Input paper: [[1]](#footnote-1) ENAV24-6.1.16

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

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

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

Agenda item [[2]](#footnote-2) 6

Technical Domain / Task Number 2 …………………………………

Author(s) / Submitter(s) Ginés Moreno, Ana Cezón, Gema Cueto-Felgueroso / GMV

Karel Callewaert, Thiago Tavares / VVA

Manuel López / European GNSS Agency (GSA)

European GNSS capabilities for improving maritime safety and security with VDES

# Summary

This paper proposes different mechanisms in which European GNSS, and in particular Galileo OS-NMA can improve maritime safety and security in the frame of VDES.

## Purpose of the document

IALA ENAV Committee is invited to consider and if found feasible, implement any of the proposed mechanisms in VDES.

## Related documents

No related documents.

# Background

The shipping industry is moving towards an e-Navigation concept where a range of electronic and radio navigation technologies will provide harmonized, safe and reliable support for navigation by mariners. GNSS and augmented GNSS such as Satellite Based Augmentation Systems (SBAS) are examples of the supporting technologies for e-Navigation and are already being used in maritime applications for navigation and positioning purposes. Accurate position, speed and heading parameters are needed to ensure safe, economic and timely navigation so accuracy and integrity are the key performance aspects that could be provided by GNSS technology.

The maritime community is also being increasingly concerned on GNSS vulnerabilities to interferences, especially to the intentional attacks such as jamming or spoofing, given that GNSS was not initially designed to cope with these threats. The Navigation Authentication Message (NMA) feature under implementation in Galileo Open Service (OS) is an example of a countermeasure which could increase protection against spoofing attacks. Galileo OS-NMA is based on the introduction of a digital signature in some reserved bits on Galileo I/NAV message, and the delayed transmission of the key to authenticate such message. This implementation allows that the same information can be received by the users regardless they process the Galileo OS-NMA bits or not.

VHF Data Exchange System (VDES) is a new radio communication system which is being defined in the context of IALA and ITU. It is built over the capabilities of current Automatic Identification System (AIS) but allowing higher data rates and wider bandwidth. VDES is expected to enable e-Navigation applications. VDES is expected to have a terrestrial component and also a space segment which can extend VDES coverage to areas where terrestrial infrastructure does not exist.

In this landscape, the combination of European GNSS with future trends on maritime domain such as VDES represent an opportunity to increase safety and security in maritime navigation. This paper identifies possible mechanisms in which both EGNSS and VDES technologies could be used for such a purpose.

# Discussion

Authentication can have many applications, even in maritime domain, where the risk to spoofing and cyber-attacks can even compromise the safety of the navigation. Maritime community is already aware of vulnerabilities to interferences, and for this reason many efforts are being dedicated to identifying resilient positioning systems.

VDES is a new communication system that is being promoted to overcome current AIS overload limitations. VDES also represents an opportunity to exploit Galileo OS-NMA capabilities in order to support the following needs in maritime domain:

* Protection against external spoofing attacks (Use Case 1): covering that the information provided by authorities or used by the vessel (e.g. GNSS SIS) can be trusted.
* Protection against false information provided by vessels (Use Case 2): mainly covering non-collaborative vessels sending false position reports. This is mainly interesting for EFCA and EMSA surveillance activities.

VDES transmissions (including ship-to-ship, ship-to-shore and shore-to-ship) can at the same time be authenticated. Let us note that in the case of ship-to-ship communications, only shores verify the authenticity of such messages since vessels can also use radar to timely detect if the positions sent by surrounding vessels are consistent.

Next table summarizes the proposed use cases through this report.

| **ID and Description** | **Protected user/ asset** | **Benefits** | **Drawbacks** |
| --- | --- | --- | --- |
| **Use of Galileo OS-NMA in maritime receivers received via SIS (Use Case 1\_1\_1)** | User (vessel or shore) with Galileo OS-NMA capable receiver | * Simplicity * Coverage * Valid for AIS * Market opportunity for Galileo * No additional technology development | * Only protects the user processing the Galileo OS-NMA * Does not guarantee VDES position reports are trustable * Does not protect against spoofing in ranging measurements |
| Galileo OS-NMA centralized processing (Use Case 1\_2\_1 | Vessel | * Vessels do not require a Galileo OS-NMA capable receiver * Enables authentication of other data | * Latency * Requires technology developments and high data rate * Depends on VDES security mechanism * Does not protect against spoofing in ranging measurements |
| Combined user-centralized OS—NMA processing (Use Case 1\_2\_2) | Vessel | * Robustness of the solution * Vessels do not require a Galileo OS-NMA capable receiver * Local spoofing area detection | * Latency * Requires technology developments and high data rate * Depends on VDES security mechanism * Does not protect against spoofing in ranging measurements |
| AIS/VDES receiver precincts (Use Case 2\_1) | Authority | * Can take benefit of Galileo OS-NMA * Simplicity * Protects against manipulation of AIS/VDES positioning reports * Certain protection against manipulation of input positioning * Robustness * Cost-effective approach | * Voluntary implementation (unless change of regulation) * Not real-time protection: only detected through inspections |
| Tachograph-like approach (Use Case 2\_2) | Authority | * Can take benefit of Galileo OS-NMA * Protection in case AIS/VDES is switched off * Already existing technology * Robustness * Cost-effective | * Voluntary implementation (unless change of regulation) * May not protect against manipulation of input information * Not real-time protection: only detected through inspections |
| Positioning receiver design (Use Case 2\_3) | Authority | * Real-time protection * Simplicity | * Voluntary implementation (unless change of regulation) * Does not provide total protection against input positioning information * Potential certification/standaridsation costs * Does not protect against manipulation of AIS/VDES position reports |
| Central processing at AtoN level (Use Case 2\_4) | Authority | * Protection against all levels of VDES information manipulation * Can be automatized * Real time protection | * Complexity |
| **Use of external/active sensors (radar, earth observation, cameras in drones) Use Case 2\_5** | Authority | * Protection against all levels of VDES information manipulation * Real time protection in case of drones | * Complexity |

# References

1. Maritime Safety Committee, MSC 85/26, Annex 20. Strategy for the development and implementation of e-navigation, 19 December 2008
2. Multisystem - Radionavigation Receiver Performance Standard MSC.401(95), 8 June 2015
3. Worldwide Radionavigation System. IMO Res. A.1046 (27) , 30 November 2011
4. “Guidelines for shipborne position, navigation and timing (PNT) data processing” (MSC.1/circ.1575), 16 June 2017
5. IALA Recommendation GNSS vulnerability and mitigation measures R-129, 07 December 2012
6. Guidelines for shipborne position, navigation and timing (PNT) data processing. MSC.1/Circ.1575, 16 June 2017
7. Galileo Open Service – Service Definition Document (OS-SDD) Issue 1.1, May 2019
8. “GSA User Technology Report”, Issue 2.0, 2018
9. Wimpenny, Gareth, Safar, Jan, Grant, Alan, Bransby, Martin, Ward, Nick, "Public Key Authentication for AIS and the VHF Data Exchange System (VDES)," Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, Florida, September 2018, pp. 1841-1851.
10. “GSA Market Report” Issue 5, 2017
11. Ignacio Fernández-Hernández, Vincent Rijmen, Gonzalo Seco-Granados, Javier Simon, Irma Rodríguez and J. David Calle. “A Navigation Message Authentication Proposal for the Galileo Open Service”. NAVIGATION: Journal of The Institute of Navigation. Vol. 63 Nº1. Spring 2016
12. IALA Guideline G1117 “VHF Data Exchange System (VDES) Overview”. Edition 2.0 December 2017

# Action requested of the Committee

The Committee is requested to:

1. Note the information within this paper.
2. Discuss the matter at an appropriate time and
3. Include the proposed into the IALA documentation if so considered by the discussion
4. Authentication techniques for VDES

Authentication can have many applications, even in maritime domain, where the risk to spoofing and cyber-attacks can even compromise the safety of the navigation. Maritime community is already aware of vulnerabilities to interferences, and for this reason many efforts are being dedicated to identifying resilient positioning systems. Most promising approaches to be implemented in maritime are based on public key dissemination mechanisms so that a message can be decrypted by any user holding such public key; but provides authentication as long as such message could only have been encrypted by the holder of a linked private key. Please note that the authentication options explored are mainly based on adding the digital signature to the data to be authenticated in plain text mode, so that it can still be processed despite not being verified. Galileo OS-NMA represents one of the first implementations at GNSS system level which can support, up to certain level, spoofing detection and mitigation based on authentication. For this reason, Galileo OS-NMA represents an excellent opportunity to increase E-GNSS penetration in maritime receivers.

1. Galileo OS-NMA

Galileo OS-NMA consists of digitally signing the Open Service Navigation message in the E1 band. It is a free-of-charge service which will become available when Galileo reaches its Full Operational capability (FOC) foreseen for 2020. Until that moment, the Galileo OS-NMA is being tested in the frame of the Galileo Commercial Service demonstrator (Authentic and Accurate Location Experimentation with the Commercial Service- AALECS- project).

Galileo OS-NMA is based on a Time Efficient Stream Loss-Tolerant Authentication (TESLA) protocol and uses a set of available spare bits in I/NAV navigation messages in the Galileo E1b signal. One of the greatest advantages of the TESLA is the low bandwidth required to transmit the authentication information, together with a tolerance to data loss in case a message is lost.

The way in which authentication based on Galileo OS-NMA works can be summarized as follows:

* The receiver receives the navigation data and a Message Authentication Code (MAC) that authenticates the plaintext navigation message.
* The receiver receives some time later a key required to authenticate the MAC.
* The receiver authenticates the key with a previous key from the chain that is considered authentic or from the root key.
* The receiver re-generates the MAC key with the data, which should match the previously received MAC.

This implementation allows that the same information can be received by the users regardless they process the Galileo OS-NMA bits or not. Let us remark that this scheme only protects against fake navigation signals, but there are no means to be protected against attacks in the range measurements. Also, let us note that the use of Galileo OS-NMA may imply a performance degradation due to the latency time and the potential use of Galileo-only solutions to compute robust PVTs. This degradation is minimum or even negligible for the latency case and significant for the Galileo-only solution with respect to multi-constellation solutions.

1. Galileo OS-NMA and VDES USE CASES

The use cases in which Galileo OS-NMA and VDES technologies authentication could be considered can be separated into two different situations:

* Use Case 1 (Protection mechanisms against external spoofing): Users (vessel and/or AtoN) can authenticate the origin of the navigation information used in its position computation or be warned of potential spoofing attacks in the surrounding area. This level of protection given to the user which authenticates the information is the same for collaborative or non-collaborative users.
* Use Case 2 (Protection against non-collaborative vessels): Analysis of positions reported by the users: a different situation is that one user, deliberately manipulates the position provided by its navigation system and shares a fake location to cheat maritime authorities or other vessels or directly does not provide a position report. These use cases are only applicable for non-collaborative users. This is mainly interesting for EMSA and EFCA.
  1. Use Case 1: Protection against external spoofing

This scenario refers to the authentication of the input information to the VDES receiver installed on-board the vessels or even at shore stations controlled by AtoNs. This authentication serves as mechanism to protect users (vessels and/or AtoNs) against external spoofing attacks and could be applicable to both collaborative and non-collaborative vessels.

The main idea behind all the scenarios in this use case is that Galileo OS-NMA enables users to verify if the Galileo navigation information used for positioning purposes (that is, compute the PVT sent to shore and other ships via AIS/VDES) comes from a trusted source, or it shall not be trusted as the user is being attacked due to some kind of spoofing. In addition, the receiver may apply additional consistency checks with the information coming from other sensors such as inertial measurement units, so that the final position reported is consistent. But as part of this use case, we are only considering the different options in which Galileo OS-NMA could be used, since the other consistency checks can be applied regardless the way in which Galileo OS-NMA has been processed by the receiver.

Regarding the Galileo OS-NMA processing, two different situations can be mainly distinguished:

* **Use Case 1\_1**: Galileo OS-NMA is processed at user receiver level (being Galileo OS-NMA capable) so that the user is the one which identifies if it is being spoofed or not. The position provided by the GNSS receiver as an input for VDES has been computed using Galileo OS-NMA from the information received directly from the space. No additional infrastructure is considered, so the Galileo OS-NMA processing is done by each user (this applies to vessels and/or AtoNs).
* **Use Case 1\_2**: Galileo OS-NMA is processed externally to a vessel by the AtoN instead of or in addition to the processing at receiver level, and the authenticated information is sent to the users via VDES. Let us remark that this scenario does not guarantee that users are not being spoofed, but it can serve as a warning mechanism (risk of spoofing attack) or even to inform users that they can use AtoNs services based on Galileo (e.g. timing as an input for R-mode).On the other hand, the vessels may also receive input messages via VDES from shore or other vessels which may be authenticated, using an authentication mechanism. Let us note that the authentication of position reports from other vessels may consist on making consistency checks with the positons provided by the radar. Consequently, only the authenticated VDES information from shore may need to be processed, At the same time, two options could be considered: Galileo-OS-NMA only processed in a centralized infrastructure (Use case 1\_2\_1) or combined user-centralized Galileo OS-NMA processing (Use Case 1\_2\_2)
  1. Use Case 2: Protection against non-collaborative vessels

Galileo OS-NMA represents a promising feature that allows users to check themselves that the information that they are receiving for positioning purposes can be trusted or not. In other words, Galileo OS-NMA can be seen as a spoofing detection mechanism for all users, either vessels or AtoNs.

However, a different situation is when the user deliberately manipulates its positioning data to confuse other users and/or to cheat maritime authorities which are monitoring vessels in their area of influence for potentially malign intentions (e.g. fishing in forbidden areas, breaking international agreements, etc.). We will assume that in all these cases the user is a non-collaborative vessel who will try cheat the maritime authorities regarding their reported position. As part of these malicious actions we include the transmission of fake or even null position reports.

The three different ways in which the AIS/VDES position reports can be manipulated are related to the different points in which the data can be modified:

* Techniques devoted to manipulating the input information used to compute the positioning information (e.g. GNSS data); such as auto-spoofing
* Techniques devoted to manipulating the position reports from AIS/VDES: either modifying the output from the positioning receiver or the input to VDES
* Switching off the positioning reporting information system (AIS/VDES)

The different protection mechanisms against such attacks can be one or a combination of the following use cases:

* **Use Case 2\_1: AIS/VDES receiver precincts:** the main idea behind is that the user cannot manipulate the information contained in the VDES messages; so that it is somehow ensured that the PVT provided by the positioning system (GNSS or MSR) is the same one contained in the exchanged AIS/VDES messages between ships and ship-to-shore modes.

It can also affect to the AIS/VDES receiver design by imposing some kind of precincts at the output of the GNSS/MSR receiver so that the computed PVT is the same introduced in AIS/VDES messages. It can be just a mechanic piece or even an electronic one which raises an alarm to the AIS/VDES system to inform authorities in case it is broken. The main drawback is that this can only be ensured through inspections.

The implementation of this technique requires the involvement of AIS/VDES receiver manufacturers so even they are the ones that implement such technique. The maritime authority would need to ensure that these protected receivers are implemented in vessels by regulation and also to ensure that inspections (periodical or ad-hoc) are done to detect manipulated precincts

* **Use Case 2\_2: Tachograph-like approaches:** This is complementary approach to the previous one in which the AIS/VDES receiver implements some kind of tachograph (as in trucks) or black boxes (as in airplanes) which store relevant vessel information which cannot be easily manipulated by the mariner. It may also send this information in real time to the authorities, so it can be monitored and detect if the tachograph has been somehow manipulated.

The success of this technique requires that maritime authorities impose this tachograph approach as mandatory carriage, since it may not be implemented voluntarily especially if the vessel intents to be used for illegal purposes.

* **Use Case 2\_3: Positioning receiver design:** In case some of the previous two mechanisms is implemented, then the only possible approach for an user to produce false positioning outputs is by manipulating the information used to compute such PVT; in other words, that the user spoofs himself.

Some GNSS receivers on the market already implement anti-spoofing (either detection and/or mitigation techniques) methodologies to protect users against external spoofing attacks, such as Galileo OS-NMA, other GNSS receiver techniques (e.g. based on signal power) or as part of the MSR, make consistency checks among input coming from different sources.

* **Use Case 2\_4: Central processing at AtoN level:** maritime authorities implement some kind of control centre in which the information coming from different sources is analysed in real time, such as all the position reports in the areas; information coming from radars etc. The novelty of our proposal is to promote that this central facility could also implement artificial intelligence techniques to also predict vessel route’s and position reports in the future based on the reported information, in order to detect any potential discrepancy in case the vessel deviates from its expected route. This can be especially beneficial to detect manipulation of input positioning data or positioning reports: for instance, in case sudden changes of speed and turn may inform from suspicious activities in certain area.

This central facility could also integrate all the information coming from active sensors (e.g. earth observation) to have an additional layer of protection and awareness.

* **Use Case 2\_5: Use of external/active sensors:** the latest way to verify the position reports by vessels is to check by external means and monitor or survey certain areas. This mechanism is closely related with the previous one, since the central processing may require the usage of active sensors to confirm a vessel location. One of the most interesting approaches is the use of Earth Observation reports such as the ones provided by Copernicus that will be analysed in future reports within this project. However, the main drawback is the latency of the information, since it may not be provided in real time. And also, it may provide reports of certain specific areas and not the desired ones. In this latter case, the use of drones with cameras could be a more suitable solution since it may be able to survey certain areas on demand and does not depend on the availability of the information from satellite observation. To take the most benefit of earth observation techniques, it is highly recommended to integrate this information with the one coming from different sources such as vessel reports.

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