**Input paper:** DTEC5-6.2.3.12

**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)

Proposal for amendmentS to CHAPTERS on GNSS AUTHENTICATION of IALA Guidelines G1117 and G1180.

# Summary

This paper presents two proposals for amendment to IALA guidelines G1117 and G1180, in the chapters about GNSS (Global Navigation Satellite System) authentication. The reason is to update the contents to novelties like Galileo OSNMA (Open Service Navigation Message Authentication), following an action from DTEC4.

OSNMA can provide GNSS authentication in maritime navigation. GNSS is a supporting infrastructure that provides the precise positioning and timing required in VDES (VHF Data Exchange System). Hence OSNMA is a protection layer not only for the navigational capability of ships, but also for their radiocommunication capability.

## Purpose of the document

The document seeks to:

* Present to IALA DTEC Committee a proposal for amendment to IALA guideline G1117 chapters on GNSS authentication, following the action item 46 in the report of the committee, after Working Group 3 meetings, at DTEC4.
* Highlight the opportunity to amend the chapters on GNSS authentication of IALA guideline G1180, aligning the document with the G1117 and updating the contents to technical novelties.

## Related documents

* IALA G1117. VHF DATA EXCHANGE SYSTEM (VDES) OVERVIEW.
* IALA G1180. RESILIENT POSITION, NAVIGATION AND TIMING (PNT).
* IALA G1192. VDES AUTHENTICATION TECHNIQUES.

# Background

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 a GNSS authentication function globally.

During the Working Group 3 meetings, at DTEC4 in March, concerns were raised about the GNSS augmentation section, where Galileo OSNMA is cited (point 3.4.2).

As a result, in the report of the committee, action item 46 invites committee members *‘to propose amendments to the IALA Guideline G1117 chapter on GNSS for the DTEC5 to provide more structure and overview of the different helping technologies for GNSS and how the architecture on shore and ship would need to look like to consume them. This change could include the proposed changes by ESSP, EUSPA and CML’*.

The authentication is also cited, for example, in relation to the authentication of position reports (point 3.2.1), and the secure ship reporting (point 3.7.4).

On this point, Galileo OSNMA can be used for authentication of positioning before the position report is sent with VDES authentication. In this way a double authentication can 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 interferences are suspected of being behind an increasing number of events (e.g.: track diversion, grounding, ships collision).

As presented 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 (points 4.1 and 4.2).

Additionally, the mentioned guideline identifies 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.

In this regard, Galileo OSNMA can play a role in maritime navigation, through the authentication of the navigation data. This protection layer supports not only the position, navigation and timing (PNT) in GNSS, but also the VDES communications.

In the case of the IALA Guideline G1180, about resilient PNT, authentication is presented as part of the GNSS service infrastructure (point 5.1.1), that includes the space segment and the ground segment. OSNMA is briefly presented with a text and a reference that should be updated and improved, after the service declaration. The information about the dual frequency services (a table with the status of core GNSS signals as of May 2023) is also out of date. From the user segment side (point 5.1.2.5), authentication is presented through the authentication of the navigation message, which is verified by the receiver. Galileo is cited without an explicit reference to OSNMA.

# Discussion

The IALA guideline G1117 (VDES) third edition dates from December 2022. The IALA guideline G1180 (resilient PNT) first edition is dated in December 2023. Both documents include old texts about GNSS authentication that could be corrected and improved. Two proposals are presented in the next points.

The new IALA guideline G1192 (VDES authentication techniques) first edition dates from June 2025. There is an indirect reference to Galileo OSNMA through a reference to guideline G1180. A direct reference, with citation of the main documents, could be included in the next edition, when it is applicable, to better disseminate the details of GNSS authentication techniques.

## Update of IALA guideline G1117 with GNSS AUTHENTICATION contentS

In the point ‘3.4.2. SCENARIO - BROADCASTING GNSS AUGMENTATION DATA’ a couple of paragraphs could be added at the end:

***‘As presented 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. GNSS interference can disrupt accurate transmission timing within the VDES time frame structure and prevent accurate position reporting by VDES equipped vessels. The guideline identifies attack vectors relevant to VDES, like jamming, spoofing and meaconing, that are analogous to the equivalent GNSS interferences.***

***GNSS authentication can play a role in maritime navigation. This protection layer supports not only the PNT in GNSS, but also the VDES communications. GNSS authentication is provided by Galileo OSNMA, as a free of charge service, with the positioning accuracy of the Galileo Open Service (OS), in the single frequency mode (E1). OSNMA authenticates samples of the navigation data that are used to compute the position, velocity and timing at the receiver.’***

As an alternative, the above two paragraphs could be moved at the end of the point ‘3.2.1. SCENARIO - AUTHENTICATION FOR POSITION REPORTS’.

In the point ‘3.7.4. SCENARIO - SECURE SHIP REPORTING’ a second paragraph could be added:

***‘GNSS authentication, provided by Galileo OSNMA, can be used for authentication of positioning before the position report is sent with VDES authentication. A double authentication can 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 interferences are suspected of being behind of track diversions, groundings and ships collisions in some cases.’***

## Corrections of IALA guideline G1180 with new GNSS AUTHENTICATION documents

In the point ‘5.1.1. SERVICE INFRASTRUCTURE’ the following paragraph and its reference are out of date:

*‘The European GNSS service, Galileo, plans to provide a mechanism to authenticate the open navigation signals on the E1 band (i.e. Open Service - Navigation Message Authentication (OS-NMA)) [32]. The authentication is done by adding a digital signature to the unencrypted navigation message, allowing receivers to verify that the signal is coming from a trusted source and making signal spoofing more difficult. OS-NMA is an additional feature and does not impact legacy receivers.*

*[32] ESA. Navipedia: Galileo Open Service Navigation Message Authentication.* [*https://gssc.esa.int/navipedia/index.php/Galileo\_Open\_Service\_Navigation\_Message\_Authentication*](https://gssc.esa.int/navipedia/index.php/Galileo_Open_Service_Navigation_Message_Authentication)*.’*

The above paragraph is proposed to be amended as follows:

***‘The European GNSS service, Galileo, provides the OSNMA (Open Service Navigation Message Authentication) to authenticate the navigation message of the Galileo Open Service (OS) in the data component of the E1 frequency. The service provides asymmetric authentication with loose time synchronization, using public keys, Merkle trees, digital signatures, TESLA chain keys and cryptographic functions. This authentication allows receivers to verify that the signal is coming from a trusted source and makes spoofing more difficult. OSNMA is free of charge and does not impact legacy receivers of the OS.***

***[32] 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***](https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-OSNMA-SDD_v1.0.pdf)***’***

In the point ‘5.1.2.5. Signal Authentication’ the following sentences could be edited as follows:

*‘The Galileo currently operates a free of charge authenticated service.’*

***‘The Galileo programme currently operates a free of charge authenticated service, the Galileo OSNMA.’***

# 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>

# Action requested of the Committee

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

* Consider the proposed amendment to IALA guideline G1117 chapters on GNSS authentication, following the action item 46 in the report of the committee, after Working Group 3 meetings, at DTEC4.
* Assess the proposed amendment to the chapters on GNSS authentication of IALA guideline G1180, aligning the document with the G1117 and updating the contents to technical novelties.