#EUSpace

Development of an OSNMA user implementation

EUSPA OSNMA Day 2026

Sophie DAMY

European Commission, Joint Research Centre

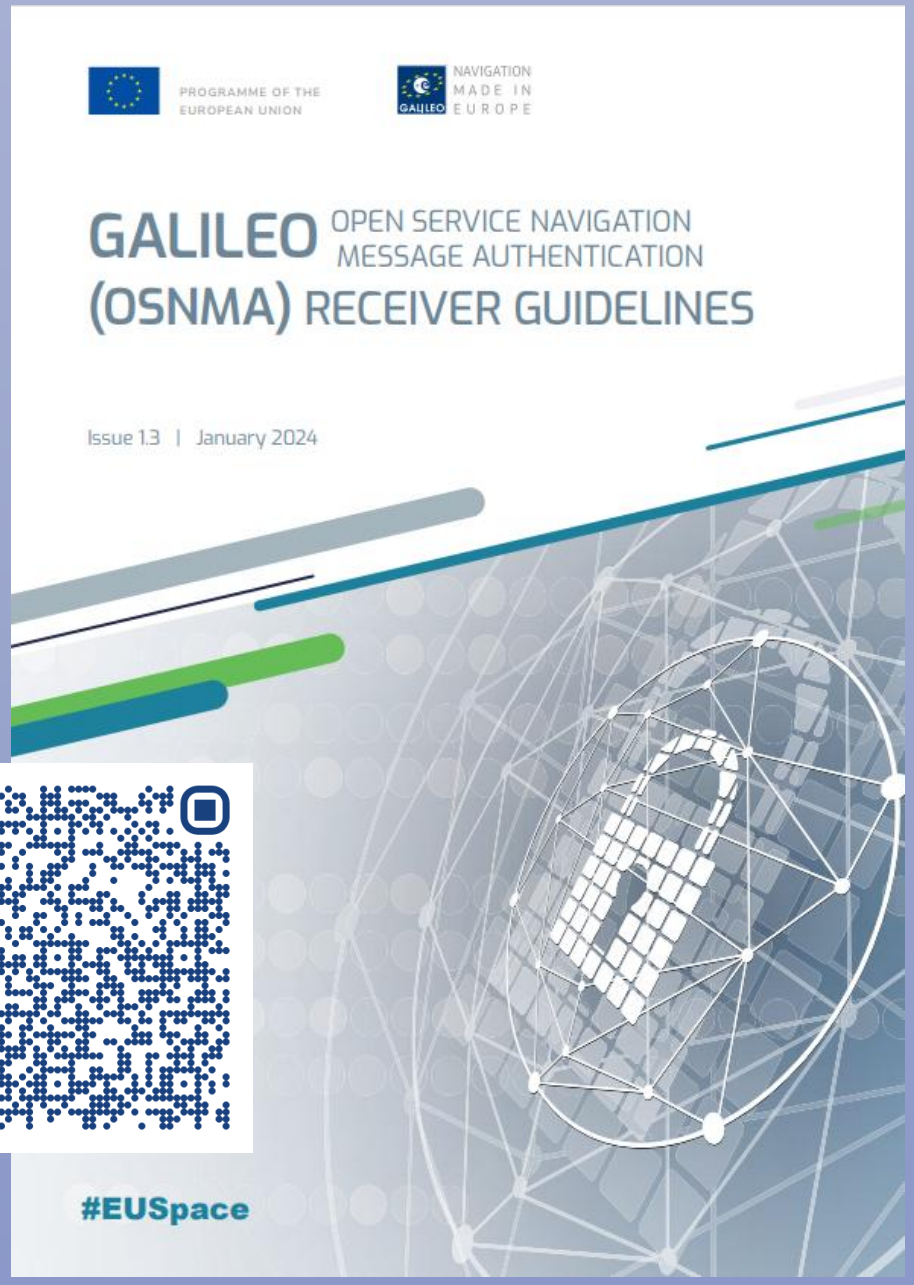
EUSPA
European Union Agency for the Space Programme

Introduction

This presentation introduces essential information and data for **developing and validating a user implementation of OSNMA**.

Key topics:

- OSNMA Receiver Guidelines
- OSNMA requirements
- Processing logic
- Test vectors
- Conclusions



OSNMA Receiver Guidelines

- This document offers **comprehensive guidelines** for implementing OSNMA functionality in the user segment.
- It covers **requirements**, **mandatory verifications**, and **optimisations**, providing the necessary information to verify the authenticity of the Galileo navigation message.
- These guidelines are designed to be **generic**, ensuring broad applicability across various platforms and applications.

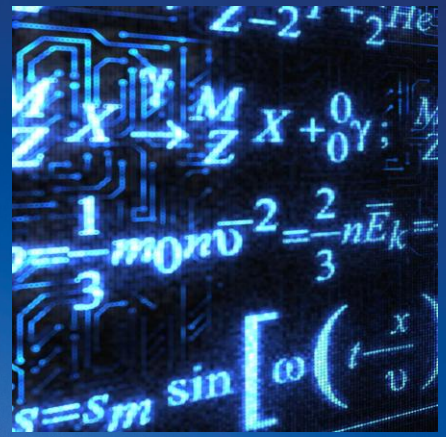
OSNMA Receiver Guidelines

Table of content

OSNMA Requirements

Time Synchronisation

Cryptographic Functions



Integrity of the cryptographic material

Interfaces

www.gsc-europa.eu

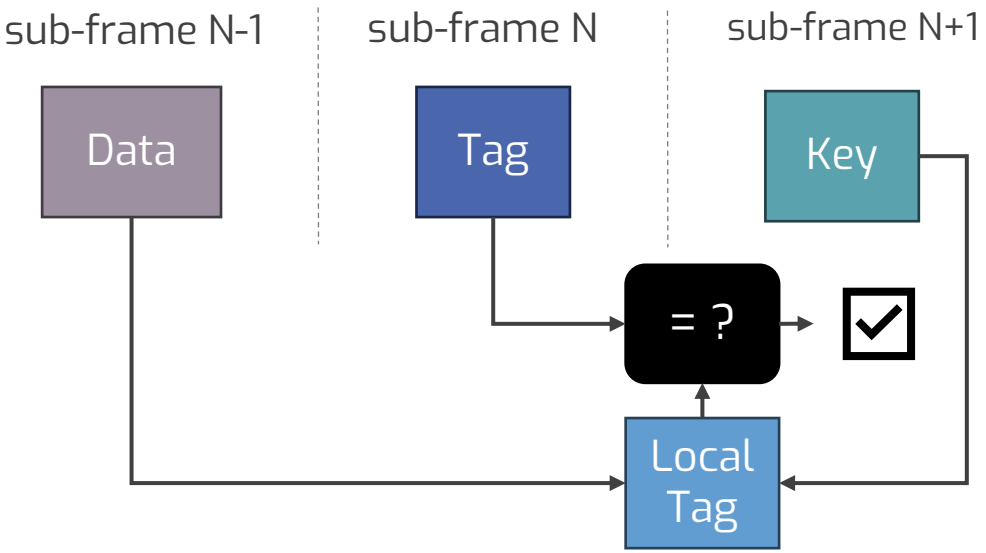
Time Synchronisation

Galileo navigation data is authenticated by using a key to generate a truncated Message Authentication Code (tag).

The security of the OSNMA protocol depends on maintaining the **secrecy of the key**.

The key is released only **after** the tag and data are broadcast. Therefore, the receiver must ensure it receives the tag before the key is transmitted to maintain security.

The receiver is required to be **synchronised with the Galileo System Time** within **30 sec** or **5 min**.



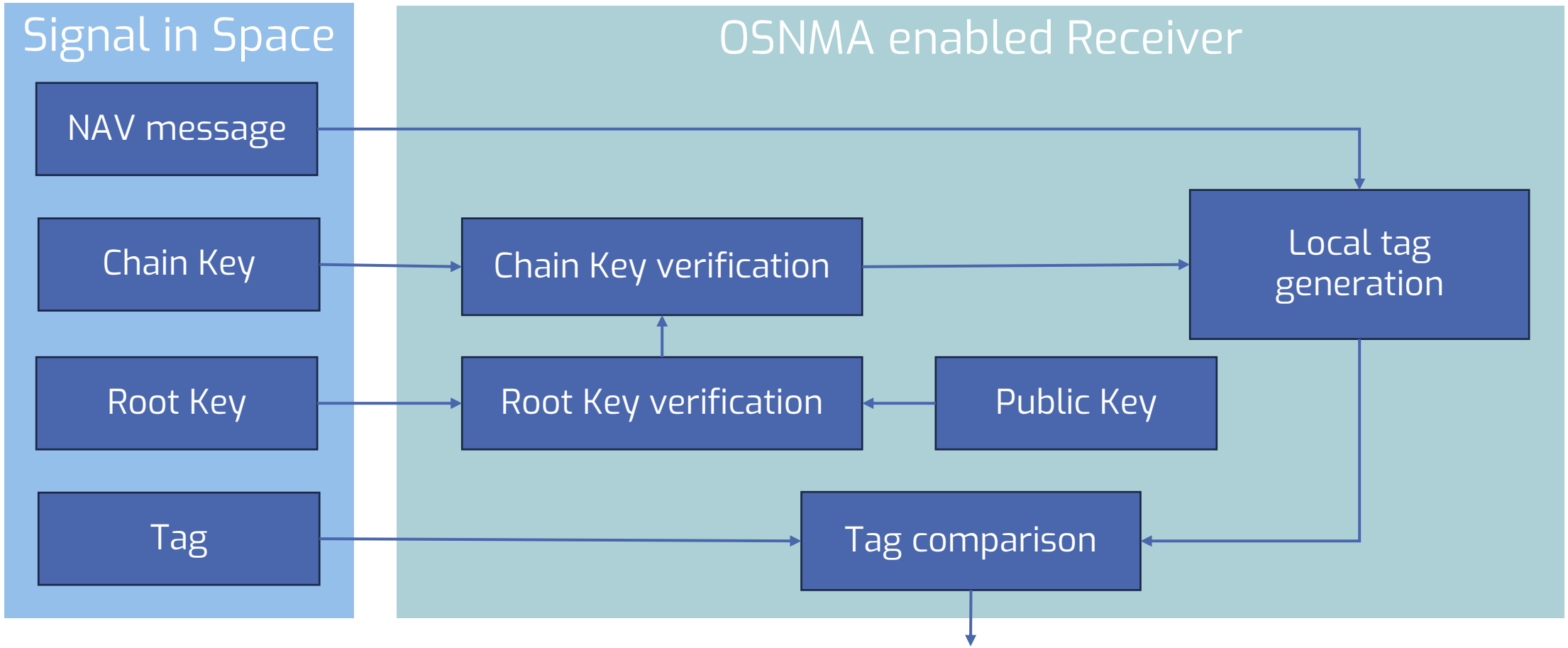
Time Synchronisation

To ensure synchronization to the Galileo system time, the receiver needs a **secure time source**, for example:

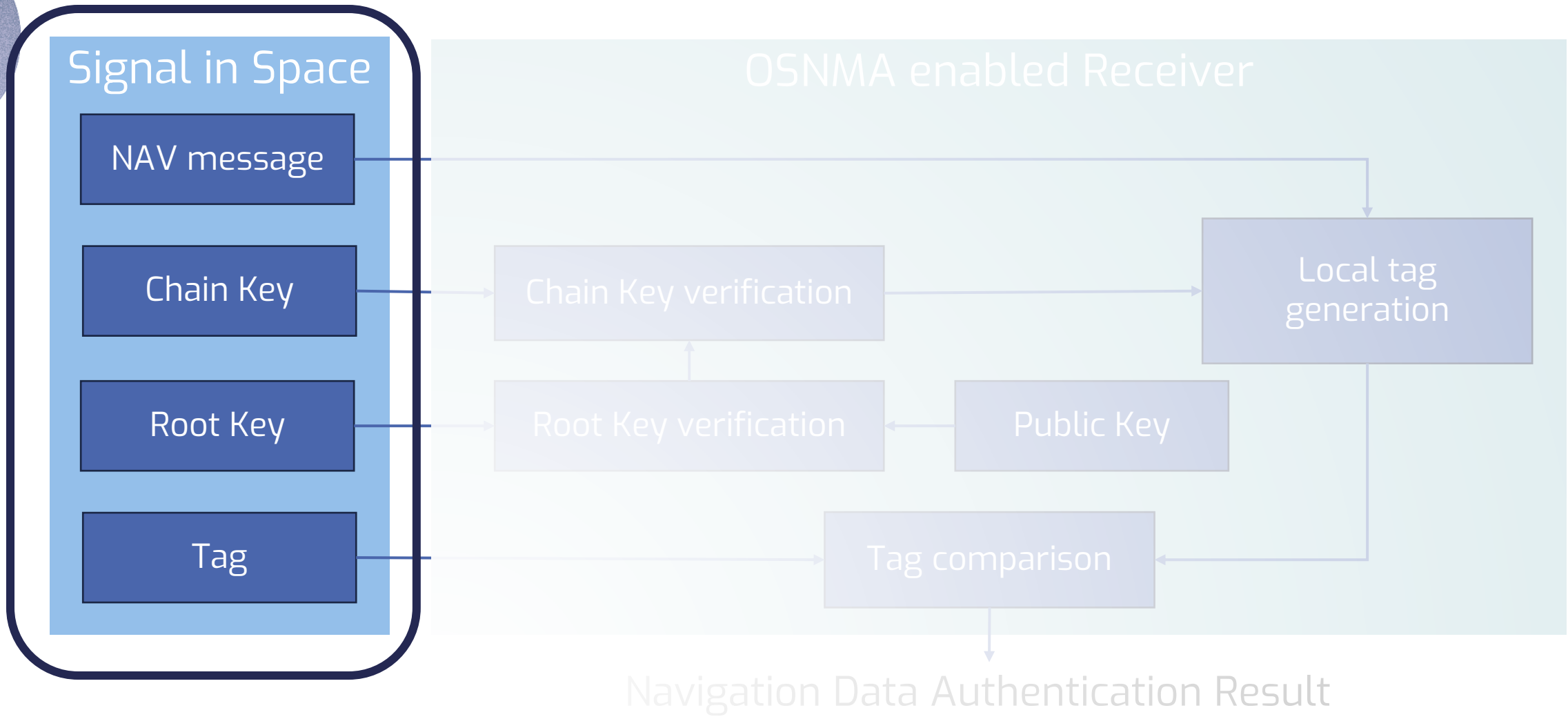
- An independent clock
- A secure network connection with a time transfer capability

If the time synchronisation requirement is not fulfilled, **the OSNMA protocol shall not be used.**

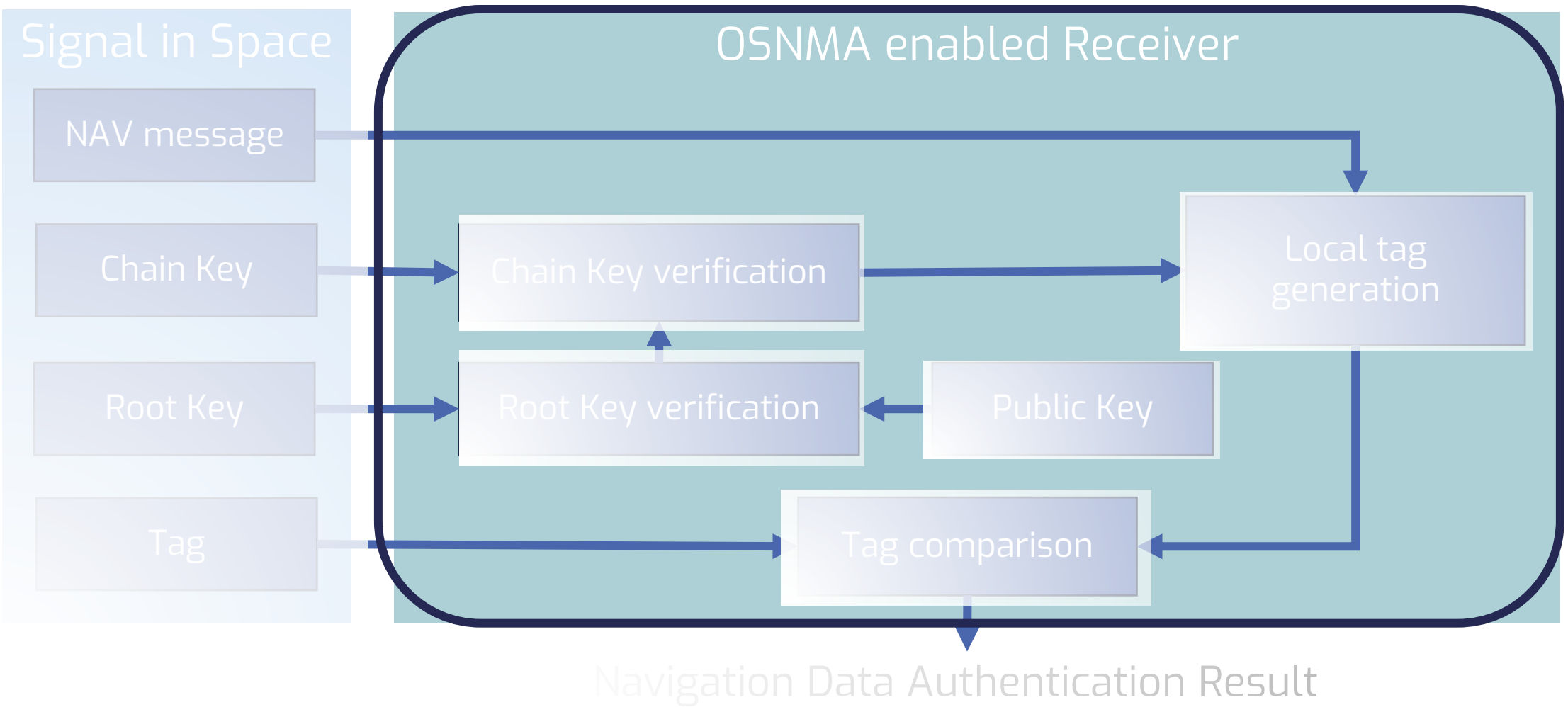
OSNMA processing logic

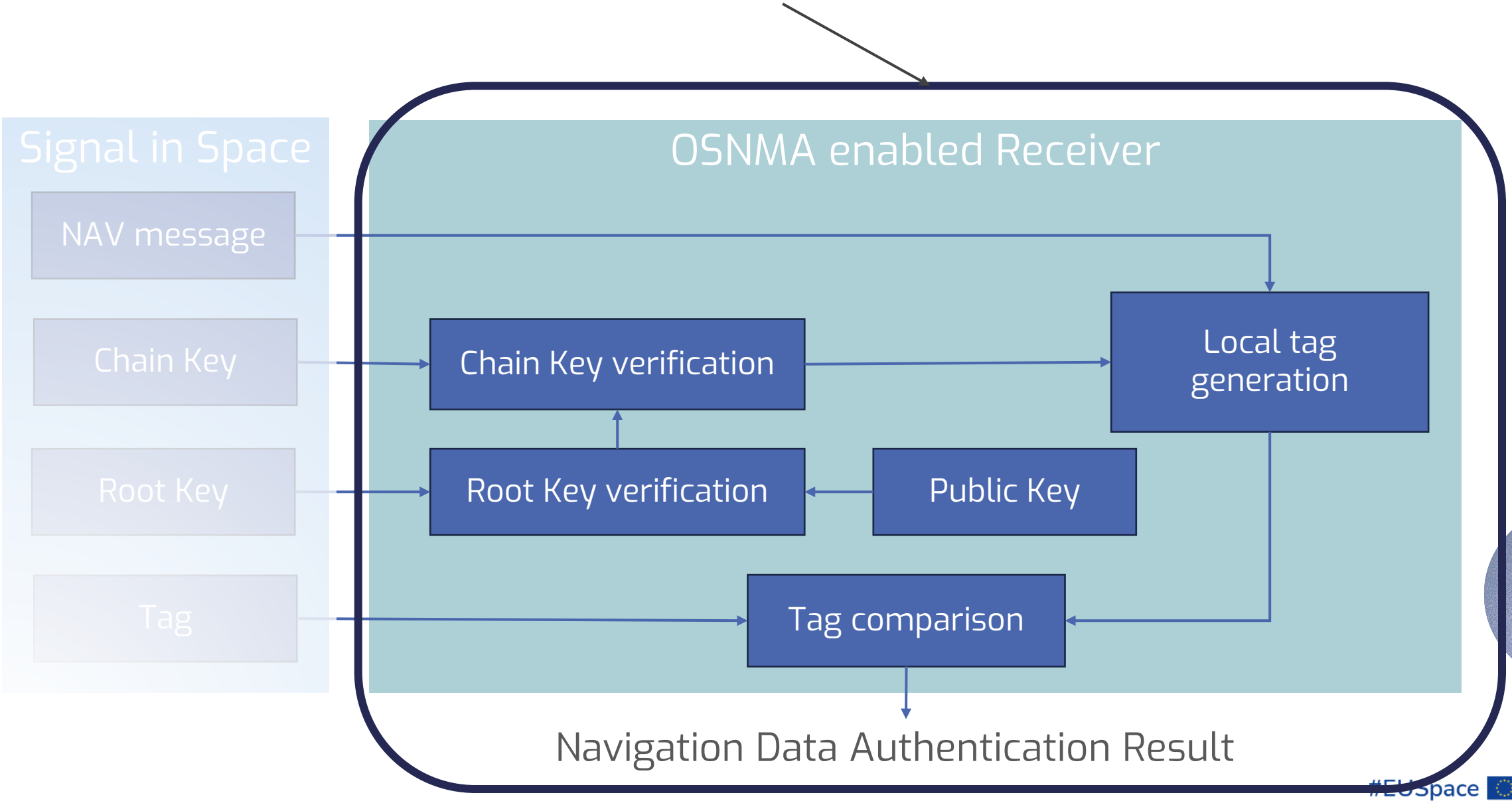


Chapter 3. OSNMA data retrieval



Chapter 4. Workflow and status monitoring




Signal in Space
NAV message
Chain Key
Root Key
Tag
OSNMA enabled Receiver
Chain Key verification
Local tag generation
Root Key verification
Public Key
Tag comparison
Navigation Data Authentication Result

OSNMA processing logic

To ensure the secure implementation of the OSNMA protocol, all requirements and mandated checks must be correctly implemented as specified in the guidelines.

Test Vectors

In addition to the Signal in Space (SiS), sample data and test vectors are provided in the annexes of the receiver guidelines. These resources facilitate:

- Individual validation of each verification step in the process.
- End-to-end testing of the implementation under nominal conditions.
- Validation of corner cases related to the renewal and revocation of cryptographic material, including the TESLA chain, public key, and Merkle tree.

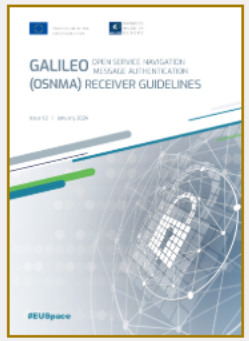
Nominal – Operational
Chain renewal (EOC)
Chain revocation (CREV)
Public Key renewal (NPK)
Public Key revocation (PKREV)
Merkle Tree renewal (NMT)
OSNMA Alert Message (OAM)

Test Vectors

The test vectors are provided as an Annex to the guidelines on the GSC web-portal.

A detailed description of the test vectors is provided in the Annex 2 of the Galileo OSNMA Receiver Guidelines.

Galileo OSNMA Receiver Guidelines (v1.3)

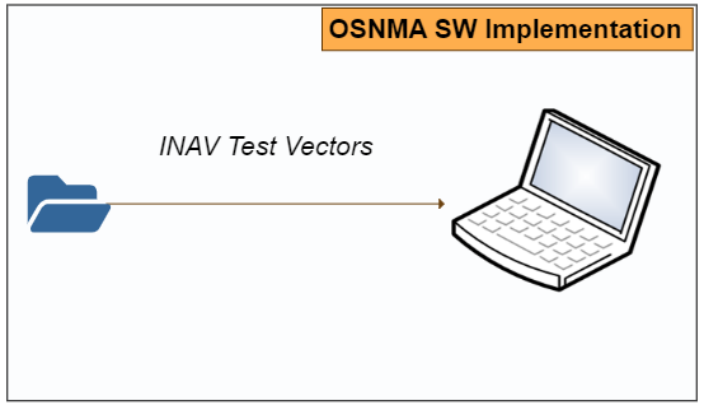


Annex B - OSNMA Test Vectors

Test Vectors

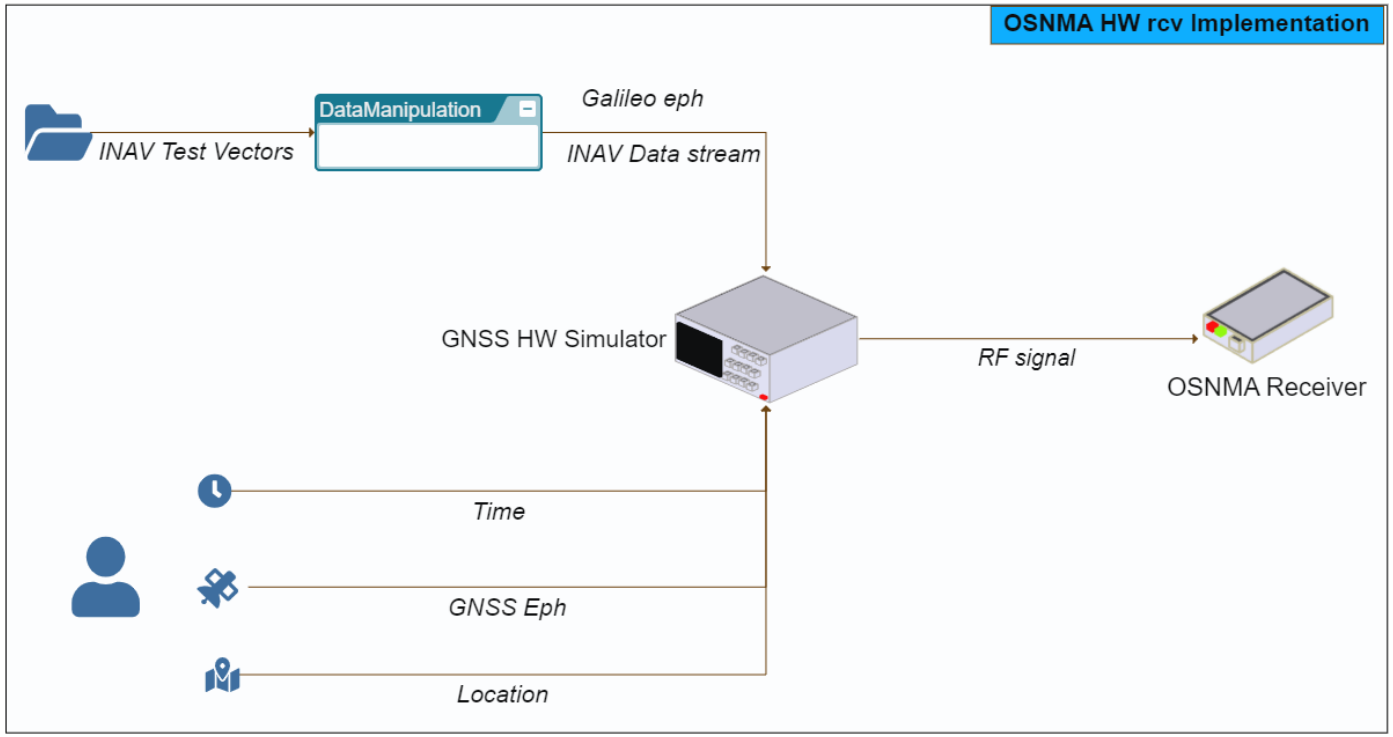
SW Implementation:

- Bypasses RF section, test the OSNMA module
- Speed and repeatability



HW Implementation:

- End-to-end test.
- Based on the use of a GNSS simulator accepting external INAV stream.
- Can be used to simulate also different testing conditions (e.g. dynamic, degraded reception).



Conclusions

- These guidelines support manufacturers and application developers in leveraging the added value of navigation data authentication.
- Users are encouraged to develop specific strategies exploiting information from OSNMA verification steps, such as handling failures, based on their unique needs.
- For any questions regarding implementation, support is available at the GSC helpdesk: helpdesk@gsc-europa.eu.

Conclusions

- OSNMA provides a means to **authenticate navigation data**, which can then be used to compute a PVT solution. However, it is important to note that since PVT computation relies on non-verified ranging data, it cannot be considered authenticated.
- Future services, such as **SAS** and **Galileo 2nd Generation** services, will provide range authentication.
- OSNMA serves as a valuable **contribution** from the Galileo system aimed at enhancing the resilience of its signals. To ensure a robust PVT calculation, it is recommended to supplement OSNMA with additional verification checks (Annex D).

#EUSpace

EUSPA
European Union Agency for the Space Programme

Linking space to user needs

Get in touch with us

www.euspa.europa.eu

EUSPA | EU4Space | EUSPA | space4eu | EUSPA

EUSPA OSNMA Day 2026