# 7th SSN LRIT Group Meeting

## Security and Interoperability Solutions for SSN. Project Status

Agenda item 7.4.2

Diego Molero / Project Officer
Department 3. Unit 3.3 Simplification

Lisbon / 13 May 2020

EMSA
European Maritime Safety Agency

# Background

- **Provides recommendations for security and interoperability solutions for SSN**

- **Focuses on the security measures to be implemented in the Central SSN system, in National SSN systems and in the interfaces between them**

- **Executed under the grant agreement between EMSA and the Commission's DG MARE**

# Project Structure

- **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**

# Deliverables

- **Contributions from EMSA, DG MOVE, DIGIT, CERT-EU, and ENISA**
- **An Interim Report per Task**
- **Final Report consolidating the four interim reports in a single document**
- **Revised SSN Security Guidelines in line with the target architecture identified in Task 3**

# Data Protection

| Data protection gaps and attention points | | Recommendations |
|---|---|---|
| 1 Attention Point Data Protection | EMSA should conduct a DPIA with consultation with the EDPS prior to the start of the upgraded SSN. | This attention point should be addressed in the Information Security Management System (ISMS) for SSN. |
| 2 Attention Point Data Protection | Both EMSA and Member States operate as data controller of their respective SSN systems, so they are co-controllers for the SSN data cycle. Therefore, a clear data protection statement with the attribution of roles will be part of the upgraded SSN Security Guidelines. This statement will also include the minimum requirements in terms of data protection. In order to support awareness across SSN stakeholders, it is advisable to host a workshop on data protection topics for SSN. | The implementation of a Privacy Information Management System (PIMS) in alignment with ISO/IEC 27701:2019 (PETA_1) provides a technical option addressing data protection for the SSN. PETA_1 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. |

# Interoperability

| Interoperability protection gaps and attention points | | Recommendations |
|---|---|---|
| 1 Gap Interoperability | Points of attention/gaps were identified with regard to the applicable network and information security standards, in line with the Security gaps above. | This gap should be addressed by implementing an Information Security Management System (ISMS) for SSN. |
| 2 Gap Interoperability | Without a consistent involvement from key SSN stakeholders on security-related aspects of the system, there is a risk of misalignment of security baselines between EMSA and the MSs, and also of inadequacy of deployment of 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. | Security and interoperability topics should be addressed through specific agenda items of the SSN group and when necessary of the HLSG. |
| 1 Attention Point Interoperability | 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 identifies guidelines for interoperability. These guidelines and recommendations should not introduce new requirements for SSN in addition to the relevant technical standards. However, they should specify how those requirements should be met for the purpose of establishing robust and stable interoperability arrangements with the Member States. | Security and interoperability topics should be addressed through specific agenda items of the SSN group and when necessary of the HLSG. |

# Security

| Security gaps and attention points | | Recommendations |
|---|---|---|
| 1 Gap Security | 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". | This gap should be addressed by updating the 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. |
| 2 Gap Security | Central SSN does not have its own controls for authorization of users but does 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 its 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. | A federated IAM adopting third-party authentication is recommended. It should comply with Art. 12 of the EMSWe Regulation that requires a common user registry and access management, federated user management and EU-level monitoring. |
| 3 Gap Security | 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 relate to SSN archiving practices of operational records, e.g. records, logs, and incident reports that may contain personal data or commercial data. | A tailored data storage solution for archiving based on commercial solutions provides a suitable technical option for implementing digital archiving strategies in the context of SSN. |

# Project Status

- **Task 1 and Task 2 Interim Reports were presented to the project's steering committee and approved on 23 October 2019**

- **Task 3 and Task 4 Interim Reports were presented to the project's steering committee and approved on 2 April 2020**

**emsa.europa.eu**

twitter.com/emsa_lisbon

facebook.com/emsa.lisbon

EMSA

European Maritime Safety Agency