**Input paper:** DTEC5-6.2.2.13

**Input paper for the following Committee(s):** **Purpose of paper:**

(Select as appropriate)

ARM  ENG  PAP  Input

DTEC VTS  Information

**Agenda item** 6.0

**Technical domain/ Task number** 2 …………………………………

**Author(s)/Submitter(s)** **GSC / EUSPA**

(European GNSS Service Centre /

European Union Agency for the Space Programme)

GNSS AUTHENTICATION AS AN EMERGING DIGITAL TECHNOLOGY AND POTENTIAL APPLICATIONS WITH VDES.

# Summary

This paper presents the main characteristics of Galileo OSNMA (Open Service Navigation Message Authentication) as an emerging digital technology for maritime navigation.

The increasing number of GNSS (Global Navigation Satellite System) interference is affecting the navigational capability of ships, resulting in disruptions to maritime operations and risk of collisions and groundings.

Additionally, the mentioned events may lead to reduced radiocommunication capability, as GNSS is a supporting infrastructure that provides the precise positioning and timing required in VDES (VHF Data Exchange System).

OSNMA can provide GNSS authentication in maritime navigation. As a protection layer, OSNMA supports the position, navigation and timing (PNT) of the vessels, besides their VDES communications.

Some potential applications of OSNMA, where VDES communications are available between shore and ship, are also presented.

## Purpose of the document

The document seeks to:

* Present to IALA DTEC Committee the status and benefits of Galileo OSNMA to fulfil the role of GNSS authentication.
* Promote the performance of OSNMA for maritime navigation and communications, that supports PNT of vessels and position reporting with VDES.
* Highlight the opportunity to engage VDES transceivers and OSNMA receivers to provide more resilient performance.
* Promote the GNSS authentication alongside the VDES authentication, as both protections layers are needed in the maritime operations, particularly in conflicting areas.
* Encourage the Committee to assess the feasibility to amend standards, guidelines or recommendations.

## Related documents

* IALA G1117. VHF DATA EXCHANGE SYSTEM (VDES) OVERVIEW.
* IALA G1158. VDES R-MODE.
* IALA G1180. RESILIENT POSITION, NAVIGATION AND TIMING (PNT).
* IALA G1192. VDES AUTHENTICATION TECHNIQUES.
* “PROPOSAL FOR DEVELLOPPING A GUIDELINE FOR EXCHANGING GNSS INTERFERENCE DATA FOR NAVIGATIONAL SAFETY”, presented in the IALA DTEC4, WG3, by FinTraffic.
* IMO. NCSR12/9. Report of the Correspondence Group on VDES. Development of amendments to SOLAS chapters IV and V and performance standards and guidelines to introduce VDES.

# Background

In May 2025, three United Nations agencies, one of them the IMO, called for action to halt GNSS interferences, which are most often associated with state operations in the Baltic, Black Sea, Strait of Hormuz, South China Sea and Western Pacific.

Jamming causes loss of the GNSS signals, affecting the navigational capability, resulting in disruptions to maritime operations. Spoofing can mislead vessels, raising the risk of collisions and groundings. Additionally, both jamming and spoofing may lead to reduced radiocommunication capability, due to the loss of time synchronization.

Previously, the IMO Maritime Safety Committee had urged Member States to take actions against GNSS interferences, like minimizing unintentional events, issuing warning notices to mariners about periods and areas impacted by any detected interference, and counteracting unauthorized transmissions on GNSS frequencies.

In June 2025, thirteen Member States of the European Union called on the European Commission to respond to interference with GNSS. Jamming and spoofing events have been observed in the Baltic Sea Region, being a threat to various modes of transport, particularly civil aviation and maritime navigation. Thousands of occurrences are detected every month.

In recent years, GNSS interferences have become a major challenge, severely impacting the maritime industries. During 2024, the rate of incidents increased almost threefold, compared with previous year. The situation is worse in 2025.

Spoofing events are likely behind accidents at sea. Some examples are groundings in the Baltic Sea in December 2024 (bulk carrier Meghna Princess), and the Red Sea in May 2025 (container ship MSC Antonia). As well as a collision between two ships that caught fire in the Gulf of Oman in June 2025 (crude oil tankers Front Eagle and Adalynn).

On the other hand, as stated in the IALA guideline G1192, for VDES authentication techniques, GNSS is a supporting infrastructure that provides the precise positioning and timing required for VDES operation. In such a way that a GNSS interference can disrupt accurate transmission timing within the VDES time frame structure and prevent accurate position reporting by VDES equipped vessels.

Galileo OSNMA can play a role in maritime navigation, through the authentication of the navigation data. This protection layer supports not only the PNT in GNSS, but also the VDES communications.

In fact, the mentioned guideline identified attack vectors relevant to VDES, like jamming, spoofing and meaconing, that are analogous to the equivalent GNSS interferences. That is why the guideline presents the GNSS authentication techniques as an example to follow for the authentication of VDES communications.

# Discussion

Galileo OSNMA is an authentication service free of charge provided for Galileo satellites, with the positioning accuracy of the Galileo Open Service (OS), in the single frequency mode (E1). It has been declared operational by EUSPA in July 2025. Previously, it was running in test mode, with several manufacturers and receivers already in the market at that moment.

OSNMA authenticates samples of the navigation data that are used to compute the position, velocity and timing (PVT) at the receiver. Specifically, OSNMA authenticates the navigation message (I/NAV) of the Galileo OS in the data component of the frequency (E1-B).

Galileo is the first constellation able to provide an authentication function globally through the SIS (Signal in Space). OSNMA provides this authentication at data level also by terrestrial means (IDD, Internet Data Distribution).

Authentication data are transmitted in 40 bits of odd pages of navigation message (NM). OSNMA receivers can use these bits for the authentication process. While standard Galileo OS receivers can ignore the dedicated fields of I/NAV.

Authentication data are generated on the OSNMA server (GSC) and transmitted to some satellites for broadcast. This is a self-authentication process. Satellites which do not transmit OSNMA data can have their NM authenticated, with the data retrieved from satellites transmitting OSNMA. This is called cross-authentication.

OSNMA provides asymmetric authentication with loose time synchronization. OSNMA authentication uses public keys, Merkle trees, digital signatures, TESLA chain keys and crypto functions:

* Public key + Merkle tree. The Merkle tree is used to organize public keys. The idea is to iteratively call hash function, to check the received nodes against the calculated nodes, from the public key to the tree root. OSNMA uses the Merkle tree to verify the public key.
* Public key + Digital signature. A digital signature is an example of an asymmetric cryptographic protocol. Signing each data packet provides secure broadcast authentication. But it is expensive in terms of time and computing. OSNMA uses digital signatures only in one step, to verify the TESLA root key.
* TESLA protocol (Timed Efficient Stream Loss-tolerant Authentication). Broadcast authentication can be provided to the receiver using symmetric cryptography like MACs (Message Authentication Codes), based on the delayed disclosure of keys by the sender. In TESLA the sender attaches to each packet a MAC computed with a key. The receiver buffers the received packet, but it is unable to authenticate it. Provided that the receiver has synchronized its clock with the sender, a short time later, the sender discloses the key, and the receiver can authenticate the packet.

The European GNSS Service Centre (GSC) is responsible for the publication of the OSNMA crypto material: the public key, the Merkle tree root and associated certificates.

The OSNMA process is a five-step process. The user equipment receives the navigation data and the corresponding OSNMA data: tag, TESLA chain key and TESLA root key. The tag will authenticate the navigation data associated and transmitted before. The five steps are as follows:

* The public key, that shall be available at the receiver, is verified with the Merkle tree, checking the nodes, received and computed, up to the root.
* The TESLA root key is authenticated by means of its digital signature using the public key.
* The receiver verifies the TESLA chain key with the TESLA root key, or with a previously authenticated key from the TESLA chain.
* The receiver computes locally the tag with the verified TESLA chain key and a number of bits of the navigation data. The tag is received before its associated TESLA chain key.
* The receiver checks whether the computed tag is equal to the received tag. If the result of all these steps is successful, the user shall consider the navigation data as authentic. Then the receiver computes the position, and the Galileo OS performance is achieved.

## USE OF GNSS AUTHENTICATION BEFORE REPORTING

In the report of the Correspondence Group about the amendments of standards and guidelines to introduce VDES, in the NCSR 12/9 of IMO, at the point about integrity and authentication requirements (7.2), a recommendation is proposed: “VDES should be capable of providing authentication of position reports”.

On the other hand, the IALA guideline G1192, for VDES authentication techniques, was approved by the Council in June 2025. It is the first IALA document to include a detailed solution for authentication of the AIS message using VDES. This guideline introduces cryptographic authentication for VDES, addressing the problem of data authenticity in AIS. The first edition is focused on safety-critical transmissions like Virtual AtoN (Aids to Navigation) reports.

On the Galileo side, one previous step could be to use OSNMA for authentication of positioning before the position report is sent. In this way a double authentication could be achieved, for the positioning first and for the report later, to avoid sending an authenticated report with information that can be false.

This operational mode could be applicable, at least, in conflict areas where GNSS jamming and spoofing are suspected of being behind different events (e.g.: track diversion, grounding, ships collision), that unfortunately can be found more often every week in the news. This proposal is linked with the following one.

## GNSS AUTHENTICATION IN AREAS OF GNSS INTERFERENCE

In the “PROPOSAL FOR DEVELLOPPING A GUIDELINE FOR EXCHANGING GNSS INTERFERENCE DATA FOR NAVIGATIONAL SAFETY”, presented in the IALA DTEC4, WG3, by FinTraffic, a standard method was proposed to exchange GNSS interference data between vessels and shore, to improve the maritime safety.

The final report of the working group from the meeting cited this proposal in relation to a future update of the IALA guideline “G1158 VDES R-MODE”. The operation, in case of GNSS interference, is supposed to be reporting the event and changing the navigation mode to the R-mode of VDES.

On the Galileo side, one previous step could be to use OSNMA before stopping using GNSS. If the authentication of the navigation messages is successful, then the Galileo Open Service performance is available for secure navigation.

## USE OF GNSS AUTHENTICATION for records in accident investigation

During the Maritime and IWW (Inland WaterWays) session in the UCP 2024, the User Consultation Platform organized by EUSPA, concerns were raised about growing international uncertainties and GNSS interferences. Therefore, efforts to enhance the resilience of PNT services are gaining importance, and authentication has become a key user requirement for vessels navigation and tracking. Galileo OSNMA is expected to be a key component to meet this market demand.

On this point, the EMSA (European Maritime Safety Agency) presented the need for risk analysis and mitigation in case of jamming and spoofing.

Additionally, authentication was identified in the UCP as a key element in the case of accident investigation, as part of a resilient PNT. Without positioning authentication, the records to be used during the investigation could be questioned by the insurance company.

Galileo OSNMA can be a safety measure and a security layer for maritime navigation. In such a way that in case of accident the OSNMA records, when they are available, can be used to determine during the investigation the reliable position of the ships involved.

# References

* Galileo Open Service Navigation Message Authentication (OSNMA) Service Definition Document (SDD).

<https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-OSNMA-SDD_v1.0.pdf>

* Galileo OSNMA Receiver Guidelines.

<https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_Receiver_Guidelines_v1.3.pdf>

* Galileo OSNMA Info Note.

<https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_Info_Note.pdf>

* ITU-ICAO-IMO letter and joint statement on protection of the radio navigation satellite service from harmful interference. 17th March 2025.
* IMO. Maritime Safety Committee. MSC.1/Circ.1644. Deliberate interference with GNSS. 18th October 2021.
* EUSPA. Report on Maritime and Inland Waterways, User Needs and Requirements, 2024.

# Action requested of the Committee

The Committee is requested to take note and action as appropriate to:

* Consider Galileo OSNMA as an emerging digital technology for the maritime domain.
* Assess the potential applications of OSNMA with VDES communications.
* Consider promoting workshops or tests with shipping companies and VDES manufacturers.
* Amend the IALA publications if applicable.