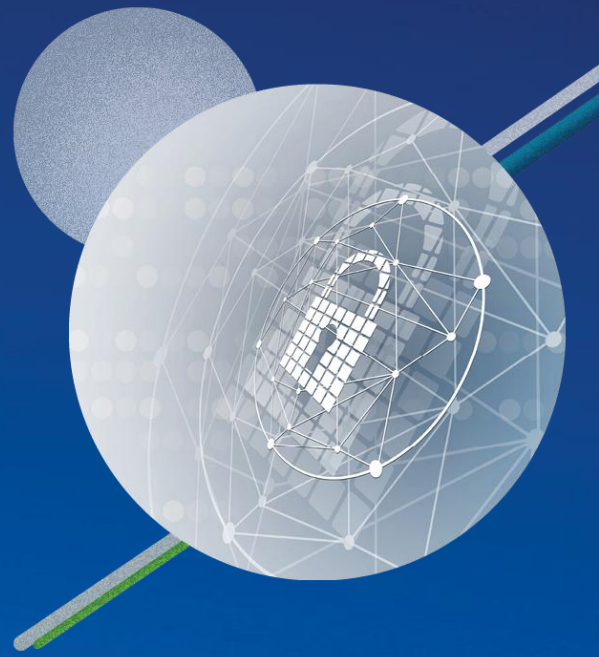
#EUSpace



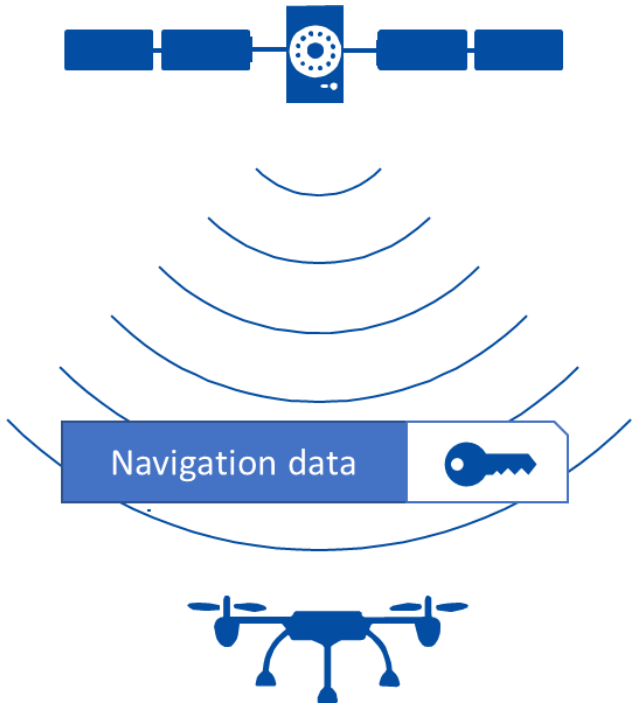
OSNMA definition, status and future developments

EUSPA OSNMA Day 2026

Javier Simon. OSNMA Service Manager. EUSPA

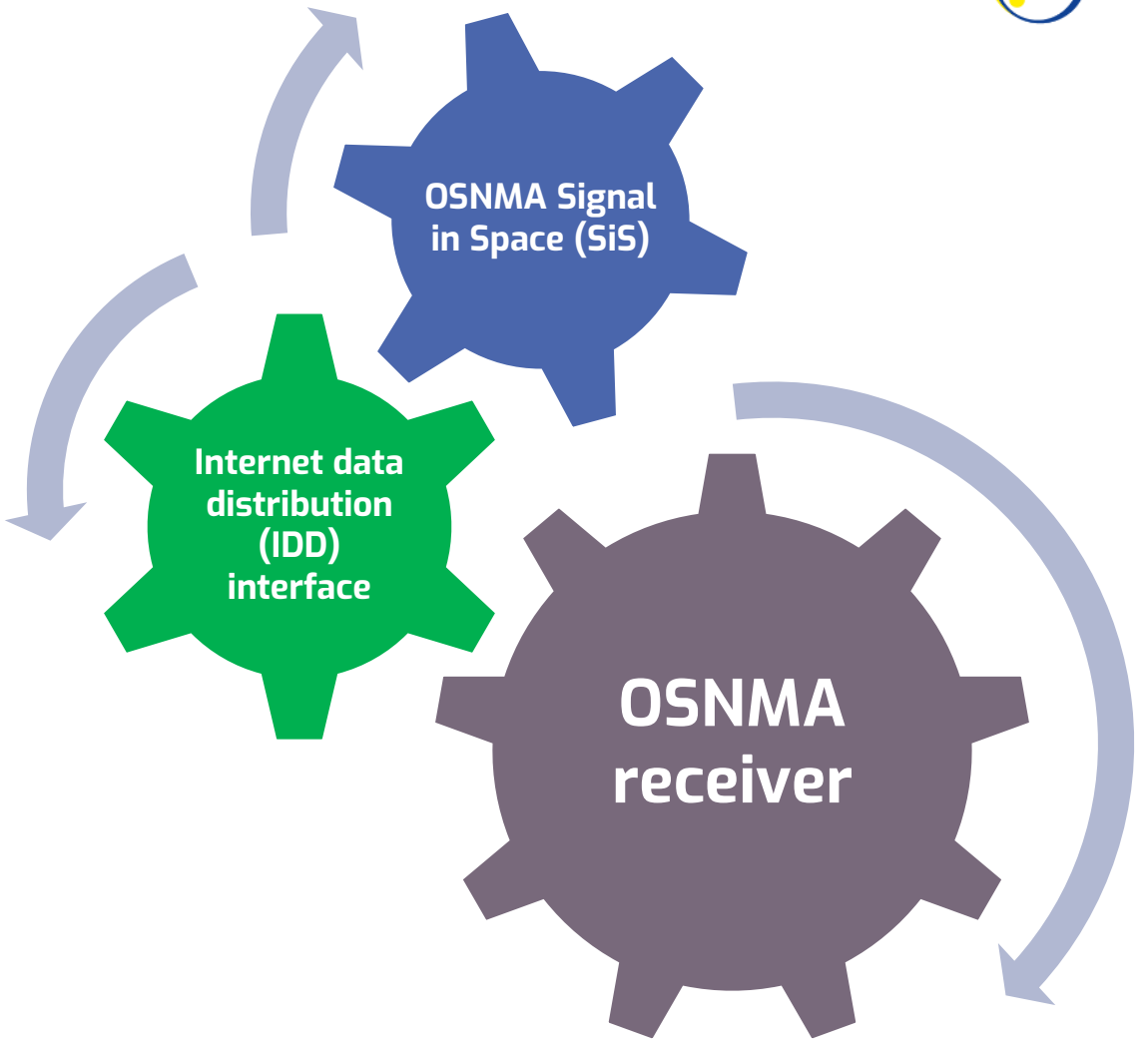
EUSPA
European Union Agency for the Space Programme

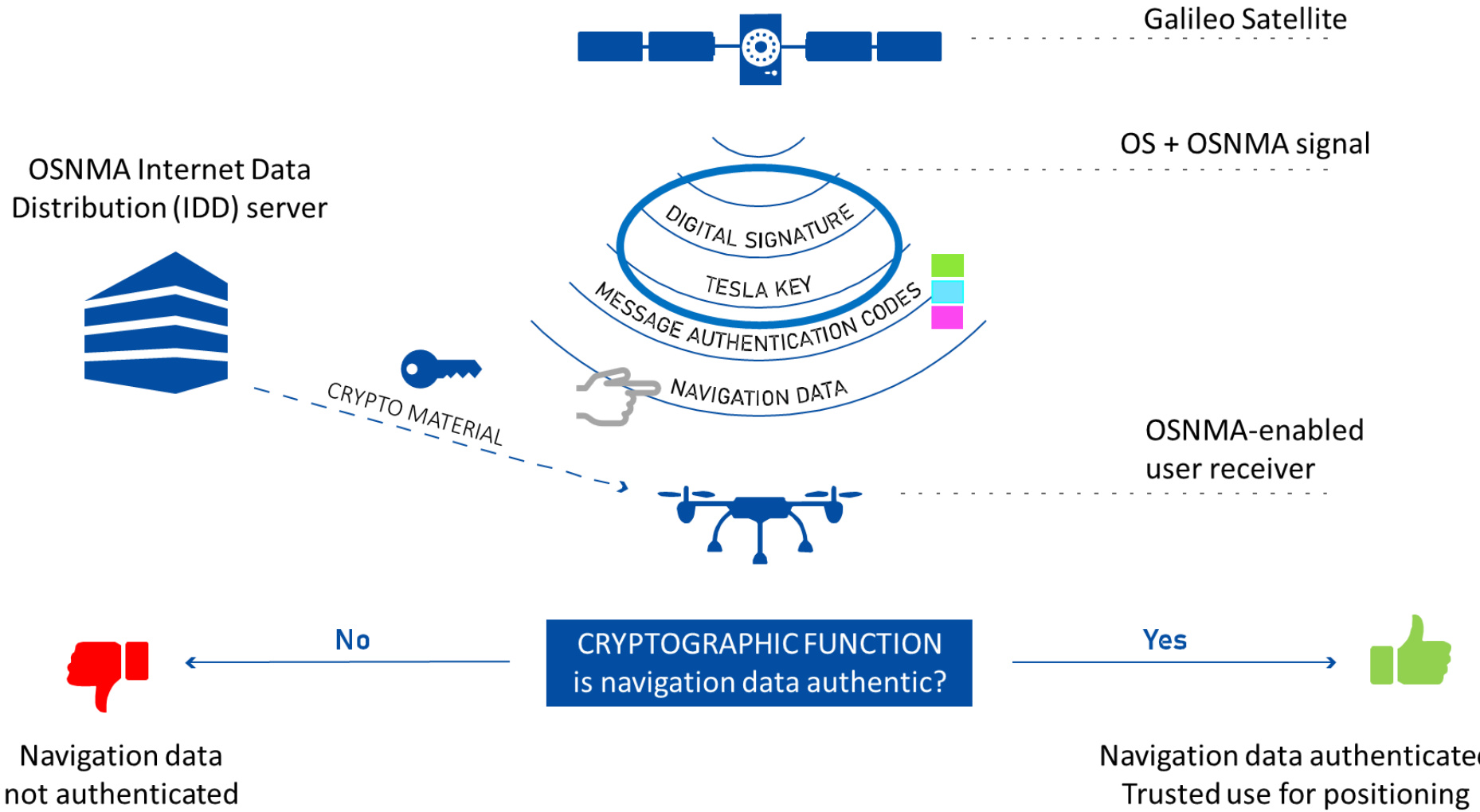
OSNMA Definition

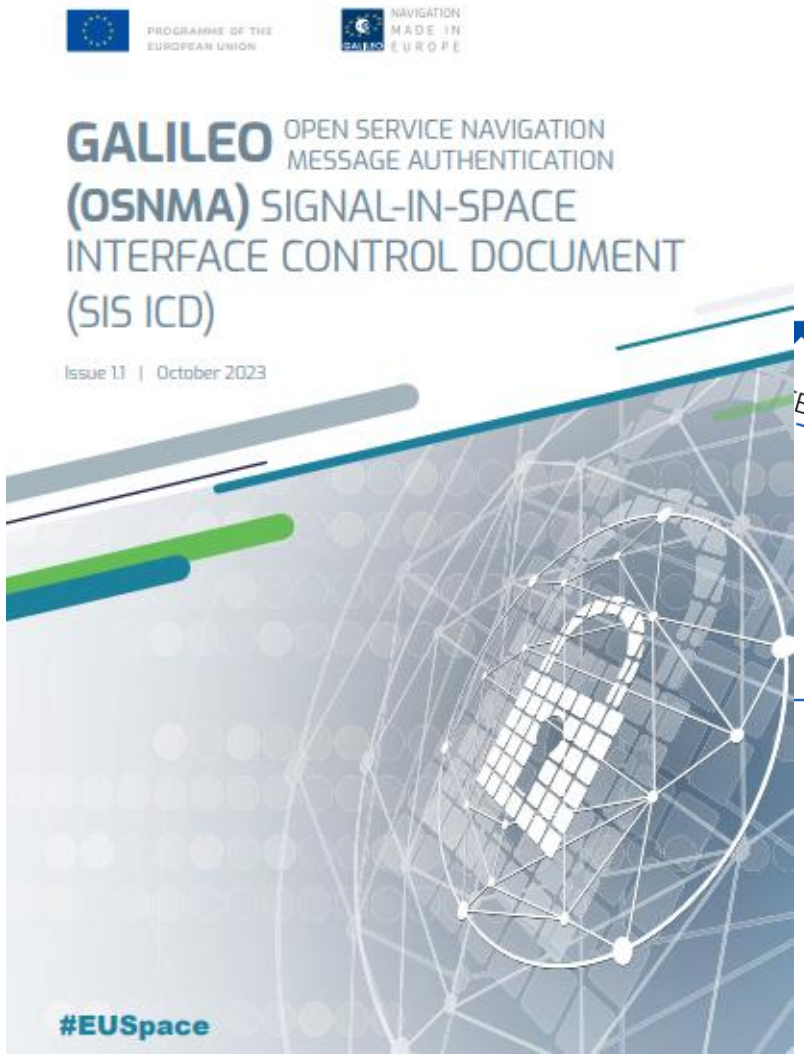


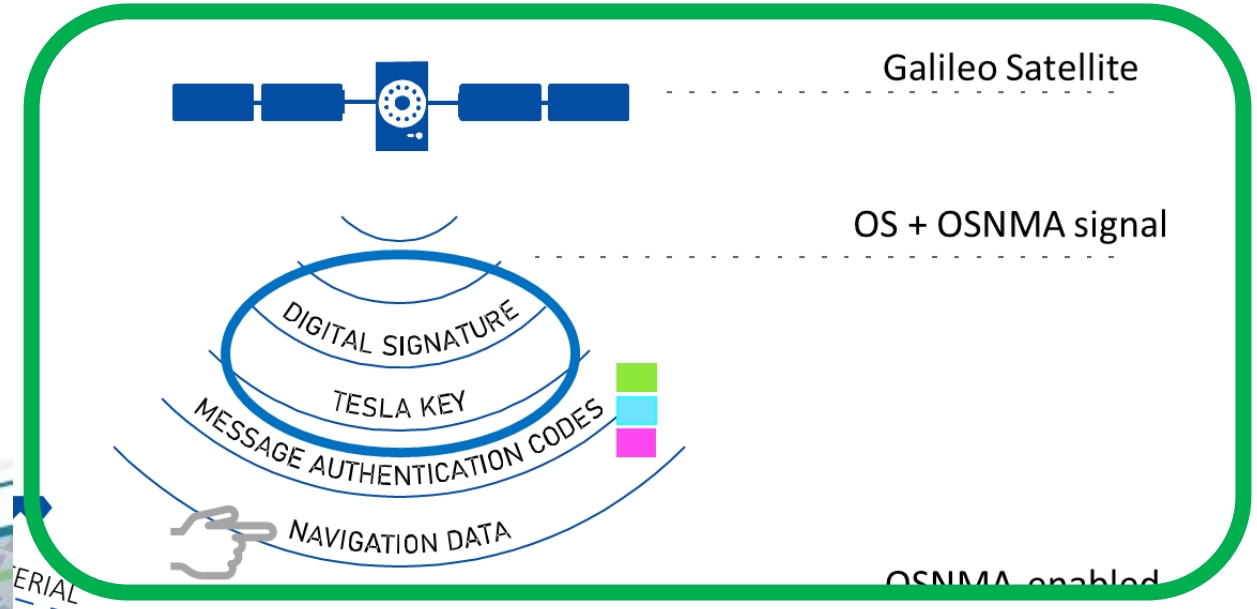
- **Galileo first generation** contribution to increase the robustness of the Open Service user position
- Fully **backwards compatible**
- Disseminated on the first Galileo frequency (**E1B**)
- Targets same positioning performance as for standard Open Service user: **accuracy, availability**
- **No need to store secret keys in the receiver** (public material needed). Need to guarantee integrity of stored material in Receiver. Additional user synchronization requirements.
- Follows current **cryptographic standards**

- Data authentication service on a one-way channel
- Interfaces towards users via Signal in Space and Internet Data Distribution interface
- Receiver contribution is key to achieve the authentication: **receiver logic and requirements**

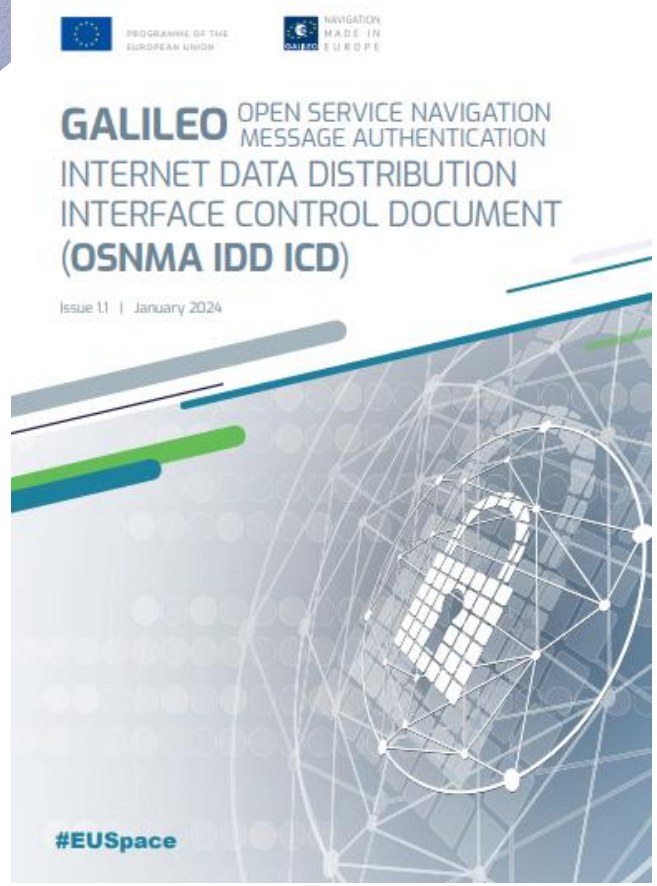


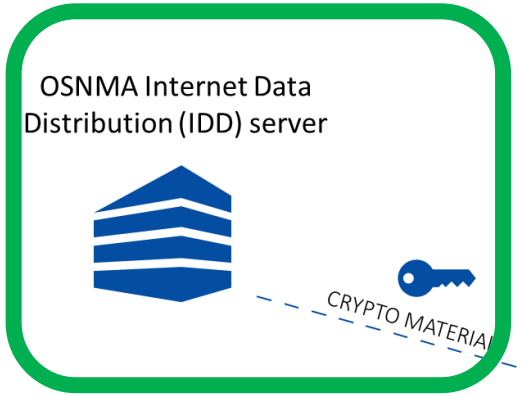

Galileo Satellite
OS + OSNMA signal
OSNMA Internet Data Distribution (IDD) server
DIGITAL SIGNATURE
TESLA KEY
MESSAGE AUTHENTICATION CODES
NAVIGATION DATA
CRYPTO MATERIAL
OSNMA-enabled user receiver
No
CRYPTOGRAPHIC FUNCTION is navigation data authentic?
Yes
Navigation data not authenticated
Navigation data authenticated Trusted use for positioning



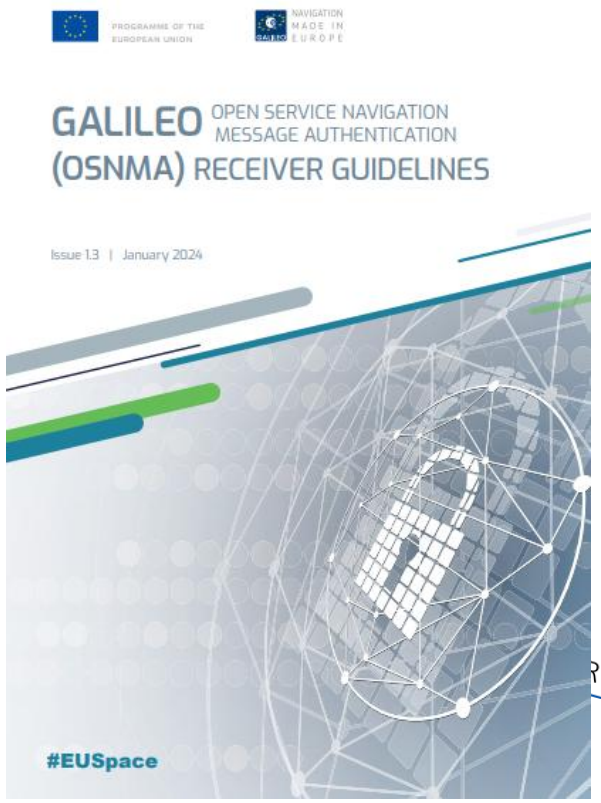


- 600 bits of OSNMA data every 30 seconds (I/NAV subframe) from a satellite transmitting OSNMA data (dynamic). Cross authentication for satellites not transmitting OSNMA: **Digital Signature, TESLA keys, Message Authentication Codes**.
- Three different authentication types (Message Authentication Codes / Tag):
  - Authentication for I/NAV navigation message data of Word Types 1 – 5 (ADKD0 and ADKD12 for receivers with lower synchronization performance).
  - Authentication for GST-UTC and GST-GPS conversion parameters (ADKD4).
- OSNMA Signal in Space has the capability to renew/revoke cryptographic material, without requiring frequent connection to the server. Need to connection to the server notified through the Signal in Space.

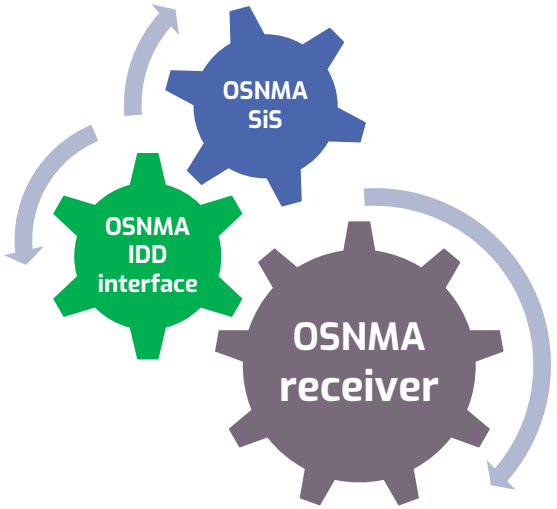


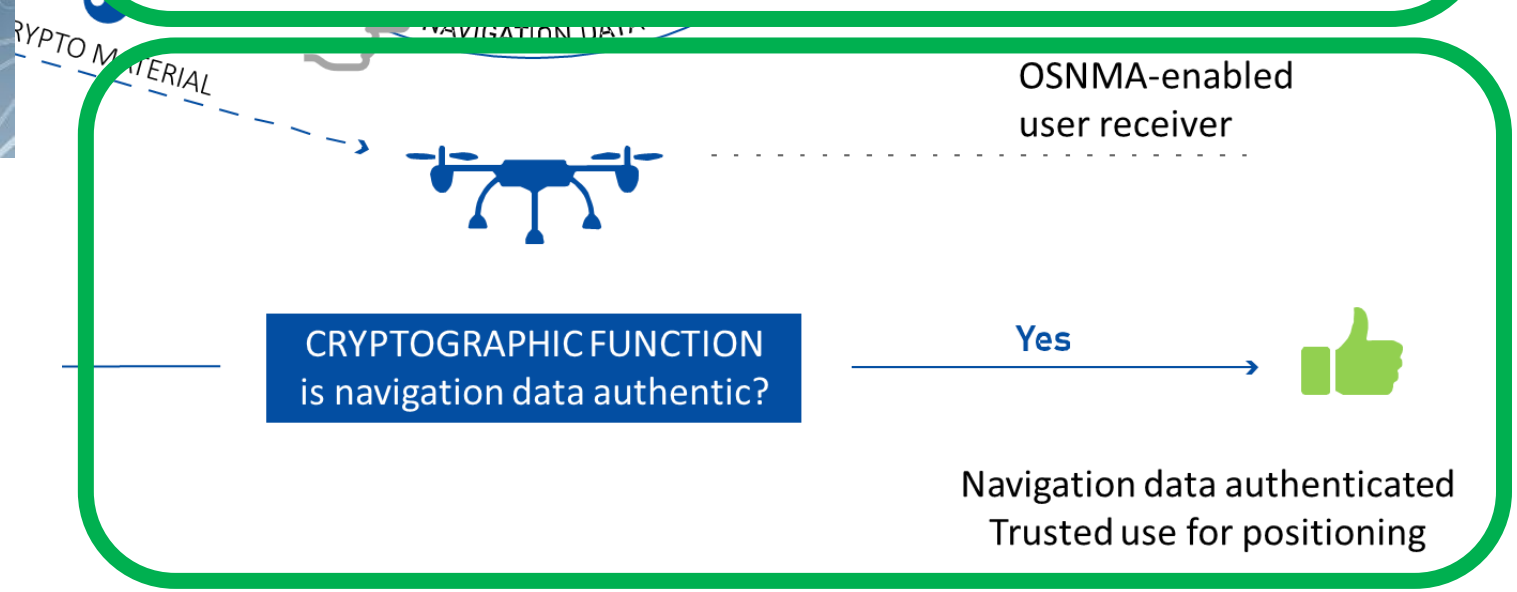


- Provision of **offline** OSNMA cryptographic material to the OSNMA user segment: **Merkle tree root (mandatory element)** and **Public Keys** (*GSC webportal – registration*) and associated **digital certificates** generated by **EUSPA Public Key Infrastructure** (*GSC webportal – registration – and EUSPA webportal*).
- **Public Key Infrastructure** provides a chain of trust to inject OSNMA cryptographic material in the user segment.
- Merkle tree root renewal is expected to take place very rarely, typically after more than 10 years. New Merkle tree to be published two years in advance of a renewal.
- Associated Certificate Policy and Certification Practice Statement (CP/CPS) for each certification authority (RCA, SCA and ICA) of the EUSPA PKI infrastructure published.



- Specification of the user segment implementation to ensure the End-to-End authentication process.
- Requirements on user segment side:
  - Time synchronization requirement (2 levels for processing of ADKD0/ADKD4 or ADKD12)
  - Integrity of cryptographic material and functions
- Examples of OSNMA verifications and OSNMA test vectors to support user segment development.



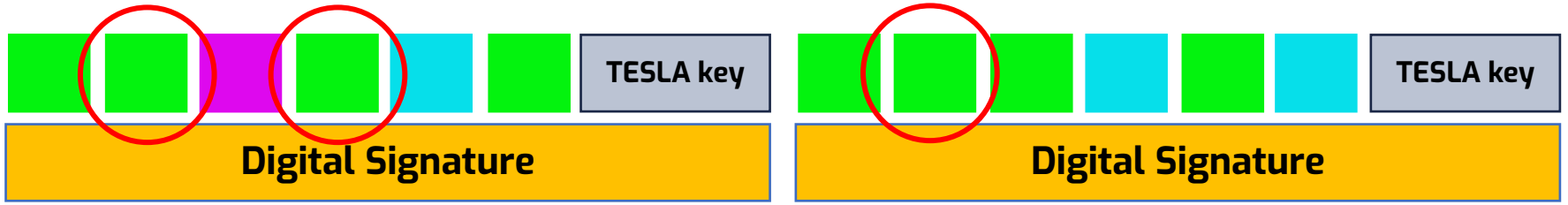


OSNMA user documentation tree

- Documentation available in the European GNSS Service Center (GSC) webportal (https://www.gsc-europa.eu/electronic-library/programme-reference-documents):
  - OSNMA Signal in Space Interface Control Document (OSNMA SiS ICD).
  - OSNMA Internet data Distribution Interface Control Document (OSNMA IDD ICD).
  - OSNMA Receiver guidelines.
- OSNMA cryptographic material available as of 16/01/2024:
  - Merkle Tree Root and Public Key (GSC webportal – registration).
  - Associated Digital Certificates generated by EUSPA Public Key Infrastructure (GSC webportal – registration – and EUSPA webportal).

OSNMA Initial Service Configuration

Parameter	Configuration
Public Key Type	ECDSA P-256
TESLA Chain Hash Function	SHA-256
MAC Function	HMAC-SHA-256
TESLA Key length	128 bits
Public Key	Public Key ID = 1. Applicable as of 2024-01-15T10:00:00 UTC Public Key ID = 2. Applicable as of 2025-12-10T10:00:00 UTC
Merkle Tree Root	Applicable as of 2024-01-15 10:00:00 UTC
MAC Lookup Table	ID =34 1st I/NAV subframe (30 seconds) : 00S, **FLX**, 04S, **FLX**, 12S, 00E 2nd I/NAV subframe (30 seconds): 00S, **FLX**, 00E, 12S, 00E, 12E



I/NAV subframe #N

I/NAV subframe #N+1

The OSNMA Service Definition Document

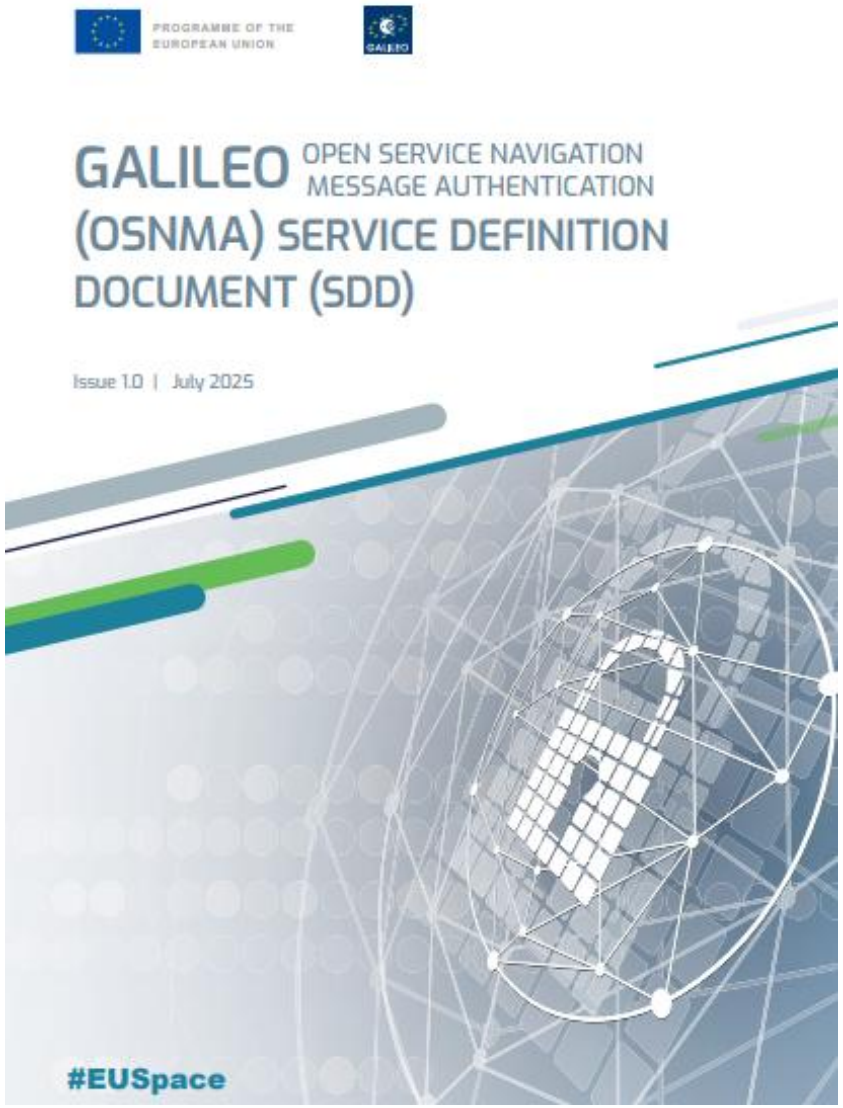


TABLE OF CONTENTS

"With OSNMA, Galileo provides Navigation Message Authentication (NMA) for relevant elements of the broadcast Open Service navigation data. Subject to the terms and conditions of the present document, this gives the OSNMA enabled receivers the assurance that the received Galileo navigation message is coming from the system itself and has not been modified, thus increasing the likelihood of detecting spoofing attacks at data level and significantly contributing to the security of the solution"

Usage conditions and performance objectives

Usage conditions

- User implementation of requirements and processing logic from OSNMA receiver guidelines.
- The tag length to be verified for a given navigation data set, is set to 40 bits for OSNMA Initial Service.
- Service in Operational status and the use of the applicable cryptographic material.

Performance objectives

- To provide OSNMA and OS equivalent navigation performance for users with nominal synchronization capabilities (ADKD0 Tags).
- To provide authentication data for at least four satellites in view from a user location for users with nominal and low synchronization capabilities (ADKD12 Tags).
- To provide authentication for broadcast timing parameters (ADKD4 Tags) for at least one satellite in view from a user location.

MPL = Minimum Performance Level

OSNMA Minimum Performance Levels (MPL)

OSNMA MPL at data broadcast level: availability of OSNMA data for the 3 authentication types

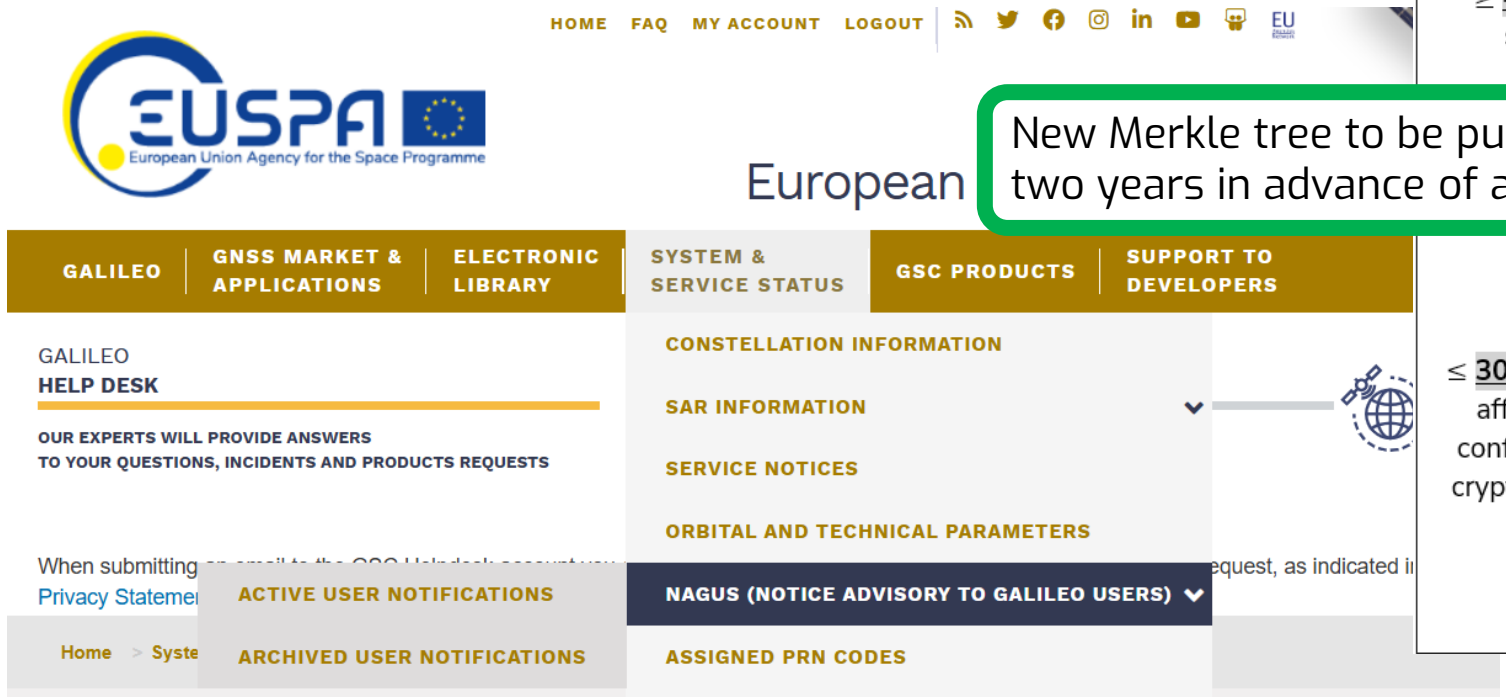
FIGURE OF MERIT	MPL	CONDITIONS AND CONSTRAINTS	
Availability of OSNMA data (I/NAV navigation message, ADKD0)	≥ 95%	For **at least four** Galileo nominal or auxiliary satellites in view within a period of 30 seconds	• From any point in the service coverage. • Above a minimum elevation angle of 5 degrees. • Calculated over a one-year period. • Including planned and unplanned outages. • When the data being authenticated is broadcast in the SIS. • Excluding dummy tags.
	≥ 80%	For **all** Galileo nominal or auxiliary satellites in view within a period of 600 seconds	
Availability of OSNMA data (I/NAV navigation message, ADKD12)	≥ 95%	For **at least four** Galileo nominal or auxiliary satellites in view within a period of 240 seconds	
Availability of OSNMA data (GST-UTC and GGTO parameters, ADKD4)	≥ 97%	For **at least one** Galileo nominal or auxiliary satellite in view within a period of 60 seconds	

OSNMA Minimum Performance Levels (MPL)

OSNMA MPL at positioning level: availability of authenticated satellites versus satellites available for standard Open Service

FIGURE OF MERIT	MPL	CONDITIONS AND CONSTRAINTS
Availability of OS-equivalent OSNMA navigation solution (I/NAV navigation message, ADKD0)	≥ 95%	• Same satellites used by the OS and the OSNMA user. • From any point in the service coverage. • Above a minimum elevation angle of 5 degrees for PVT calculation. • Calculated over a one-year period. • Including planned and unplanned outages. • Excluding dummy tags.

OSNMA Minimum Performance Levels (MPL)



New Merkle tree to be published two years in advance of a renewal

MPL OF THE TIMELY PUBLICATION OF NAGUs	CONDITIONS AND CONSTRAINTS
≥ 48 hours before the service is affected	• Notification to users of scheduled service outages impacting the OSNMA broadcast, or updates of OSNMA related crypto material (renovation of OSNMA Public key, TESLA key chain or Merkle Tree).
≤ 30 hours after the event affecting the service is confirmed or the OSNMA crypto material is updated	• Notification to users of unscheduled service outages impacting the OSNMA broadcast, or updates of OSNMA related crypto material (revocation of OSNMA Public key or TESLA key chain) or the OAM broadcast.

OSNMA performance

NAVIGATION SOLUTIONS POWERED BY EUROPE

EUROPEAN GNSS (GALILEO)

OSNMA

QUARTERLY PERFORMANCE REPORT

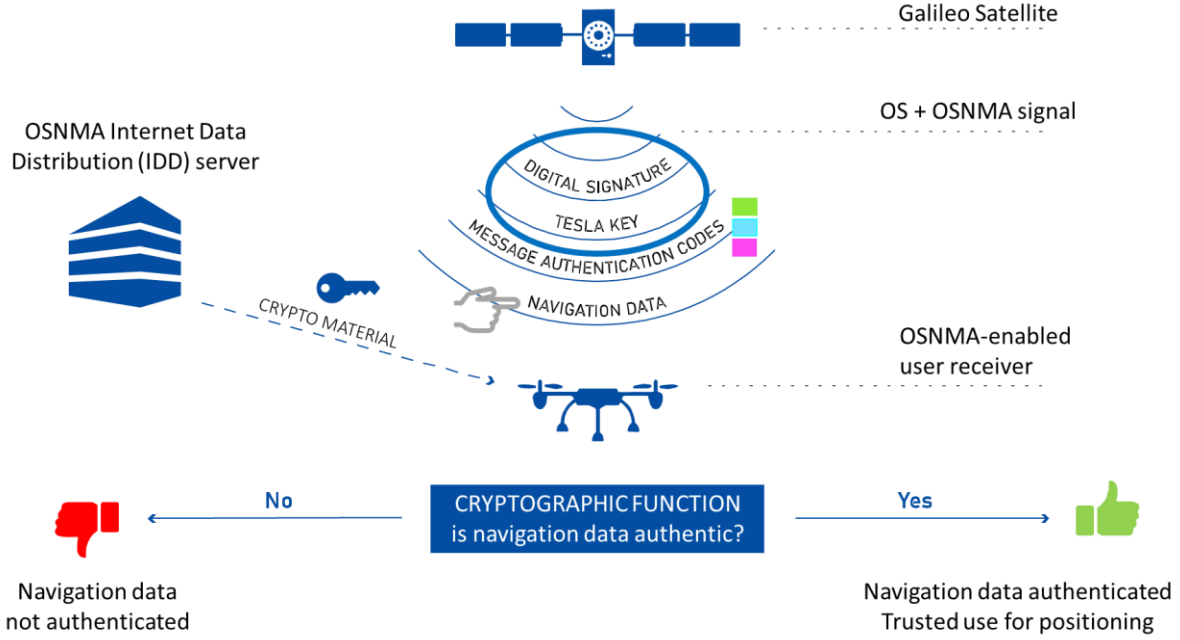
JULY - SEPTEMBER 2025

OSNMA performance – MPL compliance

OSNMA Performance Parameter Conditions and Constraints	MPL	August	September	October	November	December
Availability ADKD0, I/NAV navigation message						
For at least four Galileo nominal or auxiliary satellites in view within a period of 30 seconds.	≥ 95%	99.33%	99.60%	99.64%	99.70%	99.68%
For all Galileo nominal or auxiliary satellites in view within a period of 600 seconds	≥ 80%	94.95%	95.59%	95.42%	96.07%	96.28%
Availability ADKD12, I/NAV navigation message						
For at least four Galileo nominal or auxiliary satellites in view within a period of 240 seconds.	≥ 95%	98.32%	99.13%	99.20%	99.26%	99.20%
Availability ADKD4, GST-UTC and GGTO parameters						
For at least one Galileo nominal or auxiliary satellites in view within a period of 60 seconds.	≥ 97%	99.55%	99.77%	99.80%	99.83%	99.82%
Availability of OS-equivalent OSNMA navigation solution						
Same satellites used by the OS and the OSNMA user	≥ 95%	99.55%	99.77%	99.67%	99.20%	99.21%

OSNMA performance – time to fix

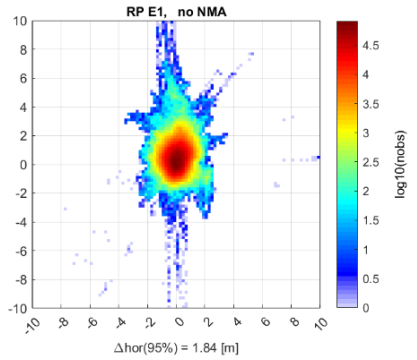
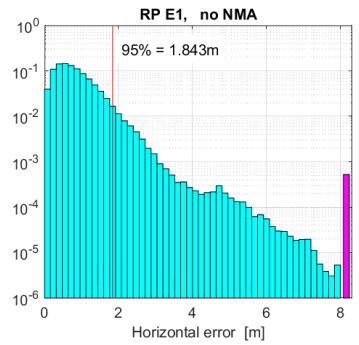
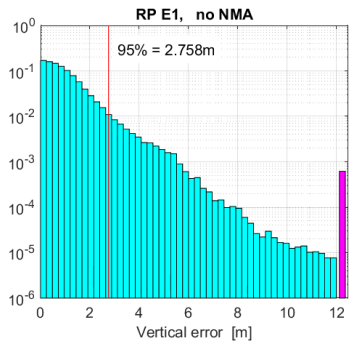
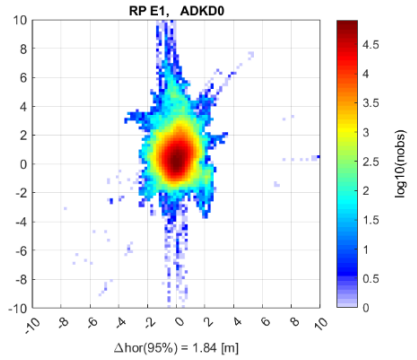
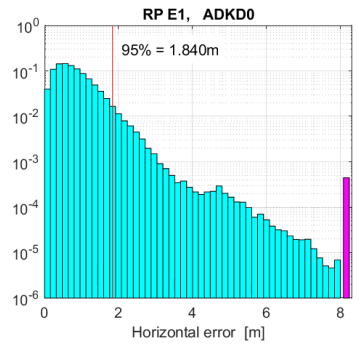
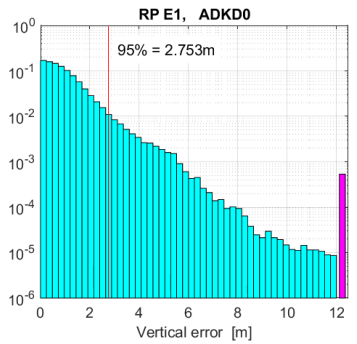
- OSNMA Cold Start: Public Key not available (Merkle tree root available):
  - Retrieved from SiS.
  - Possibility to retrieve it from IDD interface (connected devices).
- OSNMA Warm Start: Public Key available; TESLA Root Key missing.
- OSNMA Hot Start: Public Key and TESLA Root Key available.



MAC type	Hot start 95%	Warm start 95%	Cold start 95%
ADKD0	130 seconds	300 seconds	≤ 6 hours
ADKD12	460 seconds	520 seconds	≤ 6 hours

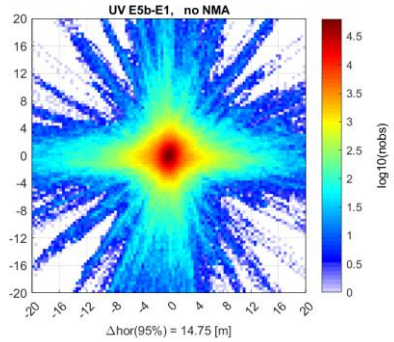
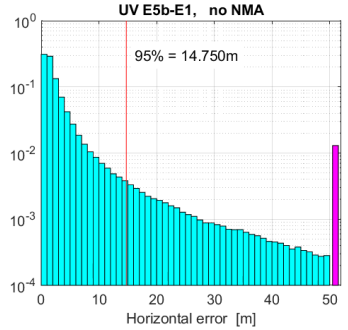
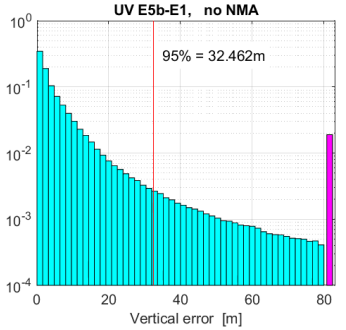
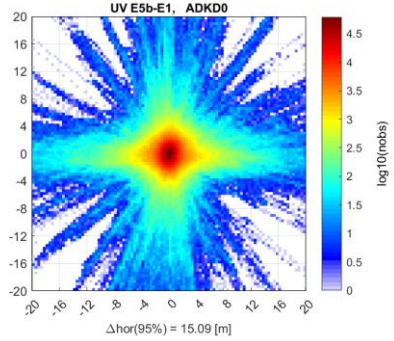
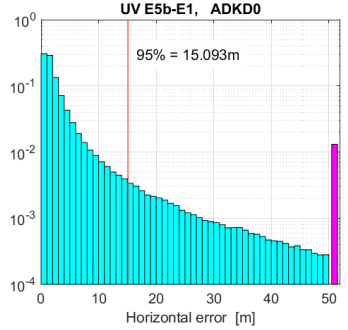
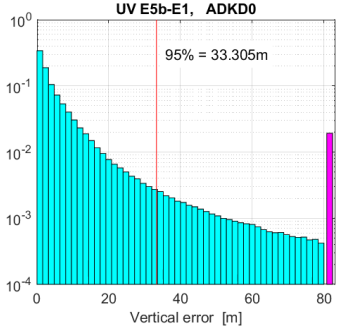
OSNMA performance

OSNMA performance

Scenario	Error distribution		
	Horizontal (2-D)	Horizontal	Vertical
OS			
OSNMA (ADKD0)			

Accuracy performance in rural static scenario using OSNMA

OSNMA performance

Scenario	Error distribution		
	Horizontal (2-D)	Horizontal	Vertical
OS			
OSNMA (ADKD0)			

Accuracy performance in urban static scenario using OSNMA

OSNMA future developments

- OSNMA will provide authentication of additional data types (e.g: Galileo F/NAV navigation data) and will be broadcast in additional Galileo signal components. Final target is that every broadcast Galileo navigation data is authenticated.

- OSNMA will provide authentication data for GPS broadcast navigation message (L1 C/A).

- OSNMA will evolve to face the quantum threat (public specifications not available yet).

- OSNMA will be complemented with additional capabilities, starting from Signal Authentication Service (SAS) to provide users the means to compute an authenticated PVT. Receiver contribution will remain critical.

#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