_4	User responsibilities	Establishes a process whereby users shall be required to comply with practices in the use of secret authentication information.	Implemented
AC_5	System and application access control	Establish processes for information access restrictions, secure log-on, password management and privileged access management.	Implemented
AC_6	Review of user access rights	Taking into account the proposal of a federated Identity and Access Management solution, EMSA shall conduct a review of user access rights.	Implemented
AC_7	Removal or adjustment of access rights	Taking into account the proposal of a federated Identity and Access Management solution, EMSA shall conduct remove or adjust user access rights accordingly.	Implemented

**Table 8 ISMS activities for Operations security**

ID	Activity	ISMS Activities Description	Status
OS_1	Documented operating procedures	Establish clear operating procedures communicate them to all relevant users	Implemented
OS_2	Change management	Ensure that an iterative process that supports the logging of changes to the organization, business processes, information processing facilities and systems that affect information security.	Implemented
OS_3	Logging and monitoring – event logging	For all relevant SSN processing activities and events, event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed. This activity needs to review the current maintained logs and updates the list of logs.	Implemented

ISMS Activities			
ID	Activity	Description	Status
		This may involve specific archiving solutions separated from operational data.	
OS_4	Logging and monitoring – protection of log information	Logging facilities and log information shall be protected against tampering and unauthorised access. This may involve specific archiving solutions separated from operational data.	Implemented
OS_5	Logging and monitoring – administrator and operator logs	Activities of Central SSN System administrator(s) and operator(s) shall be logged and the logs protected and regularly reviewed. This may involve specific archiving solutions separated from operational data.	Implemented

**Table 9 ISMS activities for Information systems audit considerations**

ISMS Activities			
ID	Activity	Description	Status
SA_1	Information systems audit controls	Establish clear audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	To be implemented

**Table 10 ISMS activities for Communications security**

ISMS Activities			
ID	Activity	Description	Status
CS_1	Network controls	Establish a process for networks to be managed and controlled to protect information in systems and applications.	Implemented
CS_2	Security of network services	Define processes for security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Implemented
CS_3	Segregation in networks	Establish groups of information services, users and information systems shall be segregated on networks.	Implemented

**Table 11 ISMS activities for Information transfer**

ISMS Activities			
ID	Activity	Description	Status
IT_1	Information transfer policies and procedures	Establish formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Implemented
IT_2	Agreements on information transfer	Establish clear agreements with the relevant National Authorities and Member States addressing the secure transfer of information between the Central SSN and the National SSN systems.	Implemented
IT_3	Confidentiality or non-disclosure agreements	Define, regularly review and document the requirements for confidentiality or non-disclosure agreements reflecting the operational needs of the Central SSN system in order to protect both operational as well as exchanged information.	Implemented

**Table 12 ISMS activities for Security in development and support process**

ISMS Activities			
ID	Activity	Description	Status
SD_1	Secure development environment	EMSA shall maintain and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle for the Central SSN architecture.	Implemented

ISMS Activities			
ID	Activity	Description	Status
SD_2	System security testing	EMSA shall perform testing of security functionalities of the Central SSN during development.	Implemented
SD_3	Restrictions on changes to software packages	EMSA shall ensure that modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Implemented

**Table 13 ISMS activities for Information security incident management**

ISMS Activities			
ID	Activity	Description	Status
ISIM_1	Reporting information security weakness	EMSA shall define policies for reporting information security weakness for all employees and contractors using the Central SSN system and related services. They shall be required to note and report any observed or suspected information security weaknesses in the Central SSN system and related services.	Implemented
ISIM_2	Assessment of and decision on information security incidents	EMSA shall define processes for assessing information security events. Such processes shall support decision-making in order to classify assessed events as information security incidents.	Implemented
ISIM_3	Response to information security incidents	EMSA shall define and document procedures in order to respond to information security incidents affecting the Central SSN.	Implemented
ISIM_4	Collection of evidence	EMSA shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence for the investigation of security incidents affecting the Central SSN system.	Implemented

**Table 14 ISMS activities for Information security aspects of business continuity management**

ISMS Activities			
ID	Activity	Description	Status
BC_1	Planning information security continuity	Establish requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Implemented
BC_2	Implementing information security continuity	Establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Implemented

**Table 15 ISMS activities for Compliance**

ISMS Activities			
ID	Activity	Description	Status
CO_1	Identification of applicable legislation and contractual requirements	Define a view all relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Implemented

In line with ISO/IEC 27001/2 a core element of the ISMS is to align security objectives with business requirements and the relevant legal landscape. EMSA has developed SafeSeaNet under the leadership of the European Commission (Directorate-General for Mobility and Transport - DG MOVE), in coordination with Member States. EMSA is responsible for its development, operation and maintenance, and interacts with users on an operational basis. The Member States, as data providers, are recognised as the owners of the data. Among all controls and activities identified, EMSA needs to implement two additional controls and associated activities concerned with Information classification (IC\_2) and Information systems audit considerations (SA\_1).

FINAL



# 5 Security, data protection and interoperability criteria for SSN

This section defines security, data protection and interoperability criteria for the assessment of architectural options. The security, data protection and interoperability criteria guide the assessment of the suitability of CEF Building Blocks as well as of the proposed alternative architectural options. The identified criteria take into account previous architectural studies on security and interoperability conducted for other EU agencies. Table 16 lists and defines (8) security, (4) data protection and (6) interoperability criteria for SSN.

**Table 16 Security, data protection and interoperability criteria for SSN**

Domain	Criterion ID	Criterion	Description
Security	SEC-01	Security Domains	The extent to which the architectural elements are segregated in function of their security levels and requirements.
	SEC-02	Data Security	The extent to which the architectural elements may preserve confidentiality, integrity and availability of data.
	SEC-03	Security Functions	The extent to which the architectural elements may support the implementation of security functions in alignment with relevant security policies.
	SEC-04	Complexity and Coupling of Security Functions	The degree of complexity and coupling of implementing security functions.
	SEC-05	Operational Security	The extent to which the architectural elements support and are in alignment with organisational security processes and procedures including roles and responsibilities.
	SEC-06	Architectural Exposure to Threats	The degree of exposure of the architectural elements to threats.
	SEC-07	Security Maintainability and Evolvability	The extent to which the security architectural elements are easy to integrate, modify, remove and evolve.
	SEC-08	Security Compliance	The extent to which the architectural elements support the provision of appropriate measures in full compliance with relevant security standards and regulations.
Data Protection	DP-01	Data Protection Compliance	The extent to which the architectural elements support the provision of appropriate safeguards in regard to personal data in full compliance with relevant data protection regulations.
	DP-02	Privacy Architecture	The extent to which architectural elements support the provision of appropriate measures in full compliance with relevant privacy architectural principles and frameworks.
	DP-03	Privacy by design and by default	The extent to which architectural elements ease the implementation of relevant data protection requirements and principles.
	DP-04	Operational Data Protection	The extent to which the architectural elements support and are in alignment with organisational data protection processes and procedures including roles and responsibilities.
Interoperability	INT-01	Interoperability Compliance	The extent to which the architectural elements support the provision of appropriate measures in full compliance with relevant interoperability standards and regulations.
	INT-02	Integration and interconnectivity	The extent to which architectural elements may be integrated and interconnected among each other.
	INT-03	Functional Maintainability and Evolvability	The extent to which the functional architectural elements are easy to integrate, modify, remove and evolve.
	INT-04	Elasticity and Scalability	The extent to which architecture elements support changing demands in terms of capacity and performance.
	INT-05	Technology readiness	The maturity of technological solutions for being integrated into the architecture.
	INT-06	Legacy and Migration	The extent to which architectural elements may integrate with and support the migration of legacy systems and services.

These criteria provide a means for assessing systematically and consistently the CEF Building Blocks as well as the identified architectural options for SSN.



# 6 Assessment of CEF Building Blocks

This section provides an assessment of the suitability of the Connecting Europe Facility (CEF) Building Blocks with regards to the security, data protection, and interoperability measures for SSN identified in Task 2, taking into account the relevant criteria for SSN.

## 6.1 Overview of CEF Building Blocks selected for analysis in the SSN context

This section provides an overview of the CEF Building Blocks considering available information on them. The Connecting Europe Facility (CEF) Building Blocks are Digital Service Infrastructures (DSI) offering wide-implementation solutions for European projects. The basis for the CEF building blocks are interoperability agreements that facilitate the communication between the IT systems of EU Member States and the EU citizens, businesses and/or public administrations, regardless of the location the digital public services may have in Europe. Thus, adopting the building blocks will facilitate the interoperability and reduce the communication barriers when delivering digital public services across-borders, on a more evolving digital era.

The European Commission provides a hub, the Core Service Platform (CSP), for each building block that is comprised of three layers:

- ✓ **Technical specifications** and standards that must be complied with, at the core of each building block.
- ✓ **Sample software** that complies and assists with the implementation of technical specifications and standards.
- ✓ **Services** (e.g. conformance tests, help desk support, etc.) that simplify the adoption of technical specifications and standards.

Table 17 provides a brief overview of selected CEF Building Blocks, which may provide technological solutions for future architectural developments for SSN.

**Table 17 Overview of Selected CEF Building Blocks**

CEF Building Block	Overview
<b>eArchiving</b>	<p><b>Description:</b> Simplifies the long-term digital information workflow (storage, preservation, access).</p> <p><b>End users:</b> Users with data to be stored, entities carrying out archiving activities, technical developers/researchers</p> <p><b>Usage/services:</b> Software; Support; Stakeholder Management; Developers Community</p> <p><b>General overview of steps for integration:</b></p> <ol style="list-style-type: none"> <li>Get familiar with standards and legislation</li> <li>Determine requirements for digital archiving</li> <li>Define a plan and a strategy to enable digital archiving</li> <li>Implement, integrate and test the solution</li> <li>Archive and retrieve the data</li> </ol> <p><b>Regulatory framework:</b> Core standard is the Reference Model for an Open Archival System (OAIS): ISO 14721:2012</p> <p><b>Implementation examples:</b> DG TAXUD and EU publication office are using eArchiving. It has also been implemented in National Archives of Estonia, to ensure preservation and usability of data records.</p>
<b>eDelivery</b>	<p><b>Description:</b> Secure message exchange system, according to OASIS's AS4 and the eIDAS Regulation's security requirements.</p> <p><b>End users:</b> Private/public entities/agencies; software service providers</p> <p><b>Usage/services:</b> Self-assessment; Open source sample software; Training sessions and deployment; Connectivity and conformance testing; Service desk</p> <p><b>General overview of steps for integration:</b></p> <ol style="list-style-type: none"> <li>Gather business needs and requirements</li> <li>Feasibility study</li> <li>Choose the approach / Develop the solution</li> <li>Deploy, integrate and test the solution</li> <li>Operate and promote</li> </ol> <p><b>Regulatory framework:</b> eIDAS Regulation (Regulation 910/2014).</p> <p><b>Implementation examples in EC:</b> DG TAXUD and EU publication office are using eDelivery. It has already been used in a project for Port Administration of Lisbon, to reduce the cost of exchanging information between different actors across transportations borders. Study on eDelivery and eSignature integration with TACHOnet.</p>
<b>eID</b>	<p><b>Description:</b> Cross-border access to digital services mainly for MSs, through an eIDAS node (compliant with EU legislation on electronic identification). Offers a means of effective and secure cross-border authentication through the mutual recognition of national eID schemes.</p> <p><b>End users:</b> Public/private entities</p> <p><b>Usage/services:</b> eIDAS eID Profile; : eIDAS-Node integration package; Testing (eID interoperability readiness testing); eID training; eID knowledge base; eID service desk</p> <p><b>General overview of steps for integration:</b></p> <ol style="list-style-type: none"> <li>Get familiar with applicable legislation</li> <li>Understand the Member State's approach</li> </ol>

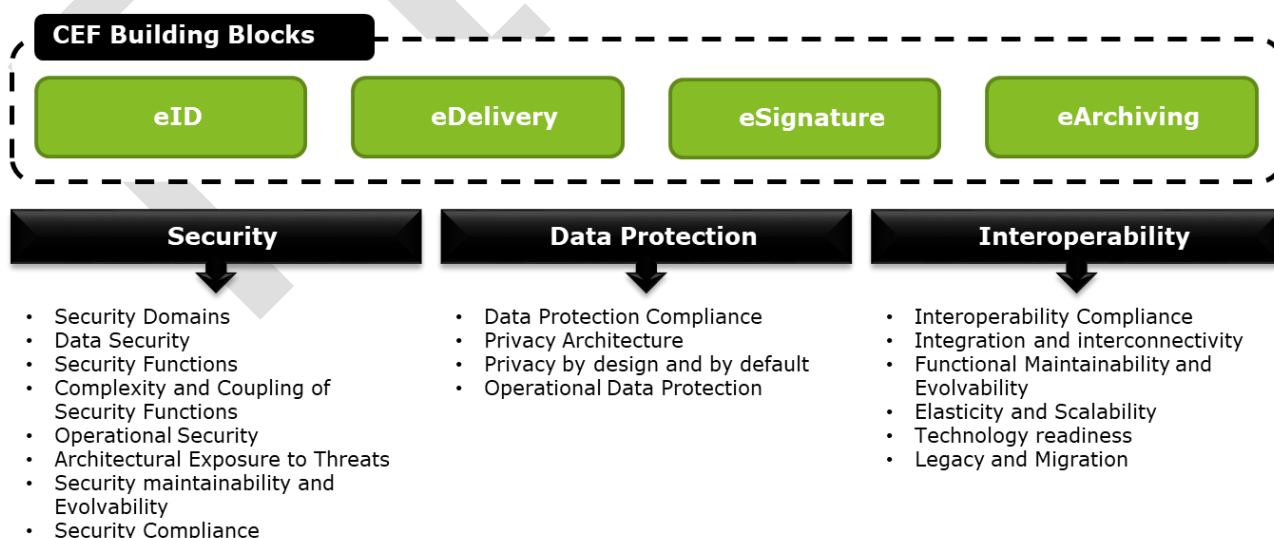
CEF Building Block	Overview
	c) Define requirements/scope d) Draft an integration plan e) Integrate and test f) Go live and promote <b>Regulatory framework:</b> eIDAS Regulation (Regulation 910/2014). <b>Implementation examples in EC:</b> Dutch public administrations are compliant with eIDAS Regulation and accept eIDs from other EU countries, in line with the standard, decreasing bureaucratic hurdles for citizens and businesses. The Estonian Information System Authority (RIA) expanded more than 3,500 services across Europe with eID and eSignature. Study on eID usage with DIGIT's European Citizens' Initiative.
<b>eSignature</b>	<b>Description:</b> Package for creating and verifying electronic signatures (Digital Signature Services (DSS)). <b>End users:</b> Citizens of EU countries, Iceland, Norway and Liechtenstein; Public/private entities and agencies, service/solution providers. <b>Usage/services:</b> DSS open-source library; Trusted list browser; e-sig validation tests. <b>General overview of steps for integration:</b> <ol style="list-style-type: none"> <li>Get familiar with applicable legislation and standards</li> <li>Identify the needs and select the type of e-signature</li> <li>Define the IT specification and how to enable digital signatures</li> <li>Use the eSignature DSS open-source library</li> <li>Obtain a digital certificate from a Trust Service Provider</li> <li>Start e-signing documents</li> </ol> <b>Regulatory framework:</b> eIDAS Regulation (Regulation 910/2014). <b>Implementation examples in EC:</b> eSignature facilitated the first electronic signature of a Security of Gas Supply EU Regulation, by the Estonian Presidency of the Council. The European e-Justice Portal uses eSignature for the creation and validation of electronic signatures. Study on eDelivery and eSignature integration with TACHOnet.

## 6.2 Assessment of relevant CEF Building Blocks

This section provides the results of the assessment of the CEF Building Blocks with regards to the SSN security and interoperability measures identified in the Task 2 of this study. The Connecting Europe Facility building blocks (CEF) were developed to be used, single or combined, in projects at European, national or local level, providing access to the public good to the European digital services.

To assess the possibility of integration, between CEF building blocks and SafeSeaNet, there are some criteria that must be considered in the assessment scope in order to determine the risk appetite of the CEF building block use and the risk that can be added into target system with such integration.

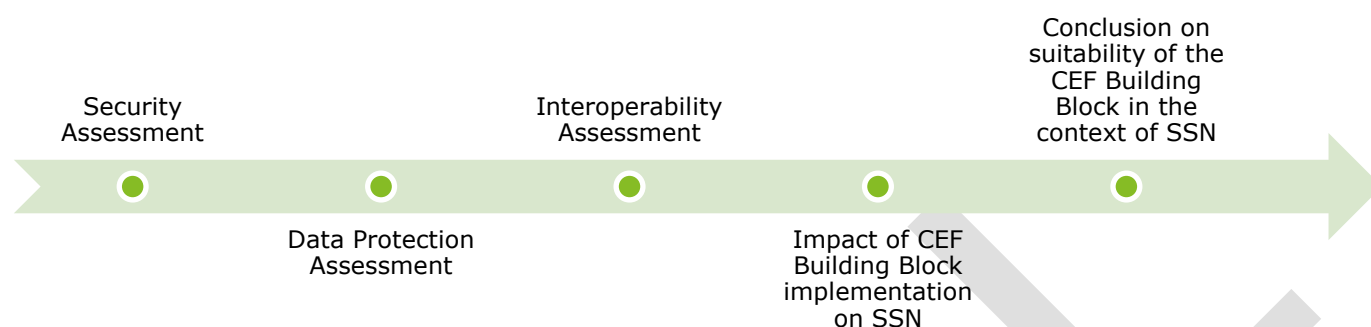
Despite the existence of several CEF building blocks this section provides an overview of the results obtained from the assessment focus on the following prioritized CEF building blocks, considering the domains and architectural criteria listed below and detailed in the **Section 5 Security, data protection and interoperability criteria for SSN**.



**Figure 2 Relevant CEF Building Blocks**

In order to classify each of the domains and criteria evaluated in the scope of this assessment, a three-level scale (high, medium, low) was used to provide a graphical vision of the high-level state of each building block in the three different domains. The analysis provides an assessment of advantages or disadvantages of integrating and adopting

(individually) each selected CEF Building Block in SSN. For a given building block, if the assessment identifies any restriction regarding the security, data protection or interoperability, the specific criteria will result in a Medium evaluation. Regarding security, it may be necessary a thorough analysis of the architectural components of a CEF Building block in order to accurately determine the extent of the impact in the architectural exposure to threats. For such cases, the assessment of the specific criteria will result in a Medium evaluation. The assessment takes also into account any relevant insights drawn from previous experiences<sup>1</sup> with the CEF Building Blocks and includes the following information:



## 6.2.1 Assessment of eID suitability in the context of SSN

This section assesses the eID building block according to the security, data protection and interoperability criteria for SSN (defined in **Section 5**).

### 6.2.1.1 Security assessment

It is necessary to harmonise current authentications systems adopted across the SSN ecosystem. The complexity of the currently adopted authentication systems is a consequence of different authentication systems deployed locally. This may expose the Central SSN as well as the National SSN systems to potential attacks exploiting vulnerabilities across deployed authentication systems. Harmonised and interoperable authentication systems covering Central SSN and National SSN would support mitigating such risk.

Table 18 provides an overview of the security assessment of eID for SSN. The use of the protocols between different eIDAS eID profiles, for example eIDAS-Nodes developed by the EC, ensures the security of the cross-border process through several standard protocols. That is, Member States can develop eIDAS compliant eID profiles in accordance with technical specifications developed by EC. The eIDAS-Node can request or provide cross border authentication, thus may present itself as a good solution for communication between SSN systems and MS<sup>2</sup>.

Recognised protocols such as TLS protocol and Security Assertion Markup Language (SAML) are used in the communication exchange between the MS ensuring the mutual recognition of national eID schemes. SAML 2.0 is the latest version of the SAML standard<sup>3</sup>. It is used for exchanging authentication and authorization data between security domains. SAML 2.0 is an XMLbased protocol that uses security tokens containing assertions to pass information about an agent (usually an end user) between a SAML authority (named an Identity Provider) and a SAML consumer (named a Service Provider).

The eID node operators<sup>4</sup>, i.e. Member States, should be ISO/IEC 27001 certified (or equivalent) or be compliant with applicable national legislation.

Before eID is adopted for SSN, it is necessary to conduct an analysis of technical constraints for the authentication systems (e.g. certification validation schema) at the implementation level. In order to assess the adoption of eID, it is also necessary to take into account the required interactions (in terms of authentication and authorisation) between the Central SSN and the National SSN systems. For example, if only the national SSN shall need the adoption of eID, it is possible to use a PKI based on e-Delivery building block and audit logging by the Member States, ensuring more traceability based on the individual identity. However, due to need for harmonisation and interoperability, it is necessary to move towards a federated solution for identification and authorisation. The overall

<sup>1</sup> Study on TACHOnet use of eDelivery and eSignature DRAFT Final Report, V0.8, 25 October 2017.

<sup>2</sup> This considers eIDAS-Node as an example, as it is developed by the EC and already complies with technical specifications (e.g. interoperability and crypto requirements) and regulations (e.g. Regulation 910/2014 and Commission Implementing Regulation 2015/1501).









<sup>3</sup> The European Commission has used the Common Assessment Method for Standards and Specifications (CAMSS) for assessing the SAML protocol.

<sup>4</sup> A node operator is the entity responsible for ensuring that the eID node performs correctly its functions as a connection point.

assessment of the eID building block shall consider any possible difficulties of implementation across all Member States. The implementation of the eID building block would require the agreement and adoption from all Member States and National Competent Authorities operating the National SSN systems. Without such agreement, the adoption of the eID building block is unfeasible.

**Section 7.2** provides alternative federated Identity and Access Management (IAM) solutions for the SSN ecosystem with third-party technologies or eID building blocks. EMSA in coordination with the MS will have to define a roadmap of actions for implementing a federated IAM solution for the Central SSN and the National SSN systems.





**Table 18 Security assessment of eID for SSN**

Domain	Criterion ID	Criterion	Assessment
Security	SEC-01	Security Domains	High 
	SEC-02	Data Security	High 
	SEC-03	Security Functions	High 
	SEC-04	Complexity and Coupling of Security Functions	Medium 
	SEC-05	Operational Security	High 
	SEC-06	Architectural Exposure to Threats	Medium 
	SEC-07	Security Maintainability and Evolvability	Medium 
	SEC-08	Security Compliance	High 

#### 6.2.1.2 Data protection assessment

Table 19 provides an overview of the data protection assessment of eID for SSN. The eID building block acts as part of the authentication process without storing data from the owner of the request. The request for the authentication is sent into the target member state that validates the authentication process in his own service/identity provider. Identity providers are responsible for operating the authentication procedure of the end user, thus being liable to the same extent as Member States for damage caused to any natural or legal person, due to a failure to ensure the correct operation of the authentication process. The protection of the data in transit is ensured by eIDAS-Nodes that is responsible for the standards for which electronic signatures, qualified digital certificates, electronic seals, timestamps, and other proof for authentication mechanisms enable electronic transactions. Additionally, the SAML framework used for the exchange of authentication information within the eIDAS and the eIDAS-Nodes (which need to be deployed in Central SSN and National SSN systems) is also used to protect the confidentiality and integrity of the data in transit, between EMSA, data providers and the Member States. As per Regulation 910/2014 (eIDAS Regulation), the eIDAS nodes shall not store any transition data containing personal data beyond as required by Article 9 and the use of pseudonyms in electronic transitions is permitted.

**Table 19 Data protection assessment of eID for SSN**

Domain	Criterion ID	Criterion	Assessment
Data Protection	DP-01	Data Protection Compliance	High 
	DP-02	Privacy Architecture	High 
	DP-03	Privacy by design and by default	High 
	DP-04	Operational Data Protection	High 

#### 6.2.1.3 Interoperability assessment

Table 20 provides an overview of the interoperability assessment of eID for SSN. The eID building block complies with the eIDAS Regulation on electronic identification and trust services and can be used simultaneously with other building blocks (e.g. eArchiving, eSignature) improving the overall interoperability between SSN and other EU services and applications.

The European Commission has implemented a dedicated identification mechanism to facilitate users' access to a wide range of Commission information systems, known as EU Login. This system is ready to connect to the eIDAS network, allowing users to identify and authenticate to the services thanks to their nationally-issued electronic







identification (eID). It is therefore possible to integrate SSN with eID and EU-Login, but this possibility should be further analysed in detail.

Interoperability advantages of the adoption of eID, may include:

- ✓ Providing a legal basis, and therefore legal obligation, for the recognition of eIDs across borders (respecting data protection legislation in both originating and receiving countries).
- ✓ Clarifying and detailing the organisational relationship between the different Member States and the necessary operational management related process.
- ✓ Ensuring that the electronic identification information exchanged in a cross-border scenario is transmitted in a meaningful way to and from external sources to ensure that the precise meaning of exchanged information is understood and preserved throughout exchanges between parties.
- ✓ Ensuring that the technical elements of cross-border eID authentication are compatible - when interconnecting the different national eID solutions, it should be technically possible to link the different eID information systems.
- ✓ Ensuring an effective interoperability with cross-border authentication through mutual recognition of national eID schemes it also offers two different implementing models (proxy, middleware) depending on the considerations such as: liability, scalability, legal requirements, among others.

The eIDAS eID profile specifications were also developed in line with Commission Implementing Regulation (EU) 2015/1501 on the interoperability framework. Additionally, CEF also offers a testing service, i.e., the eID Interoperability Readiness Testing, to help verify the interoperability of nodes, by simulating the behaviour of an eIDAS-Node located in another Member State.

**Table 20 Interoperability assessment of eID for SSN**

Domain	Criterion ID	Criterion	Assessment
Interoperability	INT-01	Interoperability Compliance	High 
	INT-02	Integration and interconnectivity	High 
	INT-03	Functional Maintainability and Evolvability	High 
	INT-04	Elasticity and Scalability	High 
	INT-05	Technology readiness	High 
	INT-06	Legacy and Migration	Medium 

#### 6.2.1.4 Impacts of eID implementation on SSN

The integration of this building block in SSN may leverage the authorization mechanisms currently in place, which are operated locally and guarantee information exchange between Central and National SSN systems. However, as previously analyzed by Task 1, The Central SSN has limited controls on the identification, authentication, and authorization of users of the National SSN systems operated by MSs. The eID building Block provides limited support for addressing such problem by end-to-end authorization mechanisms. The implementation of eID's eIDAS-Node would simplify the communication between SSN and the Member States and comply with eIDAS Regulation regarding mandatory mutual recognition of eID schemes across Europe. However, and since eID only acts as an authentication system but does not address authorisation, a possible solution for this integration in SSN would be the implementation of a federated IAM solution alongside with eID. This combination would still be aligned with Regulation (EU) 2019/1239 and enhance the overall security of the data exchanged between the different systems.

#### 6.2.1.5 Conclusion on eID suitability in the context of SSN

The eID is mainly designed for supporting identification of citizens who are registered for services in Member States. Public sector service providers can connect to an existing eIDAS-Node in order to offer online services capable of identifying citizens and businesses from other Member States. Taking into account the analysis of the eID (which provides limited support for implementing end-to-end authorisation, authentication and identification mechanisms across the SSN ecosystem) and the operational needs of the Central SSN system, and its interaction with National SSN systems (which involve different users registered locally and systems not necessary integrated with other public sector services), the eID is assessed to be unsuitable for the context of SSN.

**This conclusion needs to be revisited when a security study will include the declarants to the EMSWe.**



## 6.2.2 Assessment of eDelivery suitability in the context of SSN

This section assesses the eDelivery according to the security, data protection and interoperability criteria for SSN (defined in **Section 5**).

### 6.2.2.1 Security assessment

The eDelivery building block helps to exchange data and documents in a reliable way, ensuring that:

- ✓ Documents are encrypted during transmission (Confidentiality).
- ✓ Data and documents are secured against any modification (Integrity).
- ✓ Non-repudiation of origin and recipient of the message is guaranteed.
- ✓ The origin and the destination of the data and documents are trustworthy.
- ✓ There is access to configurable logging of events related to the exchange of data and documents.









This building block is comprised of a four-corner model, where the backend systems exchange messages via the access points and using digital certificates, either through a Public Key Infrastructure (PKI) or through mutual exchange, assuring a secure transmission of data at the messaging and transport layer, using TLS.

The AS4 messaging protocol<sup>5</sup> used by eDelivery helps in the creation of a secure channel for the electronic transmission of documents and data, protecting it against any loss, theft or tampering. Designed to support both one-way and two-way exchanges, it may be used for several types of documents/messages and supports the use of digital certificates for signing and encryption. Additionally, the WS-Security extension helps to assure non-repudiation and data confidentiality.

It is also possible to set up eDelivery by re-using a conformant open source solution, buying a solution from a vendor or building a custom solution following technical specifications. The degree of threat exposure, complexity of security compliance of its functions may vary based on the chosen solution for implementation. The configuration of Access Points (through which the backend systems exchange messages) is also of the responsibility of the message senders/receivers, which may also impact data privacy architecture.

The CEF eDelivery Security Controls' guidance document<sup>6</sup> includes security controls and recommendations applicable to comply with the eIDAS regulation and mapped with security controls of qualified ERDS (QERDS). These security controls are not mandatory but are strongly recommended to ensure a maximum compliance with these controls. Table 21 provides an overview of the security assessment of eDelivery for SSN.

**Table 21 Security assessment of eDelivery for SSN**

Domain	Criterion ID	Criterion	Assessment
Security	SEC-01	Security Domains	High 
	SEC-02	Data Security	High 
	SEC-03	Security Functions	High 
	SEC-04	Complexity and Coupling of Security Functions	Medium 
	SEC-05	Operational Security	High 
	SEC-06	Architectural Exposure to Threats	Medium 
	SEC-07	Security Maintainability and Evolvability	Medium 
	SEC-08	Security Compliance	Medium 

### 6.2.2.2 Data protection assessment

In the context of messaging, this building block relies on trust models to establish a secure and trusted communication with one another. In this case, the trust models are rules to ensure the legitimacy of digital certificates used by eDelivery components, crucial to ensure user identification and the authenticity, confidentiality, integrity and non-repudiation of data moving across systems. The evidences produced during the exchange of data

<sup>5</sup> AS4 (Applicability Statement 4) is a message protocol based on web services to securely exchange B2B messages between trading partners. The protocol was developed by the technical committee of OASIS (Organization for the Advancement of Structured Information Standards) for ebXML Messaging Services.

<sup>6</sup> CEF eDelivery Security Controls' guidance document, V1.0, 14 December 2018.





with eArchiving provide a guarantee that data and documents are delivered only once and the messages are delivered, even if the channels are temporarily unavailable. Actually, eArchiving itself is not needed to provide an only-once delivery. It is the retry mechanism, together with duplicate detection that guarantees only once delivery. eArchiving facilitates but is not an absolute requirement for guaranteeing traceability of data. Even without archiving, messages and metadata can be kept in the database to cover this. eArchiving just facilitates the long-term storage and preservation of this data.

Regarding the applicability in SSN, if used alongside with eArchiving, it helps to guarantee traceability of data. This way it is possible to ensure that messages are signed and archived/retained for proof without use of eSignature. The receiver does have the information from the sender in the format of a signed AS4 Non-Repudiation Receipts upon successful reception of a message.

With eDelivery, upon the successful delivery of the message, the receiver receives information from the sender through a signed AS4 non-repudiation receipt. Senders/receivers are responsible for the configurations of their own environments in order to deploy eDelivery. To that extent, protection of data may depend on the configuration, as there are optional controls that may or not be implemented through the access point's parameters.

Table 22 provides an overview of the data protection assessment of eDelivery for SSN.







**Table 22 Data protection assessment of eDelivery for SSN**

Domain	Criterion ID	Criterion	Assessment
Data Protection	DP-01	Data Protection Compliance	High 
	DP-02	Privacy Architecture	Medium 
	DP-03	Privacy by design and by default	High 
	DP-04	Operational Data Protection	High 

### 6.2.2.3 Interoperability assessment

Table 23 provides an overview of the interoperability assessment of eDelivery for SSN. The eDelivery building block complies with the eIDAS Regulation on electronic identification and trust services and can be used simultaneously with other building blocks (e.g. eArchiving, eSignature, eID) improving the overall interoperability between SSN and other EU services and applications. With eDelivery it is also possible to assure exchange of documents and/or data using a messaging protocol, instead of using emails. Since it is possible to integrate eDelivery with own backend and sender/receiver's solutions, as referred before, we can say that the building block offers a good level of interoperability. The information about the processed messages is also accessible to everyone in the data exchange network. Both sender and receiver in a specific transaction can indeed have all the information about the processing of a message, which will not be visible to other participants in the network. Only if it is a requirement of the business domain, the messaging metadata or processing information could be made available in an immutable way (e.g. by using blockchain to store metadata). The degree of legacy or functional maintainability and evolvability of the solution will depend on the chosen possibilities of integration.

**Table 23 Interoperability assessment of eDelivery for SSN**

Domain	Criterion ID	Criterion	Assessment
Interoperability	INT-01	Interoperability Compliance	High 
	INT-02	Integration and interconnectivity	High 
	INT-03	Functional Maintainability and Evolvability	Medium 
	INT-04	Elasticity and Scalability	High 
	INT-05	Technology readiness	High 
	INT-06	Legacy and Migration	Medium 

### 6.2.2.4 Impacts of eDelivery implementation on SSN

The eDelivery building block adds value to the exchange of electronic data and documents across borders while ensuring non-repudiation of receipt and/or origin of every exchange through its integrated electronic signature function. Regarding its applicability in SSN, especially if combined with eArchiving, it helps guaranteeing traceability and preservation of long-term storage data. This way it is possible to ensure that messages are signed and

archived/retained for proof. However, the receiver has no evidence from the sender as it is only possible to see that the message has been delivered. Another benefit is the guarantee that data and documents are delivered once and only once.

Regarding security of confidentiality, this building block also ensures compliance with ENISA guidelines regarding the usage of older version of TLS and SSL, i.e., TLS versions 1.0/ 1.1 and SSL versions 2.0/3.0 should not be used. As per the security assessment performed in Task 2, SSN is currently using version 1.0 of TLS protocol which is no longer deemed secure, whereas eDelivery can offer a security advantage to SSN.

The information exchanges between the Central SSN and the National SSN systems involve secure communications. The adoption of eDelivery requires its implementation in the Central SSN as well as across all National SSN systems. This corresponds to a major restructuring of communication in the SSN ecosystem. Such restructuring may potentially disrupt the SSN ecosystem and its security too (e.g. due to lack of implementation/coordination of eDelivery in all National SSN systems). Furthermore, the types of communications involve the exchange of data rather than documents. This would require tailoring eDelivery in order to define the data exchange format and the configuration of different environments (of the Central SSN and National SSN systems). This would require a major implementation effort. Taking into account such considerations, the adoption of eDelivery would have a major impact (in terms of effort required), which may increase the risk of disrupting operations (also in terms of security and interoperability).

#### **6.2.2.5 Conclusion on eDelivery suitability in the context of SSN**

eDelivery is a network of nodes for digital communications. It is based on a distributed model where every participant becomes a node using standard transport protocols and security policies. It helps public administrations to exchange electronic data and documents with other public administrations, businesses and citizens, in an interoperable, secure, reliable and trusted way. The CEF eDelivery building block is based on the AS4 messaging protocol, open and free for all, developed by the OASIS standards development organisation. To ease its adoption in Europe, eDelivery uses the AS4 implementation guidelines defined by the Member States in the e-SENS Large Scale Pilot. Organisations must install an Access Point, or use a Service Provider, to exchange information with the AS4 messaging protocol<sup>7</sup>. The eDelivery CEF Building Blocks can be used for secure exchange of messages and data. Therefore, it may be considered a suitable option for interchanges of messages and data between the Central SSN and the National SSN systems. However, taking into account that this may require a completely redesign of communication mechanisms between the Central SSN and the National SSN as well as an agreement between EMSA and the Member States, eDelivery is assessed to be unsuitable for the context of SSN.

**This conclusion needs to be revisited when a security study will include the declarants to the EMSWe.**

### **6.2.3 Assessment of eSignature suitability in the context of SSN**

This section assesses the eSignature building block according to the security, data protection and interoperability criteria for SSN (defined in **Section 5**).

#### **6.2.3.1 Security assessment**

The Digital Signature Services (DSS) is an open-source software library intended for digital signature creation, validation, and extension, designed to help achieve compliance with the eIDAS Regulation. It may be used as an applet, in a stand-alone application or in a server application. The DSS eSignature per se supports EU standards on signature formats and packaging methods and signature validation procedures. Also, to digitally sign a document, the citizen must have a valid digital certificate, which is similar to a digital ID (digital certificates are provided by Trust Service Providers).

As the eSignature supports three different types of electronic signatures, compliance with security criteria will depend on the level of electronic signature used (refer to **Section 6.2.3.2** for more information). The assessment of eSignature's compliance with security, interoperability and data protection controls highly depends on the type of signature used. Note that eSignature does not provide direct measures to protect data integrity. It needs to be combined with authorisation mechanisms addressing data security. eSignature provides an electronic indication of a person's intent to agree to the content of a document or a set of data to which the signature relates. Therefore, eSignature can support the verification of identity and integrity of the documents and data exchanged, rather than protecting the data or document per se. Additional mechanisms such as encryption and access controls shall be implemented in order to support data security.

---









<sup>7</sup> The European Commission has reviewed solutions that have passed or are in the process of passing the conformance testing according to the eDelivery AS4 profile. European Commission (2019): CEF eDelivery, Market guide for AS4 solutions and services, v1.05.



Also, as per EMSA's interview with DIGIT, to further understand the suitability of implementation of eSignature in SSN, it is necessary to determine what type of items need to be signed and if the signed item needs to be retained after data transmission. This depends on the types of data exchanged between the Central SSN and the National SSN systems. The EMSWe Regulation (EU) 2019/1239 does not clarify whether or not exchanged data need to be signed. However, implementing an eSignature for data exchange would enhance the security (in terms of integrity and authenticity) of data in SSN.

Table 24 provides an overview of the security assessment of eSignature for SSN.

**Table 24 Security assessment of eSignature for SSN**

Domain	Criterion ID	Criterion	Assessment
Security	SEC-01	Security Domains	Medium 
	SEC-02	Data Security	High 
	SEC-03	Security Functions	Medium 
	SEC-04	Complexity and Coupling of Security Functions	Medium 
	SEC-05	Operational Security	Medium 
	SEC-06	Architectural Exposure to Threats	Medium 
	SEC-07	Security Maintainability and Evolvability	Medium 
	SEC-08	Security Compliance	Medium 

#### 6.2.3.2 Data protection assessment





Table 25 provides an overview of the data protection assessment of eSignature for SSN. The eSignature comprises three levels of electronic signatures, according to the eIDAS Regulation:

- ✓ Simple electronic signatures – Something as simple as writing down a name on an e-mail may constitute a simple electronic signature.
- ✓ Advanced electronic signatures (AdES) – Involves the usage of certificates and cryptographic keys, as a unique link is created to identify the signatory and it is possible to detect changes to data.
- ✓ Qualified electronic signatures (QES) – Based on a qualified certificate for electronic signatures.

Taking into account, that SSN will exchange also personal data, it is necessary to implement stringent signature mechanisms such as AdES and QES. The eSignature building block may be adopted in SSN as a retention of message signature (eDelivery has the same functionality). The usage of simple electronic signatures may not fully comply with privacy principles, namely privacy by default principle. This is because simple signature mechanisms may guarantee the authenticity of the sender (and the exchanged information), but it lacks any specific support for relevant privacy principles (e.g. data minimisation and need to know). This may be achieved with encryption mechanisms and strategies for protecting sensitive data such as personal data. This is beyond the capabilities of eSignature. Regarding protection of personal data, it is assumed that eSignature must comply with eIDAS regulation and EU DPR.

Regarding protection of personal data, it is assumed that eSignature must comply with eIDAS regulation and EU DPR.

**Table 25 Data protection assessment of eSignature for SSN**







Domain	Criterion ID	Criterion	Assessment
Data Protection	DP-01	Data Protection Compliance	High 
	DP-02	Privacy Architecture	Medium 
	DP-03	Privacy by design and by default	Medium 
	DP-04	Operational Data Protection	High 

#### 6.2.3.3 Interoperability assessment

Table 26 provides an overview of the interoperability assessment of eSignature for SSN. Electronic signing allows significant time saving, reduces operational costs and enhances the security of processing for EU citizens. It's a lever

for businesses to integrate electronic signature processes, increasing interoperability on electronic transactions (e.g., EU legislative processes). To assure signatures can be created and validated anywhere in Europe, as per the eIDAS Regulation on electronic identification and trust services, the eSignature has a defined number of baseline profiles that comply with several standards.

**Table 26 Interoperability assessment of eSignature for SSN**

Domain	Criterion ID	Criterion	Assessment
Interoperability	INT-01	Interoperability Compliance	High 
	INT-02	Integration and interconnectivity	High 
	INT-03	Functional Maintainability and Evolvability	High 
	INT-04	Elasticity and Scalability	Medium 
	INT-05	Technology readiness	High 
	INT-06	Legacy and Migration	Medium 

#### 6.2.3.4 Impacts of eSignature implementation on SSN

The eSignature building block may support implementing measures (e.g. authenticity of modification requests to data) in order detect any unauthorized changes made to critical data stored and retained locally after data transmission. With the upcoming changes to SSN, it is expected that SSN will be processing a significant quantity of data of all passengers and crew members that reach EU ports. This may require additional measures in order to protect and process personal data in compliance with relevant data protection regulatory frameworks. The Central SSN will process (personal) data collected and communicated by the National SSN systems (hence, under the controller responsibilities of the National Authorities). It is therefore necessary to implement adequate mechanisms in order to guarantee the authenticity of requests from the National Authorities via the National SSN systems. eSignature may support such type of measure, although it provides limited support for protecting (personal) data. Therefore, it is recommended to assure cryptographic mechanisms rather than to adopt eSignature in order to protect the confidentiality and integrity of data (including personal data).

Also, as per Decision 2015/444 on the security rules for protecting EU classified information, the SSN system can be considered as an unclassified system. However, it also includes some commercial sensitive data and system security related information that should be protected during collection, processing and storage.

A possible use case of eSignature in the SSN context may be to electronically sign internal administrative procedures (e.g. Confidentiality or Non-Disclosure Agreements) rather than for exchanging data. Further analysis on what type of documents/data need to be signed and retained after data transmission shall be performed in order to understand whether eSignature may support specific needs for signing electronically documents and information.

As regards the exchanges of data between the Central SSN and the National SSN systems, it more important to implement adequate measures reflecting access controls (e.g. user credentials) rather than electronic signatures.

#### 6.2.3.5 Conclusion on eSignature suitability in the context of SSN

The eSignature building block helps public administrations and businesses accelerate the creation and verification of electronic signatures. The deployment of solutions based on this building block in a Member State facilitates the mutual recognition and cross-border interoperability of eSignatures. This means that public administrations and businesses can trust and use eSignatures that are valid and structured in EU interoperable formats. Taking into account that the data exchanges between the Central SSN and the National SSN systems involve system-to-system communications, the eSignature is assessed to be unsuitable for the context of SSN.

**This conclusion needs to be revisited when a security study will include the declarants to the EMSWe.**

### 6.2.4 Assessment of eArchiving suitability in the context of SSN

This section assesses the eArchiving building block according to the security, data protection and interoperability criteria for SSN (defined in **Section 5**).

#### 6.2.4.1 Security assessment

As the transfers of information are built upon the use of standards and their transfer formats in order to secure reliable information storage, the eArchiving specifications are based on standards for transferring data from source information systems or databases to long-term repositories, describing and preserving digital data, mainly the Open









Archival Information System (OAIS) Reference Model, a conceptual framework of a digital archive that is the common specification information package (CSIP). The CSIP delivers basic core specifications for institutions on EU to securely pack their data and documents. Besides the CSIP there are other available packages (for sending, storing or accessing material from repositories) that each individually have to be evaluated, regarding security criteria. The CEF eArchiving technical specifications varies from the available profiles:

- ✓ E-ARK SIP: open formats for packaging data and metadata for transfer to archival repositories.
- ✓ E-ARK AIP: for the preservation over extended periods.
- ✓ E-ARK DIP: reuse of archived content.

The most common principles and requirements are presented separately within the E-ARK Common Specification for Information Packages. As the technical specifications vary, it is not possible to determine exactly the extent of full compliance with the mentioned security and interoperability controls.

This building block is similar to cloud storage services and may be implemented alongside eDelivery to ensure digital archiving services. It may contribute to improve further current SSN archiving practices. It ensures confidentiality and integrity of documents/data and is possible to use big data techniques to analyse large quantities of archived data. The eDelivery does not provide itself big data techniques, however it can be combined with the Big Data Test Infrastructure (BDTI) building block. The BDTI building block provides a set of data and analytics services from infrastructure to tools and advisory, allowing European organisations to experiment with Big Data technologies and move towards a data-driven policy making. More specifically, BDTI is a big data platform that offers virtual environments, allowing public organisations to: experiment and launch pilot projects on big data and data analytics; share various data sources; acquire support; have access to best practices and methodologies on big data. Table 27 provides an overview of the security assessment of eArchiving for SSN.





**Table 27 Security assessment of eArchiving for SSN**

Domain	Criterion ID	Criterion	Assessment
Security	SEC-01	Security Domains	High 
	SEC-02	Data Security	High 
	SEC-03	Security Functions	Medium 
	SEC-04	Complexity and Coupling of Security Functions	Medium 
	SEC-05	Operational Security	Medium 
	SEC-06	Architectural Exposure to Threats	High 
	SEC-07	Security Maintainability and Evolvability	Medium 
	SEC-08	Security Compliance	Medium 

#### 6.2.4.2 Data protection assessment

Table 28 provides an overview of the data protection assessment of eArchiving for SSN. It is possible to define format, specifications, and rules for data archiving, as well as search functionalities based on attributes and extraction of records and define a specific retention period. This particular building block also allows the possibility to safely dispose of documents/data after a specific period of time, providing a correct and secure handling of sensitive and confidential information. eArchiving also provides certainty on whether the data is secured against modifications and during the transmission. It is also possible to have access to metadata that describes the context of documents. All information packages of eArchiving use the GDPR as standard to assure data protection.







**Table 28 Data protection assessment of eArchiving for SSN**

Domain	Criterion ID	Criterion	Assessment
Data Protection	DP-01	Data Protection Compliance	High 
	DP-02	Privacy Architecture	High 
	DP-03	Privacy by design and by default	High 
	DP-04	Operational Data Protection	High 

### 6.2.4.3 Interoperability assessment

The CEF eArchiving building block allows short, medium and long term storage, access and re-use of information. Using the eArchiving information packages, it's possible to access data across-borders, fostering interoperability synergies with EU institutions and user communities. It also adds an increased cross-frontier availability of commercial eArchiving services for the public and private sectors. Table 29 provides an overview of the interoperability assessment of eArchiving for SSN.

**Table 29 Interoperability assessment of eArchiving for SSN**

Domain	Criterion ID	Criterion	Assessment
Interoperability	INT-01	Interoperability Compliance	High 
	INT-02	Integration and interconnectivity	High 
	INT-03	Functional Maintainability and Evolvability	Medium 
	INT-04	Elasticity and Scalability	High 
	INT-05	Technology readiness	Medium 
	INT-06	Legacy and Migration	Medium 

### 6.2.4.4 Impacts of eArchiving implementation on SSN

The eArchiving despite similar to data storage, is designed to store bulk data and metadata in a platform-independent, authentic and for long-term usage. It is similar to cloud storage services and alongside eDelivery it ensures digital archiving services.

This building block provides key functionalities, depending on the used profile, such as:

- ✓ Definition of format, specifications and/or rules for data to be archived.
- ✓ Search functionality available based on attributes and extraction of records, i.e. it is possible to include attributes for search queries in long term archives.
- ✓ Definition of specific retention periods, including delete data from production.

Currently SSN archiving practices can be further improved by adopting a dedicated service such as the one supported by eArchiving. For example, the EMSWe regulation foresees the possibility that the maritime National Single Window could retrieve relevant information that has already been submitted through the entry summary declaration. In this case, measures such as eArchiving should be taken at the level Central and National SSN level. It is also necessary to update current SSN data retention policy in order to take into account applicable regulatory requirements (including EMSWe regulation, EU DPR, etc.) and specific SSN data archiving policies at central and national level, including the identification of what system data should be stored and for how long it must be kept.

### 6.2.4.5 Conclusion on eArchiving suitability in the context of SSN

There is currently no legal obligation or requirements for archiving. There is no European Union Directive that governs digital archiving. However, there might exist local legal obligations, which are regulating archiving activities in different Member States. However, the results of the security assessment for the Central SSN system has highlighted that it is necessary to update current digital archiving and data classification policies. Therefore, eArchiving (as well as other commercial solutions) may provide a suitable option for implementing digital archiving strategies in the context of SSN.

**The eArchiving can also be used to support the data providing process of the declarants to the EMSWe.**

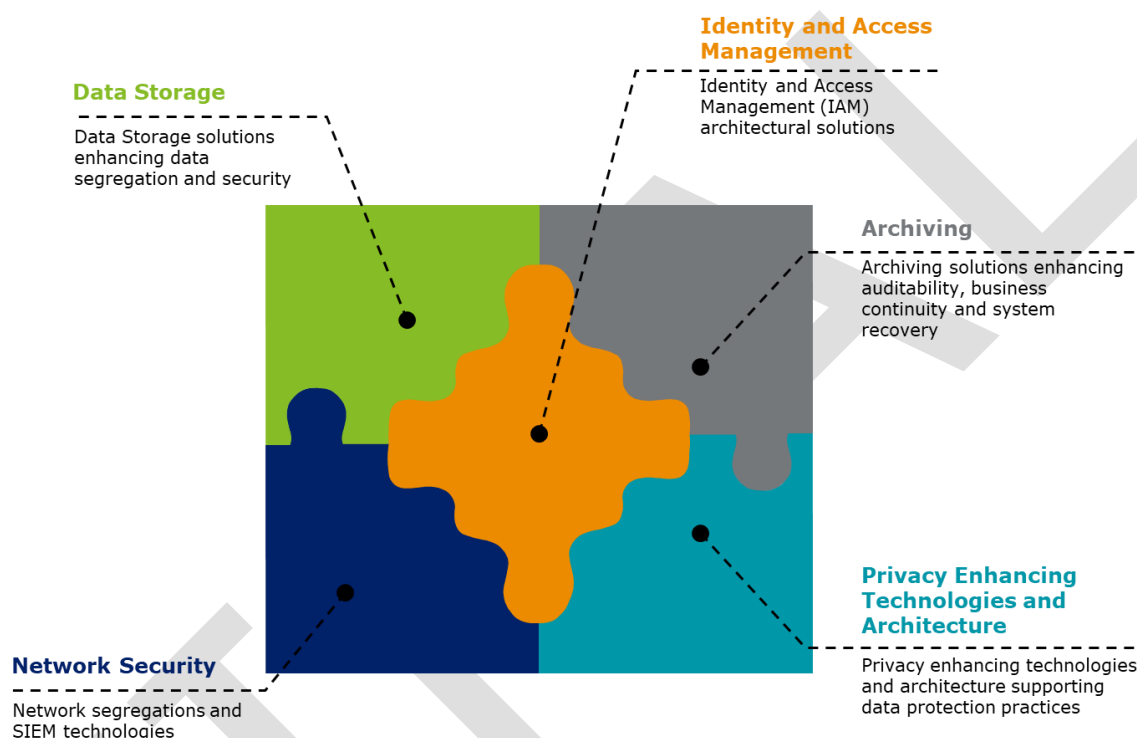
The security study requested includes only the Central and National SSN. It is important to highlight as a conclusion that this security study needs to be supplemented with the additional elements related to the new systems interlinked with SSN (e.g. Thetis, CSN, IMS, SAT-AIS etc). Furthermore this new study needs to include the entire information chain from the declarant (or the data provider) up to the end users (including all the Authorities defined by the EMSWe regulation as depicted in the figure below .



# 7 Assessment of technical options for SSN

## 7.1 Overview

Taking into account the results of D1-10-1 Interim Report for Task 1 and D2-5-1 Interim Report for Task 2, this section provides different architectural options for SSN. These architectural options take into account the results and analyses (in particular the identified security, data protection and interoperability gaps) of the Central SSN system and its evolution due to Regulation 2019/1239 (EMSWe) and Directive 2017/2109 (on the registration of persons on board passenger ships). Figure 3 shows the selected architectural areas (i.e. Identity and Access Management, Data Storage, Archiving, Privacy Enhancing Technologies and Architecture, and Network Security) for which technical options are described.



**Figure 3 Architectural areas**

The remainder of this section describes the identified technical options for these architectural areas and provide an assessment according to the security, data protection and interoperability criteria for SSN.

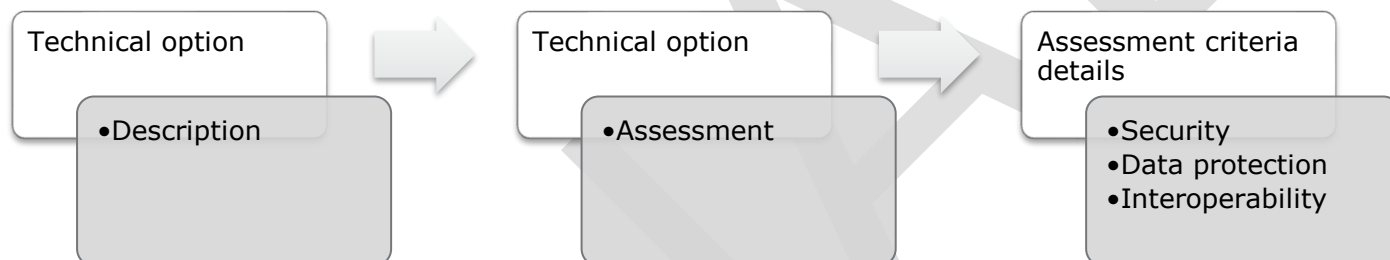
This section contains an overview of the following identified technical options for SSN:

Architectural areas	Technical options
<b>Identity and Access Management</b>	<ul style="list-style-type: none"> <li>✓ <b>IAM_1:</b> Delegated identity (relying on centralised identification).</li> <li>✓ <b>IAM_2:</b> Delegated authentication (relying on local authorisation).</li> <li>✓ <b>IAM_3:</b> Federated IAM adopting third-party authentication.</li> <li>✓ <b>IAM_4:</b> Federated IAM adopting eID complying with eIDAS.</li> </ul>
<b>Data Storage</b>	<ul style="list-style-type: none"> <li>✓ <b>DS_1:</b> Logically separated databases, relying on shared data storage infrastructures.</li> <li>✓ <b>DS_2:</b> Physically separated databases, relying on different data storage infrastructures.</li> <li>✓ <b>DS_3:</b> Virtually distributed databases, relying on infrastructures as a service such as private cloud.</li> </ul>
<b>Archiving</b>	<ul style="list-style-type: none"> <li>✓ <b>Archive_1:</b> Data storage solutions tailored for archiving purposes.</li> <li>✓ <b>Archive_2:</b> Dedicated eArchiving building block</li> </ul>






Architectural areas	Technical options
<b>Privacy Enhancing Technologies and Architecture</b>	<ul style="list-style-type: none"> <li>✓ <b>PETA_1:</b> Implementation of a Privacy Information Management System (PIMS) in alignment with ISO/IEC 27701:2019 (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines).</li> <li>✓ <b>PETA_2:</b> Implementation of PETs in order to support privacy controls and data protection principles.</li> <li>✓ <b>PETA_3:</b> Compliance with the Privacy Architecture framework in alignment with the ISO/IEC 29101:2018 (Information technology — Security techniques — Privacy architecture framework).</li> </ul>
<b>Network Security</b>	<ul style="list-style-type: none"> <li>✓ <b>NS_1:</b> Physical network segmentation creating distinct security domains for the Central SSN system and other critical digital assets, including the EMSWe.</li> <li>✓ <b>NS_2:</b> Logical network segmentation adopting Software Define Networking (SDN) and Network Function Virtualisation (NFV) creating security domains for the Central SSN system and other critical digital assets, including the EMSWe.</li> </ul>




For each identified technical option, the following sections of this document include:



Moreover, we include below an overview of the manner the identified technical options for SSN are linked to, and therefore may be addressing the identified **gaps** and **attention points** with regards to the SSN organisational and technical measures related to security, data protection and interoperability. The following gaps and attention points have been identified as part of the Task 2 of this study (see separate report on this topic):

Security gaps and attention points	Architecture considerations
<p> <b>1</b> <b>Gap Security</b></p> <p>According to Article 9 of the Commission Decision 2017/46, the system owner has the obligation to prepare an IT Security Plan, "including were appropriate details of the assessed risks and any additional measure required".</p>	<p>This gap is concerned with a policy obligation, which is addressed by developing an IT Security Plan, including were appropriate details of the assessed risks and any additional measure required, according to Article 9 of the Commission Decision 2017/46. A specific action is included in the roadmap for implementation of SSN security, data protection and interoperability measures.</p>
<p> <b>2</b> <b>Gap Security</b></p> <p>EIS does not have its own controls for authorization of users but does do authorization. It uses the user id to do the authorization based on the roles assigned to that user by IdM. This implies that each request reaching SSN is handled as a legitimate one. SSN does not have own controls on the identification, authentication, and authorization of users when this is delegated to MSs (i.e. implemented in the National SSN systems). An end-to-end identity and user access management control will become critical with the future developments of SSN network.</p>	<p><b>IAM_1, IAM_2, IAM_3, and IAM_4</b> provide alternative technical options addressing this security gap. <b>IAM_1</b> and <b>IAM_2</b> support a centralised approach whereas <b>IAM_3</b> and <b>IAM_4</b> support a federated approach. The IAM solutions need to be integrated with the other architectural options for Data Storage, Archiving, Privacy Enhancing Technologies and Architecture, and Network Security.</p>
<p> <b>3</b> <b>Gap Security</b></p> <p>SSN security policies should be revised in order to take into account operational needs (e.g. business continuity, incident management, data archiving) in compliance with relevant legislation, i.e. Commission Decision 2017/46, EU DPR, and Regulation 2019/1239. This is particularly relevant for security policies which concerns to SSN archiving practices of operational records,</p>	<p><b>Archive_1, Archive_2</b> provide alternative options addressing this security gap. Commercial solutions (<b>Archive_1</b>) as well as eArchiving (<b>Archive_2</b>) may provide suitable options for implementing digital archiving strategies in the context of SSN.</p>

e.g. records, logs, and incidents reports that may contain personal data or commercial data.

Interoperability protection gaps and attention points		Architecture considerations
 <b>1 Gap Interoperability</b>	Points of attention/gaps were identified with regard the applicable relevant network and information security standards. See Section 7.3 Outcome of the security impact assessment.	This gap will be assessed by the implementation of the Information Security Management System (ISMS) for SSN. This is addressed by a specific action of the roadman for implementation of SSN security, data protection and interoperability measures.
 <b>2 Gap Interoperability</b>	Without a coherent involvement from key SSN stakeholders on security-related aspects of the system, there is a negative impact of alignment of SSN security baselines between EMSA and the MSs, and also on the adequacy of deploying key security controls, with a direct impact on confidentiality and integrity of data. Even though SSN is governed by several groups (HLSG, SSN Group), to date there is no dedicated/specialised workgroup of SSN stakeholders focused on security and data protection aspects (governance, operational, technical). Current SSN groups are covering some interoperability aspects.	This gap is concerned with the establishment of Security and Interoperability working group involving EMSA operating the Central SSN and the Member States operating the National SSN systems. This dedicated working group will be responsible for harmonising and deciding security and interoperability solutions for the SSN systems.
 <b>1 Attention Point Interoperability</b>	EMSA should develop Guidelines and Recommendations with a view to establishing consistent, efficient, and effective assessments of interoperability arrangements for SSN with the involved actors from the Member States. At this stage, EMSA has different guidelines supporting interoperability (e.g. Interface Guide, HAZMAT Guidelines, etc.). These guidelines need to be revised together with the future developments of SSN. Task 3 Report will identify guidelines for interoperability. These guidelines and recommendations should not introduce new requirements for SSN in addition to the relevant technical standards. However, they specify how those requirements should be met for the purpose of establishing robust and stable interoperability arrangements with the Member States.	This attention point can be addressed by the establishment of Security and Interoperability working group involving EMSA operating the Central SSN and the Member States operating the National SSN systems. This dedicated working group will be responsible for harmonising and deciding security and interoperability solutions for the SSN systems.
Data protection gaps and attention points		Architecture considerations
 <b>1 Attention Point Data Protection</b>	EMSA should conduct a DPIA with consultation with the EDPS prior to the start of the upgraded SSN.	This attention point is concerned with a data protection obligation, which will be addressed by a specific action in the implementation of the Information Security Management System (ISMS) for SSN.
 <b>2 Attention Point Data Protection</b>	Both EMSA and Member States operate as data controller of their respective SSN systems, so they are co-controllers for the SSN data cycle. Taking into account that the Central SSN system is receiving data collected by the National SSN systems, it would be necessary to clarify for what data EMSA is operating as data controller. Therefore, a clear data protection statement with the attribution of roles will be part of the upgraded SSN documentation. This statement will also include the minimum requirements in terms of data protection. In order to support awareness across SSN stakeholders is advisable to host a workshop on data protection topics for SSN.	<b>PETA_1</b> , <b>PETA_2</b> and <b>PETA_3</b> provide alternative options addressing data protection for the SSN. <b>PETA_1</b> consists of a full Implementation of a Privacy Information Management System (PIMS). This will extend the ISMS for SSN with aspects of data protection and privacy. <b>PETA_2</b> involves the implementation of different PETs concerned with different aspects of data protection. This represents an incremental option. <b>PETA_3</b> is concerned with compliance with privacy architecture standard in order to align security and data protection controls with the SSN architecture.



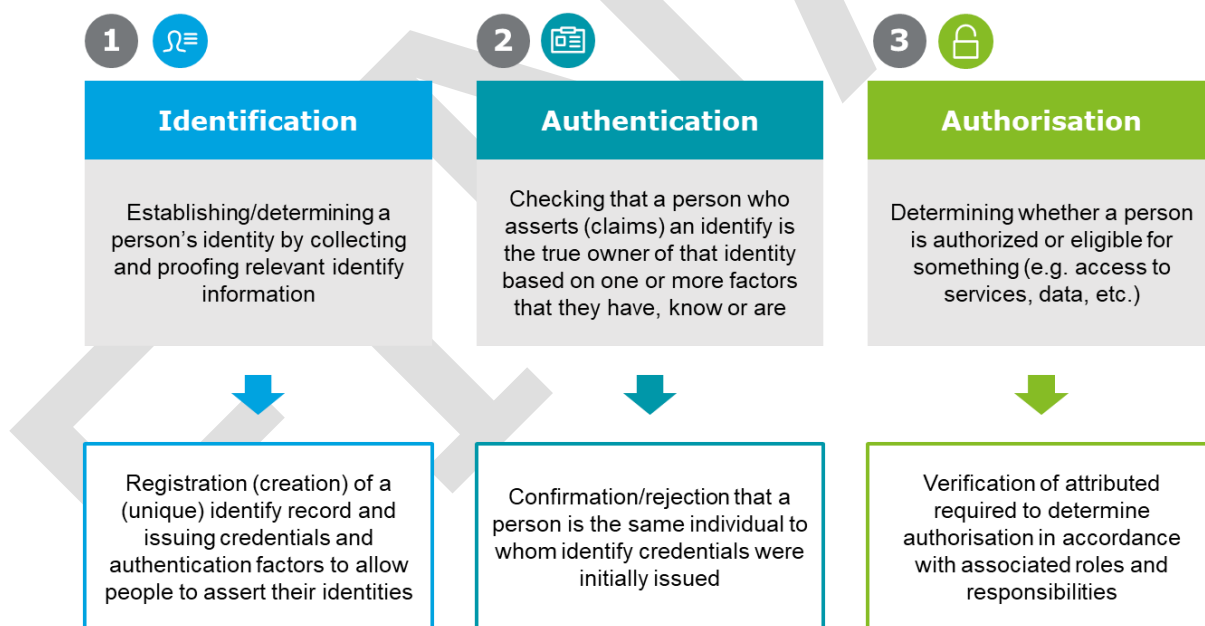
## 7.2 Identity and Access Management - description and assessment of suitability in the SSN context

This section provides a description of the technical options identified and proposed for SSN. The technical options take into account the identified gaps and also the results of the assessment of the CEF Building Blocks. The evaluation of the technical options takes into account the same security, data protection and interoperability criteria.

### 7.2.1 Identity and Access Management – description of the technical options

Identity and Access Management (IAM) is a critical architectural area, which can address security aspects of systems, networks and data. Currently, there is limited control over the full cycle of identification and authorisation for the Central SSN system, in particular regarding authorised accesses of operators of National SSN systems. EMSA is using an OIM solution (Oracle) and is conducting an analysis process to determine if it will be renewed or decommissioned in order to adopt OAuth2.0 and OpenID (most likely) or other technology / solutions. Hence, it is possible to implement alternative IAM options, which can be combined for redesigning the access and authorisation of the Central SSN system. This is relevant for the interactions between the Central SSN system and the National SSN systems as well as the interactions between the maritime data providers (e.g. Coastal Station, Port State Control, NMSW Declarants, etc.) and the new European Maritime Single Window environment (EMSWe).

In order to define alternative options for IAM solutions, this section takes also into account good practices drawn from other sectors (e.g. banking<sup>8</sup>) having stringent IAM requirements. IAM solutions enable the collection and validation of identity attributes in order to establish a person's identity and provide proof of that identity in the form of credentials (e.g. unique ID number, card, certificate, mobile ID, etc.). These credentials can be used by the person through some method of authentication to assert or prove their identity to third parties (e.g. government agencies, employers, etc.), who require assurance of who they are in order to access specific services and data with defined credentials and authorisations. Figure 4 provides a schematic representation of the basic functional elements (i.e. Identification, Authentication and Authorisation) of IAM solutions.



**Figure 4 Basic functional elements of IAM solutions (technical options)**

This section presents four alternative IAM solutions (technical options):

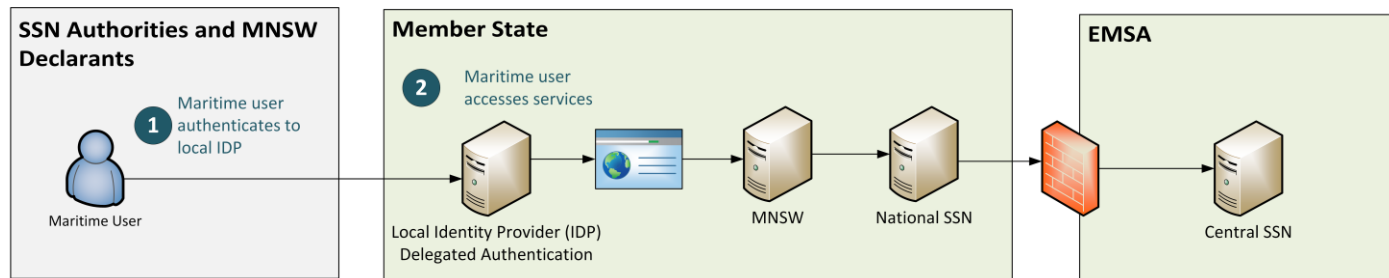
- ✓ **IAM\_1:** Delegated authentication (relying on local authorisation) – current SSN solution.
- ✓ **IAM\_2:** Delegated identity (relying on centralised identification).
- ✓ **IAM\_3:** Federated IAM adopting third-party authentication.
- ✓ **IAM\_4:** Federated IAM adopting eID complying with eIDAS.

<sup>8</sup> World Bank Group, Identification for Development (ID4D), Practitioner's Guide, Version 1.0, October 2019.

### **IAM 1: Delegated authentication (relying on local authorisation)**

The SSN systems (Central SSN as well as National SSN systems) currently implements the delegated authentication solution.

Figure 5 shows the Delegated Authentication for the Central SSN system relying on local authorisation. This is the current solution that the Central SSN implements. The Central SSN system does not have access to the local identity and authorisation system. The Central SSN system has its own identity and authorisation system and the administrator of the Central SSN system has to authorise any access to the Central SSN and any associated services.

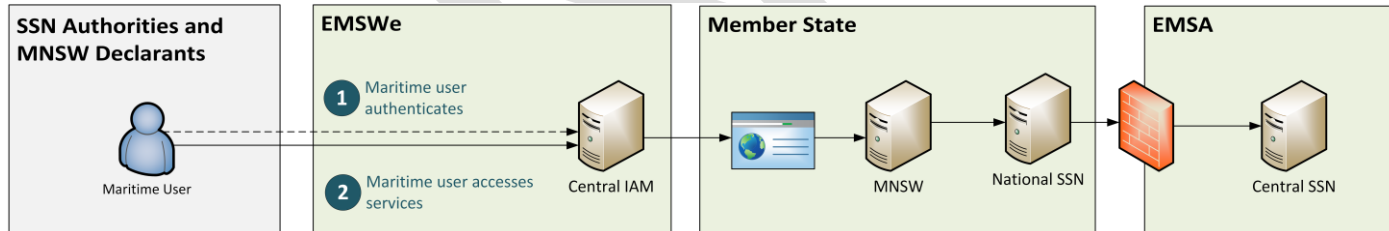


**Figure 5: IAM\_1 - Delegated Authentication for Central SSN**

This scenario is not fully in line with the EMSWe Regulation, which requires a centralised user registry and access management system. It rather depicts the current implementation of SSN in the case of access through the National SSN System.

### **IAM 2: Delegated identity (relying on centralised identification)**

Figure 6 shows a Delegated Identity solution for the Central SSN system relying on centralised identification. This solution relies on a centralised IAM logic (the EMSWe user registry and access management system, as required by Article 12 of the EMSWe Regulation), which requires maritime users (SSN Authorities and MNSW declarants) to register and authenticate with the EMSWe in order to access the MNSW. Note that the Central SSN System has its own identity and authorisation system and the administrator of the Central SSN system has to authorise any access to the Central SSN and any associated services.



**Figure 6: IAM\_2 - Delegated Identity for Central SSN**

### **IAM 3: Federated IAM adopting third-party authentication**

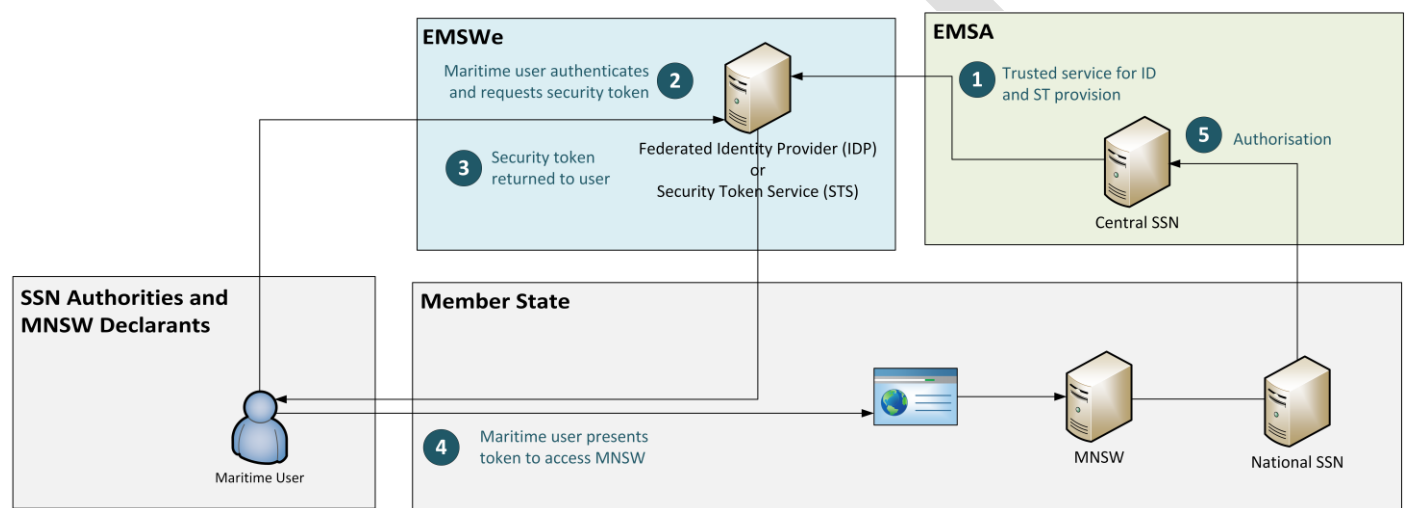
Federation is the ability of an organisation to accept another organisation's identity credentials for authentication based on inter-organisational trust. The trusting organisation (EMSA) must be comfortable that the other identity provider has acceptable relevant policies, and that those policies are being applied. Federation protocols and assurance and trust frameworks facilitate federation of digital identity between organisations. For federation to be effectively used across organisations, standards and defined assurance levels must be defined. Federation can occur at multiple levels:

- ✓ A trusting organisation can capture and send the credential to the issuing organisation (i.e. an identity provider) for verification, to authenticate an identity – after verification of the credential, the issuing organisation sends a yes/no confirmation and may, when warranted and consented, send a set of claims giving information about the person, using federation protocols like SAML (security assertion mark-up language).
- ✓ A trusting organisation can accept credentials issued by another organisation, but still authenticate and authorise the individual locally.
- ✓ A trusting organisation can accept specific attributes describing an individual from another organisation.
- ✓ A trusting organisation can accept an authorisation decision from another organisation (i.e. mutual recognition).

Note that a federated solution for IAM is in alignment with the EMSWe Regulation 2019/1239, which defines the requirements for the EMSWe user registry and access management system (Article 12): "The Commission shall establish and ensure the availability of a common user registry and access management system for declarants and data service providers that use the maritime National Single Window, as well as for national authorities that access the maritime National Single Window in cases where authentication is required. That common user registry and

access management system shall provide for a single user registration by means of an existing Union registry with Union level recognition, federated user management and Union level user monitoring.”

Figure 7 provides a schematic view of a Federated IAM solution for the Central SSN system, which relies on a third-party Federated Identity Provider<sup>9</sup> (IDP) or Security Token Service<sup>10</sup> (STS), which corresponds to the EMSWe user registry and access management system. The Federated IAM will support the authentication. However, the authorisation will still be done locally. In order to align authorisations between the Central and the National SSN systems, it is necessary to agree on a common authorisation framework associated with specific SSN roles. Maritime Users (SSN Authorities and NMSW Declarants) have to identify and obtain a token in order to access the specific services of the Central SSN system via the NMSW. Note that such IAM solutions often support strong identification mechanisms such as two-factor authentication services. In this context the EU Login services of the European Commission may be considered as a federated identity provider. This solution will imply a centralisation of IAM services by the European Commission and the integration of EU Login services with the Central SSN and National SSN systems. Taking into account the complexity of the SSN ecosystem, it has to be considered whether or not this alternative solution is feasible operationally.



**Figure 7: IAM\_3 - Federated IAM adopting third party authentication**

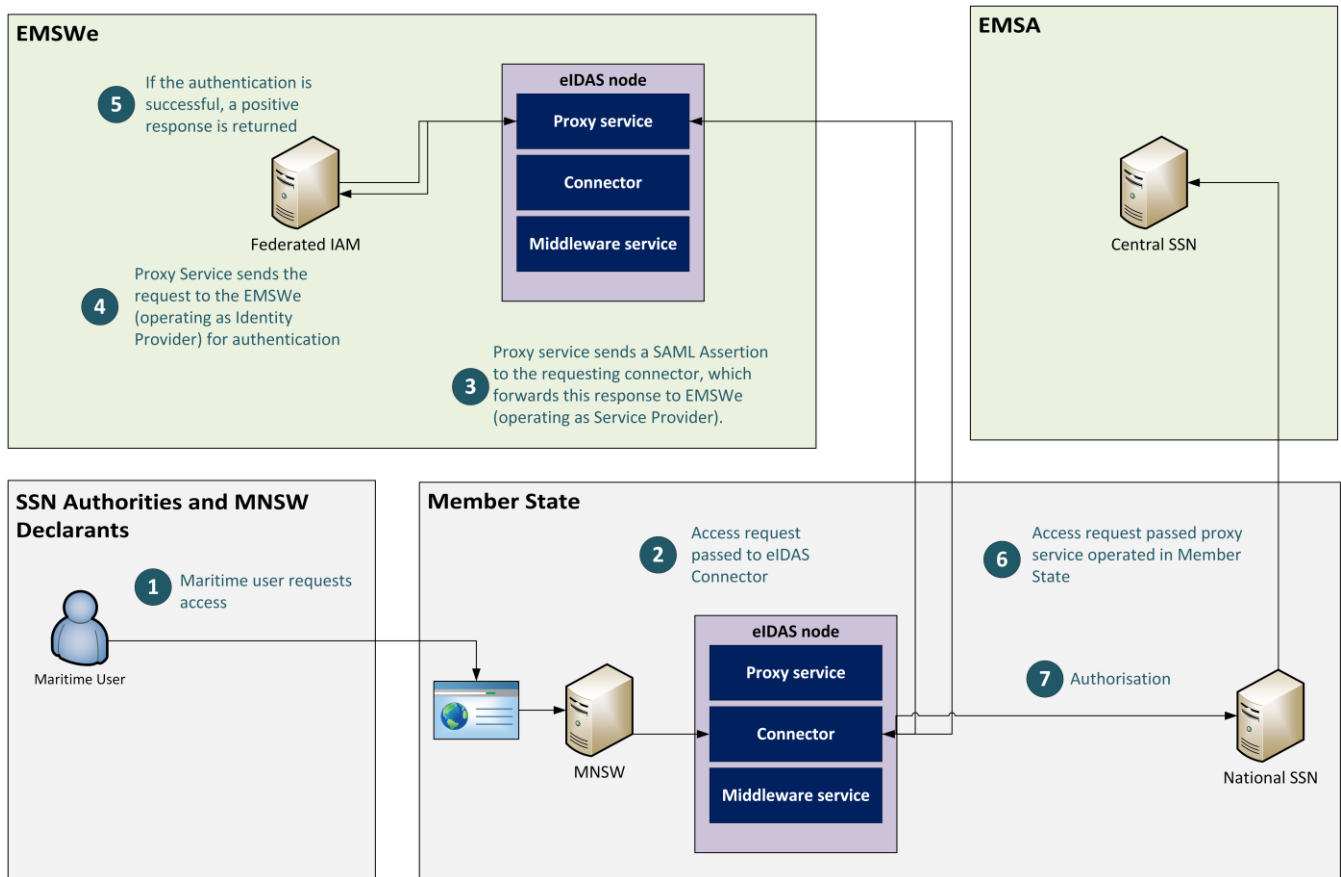
#### **IAM 4: Federated IAM adopting eID complying with eIDAS**

These IAM solutions may also integrate and rely on the eID CEF Building Block, in particular, in order to support the identification and authentication of maritime users. The CEF eID Building Block consists of European Commission services provided by the European Commission and endorsed by the Member States. Such services support public administrations and private service providers for extending the use of their online services to citizens from other Member States. This is realised through the mutual recognition of national electronic identification (eID) schemes (e.g. including smartcards, mobile and log-in), allowing citizens of one European country to use their national eIDs to securely access online services provided in other European countries. The mutual recognition of eID schemes across Europe is mandated by the eIDAS Regulation.

<sup>9</sup> Identity provider: An entity (e.g. a government agency or private firm) that issues and manages identities, credentials, and authentication processes throughout the identity lifecycle. The terms Identity Provider (IdP), Identity Service Provider, and Digital Identity Service Provider are often used somewhat synonymously and are often broken down into more specific roles (e.g. registration authority, credential service provider, attribute provider, verifier, etc.) depending on the architecture of the ID system and the various entities and roles involved.

<sup>10</sup> Security Token Service: A security token service (STS) is a Web service that issues security tokens (WS-Security). That is, it makes assertions based on evidence that it trusts, to whoever trusts it (or to specific recipients). To communicate trust, a service requires proof, such as a signature to prove knowledge of a security token or set of security tokens. A service itself can generate tokens or it can rely on a separate STS to issue a security token with its own trust statement. This forms the basis of trust brokering.

Figure 8 shows an example of a federated IAM adopting eIDAS.



**Figure 8: IAM\_4 - Federated IAM adopting eIDAS**

The identified IAM solutions require technical standards. Importantly, the type of attributes (e.g. biometrics, biographic, etc.) captured during identification and the methodologies used to record them have important implications for the assurance and trust for the authentication and authorisation in the IAM system as well as its utility and interoperability with other national and international IAM systems. Relevant standards supporting interoperability for federation protocols are:

- ✓ **SAML v2—2005 (OASIS):** Security Assertion Markup Language (SAML) defines an XML based framework for communicating security and identity (e.g. authentication, entitlements, and attribute) information between computing entities. SAML promotes interoperability between disparate security systems, providing the framework for secure transactions across organisational boundaries.
- ✓ **RFC 6749/ OAuth 2 (IETF):** OAuth 2.0 is the industry-standard protocol for authorisation providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices.
- ✓ **Open ID connect (The OpenID Foundation):** OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and Web Services-like manner.

Federation protocols such as Open ID connect and OAuth combination are being increasingly used for federation while SAML has been used extensively earlier. SAML was designed only for Web-based applications whereas OpenID Connect was designed to also support native apps and mobile applications in addition to Web applications. OpenID connect is newer and built on the OAuth 2.0 process flow. It is tried and tested and typically used in consumer websites, web apps and mobile apps. Mobile connect and Microsoft's Identity management solutions use these protocols. SAML is its older cousin, and typically used in enterprise settings (e.g. allowing single sign on to multiple applications within an enterprise using our Active Directory login). The eIDAS framework is based on SAML. Open ID connect is gaining popularity for new implementations as it can support both native apps and mobile apps in addition to web-based applications. OpenID has been also extended in order to provide identity assurance complying with the eIDAS framework. Recent research provides an overview of the technical specifications of eID services<sup>11</sup>.

<sup>11</sup> FutureTrust (2017): Overview of eID Services, D2.2, V2.0.

Recently, federated IAM has been adopted for other systems of the European Commission. For example, The European Commission and EU Member States have designed a new Customs Decisions System (CDS) based on an IT architecture containing both national and EU common components. The Central CDS is to be used for all applications and decisions which may have an impact in more than one Member State, and for any subsequent event which may affect the original application or decision (annulment, suspension, revocation, amendment). The CDS supports economic operators wishing to submit an application. When submitting an application, economic operators have to connect to the EU Trader Portal, a single electronic access point deployed at EU level for accessing the CDS. The Uniform User Management & Digital Signature (UUM&DS) project<sup>12</sup> specifies the federated authentication solutions for the EU Trader Portal.

Note that the Federated IAM implemented for the EU Trader Portal does not adopt the eID building block. It implements an ad-hoc solution for the specific system. The UUM&DS specification describes the processes of the implemented Federated IAM solution.

## 7.2.2 Identity and Access Management – assessment of the technical options

This section assesses the IAM options according to the security, data protection and interoperability criteria for SSN.

### 7.2.2.1 Security assessment

Table 30 provides a high-level security assessment of IAM options for SSN.

**Table 30 Security assessment of IAM options for SSN**

Domain	Criterion ID	Criterion	IAM_1 Assessment	IAM_2 Assessment	IAM_3 Assessment	IAM_4 Assessment
Security	SEC-01	Security Domains	Medium 	Medium 	High 	High 
	SEC-02	Data Security	Medium 	Medium 	High 	High 
	SEC-03	Security Functions	Medium 	Medium 	High 	High 
	SEC-04	Complexity and Coupling of Security Functions	High 	High 	Medium 	Medium 
	SEC-05	Operational Security	Medium 	Medium 	High 	High 
	SEC-06	Architectural Exposure to Threats	Medium 	Medium 	High 	High 
	SEC-07	Security Maintainability and Evolvability	High 	High 	Medium 	Medium 
	SEC-08	Security Compliance	Medium 	Medium 	High 	High 

### 7.2.2.2 Data protection assessment

Table 31 provides a high-level data protection assessment of IAM options for SSN.

**Table 31 Data protection assessment of IAM options for SSN**

























Domain	Criterion ID	Criterion	IAM_1 Assessment	IAM_2 Assessment	IAM_3 Assessment	IAM_4 Assessment
Data Protection	DP-01	Data Protection Compliance	Medium 	Medium 	High 	High 
	DP-02	Privacy Architecture	Medium 	Medium 	High 	High 
	DP-03	Privacy by design and by default	Medium 	Medium 	High 	High 
	DP-04	Operational Data Protection	Medium 	Medium 	High 	High 

### 7.2.2.3 Interoperability assessment

Table 32 provides a high-level data protection assessment of IAM options for SSN.

<sup>12</sup> European Commission — DG TAXUD and DG DIGIT: Access Management through UUM&DS, Your passport to EU Applications, V0.20.

**Table 32 Interoperability assessment of IAM options for SSN**

Domain	Criterion ID	Criterion	IAM_1 Assessment	IAM_2 Assessment	IAM_3 Assessment	IAM_4 Assessment
Interoperability	<b>INT-01</b>	Interoperability Compliance	Medium 	Medium 	High 	High 
	<b>INT-02</b>	Integration and interconnectivity	Medium 	Medium 	High 	High 
	<b>INT-03</b>	Functional Maintainability and Evolvability	Medium 	Medium 	High 	High 
	<b>INT-04</b>	Elasticity and Scalability	Medium 	Medium 	High 	High 
	<b>INT-05</b>	Technology readiness	High 	High 	High 	Medium 
	<b>INT-06</b>	Legacy and Migration	High 	High 	Medium 	Medium 

### 7.2.3 Identity and Access Management – conclusion on technical options assessment

The Regulation 2019/1239 (EMSWe) identifies the requirements for a federated IAM solution, which will have an impact on the Central SSN System and the National SSN systems. The eID building block provides mechanisms for implementing identification mechanisms across Member States. The eID building block is suitable for public administrations that intend to support recognised and approved identity mechanisms from other public organisations (also located in other Member States). However, since SSN involves users of registered authorities (rather than citizens) and data exchanges between the Central SSN and the National SSN systems, the eID provides limited support for such operational needs. Furthermore, the adoption of eID for a federated IAM solution would require substantial effort increasing the risk of operational disruptions (e.g. due to lack of harmonisation across the SSN systems). Hence, the most suitable solution is IAM\_3 a federated IAM solution adopting third-party or an ad-hoc solution implemented for the SSN context.



## 7.3 Data Storage - description and assessment of suitability in the SSN context

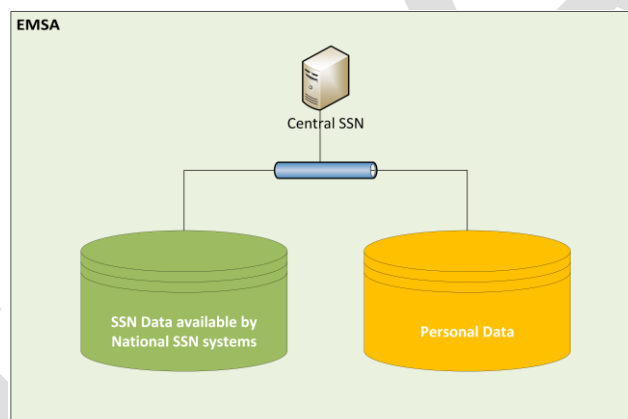
This section provides a description of the technical options identified and proposed for SSN. The technical options take into account the identified gaps and also the results of the assessment of the CEF Building Blocks. The evaluation of the technical options takes into account the same security, data protection and interoperability criteria.

### 7.3.1 Data Storage – description of the technical options

Data are critical assets of SSN, their security is critical. In order to minimise the risks affecting data security (including, confidentiality, integrity and availability), data storage has a fundamental role. This section discusses and presents three alternative Data Storage solutions:

- ✓ **DS\_1:** Logically separated databases, relying on shared data storage infrastructures.
- ✓ **DS\_2:** Physically separated databases, relying on different data storage infrastructures.
- ✓ **DS\_3:** Virtually distributed databases, relying on infrastructures as a service such as private cloud.

The overall objective is to separate data in order to take into account their sensitivity (e.g. commercial sensitive data and personal data). This will allow implanting role-based access control measures taking also into account data sensitivity. Figure 9 shows a representation of data storage involving segregated databases. As illustrative example, the figure shows the data processes by the Central SSN as identified in the Task 1 report. However, the exact dataset may involve other types of data due to the implementation of Regulation 2019/1239 (EMSWe) identifies (e.g. Ship Database, Common Location Database, etc.).



**Figure 9 Data storage involving segregated databases**

Note that virtualised distributed databases support also logically and physically separated solutions. However, it may involve the adoption of cloud Infrastructure as a Service (IaaS) with private cloud deployments. This may further support data duplication in order to enhance business continuity as well as disaster recovery. Note that EMSA shall also consider business continuity and disaster recovery in order to assess alternative deployments of the different Data Storage options. Table 33 compares alternative deployment models for data storage.

**Table 33 Alternative deployment models for data storage**

Deployment Option	capital (CAPEX) and operating (OPEX) expense	Required expertise	Control over infrastructure	Elasticity & flexibility	Network & connectivity	Data location
<b>Dedicated, agency-owned data centre</b>	CAPEX: Most expensive, including cost of equipment and datacentre facility OPEX: Most expensive, including cost of equipment, datacentre facility, and staff	Datacentre, network, physical security, server/system administration, application/database administration, cybersecurity	Full control over data and all components of the infrastructure	No elasticity, least flexibility in provided services	Good network connectivity required (and good broadband connectivity required for data sharing)	On premises
<b>Shared datacentre – collocation (government and private)</b>	CAPEX: equipment collocation OPEX: collocation costs and own equipment	Server/system administration, application/database administration, cybersecurity	Control over data and collocated equipment	No elasticity, least flexibility in provided services	Good broadband connectivity required	In country

Deployment Option	capital (CAPEX) and operating (OPEX) expense	Required expertise	Control over infrastructure	Elasticity & flexibility	Network & connectivity	Data location
<b>Shared datacentre – managed hosting (government and private)</b>	CAPEX: infrastructure And equipment are typically born by the datacentre provider but it can vary by provider OPEX: managed services	Application/database administration	Limited, as provided by the contract	Limited, as provided by the contract	Good broadband connectivity required	Typically in country
<b>Government cloud</b>	CAPEX: None, costs are born by cloud operator OPEX: resource usage (pay per use model)	Application/database administration	Control over data and own applications	Elastic. Some flexibility in service availability	Good broadband connectivity required	In country
<b>Private-sector operated public cloud</b>	CAPEX: None, costs are born by cloud operator OPEX: resource usage (pay per use model)	Application/DB administration	Control over data and own applications	Elastic. Flexible service availability	Low latency required for business critical systems	Anywhere the provider is operation datacentres
<b>Hybrid cloud</b>	CAPEX: None, costs are born by cloud operator OPEX: resource usage (pay per use model)	Application/database administration	Control over data and own apps	Elastic. Most flexibility in service availability	Good broadband connectivity required	Sensitive data stored in country; other data stored in private provider datacentres with a global scale/footprint

Besides the different architectural options and their alternative deployment models, it is convenient to implement a Data Access Component, which isolates the complexity of data access, enables additional data consistency, and ensures adjustability of handled data to meet the requirements of different users. The role of a Data Access Component is to handle the complexity of accessing data (e.g. handling additional authorisation mechanisms by enforcing role-based access controls, querying for data, etc.). Such component may also support the integration of multiple views combining different data sources in order to provide a unified access to different data storages (without storing them for data security). This also allows dealing with data stored at different data locations (including stored by different cloud providers). A Data Access Component introduces an additional layer of separation (virtualisation) for the Central SSN in order to support alternative data storage strategies.
















### 7.3.2 Data Storage – assessment of the technical options

This section assesses the Data Storage options according to the security, data protection and interoperability criteria for SSN.










#### 7.3.2.1 Security assessment

Table 34 provides a high-level security assessment of Data Storage options for SSN. Note that Data Storage assessment needs also to take into account alternative deployment options, which may have as described different cost and readiness implications.

**Table 34 Security assessment of Data Storage options for SSN**

Domain	Criterion ID	Criterion	DS_1 Assessment	DS_2 Assessment	DS_3 Assessment
Security	<b>SEC-01</b>	Security Domains	Medium 	High 	High 
	<b>SEC-02</b>	Data Security	Medium 	High 	High 
	<b>SEC-03</b>	Security Functions	Medium 	Medium 	High 
	<b>SEC-04</b>	Complexity and Coupling of Security Functions	High 	High 	Medium 
	<b>SEC-05</b>	Operational Security	Medium 	Medium 	High 















Domain	Criterion ID	Criterion	DS_1 Assessment	DS_2 Assessment	DS_3 Assessment
	<b>SEC-06</b>	Architectural Exposure to Threats	Medium 	Medium 	High 
	<b>SEC-07</b>	Security Maintainability and Evolvability	High 	High 	Medium 
	<b>SEC-08</b>	Security Compliance	Medium 	High 	High 

### 7.3.2.2 Data protection assessment

Table 35 provides a high-level data protection assessment of Data Storage options for SSN. Note that Data Storage assessment needs also to take into account alternative deployment options, which may have as described different cost and readiness implications.

The assessment shall also consider the deployment models of the storage solutions. This is particularly true in the case of a third party providing cloud-based storage, where the stakeholders may not have enough control of how/where data is stored. A detailed assessment shall be conducted by EMSA when selecting the preferred solution, during the procurement procedure.



















**Table 35 Data protection assessment of Data Storage options for SSN**

Domain	Criterion ID	Criterion	DS_1 Assessment	DS_2 Assessment	DS_3 Assessment
Data Protection	<b>DP-01</b>	Data Protection Compliance	Medium 	High 	High 
	<b>DP-02</b>	Privacy Architecture	Medium 	Medium 	High 
	<b>DP-03</b>	Privacy by design and by default	Medium 	Medium 	High 
	<b>DP-04</b>	Operational Data Protection	Medium 	High 	High 

### 7.3.2.3 Interoperability assessment

Table 36 provides a high-level interoperability assessment of Data Storage options for SSN. Note that Data Storage assessment needs also to take into account alternative deployment options, which may have as described different cost and readiness implications.

**Table 36 Interoperability assessment of Data Storage options for SSN**

Domain	Criterion ID	Criterion	DS_1 Assessment	DS_2 Assessment	DS_3 Assessment
Interoperability	<b>INT-01</b>	Interoperability Compliance	High 	High 	High 
	<b>INT-02</b>	Integration and interconnectivity	High 	Medium 	High 
	<b>INT-03</b>	Functional Maintainability and Evolvability	High 	Medium 	High 
	<b>INT-04</b>	Elasticity and Scalability	Medium 	Medium 	High 
	<b>INT-05</b>	Technology readiness	High 	High 	High 
	<b>INT-06</b>	Legacy and Migration	High 	Medium 	Medium 

## 7.3.3 Data Storage – conclusion on technical options assessment

Taking into account the above assessments, DS\_1 (Logically separated databases, relying on shared data storage infrastructures.) provides a flexible solution, which would allow configuring data storage according to required logical separation with limited costs. DS\_2 (that is, physically separated databases relying on different data storage infrastructures) identifies an incremental solution, which provides suitable security, data protection and interoperability for the SSN context. DS\_3 (that is, virtually distributed databases relying on infrastructures as a service such as private cloud) identifies a solution, which provides suitable security, data protection and interoperability for the SSN context. However, this solution may require a substantial effort and investment. The most suitable deployment model would be a private cloud infrastructure in a dedicated agency-owned data centre.

## 7.4 Archiving - description and assessment of suitability in the SSN context

This section provides a description of the technical options identified and proposed for SSN. The technical options take into account the identified gaps and also the results of the assessment of the CEF Building Blocks. The evaluation of the technical options takes into account the same security, data protection and interoperability criteria.

### 7.4.1 Archiving – description of the technical options

The archiving of data intends to support audit as well as business continuity and disaster recovery. Archiving solutions may adopt similar solutions such as data storage. However, the overall objective of archiving is different than data storage. Note that archiving solutions may include the adoption of the eArchiving CEF Building Block, which provides Information Package specifications which describe a common format for storing bulk data and metadata in a platform-independent, authentic and long-term understandable way. The eArchiving CEF Building Block is a specific instance of the reference model<sup>13</sup> for an Open Archival Information System (OAIS). Therefore, for archiving is mainly necessary to distinguish between to alternative options, archiving solutions adopting data storage solutions tailored for archiving purposes or adopting a dedicated solution such as the eArchiving building block:

- ✓ **Archive\_1:** Data storage solutions tailored for archiving purposes.
- ✓ **Archive\_2:** Dedicated eArchiving CEF building block.

















### 7.4.2 Archiving – assessment of the technical options

The assessment of archiving options would consider whether to implement archiving solutions similar to the ones proposed for data storage or whether to adopt the eArchiving CEF Building Block, for which previous sections provide assessments according to the security, data protection and interoperability criteria for SSN. This section assesses the Archiving options according to the security, data protection and interoperability criteria for SSN.

#### 7.4.2.1 Security assessment

Table 37 provides a high-level security assessment of Archiving options for SSN. Note that Archiving assessment may depend also on alternative deployment options (like for Data Storage), which may have different cost and readiness implications.

**Table 37 Security assessment of Archiving options for SSN**









Domain	Criterion ID	Criterion	Archive_1 Assessment	Archive_2 Assessment
Security	SEC-01	Security Domains	Medium 	High 
	SEC-02	Data Security	High 	High 
	SEC-03	Security Functions	Medium 	High 
	SEC-04	Complexity and Coupling of Security Functions	Medium 	High 
	SEC-05	Operational Security	Medium 	Medium 
	SEC-06	Architectural Exposure to Threats	Medium 	Medium 
	SEC-07	Security Maintainability and Evolvability	Medium 	High 
	SEC-08	Security Compliance	Medium 	High 

#### 7.4.2.2 Data protection assessment

Table 38 provides a high-level data protection assessment of Archiving options for SSN. Note that Archiving assessment may depend also on alternative deployment options (like for Data Storage), which may have different cost and readiness implications.

<sup>13</sup> Consultative Committee for Space Data Systems (2012): Reference model for an Open Archival Information System (OAIS), recommended practice, CCSDS 650.0-M-2.













**Table 38 Data protection assessment of Data Storage options for SSN**

Domain	Criterion ID	Criterion	Archive_1 Assessment	Archive_2 Assessment
Data Protection	DP-01	Data Protection Compliance	Medium 	High 
	DP-02	Privacy Architecture	Medium 	High 
	DP-03	Privacy by design and by default	Medium 	High 
	DP-04	Operational Data Protection	Medium 	High 

#### 7.4.2.3 Interoperability assessment

Table 39 provides a high-level interoperability assessment of Archiving options for SSN. Note that Archiving assessment may depend also on alternative deployment options (like for Data Storage), which may have different cost and readiness implications.

**Table 39 Interoperability assessment of Archiving options for SSN**

Domain	Criterion ID	Criterion	Archive_1 Assessment	Archive_2 Assessment
Interoperability	INT-01	Interoperability Compliance	High 	High 
	INT-02	Integration and interconnectivity	High 	Medium 
	INT-03	Functional Maintainability and Evolvability	High 	Medium 
	INT-04	Elasticity and Scalability	Medium 	Medium 
	INT-05	Technology readiness	High 	High 
	INT-06	Legacy and Migration	High 	Medium 

#### 7.4.3 Archiving – conclusion on technical options assessment

Archiving of data collected and processed has to be done in respect of the principles of Article 4 of EU DPR, notably ensuring appropriate technical and organisational measures are in place and upholding user access rights. However, there might exist National legal obligations, which are regulating archiving activities in different Member States. The results of the security assessment for the Central SSN system has identified current archiving practices at EMSA. Archive\_1, Archive\_2 provide alternative options addressing this security gap. Commercial solutions (Archive\_1) as well as eArchiving (Archive\_2) may provide suitable options for implementing digital archiving strategies in the context of SSN. The most suitable deployment model would be a private cloud infrastructure in a dedicated Agency-owned data centre.

## 7.5 Privacy Enhancing Technologies and Architecture - description and assessment of suitability in the SSN context

This section provides a description of the technical options identified and proposed for SSN. The technical options take into account the identified gaps and also the results of the assessment of the CEF Building Blocks. The evaluation of the technical options takes into account the same security, data protection and interoperability criteria.

### 7.5.1 Privacy Enhancing Technologies and Architecture – description of the technical options

Taking into account that the Central SSN system will process personal data too, this section describes relevant privacy controls that Privacy Enhancing Technologies (PETs) may implement in order to support data protection principles. This section identifies three types of architectural options<sup>14</sup>:

- ✓ **PETA\_1:** Implementation of a Privacy Information Management System (PIMS) in alignment with ISO/IEC 27701:2019 (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines).
- ✓ **PETA\_2:** Implementation of PETs in order to support privacy controls and data protection principles.
- ✓ **PETA\_3:** Compliance with the Privacy Architecture framework in alignment with the ISO/IEC 29101:2018 (Information technology — Security techniques — Privacy architecture framework).

The first proposed privacy and data protection option (PETA\_1) involves the implementation of a Privacy Information Management System (PIMS) in alignment with the ISMS based on ISO/IEC 27001/2 security controls. The ISO/IEC 27001/2 security framework provides limited account of data protection and privacy. The new standard ISO/IEC 27701:2019 (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines) addresses such limitation. It provides guidelines for extending security controls for both the controller and the processor of personal data. Note that the ISO/IEC 27701:2019 standard refers to Personally Identifiable Information (PII), therefore it will be necessary to align the application of the standard to the EU DPR and the GDPR that concern personal data. This standard provides guidance for both controller and processor in order to define a Privacy Information Management System (PIMS).

Requirements and guidance for the protection of personal information vary depending upon the context of the organisation and where national laws and regulations are applicable. ISO/IEC 27001 requires that this context be understood and taken into account. ISO/IEC 27701 gets more specific. It includes mappings to: the privacy framework and principles defined in ISO/IEC 29100, ISO/IEC 27018 and ISO/IEC 29151. However, all these mappings need to be interpreted to take into account local laws and regulations. It is also worth noting that ISO/IEC 27701 is applicable to all organisations that act as processors, controllers or both. To validate that the adequate operational controls from the standard are implemented consistently, to carry out the compliance requirements of relevant privacy and data protection regulations, measures must be taken to:

1. Map the relevant regulatory requirements against the standards controls.
2. Enumerate specific regulatory requirements that are not already fully captured by the standard controls and the conditions to which the requirements become applicable.
3. Incorporate the above into the risk assessment process in the audit cycle.

The second proposed privacy and data protection option (PETA\_2) involves implementations of selected controls, which enhance data protection practices. This section highlights privacy controls drawn from the Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53, Revision 4) and in alignment with ISO/IEC 27701. Note that there is mapping between NIST Security and Privacy Controls and ISO/IEC 27001/2 controls. Relevant privacy controls (adapted from the NIST Security and Privacy Controls) are:

- ✓ **Authority and Purpose:** identifying the legal bases that authorise a particular personal data processing or activity that impacts data protection and specifying in privacy notices the purpose(s) for which personal data are collected. This is also necessary in order to implement measures for limiting the use of personal data to the purpose/s specified in the privacy notices, in a manner compatible with those specified purposes, or as otherwise permitted by law.

---

<sup>14</sup> Note that the descriptions of Privacy Enhancing Technologies and Architecture options may use terminology in alignment with relevant ISO standards.

- ✓ **Accountability, Audit and Risk Management:** implementing effective controls for governance, monitoring, risk management, and assessment in order to demonstrate compliance with applicable data protection requirements and minimising overall privacy and data protection risks.
- ✓ **Data Quality and Integrity:** implementing measures supporting assurance that collected and maintained personal data are accurate, relevant, timely, and complete for the purpose for which they are to be used, as specified in privacy notices.
- ✓ **Data Minimisation and Retention:** implementing measures supporting data minimisation and retention of personal data that are relevant and necessary for the purpose for which they were originally collected.
- ✓ **Individual Participation and Redress:** implementing measures enabling data subjects to have active decisions regarding the collection and the use of their personal data and providing data subjects with access to their personal data and enabling them to have their personal data corrected or amended, as appropriate.
- ✓ **Data Breach Notification:** implementing measures in order to identify affected personal data (in case of data breaches) and notifying data subjects, when applicable.
- ✓ **Privacy Notice:** updating privacy notices for the Central SSN system, including the EMSWe.

In order to assess and define an adequate strategy for implementing privacy controls, ENISA defines a Privacy Enhancing Technologies (PETs) control matrix<sup>15</sup> supported by an assessment questionnaire<sup>16</sup> defining a framework for a systematic presentation and evaluation of online and mobile privacy tools for end users. The ENISA PETs control matrix and the controls drawn from ISO/IEC 27701 provide guidance for implementing privacy controls.

The third proposed privacy and data protection option (PETA\_3) involves compliance with a privacy architecture framework. At the architectural level, it is possible to adopt and implement further security measures (ISO/IEC 29101:2018 Information technology — Security techniques — Privacy architecture framework) forming a privacy architecture framework. It addresses privacy concerns for ICT systems that process personal data, lists components for the implementation of such systems, and provides architectural views contextualising these components. This privacy architecture framework is applicable to entities involved in specifying, procuring, architecting, designing, testing, maintaining, administering and operating ICT systems that process personal data.

## 7.5.2 Privacy Enhancing Technologies and Architecture – assessment of the technical options

The proposed PETA options for SSN would enhance privacy and data protection aspects of SSN. These options provide a comprehensive account of privacy and data protection in alignment with current industry practices and standards that are relevant for the SSN system. All PETA options shall be considered for implementation. The implementation of a Privacy Information Management System (PIMS) as PETA\_1 proposes provides the most comprehensive privacy and data protection option, rather than the other proposed options (PETA\_2 and PETA\_3) addressing ad-hoc relevant aspects of data protection and privacy.

<sup>15</sup> ENISA (2016): PETs controls matrix – A systematic approach for assessing online and mobile privacy tools.

<sup>16</sup> ENISA (2016): PETs control matrix – Annex 1: Assessment questionnaires.

## 7.6 Network Security - description and assessment of suitability in the SSN context

This section provides a description of the technical options identified and proposed for SSN. The technical options take into account the identified gaps and also the results of the assessment of the CEF Building Blocks. The evaluation of the technical options takes into account the same security, data protection and interoperability criteria.

On one hand, the goal of network segmentation is to introduce a layered security approach, which prevents exploitation of privileged accounts and deters attackers from moving inside the SSN operational environment. On the other hand, a federated identity management solution will support further coordination and secure collaboration between the Central SSN and National SSN systems.

### 7.6.1 Network Security – description of the technical options

The implementation of the EMSWe will extend the digital surface to protect. As a result, EMSA will be further exposed to emerging cybersecurity threats. In order to mitigate some threats, network security provides the means for mitigating threats affecting ICT systems located internally and externally to organisational digital perimeters. This section identifies two types of architectural options:

- ✓ **NS\_1:** Physical network segmentation creating distinct security domains for the Central SSN system and other critical digital assets, including the EMSWe.
- ✓ **NS\_2:** Logical network segmentation adopting Software Defined Networking (SDN) and Network Function Virtualisation (NFV) creating security domains for the Central SSN system and other critical digital assets, including the EMSWe.

Both network solutions would increase the level of network security, which can also further enhance with networking management strategies and the integration of Security Information and Event Management (SIEM) solutions in order to detect and monitor critical security events both internally and externally to organisational digital perimeters. In addition to network segmentation, other network factors (e.g. remote access/private networks between the Central SSN and the National SSN systems) may affect network security. Table 40 provides a comparison of physical network and SDN/NFV solutions.

**Table 40 Comparison of physical network and SDN/NFV solutions**

	Physical networks	Software Defined Networking (SDN) and Network Function Virtualisation (NFV)
<b>Network provisioning</b>	Different control levels	Centralised management
<b>Enterprise Management</b>	Different service controls	Harmonised and comprehensive management of enterprise services
<b>Security</b>	Fragmented security controls and policies	Centralised security controls and policies
<b>Quality of Service</b>	Limited scalability and flexibility	Dynamic adjustment and reconfiguration supporting scalability and flexibility on demand
<b>Capital (CAPEX) and operating (OPEX) expense</b>	CAPEX and OPEX directly linked to the number networks and (hardware) systems	Reduced CAPEX and OPEX due to virtualisation (relying on software solutions rather than different hardware solutions)

It is necessary to perform a scoping and design activity in order to identify a suitable network segmentation with the objective of enhancing security and privacy as well as introducing separations between digital assets. In particular, in order to define a suitable network segmentation, it is necessary to have a clear understanding of the SSN data environment, which involves people, processes, and technologies that store, process, or transmit SSN data or other sensitive authentication data. Systems and services with connectivity or access to or from the SSN data environment are considered to be connected to the Central SSN. These systems and services have a communication path to one or more SSN components in the SSN data environment. Connectivity may occur over various technologies, including physical, wireless, and virtualised:

- ✓ Physical connectivity may be via a traditional network (e.g. Ethernet or power-line communication) or direct system-to-system connection (e.g. USB, component, etc.).
- ✓ Wireless connectivity uses different radio waves and frequencies as its transport mechanism (e.g. wireless LANs, Bluetooth, cellular technologies, etc.). Wireless technologies are often connected to a physical network.
- ✓ Virtualized connectivity includes use of virtual networks, virtual machines, virtual firewalls, virtual switches, etc. Virtual devices typically share common resources, such as an underlying host system and/or hypervisor, which could be used to connect one logical partition to another.



Table 41 provides examples of activities (adapted from industry practices concerned with data intensive sectors<sup>17</sup>) for scoping and designing network segmentation alternatives.

**Table 41 Examples of activities for scoping and designing network segmentation alternatives**

Activity	Description
Identify how and where the Central SSN (EMSA) receives data (including sensitive and personal data).	Identify all channels and methods for receiving SSN data, from the point where the data are received through to the point of destruction, disposal or transfer.
Locate and document where data are stored, processed, and transmitted.	Document all SSN data flows, and identify the people, processes, and technologies involved in storing, processing, and/or transmitting of SSN data. These people, processes, and technologies are all part of the SSN data environment. This activity shall take into account the structure and organisation of SSN users.
Identify all other system components, processes, and personnel that are in scope.	Identify all processes (both business and technical), system components, and personnel with the ability to interact with or influence the SSN data environment. These people, processes, and technologies are all in scope, as they have connectivity to the SSN data environment or could otherwise impact the security of SSN data. This activity shall take into account the structure and organisation of SSN users.
Implement controls to minimise scope to necessary components, processes, and personnel.	Implement controls to limit connectivity between SSN data environment and other in-scope systems to only that which is necessary. Implement controls to segment the SSN data environment from people, processes, and technologies that do not need to interact with or influence the SSN data environment. This activity shall take into account the structure and organisation of SSN users.

These solutions would enhance network security and the ability to protect critical assets from relevant threats (e.g. insider threats, complex attacks involving subsequent lateral movements inside networks).

## 7.6.2 Network Security – assessment of the technical options

The proposed Network Security options for SSN would enhance network segregation as well as monitoring/detecting capabilities for SSN. These options in combination with the other proposed architectural options enhance the security posture and maturity of SSN as a whole. The extent to which Network Security options support security, data protection and interoperability depends on the current implementations of such options for SSN. All Network Security options shall be considered for revision (of current practices) and implementation. This section assesses the Network Security options according to the security, data protection and interoperability criteria for SSN.

### 7.6.2.1 Security assessment

Table 42 provides a high-level security assessment of Network Security options for SSN.

**Table 42 Security assessment of Network Security options for SSN**

Domain	Criterion ID	Criterion	NS_1 Assessment	NS_2 Assessment
Security	SEC-01	Security Domains	Medium 	High 
	SEC-02	Data Security	Medium 	High 
	SEC-03	Security Functions	Medium 	High 
	SEC-04	Complexity and Coupling of Security Functions	Medium 	High 
	SEC-05	Operational Security	Medium 	High 
	SEC-06	Architectural Exposure to Threats	Medium 	Medium 
	SEC-07	Security Maintainability and Evolvability	Medium 	High 
	SEC-08	Security Compliance	High 	High 

Physical segregation provides higher security levels compared to logical segregation in particular as regards attacking vectors where physical segregation provides a more challenging environment. Undeniably, centralisation has clear benefits as relates to implantation and costs.









<sup>17</sup> PCI Security Standards Council (2017): Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation.



### 7.6.2.2 Data protection assessment

Table 43 provides a high-level data protection assessment of Network Security options for SSN.













**Table 43 Data protection assessment of Network Security options for SSN**

Domain	Criterion ID	Criterion	NS_1 Assessment	NS_2 Assessment
Data Protection	DP-01	Data Protection Compliance	High 	High 
	DP-02	Privacy Architecture	High 	High 
	DP-03	Privacy by design and by default	Medium 	High 
	DP-04	Operational Data Protection	Medium 	High 

### 7.6.2.3 Interoperability assessment

Table 44 provides a high-level interoperability assessment of Network Security options for SSN.

**Table 44 Interoperability assessment of Network Security options for SSN**

Domain	Criterion ID	Criterion	NS_1 Assessment	NS_2 Assessment
Interoperability	INT-01	Interoperability Compliance	Medium 	High 
	INT-02	Integration and interconnectivity	Medium 	High 
	INT-03	Functional Maintainability and Evolvability	Medium 	High 
	INT-04	Elasticity and Scalability	Medium 	High 
	INT-05	Technology readiness	High 	High 
	INT-06	Legacy and Migration	High 	High 

## 7.6.3 Network Security – conclusion on technical options assessment

Physical network segmentation (NS\_1) provides an incremental solution, which may be implemented without substantial changes to the current SSN context. Logical network segmentation adopting SDN/NFV (NS\_2) requires a substantial investment in order to be implemented in the current SSN context. From security, data protection and interoperability perspectives, NS\_1 relies on different (often fragmented) security solutions and policies. Whereas, NS\_2 provides the opportunity to centralise and harmonise security solutions and policies.

## 7.7 Proposed target architecture for SSN

Table 45 describes the proposed target architecture, which is not centred on specific developmental criteria, combines the identified and analysed technical solutions.

**Table 45 Proposed Target Architectures**

Architectural Areas	Alternative Target Architecture Option
Identity and Access Management (IAM)	<b>Federated IAM adopting third-party authentication (IAM_3):</b> complies with Art. 12 of the EMSWe regulation that asks for a common user registry and access management, federated user management and EU-level monitoring.
Data Storage	<b>Virtually distributed databases, relying on infrastructures as a service such as private cloud (DS_3):</b> provides the most cost-effective solution and takes into account current EMSA infrastructures and data centres.
Archiving	<b>Data storage solutions tailored for archiving purposes (Archive_1):</b> makes use of simple and rather standard data storage solutions tailored for archiving purposes.
Privacy Enhancing Technologies and Architecture	<b>Implementation of a Privacy Information Management System (PIMS) in alignment with ISO/IEC 27701:2019 (PETA_1 + DPIA):</b> extends the current ISMS, already developed by EMSA as part of the SSN project, by adding the implementation of a Privacy Information Management System (PIMS) in alignment with ISO/IEC 27701:2019.
Network Security	<b>Logical network segmentation adopting Software Defined Networking (SDN) and Network Function Virtualisation (NFV) creating security domains for the Central SSN system and other critical digital assets, including the EMSWe (NS_2):</b> provides the most cost-effective solution and takes also into account current operation issues of dealing with physical segregated networks.

# 8 Roadmap of actions for implementation of SSN security, data protection and interoperability measures

## 8.1 Roadmap for SSN

Figure 10 shows the roadmap for the implementation of the proposed target architecture, as per Section 7.7, and other activities addressing recommendations for SSN.

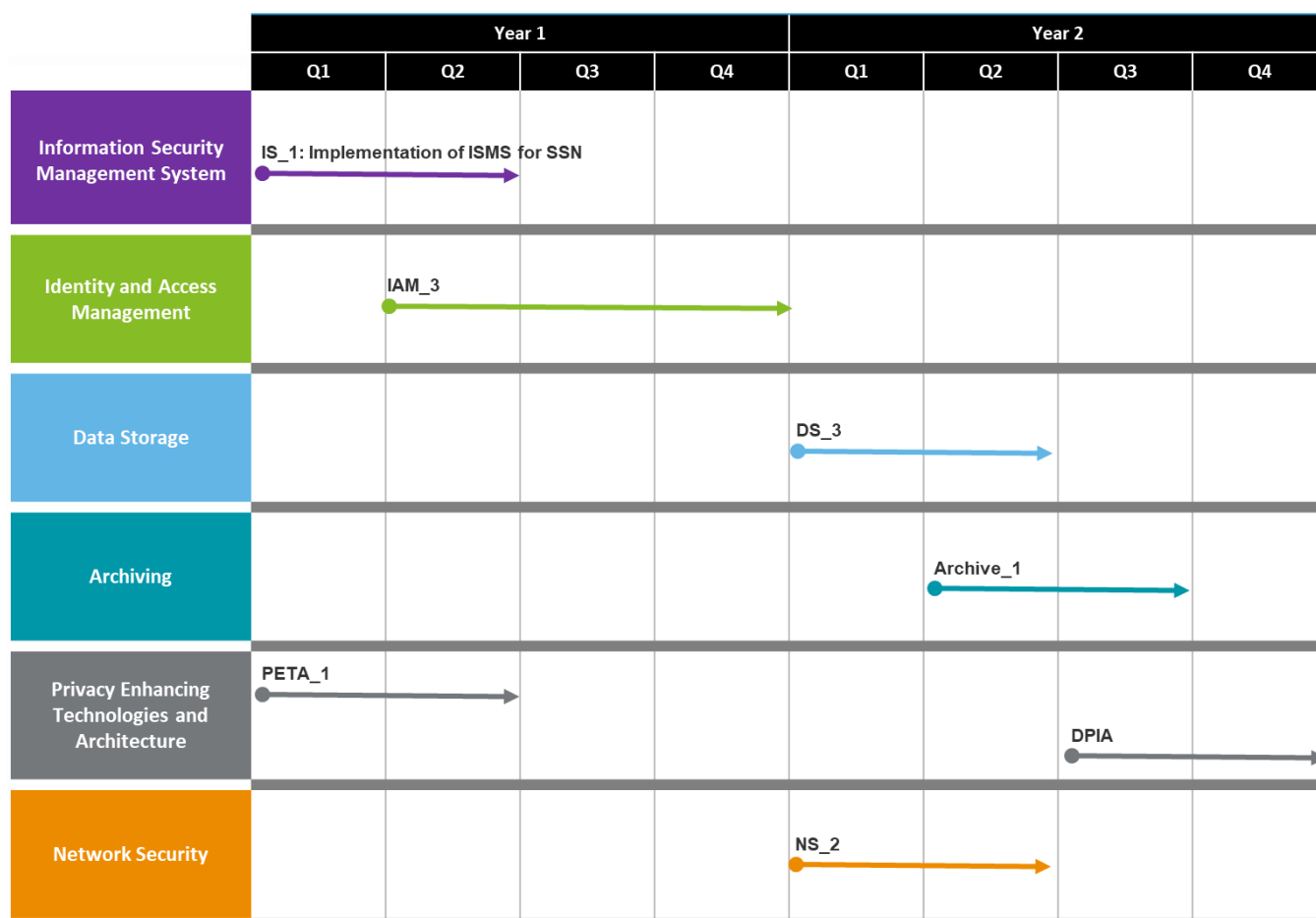


Figure 10 Roadmap of architectural options for SSN

## 8.2 Overview of the roadmap activities

This section outlines the proposed roadmap actions associated with the proposed target architecture as per Section 7.7. For each one of the domains (legal, interoperability and security), is provided a brief description of the suggested activities and an assessment of the implementation criteria, which takes into account estimated effort (in person-months).

Table 46 lists and defines activities for implementation of the ISMS for SSN.

**Table 46 Roadmap activities for ISMS**

ID	Activity	Roadmap Activities Description	Estimated Effort
IS_1	Implement ISMS	This activity is concerned with implementing the identified controls as per Section 4.2, which form an ISMS for SSN. Note that the low effort estimation takes into account the assumption that most security controls are already in place. This activity will focus on the missing controls.	3 person-months (Low effort) ↓

Table 47 lists and defines security roadmap activities for implementation in SSN.

**Table 47 Roadmap activities for IAM**

ID	Activity	Roadmap Activities Description	Estimated Effort
IAM_3	Implement Federated IAM	This activity is concerned with implementing the federated IAM solution for SSN as per Section 7.7. Note that this may involve activities for integrating the IAM solution with other systems in the SSN environment.	9 person-months (High effort) ↑

Table 48 lists and defines activities for data storage for SSN.

**Table 48 Roadmap activities for data storage**

ID	Activity	Roadmap Activities Description	Estimated Effort
DS_3	Implement Data Storage option	This activity is concerned with implementing data storage option as per Section 7.7, which relies on commercial and available data storage solutions. Note that the implementation of data storage may require reviewing policies and relevant business continuity plans, incident management and other relevant operational processes. Furthermore, it may be necessary to devise tailored data migration procedures.	9 person-months (High effort) ↑

Table 49 lists and defines activities for Archiving for SSN.

**Table 49 Roadmap activities for Archiving**

ID	Activity	Roadmap Activities Description	Estimated Effort
Archi ve_1	Implement Archiving option	This activity is concerned with implementing archiving option as per Section 7.7, which relies on commercial and available data storage solutions. Note that the implementation of archiving may require reviewing archiving policies and relevant business continuity plans, incident management and other relevant operational processes. Furthermore, it may be	9 person-months (High effort) ↑

ID	Roadmap Activities		Estimated Effort
	Activity	Description	
		necessary to devise tailored data migration procedures.	

Table 50 lists and defines activities for Privacy Enhancing Technologies and Architecture for SSN.

**Table 50 Roadmap activities for Privacy Enhancing Technologies and Architecture**



ID	Roadmap Activities		Estimated Effort
	Activity	Description	
<b>PETA_1</b>	Implement PIMS	This activity is concerned with implementing a Privacy Information Management System (PIMS) for SSN as extension of the ISMS in alignment with ISO/IEC 27001/2 controls, as per Section 7.7.	9 person-months (High effort) 
<b>DPIA</b>	Perform a DPIA	This activity is concerned with performing the Data Protection Impact Assessment (DPIA) for SSN.	3 person-months (Low effort) 

Table 51 lists and defines activities for Privacy Enhancing Technologies and Architecture for SSN.

**Table 51 Roadmap activities for Privacy Enhancing Technologies and Architecture**






ID	Roadmap Activities		Estimated Effort
	Activity	Description	
<b>NS_2</b>	Implement network segregation	This activity is concerned with network security solution based on further segregation of SSN, as per Section 7.7.	9 person-months (High effort) 

Table 52 lists and defines other roadmap activities addressing recommendations for SSN.

**Table 52 Other roadmap activities**

ID	Roadmap Activities		Estimated Effort
	Activity	Description	
<b>OS_1</b>	Security Committee	Implement a dedicated and/or specialized workgroup of SSN stakeholders, acting as a Security Committee, mainly focused on security and data protection aspects (governance, operational, technical).	3 person-months (Low effort) 
<b>OS_2</b>	Interoperability arrangements	Formalize the Guidelines and Recommendations of interoperability arrangements for SSN, with the involved Member States actors.	6 person-months (Medium effort) 
<b>OS_3</b>	Developing IT Security Plan	Review and update the IT Security Plan (ITSP), taking into account: a) The scope of the IT Security Plan for the Central SSN system; b) The SSN system asset inventory; c) Business Impact Assessment (BIA) workshops with the EMSA SSN business and IT representatives; d) The security classification for the Central SSN system; e) Risk Assessment/Analysis (RA); Define an overall monitoring process for the implementation progress and the status of the IT Security Plan for the Central SSN system.	6 person-months (Medium effort) 
<b>OS_4</b>	Strengthen SSN security coding	Implement a security testing methodology at all post-design phases (development, system integration testing, user acceptance testing) before production phase, which shall include: a) Automated code review focused on security; b) Dynamic & static vulnerability scanning; c) Access control testing; d) Validation that all identified security controls were implemented. Develop and disseminate to all developers secure coding standards for the main programming languages used to develop SSN.	6 person-months (Medium effort) 

# 9 Conclusions

## 9.1 On data protection aspects

### 9.1.1 Data Protection Impact Assessment (DPIA) [Attention point #1]

EMSA shall conduct a DPIA with consultation with the EDPS prior to the start of the new SSN.

Ensuring EMSA's compliance with EU DPR would require executing a Data Protection Impact Assessment (DPIA) for risk associated with processing of personal data. The DPIA will define the procedures necessary to properly identify personal data, label them, and assign the adequate protection measures. The EMSA DPO is fully aware on the requirements for executing the DPIA.

### 9.1.2 Roles and responsibilities [Attention point #2]

Both EMSA and Member States operate their respective SSN systems as data controller. They are therefore co-controllers for the SSN data cycle. Taking into account that the Central SSN system receives data collected by the National SSN systems, it would be necessary to clarify for what data collected by the National SSN systems EMSA is operating as data controller.

A clear data protection statement with the attribution of roles should be part of the SSN documentation. This statement should also specify the requirements in terms of data protection. In order to support awareness across SSN stakeholders, EMSA may host a workshop with Member States on data protection topics for SSN.

In order to support the awareness across SSN stakeholders, it is advisable to include in the agenda of the SSN Group and of the HLSG an item about data protection in SSN and host a workshop with Member States on data protection for SSN.

## 9.2 On interoperability aspects

### 9.2.1 Compliance with relevant network and information security standards [Interoperability gap #1]

The security impact assessment has identified some security gaps, which may impact on the interoperability of SSN systems. A reduced interoperability may also impact the security of data exchanged by SSN systems while increasing the risks (e.g. compromised data, data breaches, data losses, associated affecting data exchanges) as well. A reduced of semantic interoperability may also impact data confidentiality as well as integrity. Despite systems may exchange data, the lack of semantic interoperability may compromise confidentiality (by exchanging confidential data accidentally) and integrity (by exchanging data incorrectly). The interplay between security and interoperability is fundamental for the SSN architecture.

SSN is a system already in operation during the last 15 years. The security policies in place were elaborated in May 2016. The existing SSN Security Guidelines will be revised as part of Task 4 to take into account the results of the analysis carried out in this study.

### 9.2.2 Degree of support from different interest groups [Interoperability gap #2]

Currently there is a lack of dedicated interests groups concerned with the security (including data protection) and interoperability (including governance, operational, technical) aspects of the Central SSN system managed by EMSA and the National SSN systems managed by (National Competent Authorities of) Member States. Therefore, it is necessary to establish dedicated interest groups representing EMSA and National Competent Authorities in order to own and being accountable for the security and interoperability aspects of SSN systems.

There is a need to involve the key SSN stakeholders on security-related aspects of the system and also on the adequacy of deploying key security controls with a direct impact on confidentiality and integrity of data.

In order to support the awareness across SSN stakeholders, it is advisable to include in the agenda of the SSN Group and of the HLSG an item about data protection in SSN and host a workshop with Member States on data protection for SSN.

### 9.2.3 Transparency [Attention point #1]

The MSs will need to verify that impacts arising from the interoperability arrangements for SSN are appropriately managed and there is a high degree of confidence that the interoperable National SSN systems have rules and, where required, other arrangements that are consistent and enforceable under the interoperability arrangement for SSN. EMSA should develop Guidelines and Recommendations with a view to establishing consistent, efficient and effective assessments of interoperability arrangements for SSN with the involved MS actors.

At this stage, EMSA has different guidelines supporting interoperability (e.g. Interface Guide, HAZMAT Guidelines, etc.). These guidelines need to be revised together with the future developments of SSN.

## 9.3 On security aspects

### 9.3.1 Information security policies [Security gap #1]

As set out in Task 2 report (Section 7.3), EMSA should develop an IT Security Plan, including where appropriate details of the assessed risks and any additional measures required, according to Article 9 of the Commission Decision 2017/46. The IT Security Plan will cover at least the following aspects of IT security:

- ✓ Rationale: Benefits and value of the system IT Security Plan; Approach of building the system IT Security Plan
- ✓ System(s) in Scope: Overview of the system, purpose/functionality; Overview of personal data processing activities, types of personal data and purposes; Roles and responsibilities; System user population(s); Primary Assets details; Supporting Assets details.
- ✓ System Security Characterisation: Key Control environment (e.g. Access Control, Backup Policies, Legal, Regulatory and Contractual Details, System accreditation strategy, Assumptions and Constraints, etc.).
- ✓ System Modelling.
- ✓ System Security Needs/Business Impact Assessment: Confirmation/conclusion on system criticality from a data protection / privacy point of view (this is a minimum required work under Decision 2017/46 in order to assess the relevance of data protection aspects as part of the ITSP preparation).
- ✓ System Risk Analysis in alignment with ITS RM<sup>2</sup>.
- ✓ Risk Treatment/IT Security Plans.

### 9.3.2 Access control [Security gap #2]

Currently the Central SSN System and the National SSN systems (operated by Member States) rely on different decentralised authorisation mechanisms operated locally. Although this solution is sufficient in order to support the current information exchanges between the Central SSN System and the National SSN Systems, it provides limited support in order to implement end-to-end authorisation mechanisms, resulting in a reduced traceability and accountability, and therefore not suitable to the future developments of SSN. Implementing a centralised solution for authorisation mechanism would enhance the overall security of the data exchanged between the different systems. Such solution would support defining detailed relevant authorisation mechanisms (including access control policies) guaranteeing the security of data exchanged via SSN systems.

### 9.3.3 Compliance with security policies and standards [SSN Security gap #3]

As set out in Task 2 report (Section 7.3), SSN security policies should be revised in order to take into account operational needs (e.g. business continuity, incident management, data archiving) in compliance with relevant legislation.

SSN security policies shall be revised in order to take into account operational needs together with the future developments of SSN.

### 9.3.4 Complementary security recommendations

- ✓ Labelling of information is not required by SSN system as long as SSN does not process classified information. Nevertheless labelling at least personal data is recommended to avoid accidental information leakage.
- ✓ Periodic PENTEST should be scheduled for SSN every time a new version of the application is released or at least every two (2) years, coincidentally with the end of the life/support of different technologies that could be implemented in SSN. This recommendation could be extended to the National SSN system as well.
- ✓ It is recommended to configure TLS as an overlay protocol (on top of SOAP, REST, HTTP, etc.), between the load balancer (F5) and SSN. The certificates used, can be issued by an internal CA, and do not need to be valid for external communications.



## 9.4 On Structure and organisation of SSN users

In order to integrate the identified data protection and security roles into SSN, new data protection and security roles should be created and integrated in the access policies of SSN, as summarized in the table below.

New data protection and security SSN roles	Description	Source
<b>Data Protection Officer</b>	As required by Regulation 2018/1725 EU DPR: Each Union institution or body shall designate a data protection officer in accordance with Article 43, Section 6 in Regulation 2018/1725.	Regulation 2018/1725 (EU DPR)
<b>Data Protection third party</b>	As required by Regulation 2018/1725 EU DPR: A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data. This natural or legal will be authorised by the controller or processor.	Regulation 2018/1725 (EU DPR)
<b>Local Informatics Security Officer (LISO)</b>	As required by Commission Decision 2017/46: The officer who is responsible for IT security liaison for a Commission department.	Commission Decision 2017/46
<b>Data owner</b>	As required by Commission Decision 2017/46: The individual responsible for ensuring the protection and use of a specific data set handled by a Communication and information system (CIS).	Commission Decision 2017/46
<b>System owner</b>	As required by Commission Decision 2017/46: The individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of a Communication and information system (CIS).  Although the system owner might not require access to SSN, it is necessary to formalise the ownership and if necessary to provide access to SSN and its data following need-to-know principle, that is, accessing the system and data (only in the modes for which access is needed and only during the time frame when access is needed) in order to fulfil relevant security responsibilities.	Commission Decision 2017/46

## 9.5 On CEF Building Blocks

### 9.5.1 eID suitability

The eID is mainly designed for supporting identification of citizens who are registered for services in Member States. Public sector service providers can connect to an existing eIDAS-Node in order to offer online services capable of identifying citizens and businesses from other Member States. Taking into account the analysis of the eID (which provides limited support for implementing end-to-end authorisation, authentication and identification mechanisms across the SSN ecosystem) and the operational needs of the Central SSN system and its interaction with National SSN systems (which involve different users registered locally and systems not necessary integrated with other public sector services), the eID is assessed to be unsuitable for the context of SSN.

This conclusion needs to be revisited when a security study will include the declarants to the EMSWe.

### 9.5.2 eDelivery

eDelivery is a network of nodes for digital communications. It is based on a distributed model where every participant becomes a node using standard transport protocols and security policies. It helps public administrations to exchange electronic data and documents with other public administrations, businesses and citizens, in an interoperable, secure, reliable and trusted way. The CEF eDelivery building block is based on the AS4 messaging protocol, open and free for all, developed by the OASIS standards development organisation. To ease its adoption in Europe, eDelivery uses the AS4 implementation guidelines defined by the Member States in the e-SENS Large Scale Pilot. Organisations must install an Access Point, or use a Service Provider, to exchange information with the AS4 messaging protocol<sup>18</sup>. The eDelivery CEF Building Blocks can be used for secure exchange of messages and data.

The information exchanges between the Central SSN and the National SSN systems involve secure communications. The adoption of eDelivery requires its implementation in the Central SSN as well as across all National SSN systems.

<sup>18</sup> The European Commission has reviewed solutions that have passed or are in the process of passing the conformance testing according to the eDelivery AS4 profile. European Commission (2019): CEF eDelivery, Market guide for AS4 solutions and services, v1.05.

This corresponds to a major restructuring of communication in the SSN ecosystem. Such restructuring may potentially disrupt the SSN ecosystem and its security too (e.g. due to lack of implementation/coordination of eDelivery in all National SSN systems). Furthermore, the types of communications involve the exchange of data rather than documents. This would require tailoring eDelivery in order to define the data exchange format and the configuration of different environments (of the Central SSN and National SSN systems). This would require a major implementation effort. Taking into account such considerations, the adoption of eDelivery would have a major impact (in terms of effort required), which may increase the risk of disrupting operations (also in terms of security and interoperability).

However, taking into account that this may require a completely redesign of communication mechanisms between the Central SSN and the National SSN as well as an agreement between EMSA and the Member States, eDelivery is assessed to be unsuitable for the context of SSN.

This conclusion needs to be revisited when a security study will include the declarants to the EMSWe.

### 9.5.3 eSignature

The eSignature building block helps public administrations and businesses accelerate the creation and verification of electronic signatures. The deployment of solutions based on this building block in a Member State facilitates the mutual recognition and cross-border interoperability of eSignatures. This means that public administrations and businesses can trust and use eSignatures that are valid and structured in EU interoperable formats.

The eSignature building block may support implementing measures (e.g. authenticity of modification requests to data) in order to detect any unauthorized changes made to critical data stored and retained locally after data transmission. With the upcoming changes to SSN, it is expected that SSN will be processing a significant quantity of data of all passengers and crew members that reach EU ports. This may require additional measures in order to protect and process personal data in compliance with relevant data protection regulatory frameworks. The Central SSN will process (personal) data collected and communicated by the National SSN systems (hence, under the controller responsibilities of the National Authorities). It is therefore necessary to implement adequate mechanisms in order to guarantee the authenticity of requests from the National Authorities via the National SSN systems. eSignature may support such type of measure, although it provides limited support for protecting (personal) data. Therefore, it is suitable to assure cryptographic mechanisms rather than to adopt eSignature in order to protect the confidentiality and integrity of data (including personal data).

A possible use case of eSignature in the SSN context may be to electronically sign internal administrative procedures (e.g. Confidentiality or Non-Disclosure Agreements) rather than for exchanging data. Further analysis on what type of documents/data need to be signed and retained after data transmission shall be performed in order to understand whether eSignature may support specific needs for signing electronically documents and information. However, taking into account the exchanges of data between the Central SSN and the National SSN systems, it is more important implementing adequate measures reflecting access controls (e.g. user credentials) rather than electronic signatures in order to protect data. Taking into account that the data exchanges between the Central SSN and the National SSN systems involve system-to-system communications, the eSignature is assessed to be unsuitable for the context of SSN.

This conclusion needs to be revisited when a security study will include the declarants to the EMSWe.

### 9.5.4 eArchiving

There is currently no legal obligation or requirements for archiving. However, there might exist local legal obligations, which are regulating archiving activities in different Member States. The security assessment of the Central SSN system has highlighted that current archiving practice can be further developed by developing dedicated data storage and archiving solutions for SSN taking also into account data classification. eArchiving (as well as other commercial solutions) may provide a suitable option for implementing digital archiving strategies in the context of SSN.

This study includes only the Central and National SSN. It is important to highlight that this security study would need to be supplemented with the additional elements related to the new systems interlinked with SSN (e.g. Thetis, CSN, IMS, SAT-AIS etc). Furthermore, a study shall include the entire information chain from the Declarant (or the data provider) up to the end users (including all the Authorities defined by the EMSWe regulation).

The eArchiving can also be used to support the data providing process of the declarants to the EMSWe.

## 9.6 On target architecture

The proposed **Target Architecture** is the following:

Architectural Areas	Target Architecture
Identity and Access Management (IAM)	<b>Federated IAM adopting third-party authentication (IAM_3):</b> complies with Art. 12 of the EMSWe regulation that asks for a common user registry and access management, federated user management and EU-level monitoring.
Data Storage	<b>Virtually distributed databases, relying on infrastructures as a service such as private cloud (DS_3):</b> provides the most cost-effective solution and takes into account current EMSA infrastructures and data centres.
Archiving	<b>Data storage solutions tailored for archiving purposes (Archive_1):</b> makes use of simple and rather standard data storage solutions tailored for archiving purposes.
Privacy Enhancing Technologies and Architecture	<b>Implementation of a Privacy Information Management System (PIMS) in alignment with ISO/IEC 27701:2019 (PETA_1 + DPIA):</b> extends the current ISMS, already partially developed by EMSA as part of the SSN project, by adding the implementation of a Privacy Information Management System (PIMS) in alignment with ISO/IEC 27701:2019.
Network Security	<b>Logical network segmentation adopting Software Defined Networking (SDN) and Network Function Virtualisation (NFV) creating security domains for the Central SSN system and other critical digital assets, including the EMSWe (NS_2):</b> provides the most cost-effective solution and takes also into account current operation issues of dealing with physical segregated networks.

# Glossary and acronyms

Acronym	Glossary
<b>ACL</b>	Access Control Lists
<b>AIS</b>	Automated Information System(s)
<b>ATA</b>	Actual Time of Arrival
<b>BCF</b>	Business Continuity Facility
<b>BCM</b>	Business Continuity Management
<b>BCP</b>	Business Continuity Plan
<b>BIA</b>	Business Impact Assessment
<b>BSI</b>	British Standards Institution
<b>CA</b>	Certification Authority
<b>CAMMS</b>	Common Assessment Method for Standards and Specifications
<b>CCM</b>	Cloud Controls Matrix
<b>CCS</b>	Common Channel Signalling
<b>CEF</b>	Connecting Europe Facility
<b>CERT</b>	Computer Emergency Response Team
<b>CISE</b>	Common Information Sharing Environment
<b>CNIL</b>	Commission Nationale de l'Informatique et des Libertés
<b>CNDP</b>	Comissão Nacional de Protecção de Dados – is the Portuguese Data Protection Authority.
<b>COBIT</b>	Control Objectives for Information and related Technology +
<b>CSA</b>	Cloud Security Alliance
<b>CSO</b>	Chief Security Officer
<b>CISO</b>	Chief Information Security Officer
<b>CTO</b>	Chief Technology Officer
<b>DB</b>	Database
<b>DBMS</b>	Database Management System
<b>DEV</b>	Development Environment.
<b>DG</b>	Directorate-General
<b>DG CONNECT</b>	Directorate-General for Communications Networks, Content and Technology
<b>DG DIGIT</b>	Directorate-General for Informatics
<b>DG HR.DS</b>	Directorate-General Human Resources, Directorate "Security"
<b>DMZ</b>	Demilitarized Zone
<b>DPC</b>	Data Protection Coordinator
<b>DPG</b>	Defence Planning Guidance
<b>DPIA</b>	Data Protection Impact Assessment
<b>DPO</b>	Data Protection Officer
<b>EBIOS</b>	Expression des Besoins et Identification des Objectifs de Sécurité
<b>EIF</b>	European Interoperability Framework
<b>EIS</b>	European Index Server
<b>EC</b>	European Commission
<b>ECAS</b>	European Commission Authentication System
<b>EDPS</b>	European Data Protection Supervisor
<b>EEA</b>	European Economic Area
<b>EMSWe</b>	European Maritime Single Window environment
<b>ENISA</b>	European Union Agency for Network and Information Security
<b>EU</b>	European Union
<b>ETA</b>	Estimated Time of Arrival
<b>ETD</b>	Estimated Time of Departure
<b>EUROSUR</b>	European Border Surveillance System
<b>EUCI</b>	EU Classified Information

Acronym	Glossary
<b>(F)RAND</b>	(Fair) reasonable and Non-Discriminatory
<b>GRC</b>	Governance Risk and Compliance
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>IAS</b>	Internal Audit Service
<b>IAG</b>	International Airlines Group
<b>IAM</b>	Identity and Access Management
<b>ICO</b>	Information Commissioner's Office
<b>ICT</b>	Information and Communications Technology
<b>IDS</b>	Intrusion detection System
<b>IFCD</b>	Interface and Functionalities Control Document
<b>IMO</b>	International Maritime Organisation
<b>IMS</b>	Integrated Maritime Services
<b>IPR</b>	Intellectual Property Rights
<b>ISA</b>	Interoperability Solutions for European Public
<b>ISO</b>	International Organization for Standardization
<b>ISP</b>	Internet Service Provider
<b>IT</b>	Information Technology
<b>LISO</b>	Local Informatics Security Officer
<b>LRIT</b>	Long-Range Identification and Tracking
<b>MAC</b>	Media Access Control
<b>MS</b>	Member State
<b>MSP</b>	Multi-Stakeholder Platform
<b>MMSI</b>	Maritime Mobile Service Identity
<b>NCA</b>	National Command Authorities
<b>NFV</b>	Network Function Virtualisation
<b>NIST</b>	National Institute of Standards and Technology
<b>NSW</b>	National Single Window
<b>OS</b>	Operating System
<b>OSS</b>	Open Source Software
<b>OWASP</b>	Open Web Application Security Project
<b>PC</b>	Personal Computer
<b>PIMS</b>	Privacy Information Management System
<b>PM</b>	Project Manager
<b>PRINCE2</b>	Projects in Controlled Environments 2
<b>PRD (or PROD)</b>	Production Environment
<b>PSC</b>	Project Steering Committee
<b>RA</b>	Risk Assessment
<b>RPO</b>	Recovery Point Objective
<b>RTO</b>	Recovery Time Objective
<b>SAR</b>	Search and rescue
<b>SOAP</b>	Simple Object Access Protocol
<b>SSN</b>	SafeSeaNet
<b>SDP</b>	Ship Data Provider
<b>SDN</b>	Software Defined Networking
<b>SLA</b>	Service Level Agreement
<b>SP</b>	Solution Provider
<b>SQL</b>	Structured Query Language
<b>TEST</b>	Test Environment
<b>TLP</b>	Traffic Light Protocol

Acronym	Glossary
<b>TLS</b>	Transport Layer Security
<b>UAT</b>	User Acceptance Test
<b>UR</b>	User Representative
<b>VLAN</b>	Virtual Local Area Network
<b>VM</b>	Virtual Machine
<b>VMS</b>	Virtual Memory System
<b>VPN</b>	Virtual Private Network
<b>VTs</b>	Vessels Traffic Services
<b>WS</b>	Web Services