Input paper: [[1]](#footnote-1) ENG16-n.n.n

Input paper for the following Committee(s): check as appropriate Purpose of paper:

**□** ARM **X** ENG **□** PAP **X**  Input

**□** ENAV **□** VTS **□** Information

Agenda item [[2]](#footnote-2) n.n

Technical Domain / Task Number 2 n.n

Author(s) / Submitter(s) Héctor Llorca (GMV), Antonio R. Martín (GMV), Marcos López (GMV), Philipp Scheidemann (EUSPA).

OSNMA Implementation on Maritime GNSS Receiver

# Summary

GNSS systems have spread in the maritime sector for positioning and navigation purposes. However, its users are exposed to possible cyber-attacks that may lead to devastating consequences. That is where OSNMA plays a role, in Galileo constellation, providing a solution based on signal authentication to try to detect malicious signals and avoid them, keeping the navigation safe. EUSPA’s ASGARD project proposes its solution and leaves some other examples in which the use and raise of OSNMA is brought to light.

This document aims at presenting OSNMA, its benefits and utilities in a maritime receiver perspective.

For further information about the project please check [1], or contact Marcos López (GMV, [malopez@gmv.com](mailto:malopez@gmv.com)) and Philipp Scheidemann (EUSPA, Philipp.Scheidemann@euspa.europa.eu).

# Purpose of the document

The objective of this paper is to make IALA ENG Committee members aware of the raise of the OSNMA service that helps to improve safety during navigation. Particularly, in the maritime field, it helps to avoid some cyber-attacks in which vessels may be involved. From the EUSPA´s ASGARD project, currently under development by GMV-led consortium, it is also provided a proposal of implementation for this purpose. Furthermore, some other real examples are provided, in order to make the reader aware of the current status of the OSNMA service.

# Introduction and objectives

GNSS systems are widely used in the maritime sector. Over time, this technology has gained acceptance as the preferred positioning system. This has led to the fact that GNSS technology is now widespread for both navigation (SOLAS and non-SOLAS vessels, inland waterways) and positioning (traffic management and surveillance, Search and Rescue, fishing vessels control, port operations or marine engineering) applications in the maritime domain.

The International Maritime Organization (IMO) is a United Nations specialized agency, established in 1948, focused on shipping. One of its main activities is to create international regulations and recommendations of maritime safety and security and efficiency of navigation. In relation to GNSS, the most relevant IMO standards are the A.915(22) and the A.1046(27) resolutions.

Resolution A.915(22) establishes the minimum maritime user requirements for general navigation, gathered in Table 1. It can be seen how these requirements set reference values for characteristics of, among others, accuracy, integrity, availability, and continuity. These performance standards are undoubtedly essential for receiver characterization, but, for the moment, there has not been much progress in terms of regulations to standardize the protection against deliberate interferences as jamming and spoofing.

**Table 1** Minimum Maritime User Requirements for General Navigation. [2]

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | System level parameters | | | | Service level parameters | | | |
|  | **Absolute**  **Accuracy** | **Integrity** | | | **Availability % per**  **30 days** | **Continuity % over**  **3 h** | **Coverage** | **Fix interval**  **(s)** |
|  | **Horizontal**  **(m)** | **Alert limit**  **(m)** | **Time to**  **alarm**  **(s)** | **Integrity**  **risk**  **(per 3 h)** |
| Ocean | 10 | 25 | 10 | 10-5 | 99.8 | N/A | Global | 1 |
| Coastal | 10 | 25 | 10 | 10-5 | 99.8 | N/A | Global | 1 |
| PARW † | 10 | 25 | 10 | 10-5 | 99.8 | 99.97 | Regional | 1 |
| Port | 1 | 2.5 | 10 | 10-5 | 99.8 | 99.97 | Local | 1 |
| IW ‡ | 10 | 25 | 10 | 10-5 | 99.8 | 99.97 | Regional | 1 |

† Port approach and restricted waters.

‡ Inland waterways.

## Vulnerabilities and Spoofing Attacks

During many of the activities performed by vessels it is commonly possible to be under the influence of interference. The GNSS signals that reach the ground are very low power, so there are many sources that can interfere with the correct reception of these signals. Many of these sources of interference are unintentional, although there are also others that are created maliciously. Particularly, it is possible to generate signals that mimic GNSS signals with the intention of pretending them to be genuine signals. This type of attack is known as spoofing and, in recent years, has been a problem in navigation, especially near conflict zones. In fact, IALA provided a list of sources of vulnerability, including a list of good practices to avoid them [3].

Some of the maritime spoofing events that have been reported in recent years have been in the Black Sea in June 2017 [4], in eastern China in October 2018, in the Strait of Hormuz in July 2019, and in the Galapagos in July 2020 [5]. These attacks have increased recently after the start of the Russian and Ukraine conflict in 2022, in the zones of Kaliningrad, Eastern Finland, Black Sea and Eastern Mediterranean, as well as Northern Iraq [6]. It can be observed that spoofing attacks in the maritime field have been recurrent in recent years and, therefore, the interest in having countermeasures is becoming increasingly important. In addition, trends indicate that autonomous vessels are being pursued. These vessels are intended to use GNSS systems as one of their main sources to enable autonomous navigation, so such an attack would be even more relevant in these cases.

One of the manners to improve the robustness of receivers is through redundancy, as recommended in [7]. It is important to have in mind current approaches to improve robustness and focused on taking advantage of updates and improvements itself of GNSS at signal and system level. Originally, all the used GNSS receivers were single frequency. However, the development of GNSS receivers capable of working with more frequencies allowed eliminating errors and having more accurate measurements. Another interesting approach is to use more GNSS constellations. For example, processing GPS and Galileo information increases the number of available satellites and enhances accuracy, availability, and resilience against some attacks.

Additionally, one of the forms of defencing against these weaknesses in GNSS-based navigation, which has been increasing in importance in recent times, is through cybersecurity. By means of an authentication system it is possible to validate information coming from the satellite navigation message in order to have greater confidence in the authenticity of the message. Within the Galileo Open Service, a new data authentication functionality has been developed for users around the world called Open Service Navigation Message Authentication (OSNMA) [8]. Furthermore, this is not the unique solution that can be found. Some other vessels use the Public Regulated Service (PRS), restricted to government-authorised users, intended for sensitive applications that may require a higher level of service continuity. By default, this service is more resistant to spoofing and jamming due to its encrypted signal [9].

# OSNMA FUNDAMENTALS

The GNSS satellites continuously transmit navigation signals in two or more frequencies in L band. These signals contain ranging codes and navigation data to allow the users to compute the travelling time from satellite to receiver and the satellite coordinates at any epoch. One of the main signal components is the Navigation Data, which is a message providing the information on the satellite ephemeris, almanacs, satellite health status and some other information [10]. With this information from each satellite, the PVT solution can be computed. If this information was inaccurate, the PVT solution may not be computed with the desirable precision level.

Among the GNSS systems, Galileo is the European one, providing a highly accurate, guaranteed global positioning service under civilian control. Currently providing Initial Services, Galileo is interoperable with other constellations. By offering multi-frequency as standard, Galileo is set to deliver real-time positioning accuracy down to the metre range. The current Galileo constellation consists of 28 satellites (currently 23 active, [11]), positioned in three low-eccentricity Medium Earth Orbits (MEOs) at 23222 km altitude, with an inclination of 56 degrees to the equator [12].

Inside the Galileo services, the Galileo Open Service (OS) is providing a Navigation Message Authentication (NMA) capability. This allows the users to confirm that received Galileo Open Navigation Data was originated from the Galileo system and has not been modified by any other source. Galileo is the first constellation to provide this service, which is currently in the public test phase, free of charge for users worldwide. Due to its early state, there are very few receivers that have this functionality available despite the fact that, in the maritime sector, it is considered a functionality of great importance.

The authentication protocol is based on the Time Efficient Stream Loss-Tolerant Authentication (TESLA) protocol, specifically adapted for Galileo's open service. This protocol introduces a digital signature in the Galileo I/NAV message and transmits with some delay the key to authenticate the message. The key to authenticate the message is known in advance by the user and is transmitted in the reverse order in which it was generated. The same key is used for all satellites, which allows validation of data transmitted by other Galileo satellites.

To guarantee the security of the TESLA protocol and guarantee the authenticity of the data, the receiver must ensure it has received the navigation data before the corresponding TESLA chain key is disclosed by the system. This implies that the receiver must be synchronised with a given accuracy to the Galileo System Time (GST) before receiving and processing OSNMA information [13].

The principle of work of OSNMA also provides the possibility to authenticate satellites which do not transmit OSNMA data with the data retrieved from satellites transmitting OSNMA, referred to as cross-authentication. Currently, OSNMA is only transmitted on up to twenty satellites. The intention of this is to reduce the computation and communication overhead, as well as to increase the availability and robustness to data loss of the service.

Diagram, schematic

Description automatically generatedDiagram, schematic

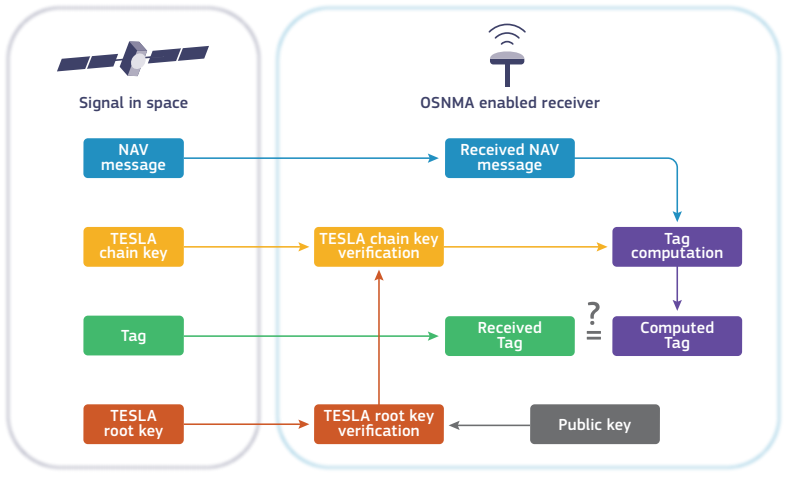
Description automatically generated

**Figure 1** OSNMA Scheme [8]

# OSNMA Solution for the receiver

At the receiver level, the process to authenticate navigation data is as follows (Processing logic represented in Figure 2):

1. The navigation data that includes the OSNMA information is received. Specifically, a tag is obtained, which will be used for the authentication of the navigation data, the TESLA root key and the TESLA chain key.
2. By using a public key, which is previously stored and available in the receiver, the TESLA root key is authenticated.
3. The TESLA chain key is then authenticated by using the TESLA root key or with a previously authenticated TESLA chain key.
4. Once the TESLA chain key is authenticated, it is used, together with the navigation data obtained, to locally generate a tag.
5. The locally generated tag is compared with the tag obtained from the navigation data. If both tags match, the navigation data is considered authentic.



**Figure 2** OSNMA receiver processing logic [14]

Within the ASGARD project, funded by the European Union Agency for the Space Programme (EUSPA), a multi-constellation, multi-frequency maritime receiver capable of processing OSNMA information is being developed at its last stages. By the date of the publication of this paper, the OSNMA service is still in test phase with already Signal-In-Space (SIS) [15]. In this context, as a future characteristic the intention is to be able to perform even cross-check within other constellations. However, during the current test phase it is not possible to use the multi-constellation mode while using OSNMA service.

# Maritime OSNMA TESTBED

In the maritime context, EUSPA and the Joint Research Centre (JRC) performed a laboratory testing campaign during 2018-19. The objective of this campaign was to help manufacturers with the implementation of Galileo in maritime shipborne receivers as well as checking compliance with standards in the International Maritime Organisation (IMO) and the International Electrotechnical Commission (IEC). The testing campaign aimed at maritime receiver manufacturers looking for independent assessment of Galileo implementation into their products and assistance with any issues linked to this implementation [16]. After this campaign, in 2022, EUSPA is also going to provide Test Vectors in order to analyse the receiver capabilities to support different OSNMA configurations and to test the public key and TESLA chain management processes [17].

Some European projects tested, using real signal data, situations where OSNMA could be tested. The RIPTIDE project [18] would be an example of this, in the ESA NAVISP programme. Its main goal is to establish a first phase in the development of a resilient PNT solution dedicated to the particularities of the Black Sea and Danube Lower Basin region. In this project, field trials in maritime environment have been performed to collect data checking for existing spoofing situations, to emulate GNSS attacks and provide a clear view of the impact at user and authority level. Several types of GNSS receivers have been tested against spoofing and jamming threats in maritime environment as part of this project. The RIPTIDE proposed approach towards resilient PNT includes OSNMA as one of the technological pillars.

In the aviation field, the AIRING project [19] addressed resilience of aviation operations to GNSS frequency jamming and cyber threats (i.e., spoofing or meaconing attacks done via a GNSS signal generator). Also, AIRING project assessed the threats on GNSS signals and resulting risks for civilian flights. Nevertheless, the project also considered whether the proposed strategies are applicable to other non-aviation domains, as the maritime one.

Finally, for those stakeholders who may be interested in testing OSNMA services, some governmental agencies [20] are allowing to perform real spoofing testing campaigns outdoors, restricted to regulated zone and a notified data. This represents another option to test the receiver with real signal in order to check the functionality of the OSNMA service. Despite these tests are not carried in maritime field due to logistics, positive results taken from them would be applicable to a receiver installed in a shipborne subjected to similar attacks.

# OSNMA VERIFICATION PLAN

Once the OSNMA functionality has been implemented in the receiver, it is important to test that it works as expected. In this context, several validation campaigns can be planned. On the one hand, in order to certify that the receiver complies with the current International Electrotechnical Commission (IEC) standard for GNSS receivers, a testing campaign can be carried out. On the other hand, some other testing can be performed based on spoofing campaigns to assess the behaviour of the receiver when facing this type of attack. This type of campaign needs to be defined ad-hoc since currently, there is no standardization at IMO/IEC level for OSNMA.

The main goal when testing the receiver with OSNMA functionality is to verify that it is capable of properly detecting and alerting on the possibility of a spoofing attack. A manner to perform a test is to leave the receiver to authenticate, and then it is expected to navigate stably with authenticated navigation data. Later, a spoofing attack could be introduced, expecting that, in a few minutes, a satellite that was previously authenticated loses the authenticated status, meaning that is probable that the receiver is under cyber-attack. The strategy will make the receiver display an alert message warning about the situation. Very often the attacker is not able to fill OSNMA broadcasted data using fake or replied data. In this case the fact we are not receiving OSNMA data in a reasonable period of time (few minutes) can be already interpreted as evidence of an attack. Finally, if the attack ceases, it is expected that the receiver can re-authenticate the navigation data and return to displaying a safe state for navigation.

# CONCLUSIONS

The OSNMA functionality is seen as a good option to improve safety in maritime navigation. The possibility of authenticating the navigation message increases the confidence in the genuineness of the signal processed by the receiver. Although OSNMA is not a spoofing detection system *per se*, it lets, by thinking a good strategy, to identify possible evidence denoting an attack.

The times selected to alert of the possible attack are reasonable times within the context of ocean navigation. In cases of port navigation, notice times may be somewhat higher than necessary. It must be considered that the IEC standard establishes a maximum of 10 seconds as the alarm time for integrity problems (as shown in Table 1). This cannot currently be achieved using only OSNMA as currently defined. Therefore, the functionality of OSNMA should be understood as an extra support for navigation, but never as an alarm system such as a RAIM or loss of position alarm.

Currently the OSNMA system is still in the testing phase and some of the planned functionalities are not yet available in the SIS. For example, it is not possible cross-authenticate other constellations like GPS. This means that, at the moment, OSNMA authenticated navigation is restricted to Galileo satellites.

It is also possible to think of solutions that complement OSNMA by using other authentication systems such as the Chimera GPS system. Some solutions are already being proposed in the community that allow combining both authentication systems to improve robustness in multi-constellation receivers [21].

# References

|  |  |
| --- | --- |
| [1] | M. Cueto, G. Cueto, M. López and P. Scheidemann, “Advanced Shipborne Galileo Receiver Double Frequency (ASGARD): objective, activities and expected added value,” in *IALA ENG15 - Committee*, 2022. |
| [2] | IMO, *Revised maritime policy and requirements for a future global navigation satellite system (GNSS),* IMO, 2001. |
| [3] | IALA, “R0129 - GNSS Vulnerability and Mitigation Measures,” IALA - AISM, Saint Germain en Laye, France, 2012. |
| [4] | M. Jones, "Spoofing in the Black Sea: What really happened?," 11 October 2017. [Online]. Available: https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/. |
| [5] | A. Androjna, M. Perkovič and I. Pavić, “CYBER SECURITY CHALLENGES FOR SAFE NAVIGATION AT SEA,” *Technologies, Techniques and Applications Across PNT,* pp. 47-61, 2021. |
| [6] | EASA, “Safety Information Bulletin - Global Navigation Satellite System Outage Leading to Navigation / Surveillance Degradation,” EASA, 2022. |
| [7] | IMO, *Performance Standards for Multi-System Shipborne Radionavigation Receivers,* 2015. |
| [8] | EUSPA, *Galileo Open Service Navigation Message Authentication (OSNMA),* 2021. |
| [9] | EUSPA, “PRS - the future is bright,” EUSPA, 23 April 2019. [Online]. Available: https://www.euspa.europa.eu/newsroom/news/prs-future-bright. [Accessed September 2022]. |
| [10] | ESA, “GNSS signal - Navipedia,” ESA, 2011. [Online]. Available: https://gssc.esa.int/navipedia/index.php/GNSS\_signal. [Accessed September 2022]. |
| [11] | EUSPA, “Constellation Information | EUSPA,” EUSPA, [Online]. Available: https://www.gsc-europa.eu/system-service-status/constellation-information. [Accessed September 2022]. |
| [12] | ESA, “ESA - What is Galileo?,” ESA, [Online]. Available: https://www.esa.int/Applications/Navigation/Galileo/What\_is\_Galileo. [Accessed September 2022]. |
| [13] | European Union, *OSNMA Receiver Guidelines for the Test Phase,* 2021. |
| [14] | EUSPA, *Galileo OSNMA: Join the Public Observation Test phase and share your feedback!,* EUSPA, 2022. |
| [15] | European Union, *Galileo Open Service Navigation Message Authentication (OSNMA) User ICD for the Test Phase,* 2021. |
| [16] | EUSPA, “GSA and JRC launch test for maritime receivers,” EUSPA, 03 October 2018. [Online]. Available: https://www.euspa.europa.eu/newsroom/news/gsa-and-jrc-launch-test-maritime-receivers. [Accessed September 2022]. |
| [17] | EUSPA, *1st Galileo OSNMA Public Observation Workshop,* EUSPA, 2022. |
| [18] | ESA, “ESAs NAVISP Programmes - 006 - RIPTIDE,” ESA NAVISP, 15 April 2020. [Online]. Available: https://navisp.esa.int/project/details/110/show. [Accessed September 2022]. |
| [19] | National Land Survey of Finland, “AIRING – Aviation Resilience to GNSS Frequency Jamming and Cyber Threats,” National Land Survey of Finland, 21 March 2021. [Online]. Available: https://www.maanmittauslaitos.fi/en/research/airing-aviation-resilience-gnss-frequency-jamming-and-cyber-threats. [Accessed September 2022]. |
| [20] | INTA, “INTA - Home,” INTA, [Online]. Available: https://www.inta.es/INTA/en/index.html. [Accessed September 2022]. |
| [21] | B. Motella, M. Nicola and S. Damy, “Enhanced GNSS authentication based on the joint CHIMERA/OSNMA scheme.,” *IEEE Access,* pp. 9, 121570-121582, 2021. |
| [22] | IMO, *Revised report on the study of a worldwide radionavigation system,* IMO, 2011. |
| [23] | European Union, *Galileo - Open Service - Service Definition Document,* 2021. |

# Action requested to the Committee

The Committee is requested to:

1. Note the information within this paper,
2. To have the opportunity of briefly presenting this paper to the ENG16 WG3 or Committee, and to discuss the matter at an appropriate time and
3. Include the proposed into the IALA documentation if so, considered by the discussion.

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-1)
2. Leave open if uncertain [↑](#footnote-ref-2)