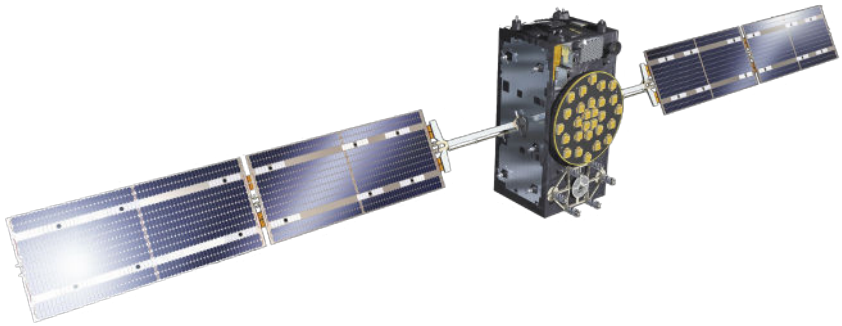
ELECTRONICS & DEFENSE

GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHETICATION (OSNMA)



Galileo Open Service Navigation Message Authentication (OSNMA)

The new generation of satellite enabled applications is relying on resilient and accurate GNSS signals as a key element for many critical projects to ensure highly accurate Positioning, navigation, and Timing (PNT) data.

Safran offers GNSS testing and simulation solutions designed to ensure the performance, resilience and accuracy of your system for complex GNSS applications.

Safran Electronics & Defense is with you every step of the way, building in the intelligence that gives you a critical advantage in observation, decision-making and guidance.

SAFRAN

The Challenges of Jamming and Spoofing Attacks

GNSS technology is the primary global technology for positioning, navigation & timing (PNT), and it is critical that it continues to evolve and become more secure and resilient. Jamming and spoofing attacks are becoming increasingly more common on GNSS systems and technologies.

Jamming is simply the ability to overpower the GNSS signals that are transmitted from satellites since they have traveled long distances. Spoofing is a more sophisticated attack where fake GNSS signals are transmitted to fool a receiver into misrepresenting its location and timing.

Open Service Navigation Message Authentication (OSNMA)

Open Service Navigation Message Authentication (OSNMA) is an authentication service that is emerging for GNSS technology – specifically in the Galileo satellite constellation. OSNMA allows GNSS receivers to verify the authenticity of received data in order to protect against potential jamming or spoofing attacks that can result in service disruptions, denial incidents, and more severe consequences. OS-NMA will be a free service for Galileo Open Service users but does require a compatible receiver to decode and authenticate.

The OSNMA service will help to build a more robust and resilient GNSS service for the European Union (EU).

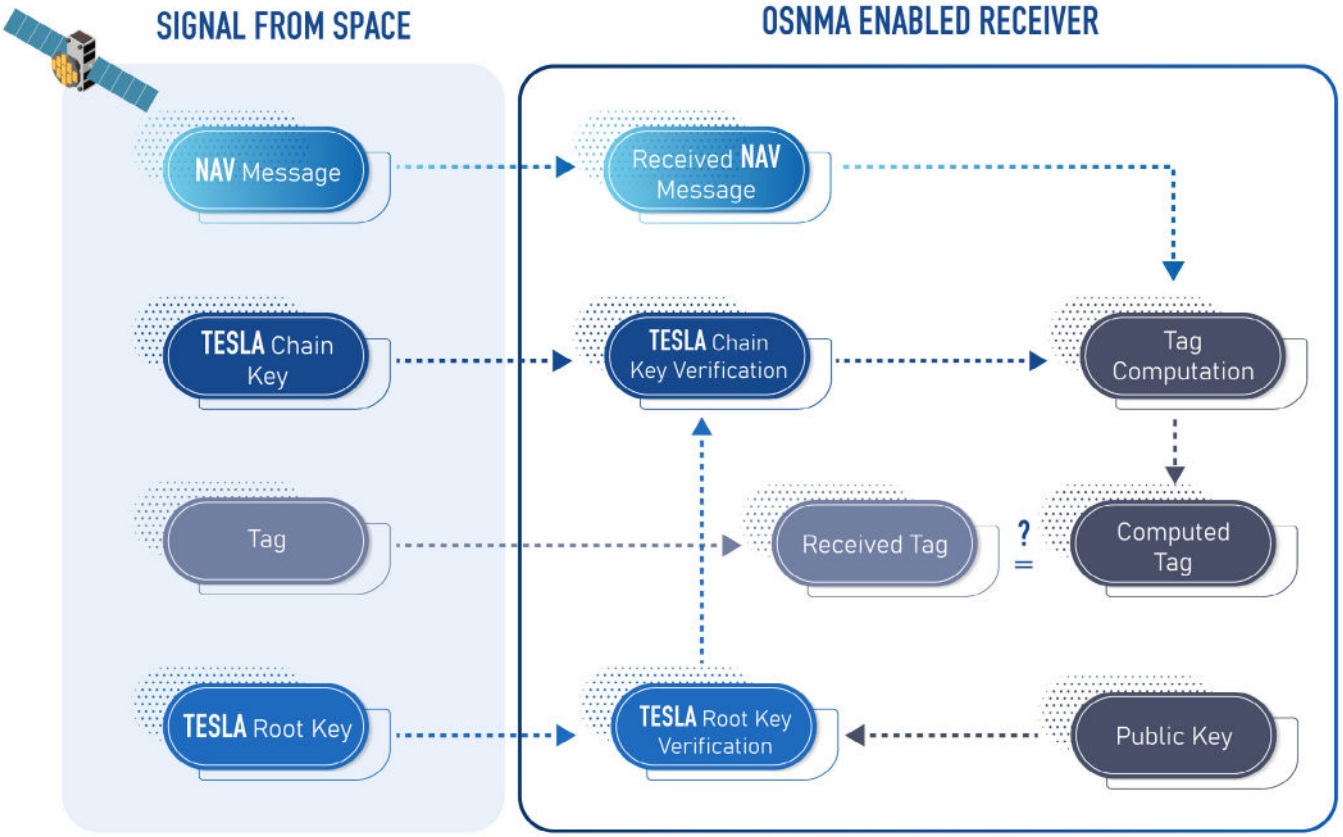
The European Union Agency for the Space Programme (EUSPA) launched the test phase in November 2020, and Galileo satellites began transmitting the authentication data. This data is currently being transmitted for public observation and evaluation.

OSNMA Authentication & Architecture

The data authentication used by Galileo OSNMA can be summarized as follows:

- The receiver demodulates the navigation data and a Message Authentication Code (MAC) that authenticates the plaintext navigation message.

- The receiver demodulates the Timed Efficient Stream Loss-tolerant Authentication (TESLA) key required to authenticate the MAC. This key is broadcast by the system with some delay (with respect the associated MAC).



- The receiver authenticates the TESLA key using a previous key from the chain that is considered authentic or from the root key. This key is part of a pre-generated one-way chain (which has a public root), and which is transmitted in reverse order with respect to its generation.

- The receiver re-generates the MAC key with the data, which should match the previously received MAC.

Safran + OSNMA

Safran now provides Galileo OSNMA simulation support in the form of two distinct yet complimentary solutions. These solutions are available to customers that have purchased the Galileo constellation license.

OSNMA Data Generation

This solution allows Skydel to generate its own data and provides full flexibility in the configuration of the scenario (time, navigation message, etc.) as well as the OSNMA authentication parameters (keys, encryption algorithms, message sequences, etc.). This solution is ideal for advanced users (e.g.: receiver manufacturers) that test receivers in a wide range of edge and corner cases.

This solution also includes the following elements in Skydel:

- A new Skydel engine supporting OSNMA SIS ICD 1.1.
- Authentication of the Galileo E1 OS Navigation Message.
- Support for the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol.
- Useful crypto material for running user-programmable simulation tests scenarios.

This feature will be ready for future software updates in accordance with the next phases recommended by EUPSA.

Test Vectors Simulation

This solution is well-suited for most receiver integrators that wish to perform EUSPA data simulation.

Available now, this solution supports the available official test vectors sample data, which supports the verification of OSNMA functionality implementation, and includes:

- Support for OSNMA Receiver Guidelines for the test phase (Issue 1.1 – October 2022) and Receiver Guidelines (Issue 1.3 – January 2023)
- List of test vectors (CSV format) and cryptographic materials (Public Key and Merkle tree root). Accessible from the EUSPA website, this raw data will be shared.
- Skydel format (SDX) scenarios.

1. Users will simply need to load a scenario corresponding to the test vector they wish to simulate.
2. This solution allows users to easily and quickly customize their scenarios. For example, users can load an OSNMA scenario, then add a jammmer/spoofer.

Sources: https://gssc.esa.int/navipedia/index.php/Galileo_Open_Service_Navigation_Message_Authentication

POWERED BY TRUST

Safran Electronics & Defense
safran-electronics-defense.com

SAFRAN

April 8, 2024