#EUSpace

Galileo OSNMA: What, why and when?

European Commission

EUSPA European Union Agency for the Space Programme

Ignacio Fernandez-Hernandez, European Commission, DG DEFIS D2

Table of Content

Galileo OSNMA

- What is Galileo OSNMA
- Why Galileo OSNMA
- Galileo OSNMA timeline

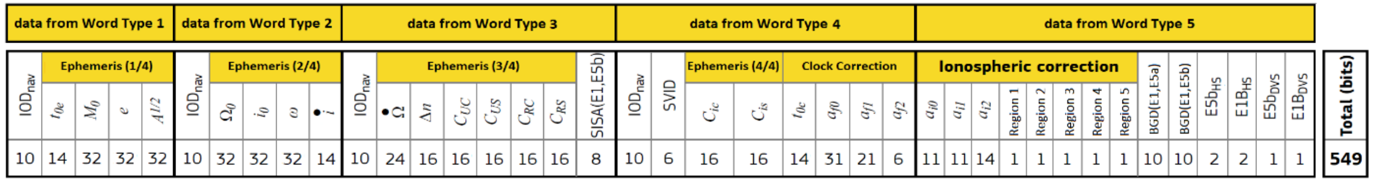
Table of Content

- **What is Galileo OSNMA**
- Why Galileo OSNMA
- Galileo OSNMA timeline

What is Galileo OSNMA

Galileo
OSNMA

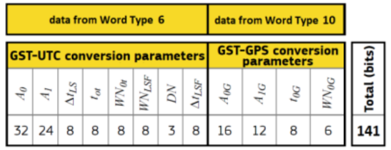
- OSNMA stands for Open Service Navigation Message Authentication
- It is a mechanism to authenticate the Galileo data used to calculate a position:
  - Satellite orbits, clock corrections, additional data (flags, SISA, biases), ionospheric information: ADKD0 (30s key delay), ADKD12 (330s key delay)



data from Word Type 1					data from Word Type 2					data from Word Type 3							
IOD$_{nav}$	Ephemeris (1/4)				IOD$_{nav}$	Ephemeris (2/4)				IOD$_{nav}$	Ephemeris (3/4)						SISA(E1,E5b)
	t_{0e}	M_0	e	$A^{1/2}$		Ω_0	i_0	ω	$\dot{i}$		$\dot{\Omega}$	Δn	C_{UC}	C_{US}	C_{RC}	C_{RS}	
10	14	32	32	32	10	32	32	32	14	10	24	16	16	16	16	16	8

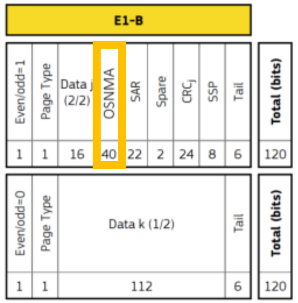
data from Word Type 4								data from Word Type 5														
IOD$_{nav}$	SVID	Ephemeris (4/4)		Clock Correction				Ionospheric correction								BGD(E1,E5a)	BGD(E1,E5b)	E5b$_{HS}$	E1B$_{HS}$	E5b$_{DVS}$	E1B$_{DVS}$	Total (bits)
		C_{ic}	C_{is}	t_{0c}	a_{f0}	a_{f1}	a_{f2}	a_{i0}	a_{i1}	a_{i2}	Region 1	Region 2	Region 3	Region 4	Region 5							
10	6	16	16	14	31	21	6	11	11	14	1	1	1	1	1	10	10	2	2	1	1	**549**

  - Galileo System Time (GST) to UTC and GPS Time conversion parameters: ADKD4



data from Word Type 6								data from Word Type 10				
GST-UTC conversion parameters								GST-GPS conversion parameters				Total (bits)
A_0	A_1	Δt_{LS}	t_{0t}	WN_{0t}	WN_{LSF}	DN	Δt_{LSF}	A_{0G}	A_{1G}	t_{0G}	WN_{0G}	
32	24	8	8	8	8	3	8	16	12	8	6	**141**

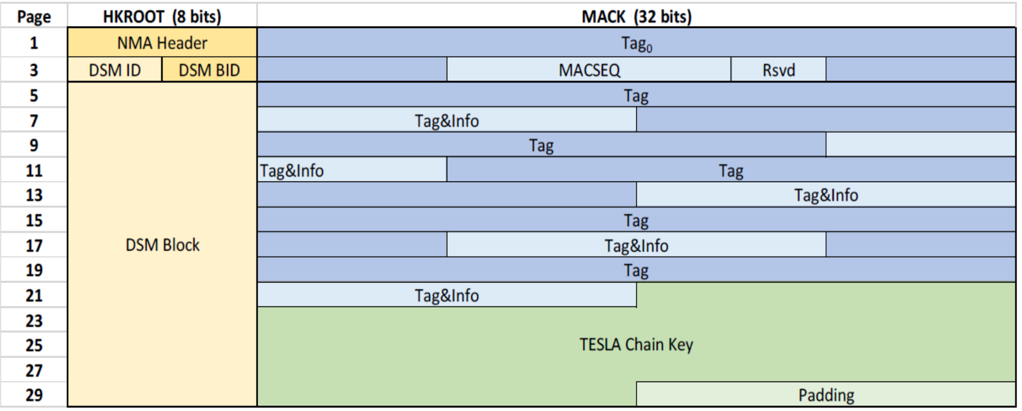
  - It is transmitted in 40 bits every 2 seconds in the Galileo E1 I/NAV (1575.42 MHz)
  - It is equivalent to a Galileo "digital signature"
  - It makes the signal unpredictable
  - **Galileo OSNMA is the first-ever civil GNSS authentication capability**



E1-B									
Even/odd=1	Page Type	Data j (2/2)	OSNMA	SAR	Spare	CRC$_j$	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

Galileo OSNMA

- How does it work?
  - The OSNMA 40-bit field transmits short (also 40 bit) message authentication codes (MACs), or *tags*, using a secret key
  - The tags carry an ‘information’ field with: what authentication type and key delay (ADKD): 0, 12, 4; what satellite is authenticated, and some other information
  - After 30 seconds (ADKD0, ADKD4), the previously secret MAC key is disclosed, allowing the receiver to authenticate the data
  - The protocol includes a so-called *TESLA keychain* to authenticate the key, and other cryptographic layers (Public Key, Merkle tree), plus some status parameters
  - Galileo OSNMA protocol is better suited for high-loss low-bandwidth channels such as those of GNSS
  - **The receiver needs an external synchronization of 30s-300s accuracy to ensure the whole signal stream is not a replay with spoofed data**



Page	HKROOT (8 bits)		MACK (32 bits)
1	NMA Header		Tag_0
3	DSM ID	DSM BID	MACSEQ Rsvd
5	DSM Block		Tag
7			Tag&Info
9			Tag
11			Tag&Info Tag
13			Tag&Info
15			Tag
17			Tag&Info
19			Tag
21			Tag&Info TESLA Chain Key
23			
25			
27			
29			Padding

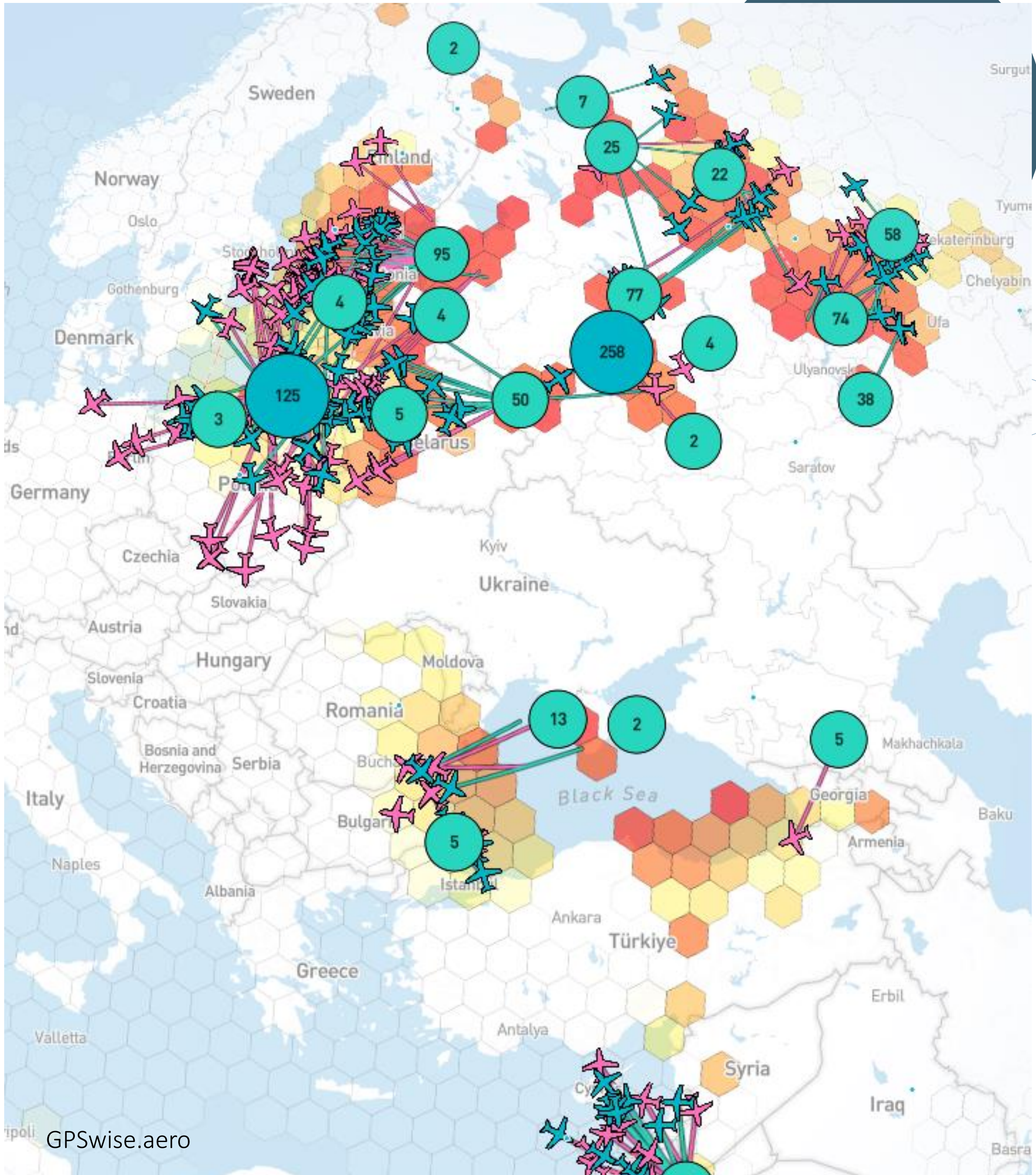
- NMA Header: General status (test, operational…), crypto status (nominal, new key, revoked…)
- DSM: Digital Siguature Message: signs root TESLA key chain or public key
- Tag: authenticate orbits and clocks or time, of current or near satellite
- TESLA Chain Key: authenticates the tags of the previous subframe

Table of Content

- What is Galileo OSNMA
- **Why Galileo OSNMA**
- Galileo OSNMA timeline

Why Galileo OSNMA

- GNSS nowadays is a utility, but it is subject to interference:
    - Jamming -> Denial of Service
    - Spoofing -> Misleading information, with hazardous consequences
- Both GNSS spoofing and jamming are happening today, massively. Spoofing threat has moved from the lab (2000s) to the field (2020s)
- GNSS is one of the few digital data that *was* not yet authenticated



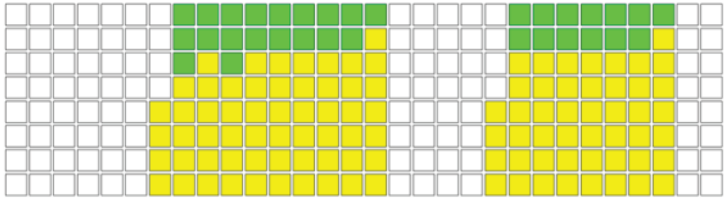
GPSwise.aero

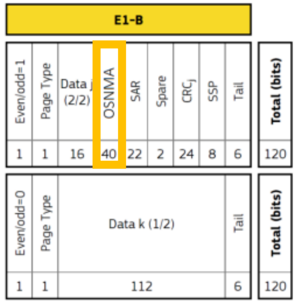
Why Galileo OSNMA

Galileo OSNMA

What can OSNMA do?

- Ensure data is protected, but data-authentic PVT can also be spoofed
- OSNMA makes the signal unpredictable and more difficult to replay
- Combined with receiver checks, it is very complicated to spoof an OSNMA receiver
- GNSS can be combined with other sources (INS, LEO, terrestrial…) for resilient PNT
- OSNMA does not require major changes to the receiver, but proper implementation is required:
    - Cryptographic operations
    - Receiver logic: data-authentication is not PVT authentication
    - Time synchronization requirement
    - Integration with other checks

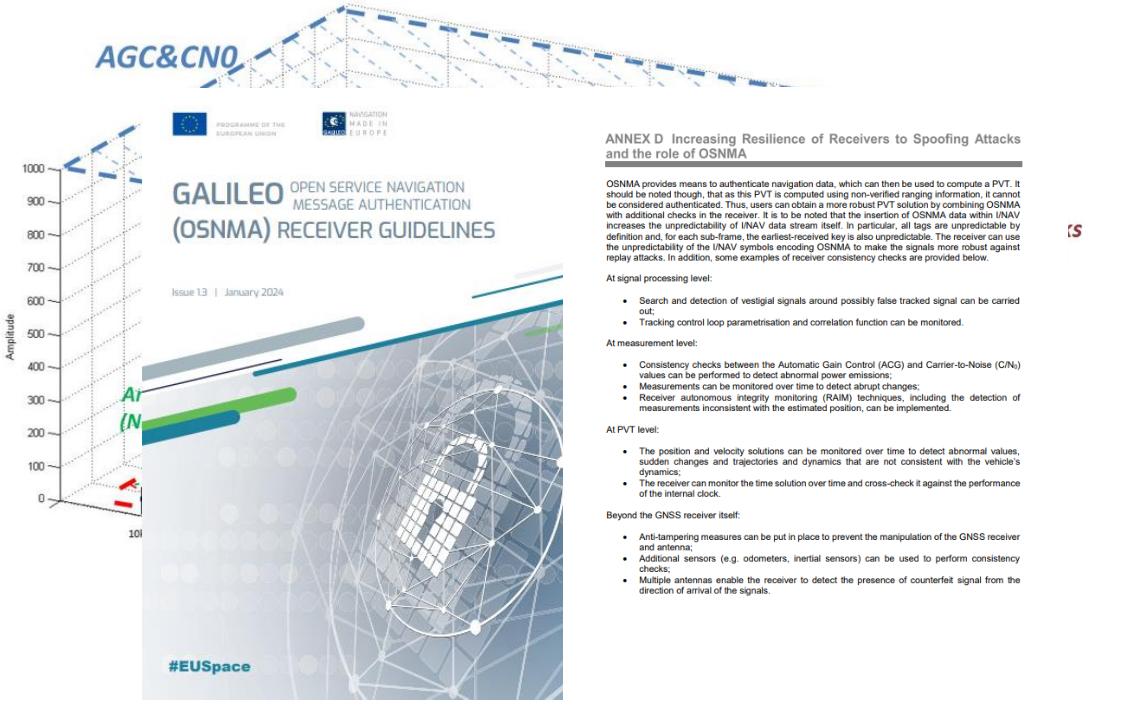




E1-B

Even/odd=1	Page Type	Data j (2/2)	OSNMA	SAR	Spare	CRC$_j$	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



GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OSNMA) RECEIVER GUIDELINES

Issue 1.3 | January 2024

#EUSpace

ANNEX D Increasing Resilience of Receivers to Spoofing Attacks and the role of OSNMA

OSNMA provides means to authenticate navigation data, which can then be used to compute a PVT. It should be noted though, that as this PVT is computed using non-verified ranging information, it cannot be considered authenticated. Thus, users can obtain a more robust PVT solution by combining OSNMA with additional checks in the receiver. It is to be noted that the insertion of OSNMA data within I/NAV increases the unpredictability of I/NAV data stream itself. In particular, all tags are unpredictable by definition and, for each sub-frame, the earliest-received key is also unpredictable. The receiver can use the unpredictability of the I/NAV symbols encoding OSNMA to make the signals more robust against replay attacks. In addition, some examples of receiver consistency checks are provided below.

At signal processing level:

- Search and detection of vestigial signals around possibly false tracked signal can be carried out;
- Tracking control loop parametrisation and correlation function can be monitored.

At measurement level:

- Consistency checks between the Automatic Gain Control (ACG) and Carrier-to-Noise (C/N_0) values can be performed to detect abnormal power emissions;
- Measurements can be monitored over time to detect abrupt changes;
- Receiver autonomous integrity monitoring (RAIM) techniques, including the detection of measurements inconsistent with the estimated position, can be implemented.

At PVT level:

- The position and velocity solutions can be monitored over time to detect abnormal values, sudden changes and trajectories and dynamics that are not consistent with the vehicle's dynamics;
- The receiver can monitor the time solution over time and cross-check it against the performance of the internal clock.

Beyond the GNSS receiver itself:

- Anti-tampering measures can be put in place to prevent the manipulation of the GNSS receiver and antenna;
- Additional sensors (e.g. odometers, inertial sensors) can be used to perform consistency checks;
- Multiple antennas enable the receiver to detect the presence of counterfeit signal from the direction of arrival of the signals.

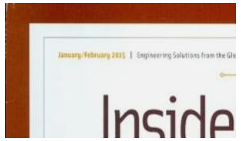
Table of Content

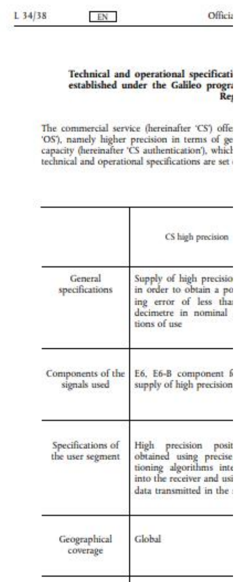
Galileo OSNMA

- What is Galileo OSNMA
- Why Galileo OSNMA
- **Galileo OSNMA timeline**

Galileo OSNMA timeline

- 2013-2015: first concepts and SIS testing, OSNMA end-to-end design and proof-of-concept
- 2016-2018: OSNMA formally introduced in Galileo service baseline; first full OSNMA test specs published
- 2019-2021: OSNMA developed in European GNSS Service Centre (GSC). First continuous SIS and start of OSNMA Public Observation Phase
- 2022-2025: OSNMA refinements and operational validation and accreditation
  - **24 July 2025: OSNMA Initial Service Declaration**
- 2026: SAS initial capability (testing) in E6C
- Post-2027: OSNMA enhanced service milestone, including better performance and new authentication messages (e.g. GPS L1C/A); SAS initial service; OSNMA G2

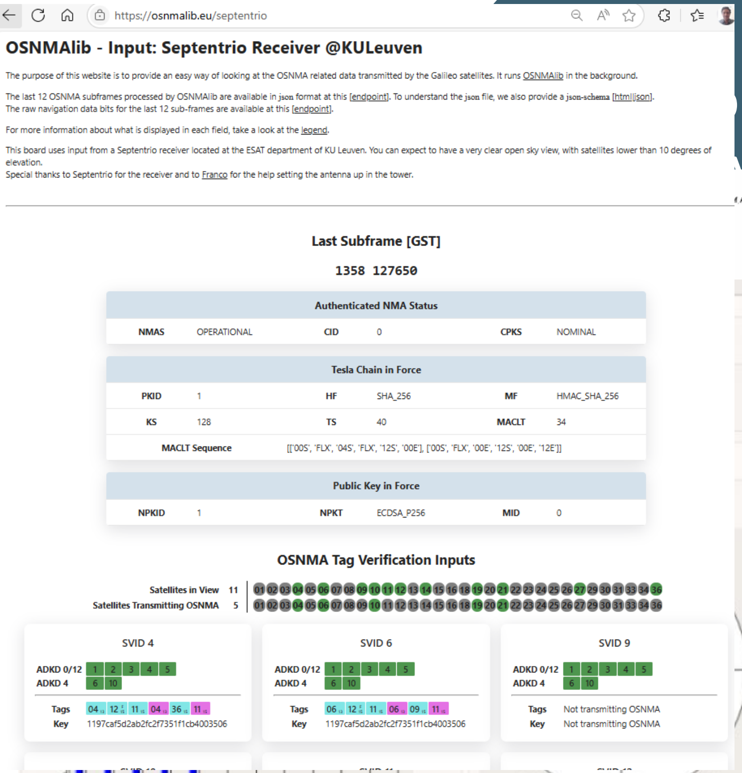



L 34/38 EN Officia

Technical and operational specificati established under the Galileo progra Re

The commercial service (hereinafter 'CS') offe 'OS'), namely higher precision in terms of ge capacity (hereinafter 'CS authentication'), which technical and operational specifications are set

	CS high precision
General specifications	Supply of high precisio in order to obtain a po ing error of less tha decimetre in nominal tions of use
Components of the signals used	E6, E6-B component f supply of high precision
Specifications of the user segment	High precision posit obtained using precise tioning algorithms inte into the receiver and usi data transmitted in the
Geographical coverage	Global


https://osnmalib.eu/septentrio

OSNMAlib - Input: Septentrio Receiver @KULeuven

The purpose of this website is to provide an easy way of looking at the OSNMA related data transmitted by the Galileo satellites. It runs OSNMAlib in the background.

The last 12 OSNMA subframes processed by OSNMAlib are available in json format at this [endpoint]. To understand the json file, we also provide a json-schema [html|json].
The raw navigation data bits for the last 12 sub-frames are available at this [endpoint].

For more information about what is displayed in each field, take a look at the legend.

This board uses input from a Septentrio receiver located at the ESAT department of KU Leuven. You can expect to have a very clear open sky view, with satellites lower than 10 degrees of elevation.
Special thanks to Septentrio for the receiver and to Franco for the help setting the antenna up in the tower.

Last Subframe [GST]

1358 127650

Authenticated NMA Status					
NMAS	OPERATIONAL	CID	0	CPKS	NOMINAL

Tesla Chain in Force					
PKID	1	HF	SHA_256	MF	HMAC_SHA_256
KS	128	TS	40	MACLT	34
MACLT Sequence	[['00S', 'FLX', '04S', 'FLX', '12S', '00E'], ['00S', 'FLX', '00E', '12S', '00E', '12E']]				

Public Key in Force					
NPKID	1	NPKT	ECDSA_P256	MID	0

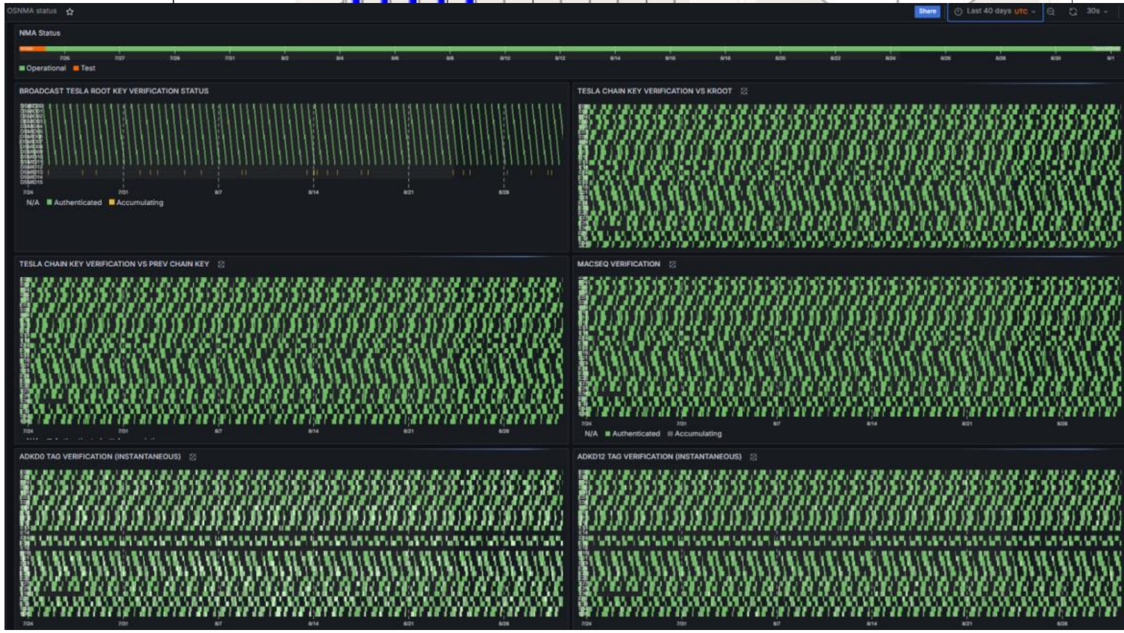
OSNMA Tag Verification Inputs

Satellites in View 11 | 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 18 19 20 21 22 23 24 25 26 27 29 30 31 33 34 36
Satellites Transmitting OSNMA 5 | 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 18 19 20 21 22 23 24 25 26 27 29 30 31 33 34 36

SVID 4
ADKD 0/12: 1 2 3 4 5
ADKD 4: 6 10
Tags: 04 12 11 04 36 11
Key: 1197caf5d2ab2fc2f7351f1cb4003506

SVID 6
ADKD 0/12: 1 2 3 4 5
ADKD 4: 6 10
Tags: 06 12 11 06 09 11
Key: 1197caf5d2ab2fc2f7351f1cb4003506

SVID 9
ADKD 0/12: 1 2 3 4 5
ADKD 4: 6 10
Tags: Not transmitting OSNMA
Key: Not transmitting OSNMA


OSNMA status
Share
Last 40 days UTC
NMA Status
Operational
Test
BROADCAST TESLA ROOT KEY VERIFICATION STATUS
N/A
Authenticated
Accumulating
TESLA CHAIN KEY VERIFICATION VS KROOT
TESLA CHAIN KEY VERIFICATION VS PREV CHAIN KEY
MACSEQ VERIFICATION
ADKD0 TAG VERIFICATION (INSTANTANEOUS)
ADKD12 TAG VERIFICATION (INSTANTANEOUS)

Sources: FhG, EUSPA; osnmalib.eu

Summary

Galileo OSNMA

- OSNMA authenticates Galileo navigation message (orbits, clocks, flags, ionosphere, time). It is the first-ever GNSS global and civil authentication capability
- Spoofing attacks are happening massively every day. OSNMA makes spoofing much more difficult, especially when benefiting from other receiver checks and signal unpredictability
- OSNMA launched operationally on 24 July 2025. Galileo will continue enhancing authentication services over the next years (SAS, OSNMA enhancements, G2G)

#EUSpace

Thank you

Ignacio Fernandez-Hernandez, European Commission, DG DEFIS D2

European Commission

EUSPA

European Union Agency for the Space Programme