Study on the benefits and uses of OSNMA in maritime navigation

ION GNSS+ 2023

Wednesday, September 13, 2023

Héctor Llorca (GMV)
Marcos López (GMV)
Enrique Domínguez (GMV)
Tobias Tisell (SAAB)
Philipp Scheidemann (EUSPA)

gmv INNOVATING SOLUTIONS

Index

- Introduction
- OSNMA fundamentals
- OSNMA/Spoofing test campaign
- OSNMA Receiver Architecture
- Conclusions

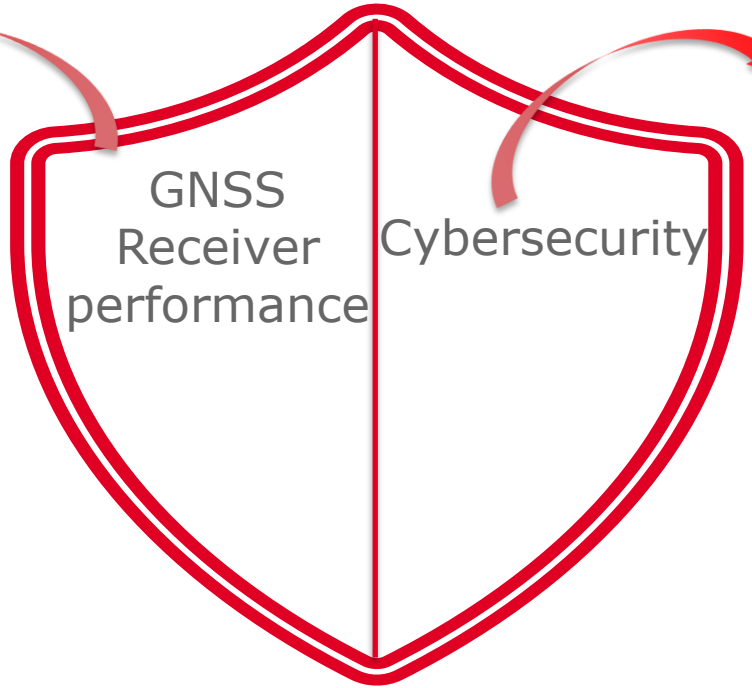
Introduction

Maritime context

The International Maritime Organization (IMO) has always paid great attention to the improvement of **maritime navigation safety**.

Resolutions:
A.915(22)
A.1046(27)

Requirements on:
Accuracy
Integrity



Resolution:
MSC.428(98)
Maritime Cyber Risk Management in Safety Management Systems

Other guidelines:
Guidelines on Cyber Security Onboard Ships

Maritime navigation safety

Interferences and Spoofing context

GNSS signals are weak in terms of power when they reach the ground

Vulnerability → Interferences { Unintentional; Deliberate → **Jamming & Spoofing** }

Spoofing can lead to many problems on a vessel (from the failure of some system to even a collision)

This is a **real problem** that it is taking place right now worldwide, especially near conflict zones

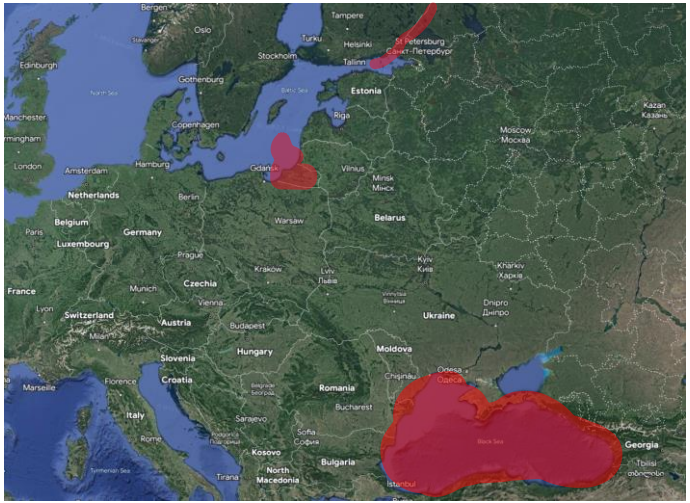


Image based on description provided in EASA, "Safety Information Bulletin - Global Navigation Satellite System Outage Leading to Navigation / Surveillance Degradation,". 2022

ASGARD GNSS receiver

Through the context of the ASGARD project, co-funded by the European Union Agency for the Space Programme (EUSPA), an advanced maritime dual frequency multi-constellation navigation equipment has been developed (2021 – 2023).

One of the main objectives of the project has been the **implementation of the Galileo OSNMA functionality** in the receiver.

ASGARD receiver has also undergone laboratory tests where it has **obtained IEC GNSS type approval** under the European MED WheelMark.

OSNMA Fundamentals

OSNMA fundamentals

The Galileo Open Service Navigation Message Authentication (OSNMA) is an **authentication protocol** based on the TESLA protocol specifically tailored for Galileo Open Service currently transmitted in SIS.

Transmitted through **I/NAV message**

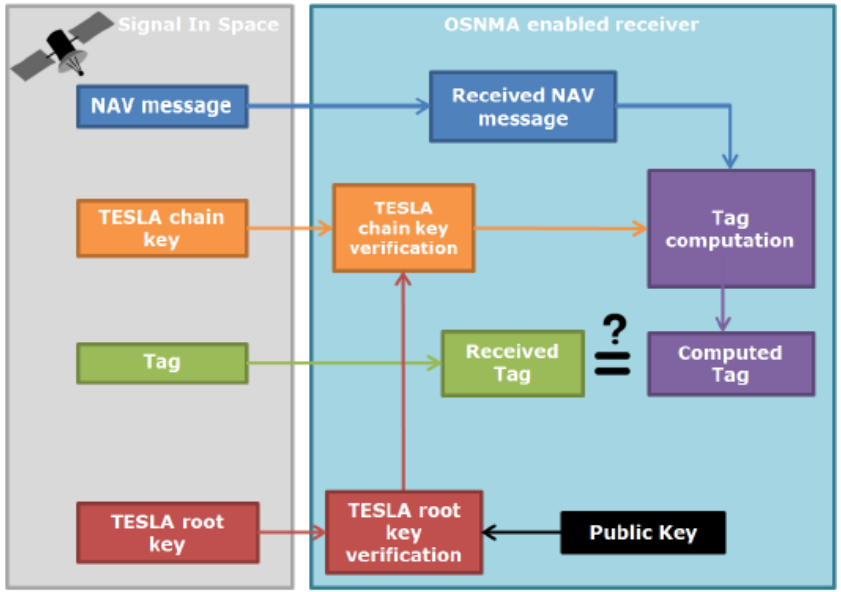
E1-B

Even/odd=1	Page Type	Data j (2/2)	OSNMA	SAR	Spare	CRCj	SSP	Tail	Total (bits)
1	1	16	40	22	2	24	8	6	120

Even/odd=0	Page Type	Data k (1/2)	Tail	Total (bits)
1	1	112	6	120

Source: OSNMA User ICD for the Test Phase. Issue 1.0.

Authentication process



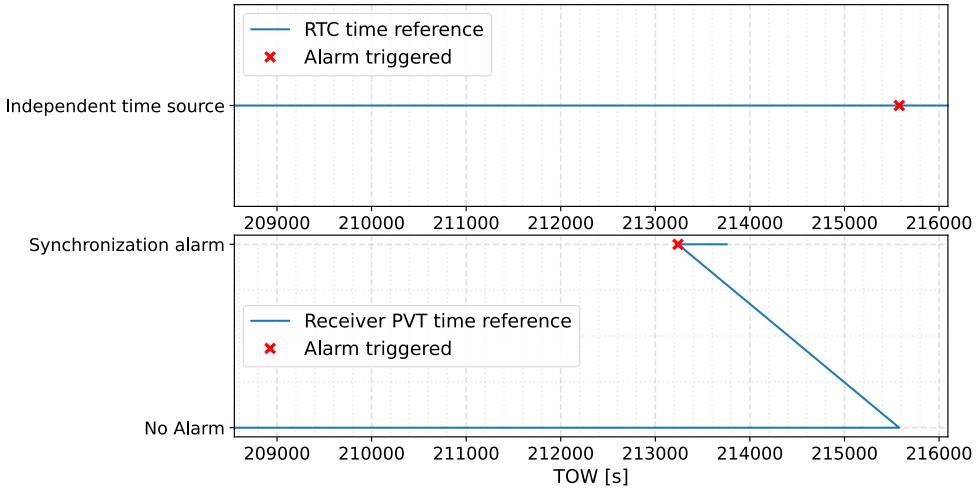
Source: OSNMA Receiver Guidelines for the Test Phase. Issue 1.1.

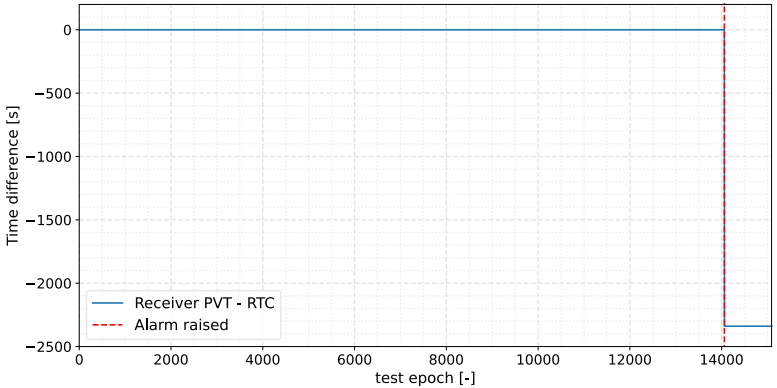
OSNMA/Spoofing test campaign

Meaconing test

Type of spoofing attack based on recording the authentic GNSS signal and then replaying and transmitting it to the target receiver of the attack.

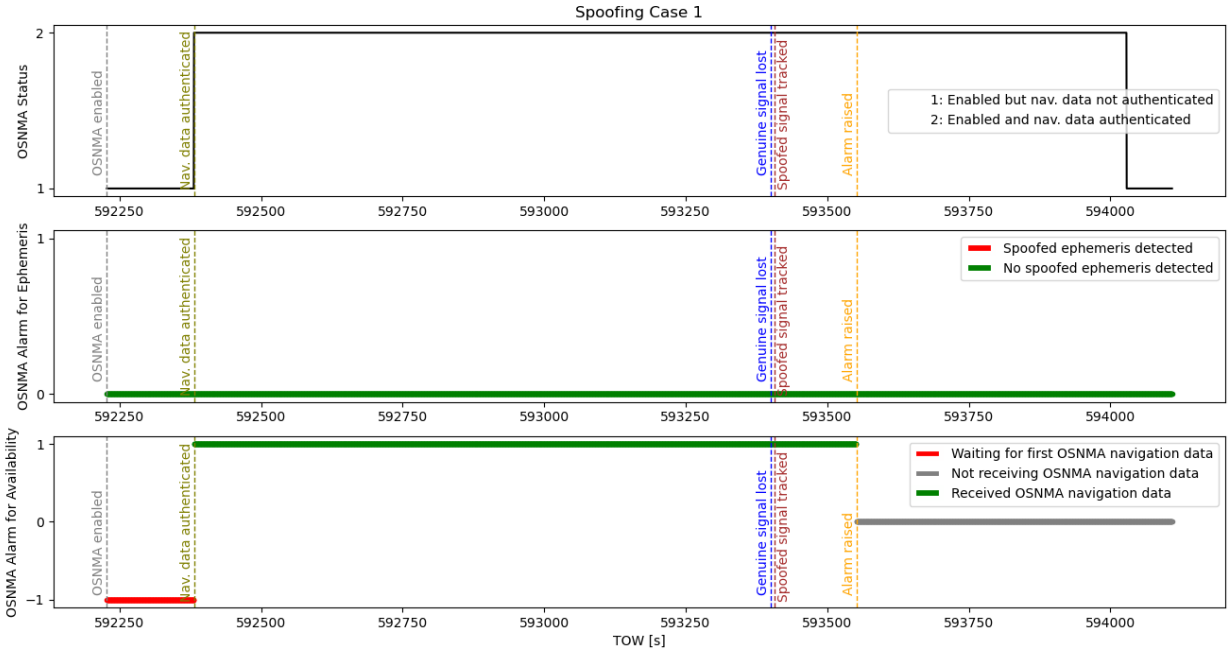
The OSNMA Receiver Guidelines specifies that there must be a time synchronization requirement with the Galileo System Time (GST). The ASGARD solution has an **independent time source** (RTC).





Spoofing Replicating SIS without OSNMA Information

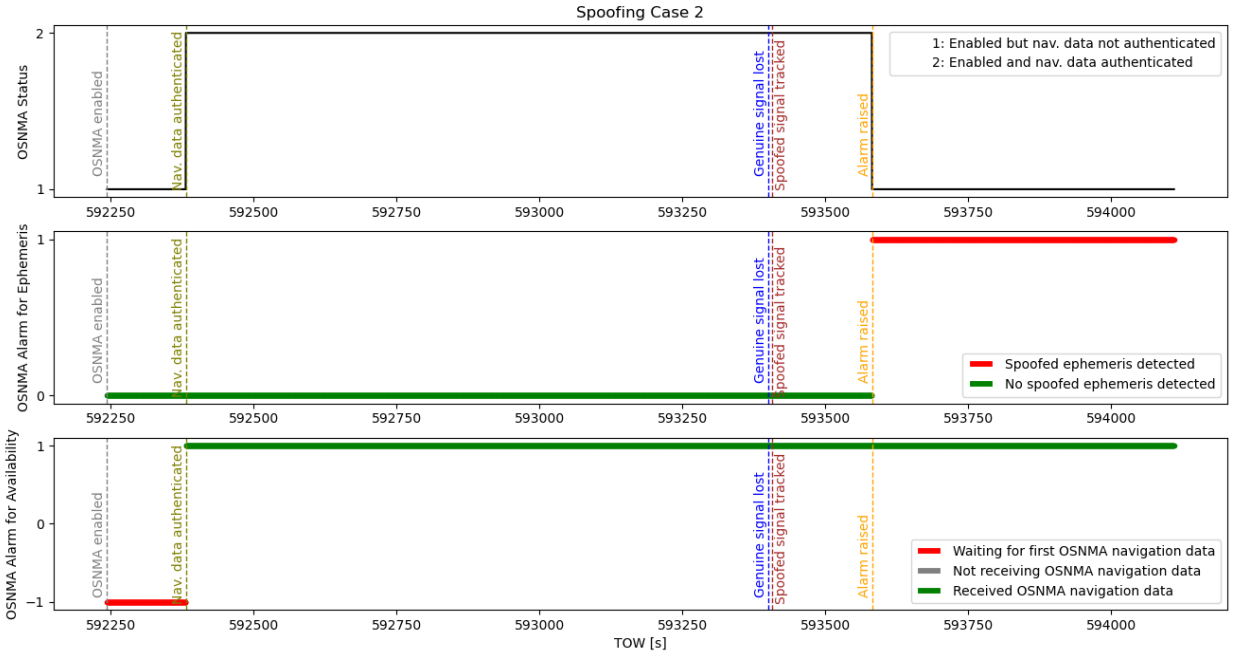
An attack is generated that contains exactly the same information available in SIS, but with the bits that contain OSNMA information set to 0.



Key Moment	Time	Delta time
OSNMA enabled	20:30:09.5	-
Navigation data authenticated	20:32:43.5	+00:02:34.0
Genuine signal lost	20:49:42.0	+00:16:58.5
Spoofed signal tracked	20:49:49.0	+00:00:07.0
Alarm raised	20:52:13.5	+00:02:24.5
Navigation data not authenticated	21:00:11.0	+00:07:57.5

Spoofing with OSNMA Information Replicated as in SIS

An attack with false ephemeris data but that replicates the OSNMA bits from SIS



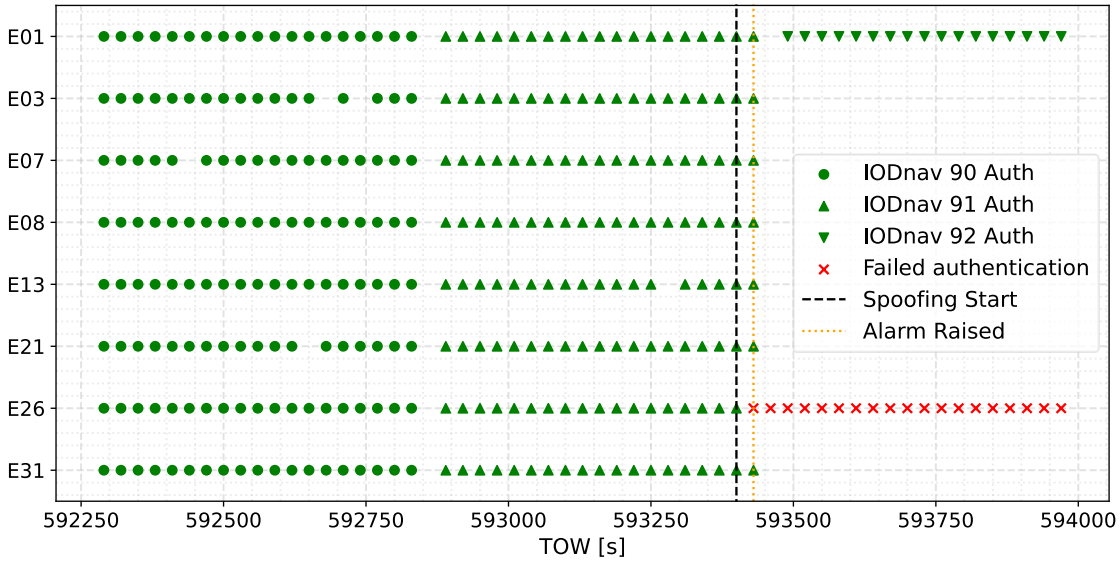
Key Moment	Time	Delta time
OSNMA enabled	20:30:25.5	
Navigation data authenticated	20:32:43.5	+00:02:18.0
Genuine signal lost	20:49:42.0	+00:16:58.5
Spoofed signal tracked	20:49:49.0	+00:00:07.0
Alarm raised	20:52:43.5	+00:02:54.5
Navigation data not authenticated	20:52:43.5	+00:00:00.0

Spoofing of Only Some Satellites in View (Cross Authentication)

An attack in which not all satellites are spoofed. With OSNMA there is also the possibility to have **cross authentication** between Galileo satellites

Context	Data
Galileo satellites in view (ID)	1, 3, 7, 8, 13, 21, 26, 31
IOD_{nav} received during the test	IOD_{nav} 90, IOD_{nav} 91 and IOD_{nav} 92
Spoofed satellite with false ephemeris	26
Satellite not spoofed providing cross-authentication data	1
Spoofing attack start	20:50:00 (TOW = 593400.0)

30 seconds after the attack the receiver is unable to authenticate the information from satellite 26 and raises a spoofing alarm.

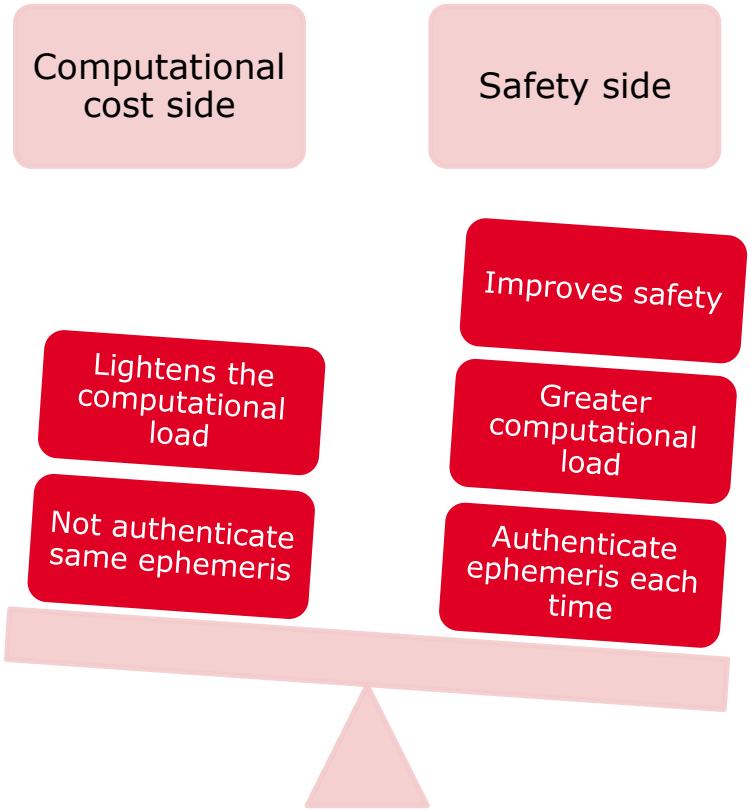


Spoofing with OSNMA Information Replicated as in SIS Keeping the Same IODs

An attack in which the IODnav is not updated despite having false ephemerides

The received ephemeris is identified by an IODnav, a criterion that can be used to know if the information you are receiving is the same or not.

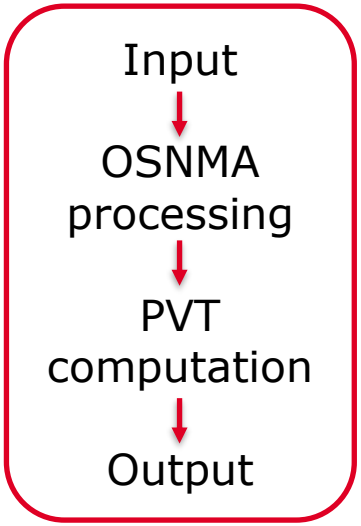
For a safety-side receiver the results are the same as those seen when the attack also sent new IODs. **The attack is detected**.



OSNMA Receiver Architecture

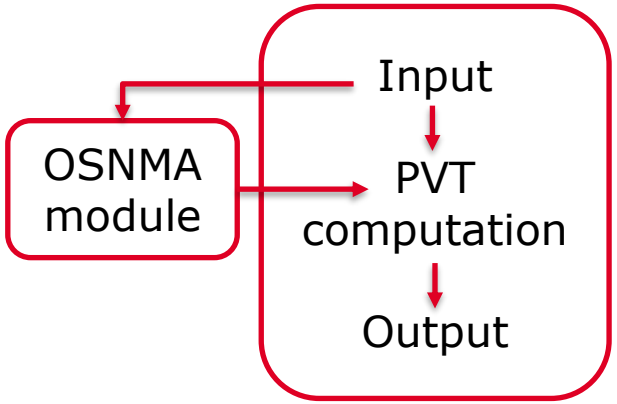
OSNMA Receiver Architecture

There are different ways of approaching the architecture of a receiver with OSNMA



OSNMA processes embedded in the receiver

- ☑ It can be optimized for a specific receiver



OSNMA external module implemented outside the receiver flow

- ☑ Easier to test the module
- ☑ Can be used for different receivers
- ☑ Can be used as a generic navigation message authentication tool

Conclusions

Conclusions

- Safety in navigation is increasingly relevant and it is important to also take **cybersecurity** aspects into account.
- **OSNMA** is presented as an interesting tool to improve cybersecurity in GNSS receivers.
- There are many ways to pose a **spoofing attack**.
- OSNMA capability can **detect** a wide variety of spoofing attacks.
- There are **different logic or strategies** when implementing the OSNMA functionality.
- To correctly **test** the OSNMA mechanism, it should not be based only on functional tests.
- OSNMA does not allow authenticating that the pseudo ranges used to calculate the position.
- **Investing** in the development, use and regulation of OSNMA is worthwhile.

Thank you

Héctor Llorca Llorca
hector.llorca@gmv.com

INNOVATING SOLUTIONS