



EU SPACE



# Galileo Open Service Navigation Message Authentication

Ignacio Fernández Hernández  
European Commission  
12 Oct 2022

# Table of contents

- What is Galileo OSNMA
- Current status
- Performance
- Next steps

# Table of contents

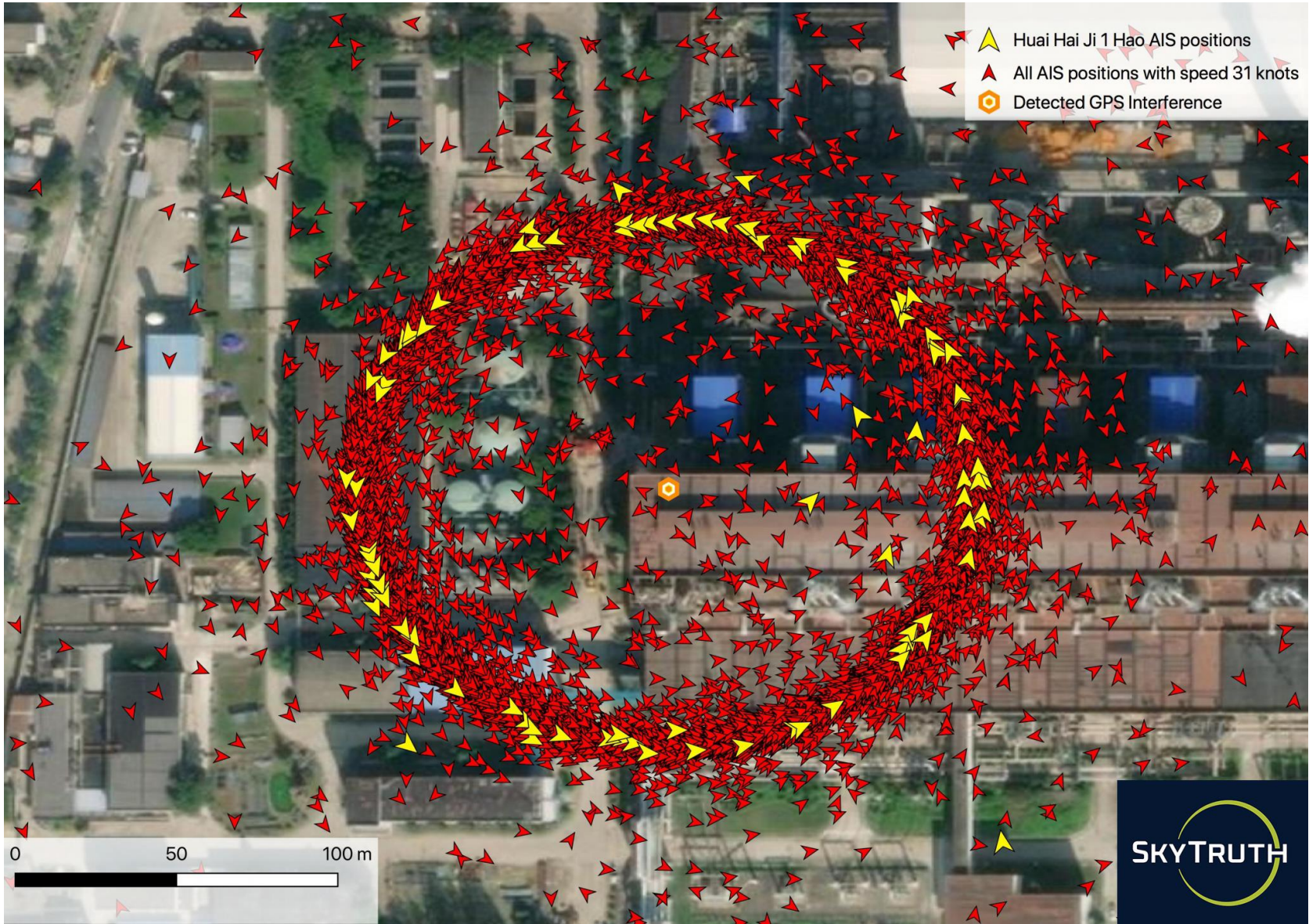
- **What is Galileo OSNMA**
- Current status
- Performance
- Next steps

# What is Galileo OSNMA

- What is Galileo OSNMA?
  - Stands for Open Service Navigation Message Authentication
  - Mechanism to authenticate the Galileo data used to calculate a position: satellite orbits and clock corrections, satellite status flags, time...
  - Equivalent to a Galileo “digital signature”
  - Transmitted in 40 bits every other second in the Galileo I/NAV message, E1B component, 1575.45 MHz
  - Makes the signal unpredictable
- Why OSNMA?











gps spoofing



### GPS Spoofing With The HackRF On Windows

69,218 visualizaciones · hace 2 años

Tech Minds

Note: I said 2.5ghz in the video but I meant 1.5Ghz for GPS signals. My antenna was 430mhz Would you like to help me fund a ...

4K



### GPS/GNSS Spoofing and How To Detect It

5592 visualizaciones · hace 2 años

GPSPATRON

00:18 GNSS Interference Issues 00:47 What is GNSS Spoofing? 01:35 Spoofing Detection Solution In this video, we describe ...

Subtítulos

GNSS Interference Issues | What is GNSS Spoofing? | Spoofing Detection Solution

3 momentos



### GPS Spoofer with HackRF One and Android Phone - Shockingly easy!

56,450 visualizaciones · hace 2 años

GPSPATRON

0:15 What is needed for a GNSS spoofing attack 1:36 Config and run gps-sdr-sim 2:45 Live spoofing experiment setup 3:36 ...

4K Subtítulos

What is needed for a GNSS spoofing attack | Config and run gps-sdr-sim | Live spoofing experiment...

8 momentos



### How to fool a GPS - Todd Humphreys

213,553 visualizaciones · hace 9 años

TED-Ed

Todd Humphreys forecasts the near-future of geolocation when millimeter-accurate GPS "dots" will enable you to find pin-point ...

11:55 ... hard and we wanted to be the first to build one so we could get out in front of the problem and help protect against GPS spo...



### How to Spoof Location on iPhone (2 Easy Ways Including Free One)

31,850 visualizaciones · hace 3 meses

Nick S

Hey guys, this video will show you how to spoof location on any iPhone with the help of two different methods including a free one ...

4K Subtítulos

Spooing GPS Location on iPhone with the Free Xcode

4 capítulos

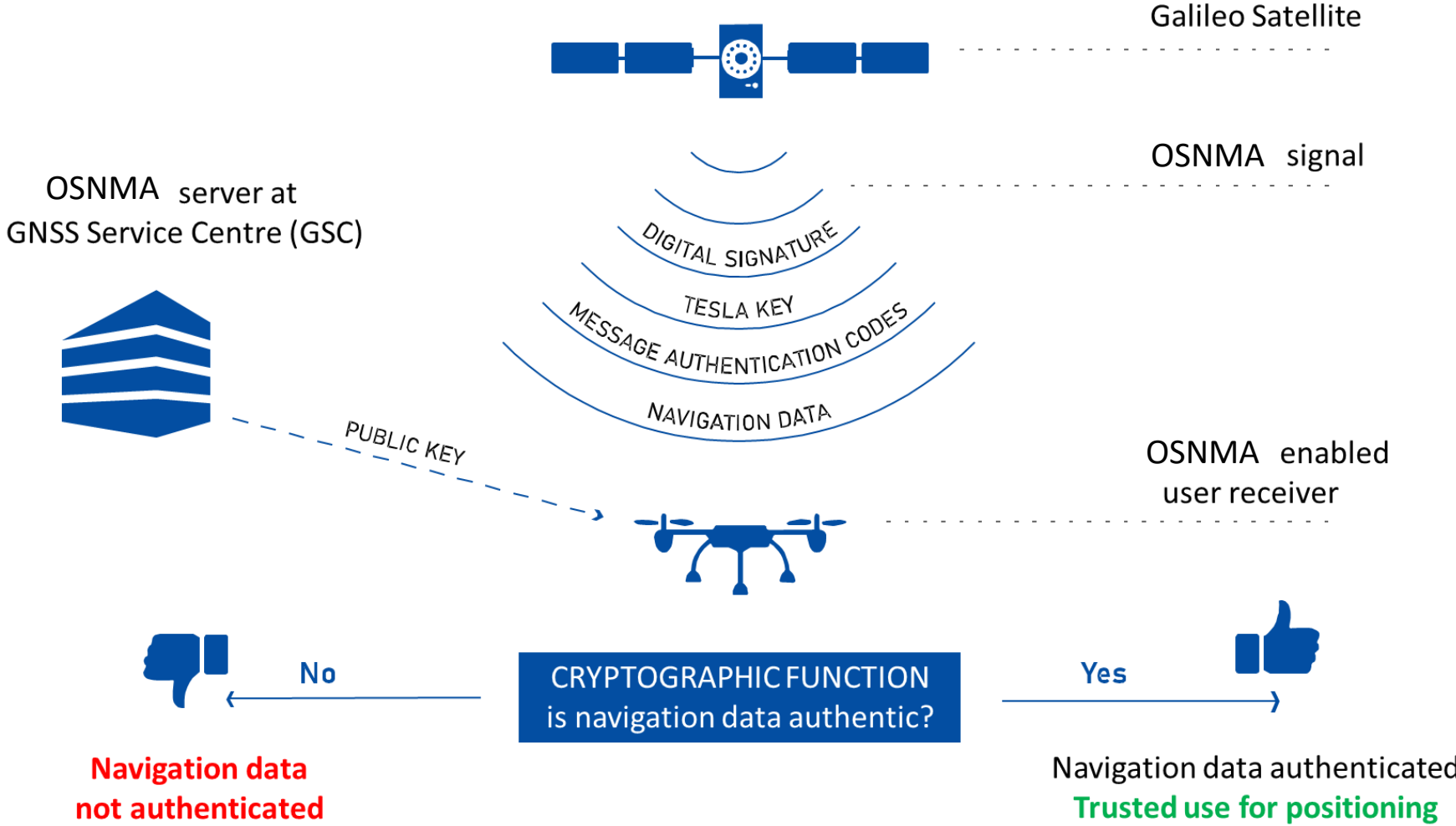


### Demonstration of a Remote Unmanned Aerial Vehicle Hijacking via GPS Spoofing

42,135 visualizaciones · hace 10 años

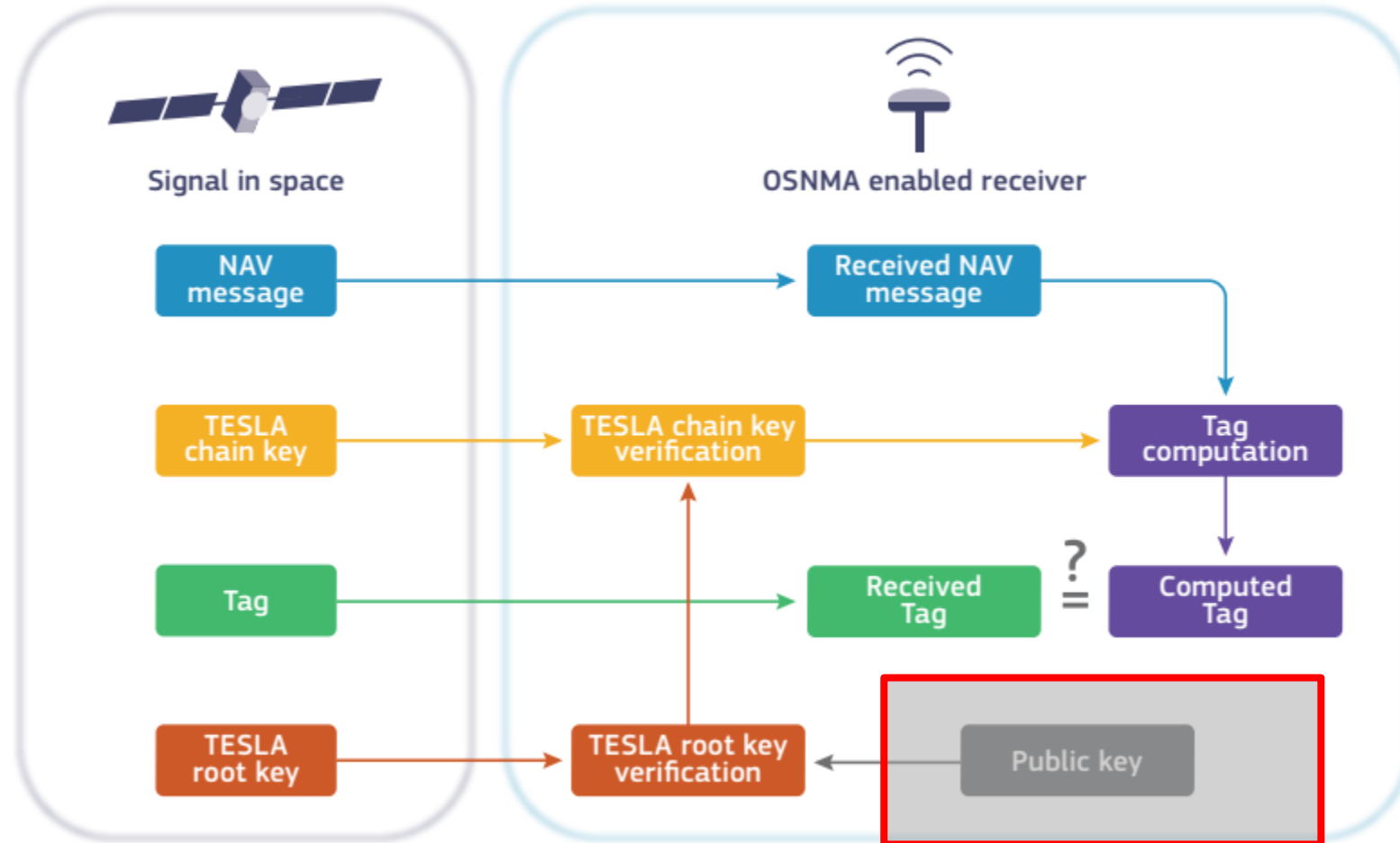
CockrellSchool

# What is Galileo OSNMA

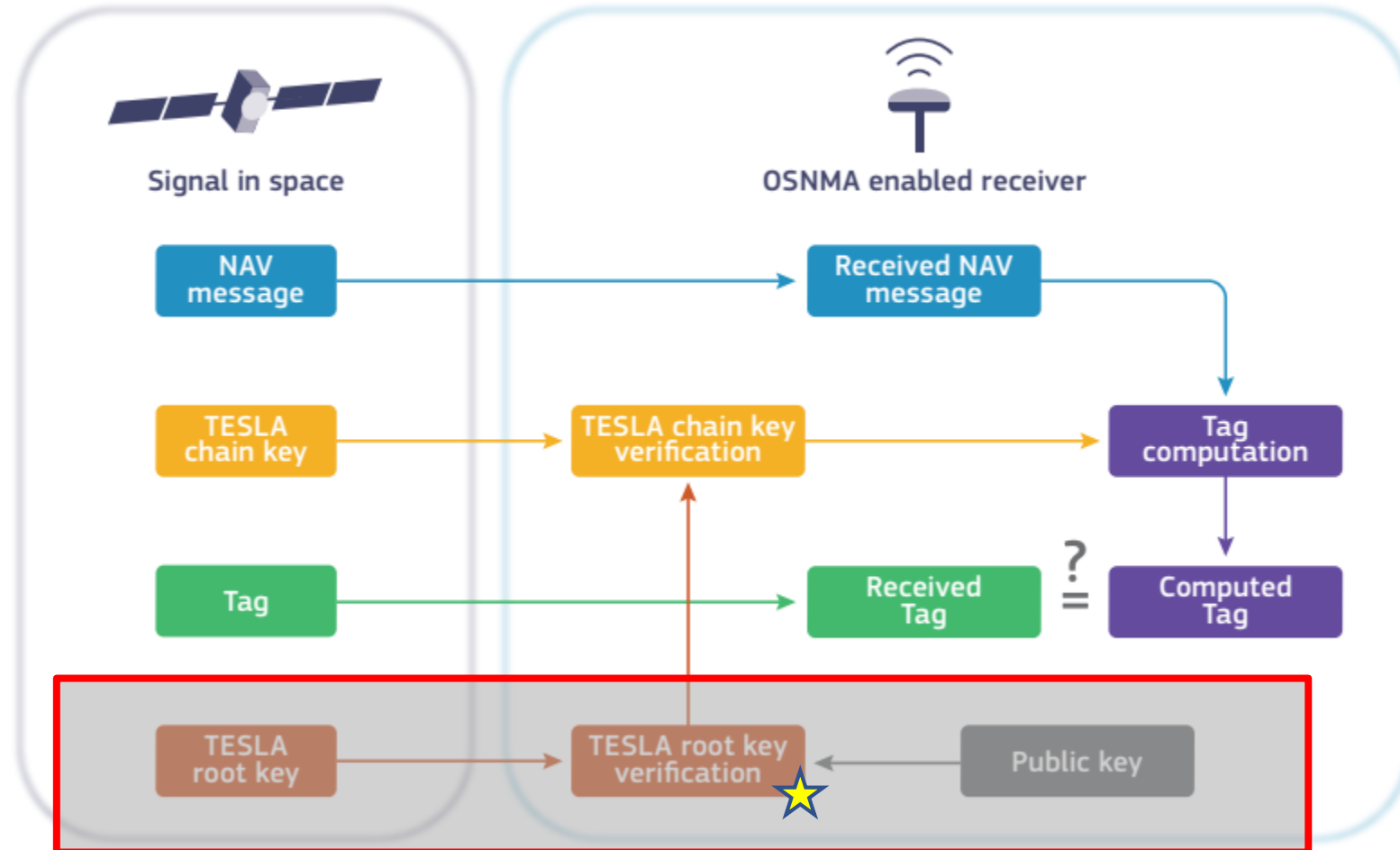




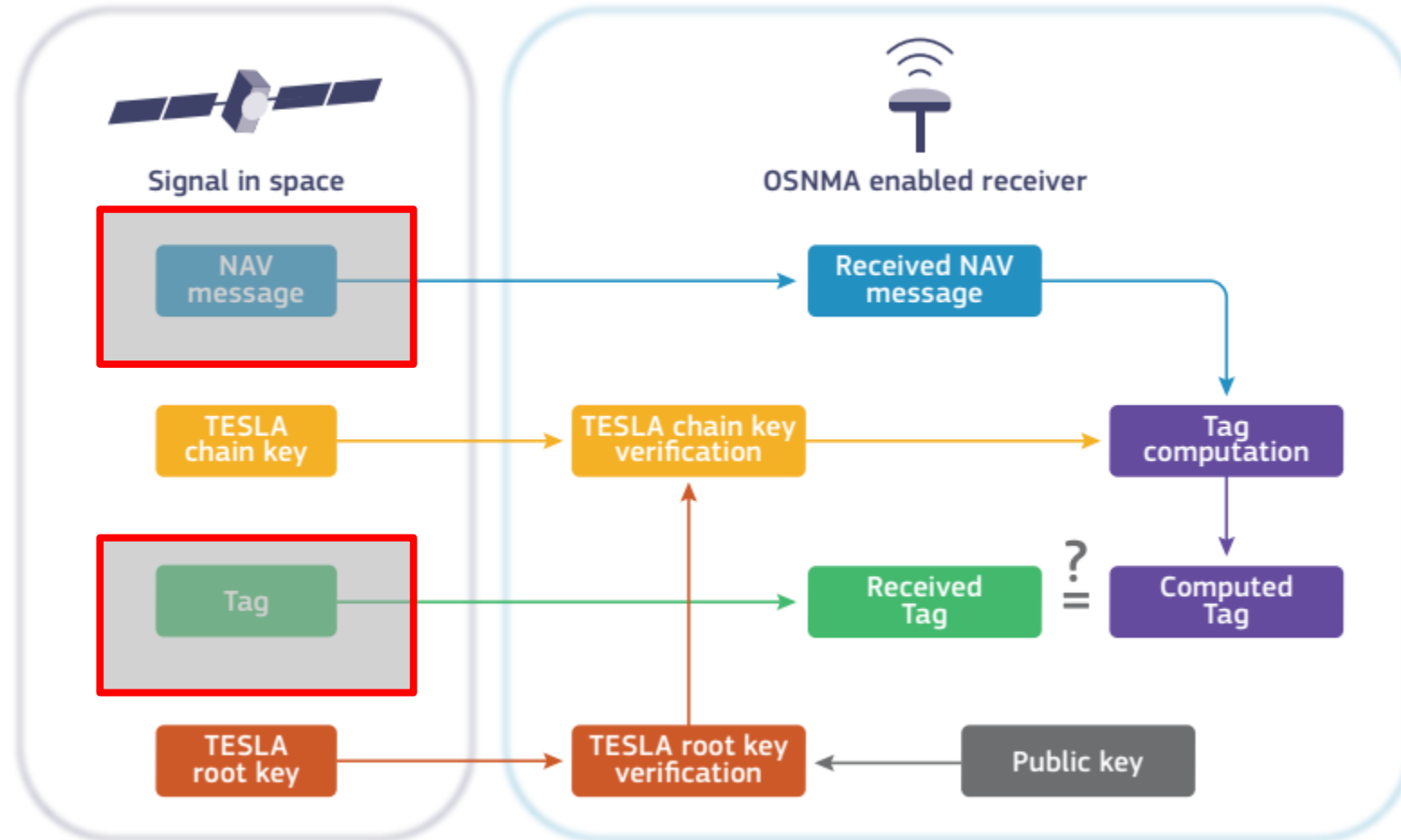
# OSNMA Receiver processing logic



# OSNMA Receiver processing logic

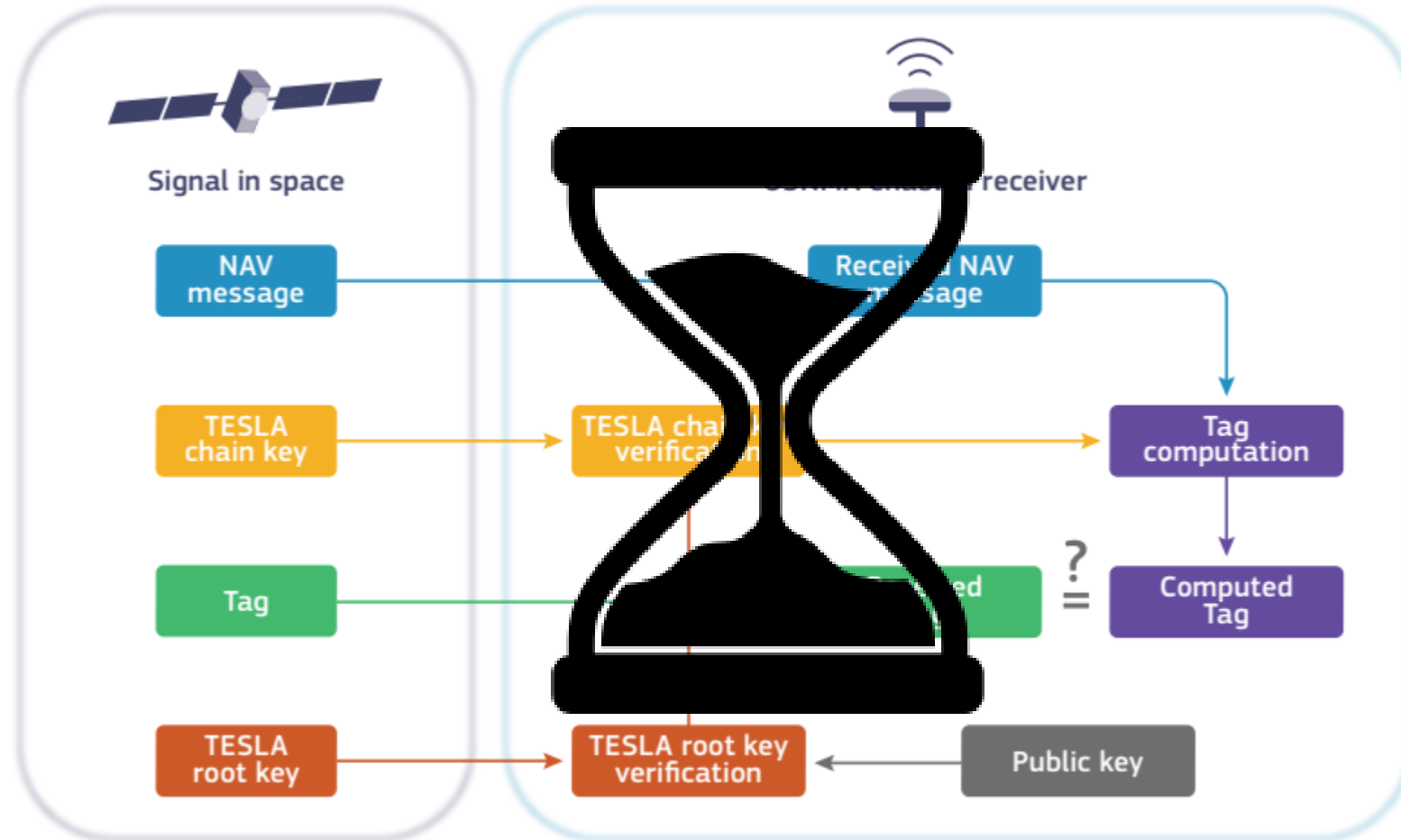


# OSNMA Receiver processing logic

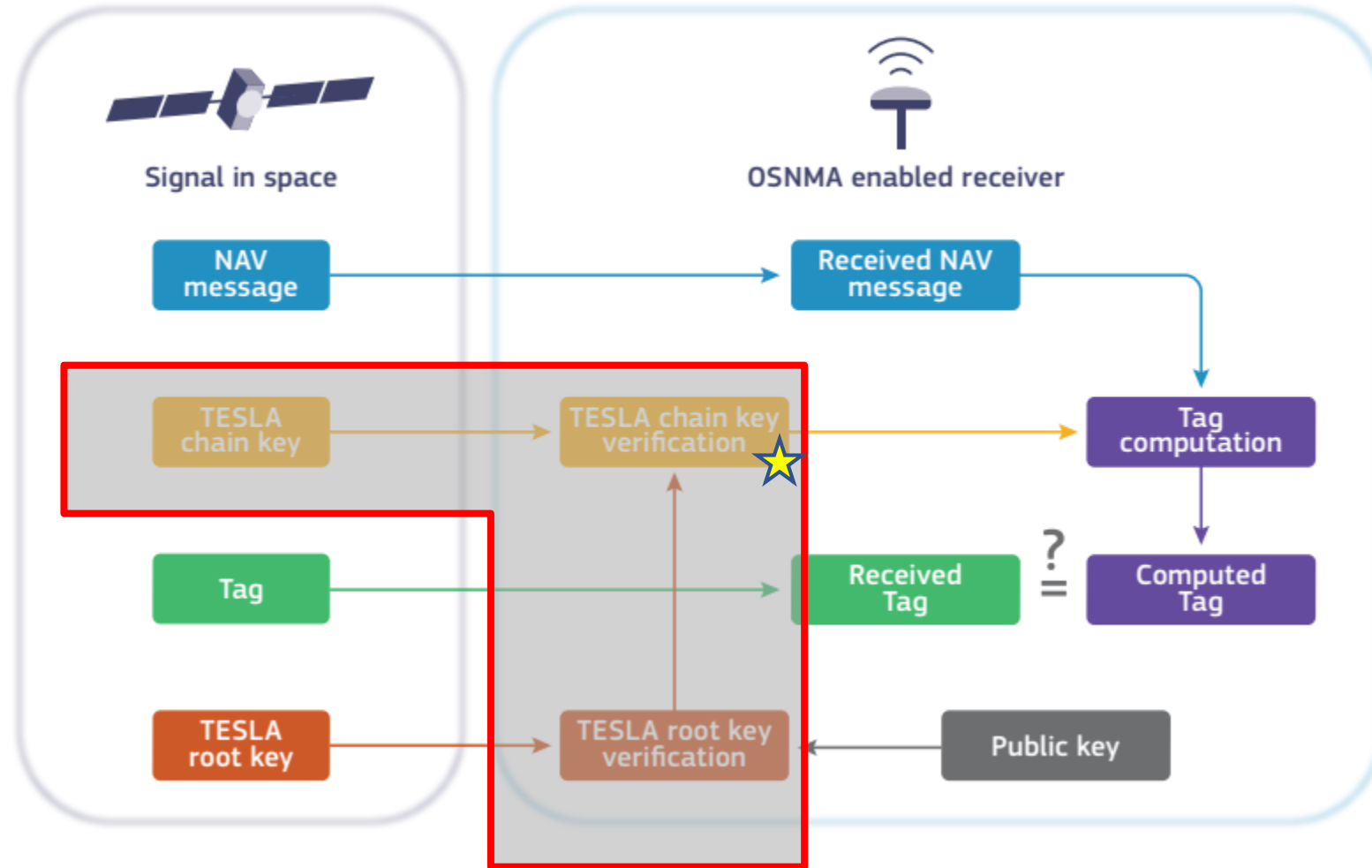




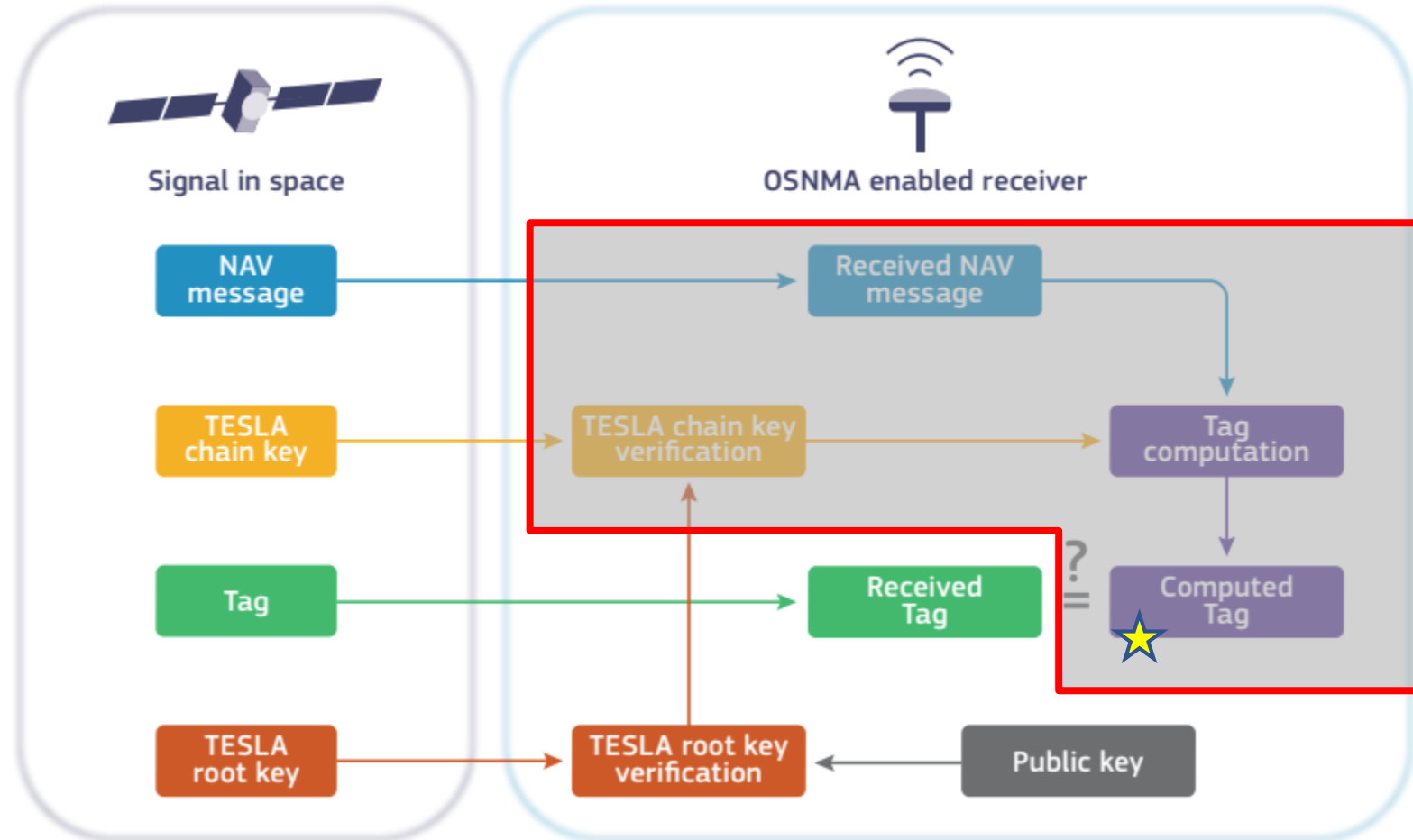
# OSNMA Receiver processing logic



# OSNMA Receiver processing logic

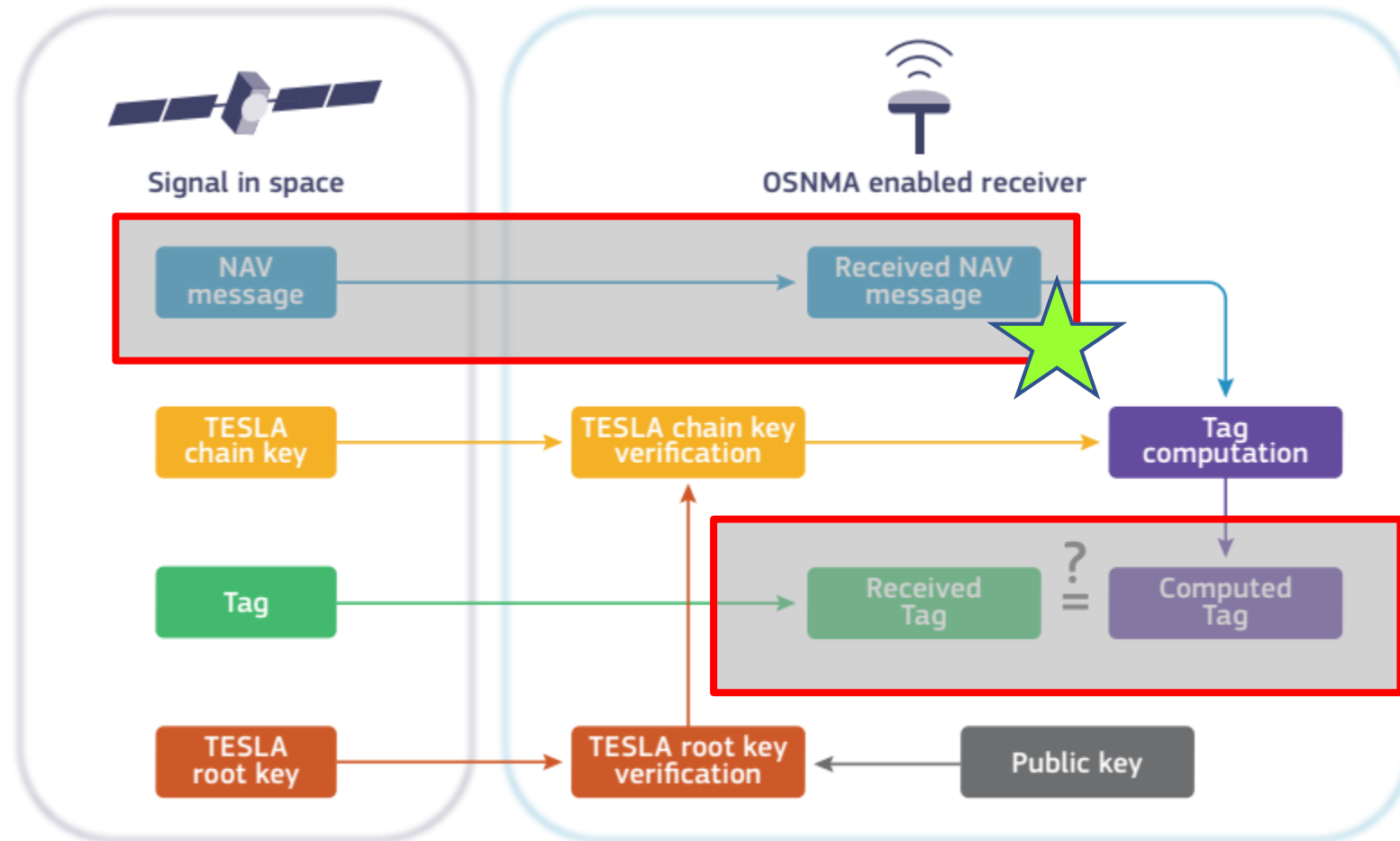


# OSNMA Receiver processing logic





# OSNMA Receiver processing logic



# Loose time synchronization

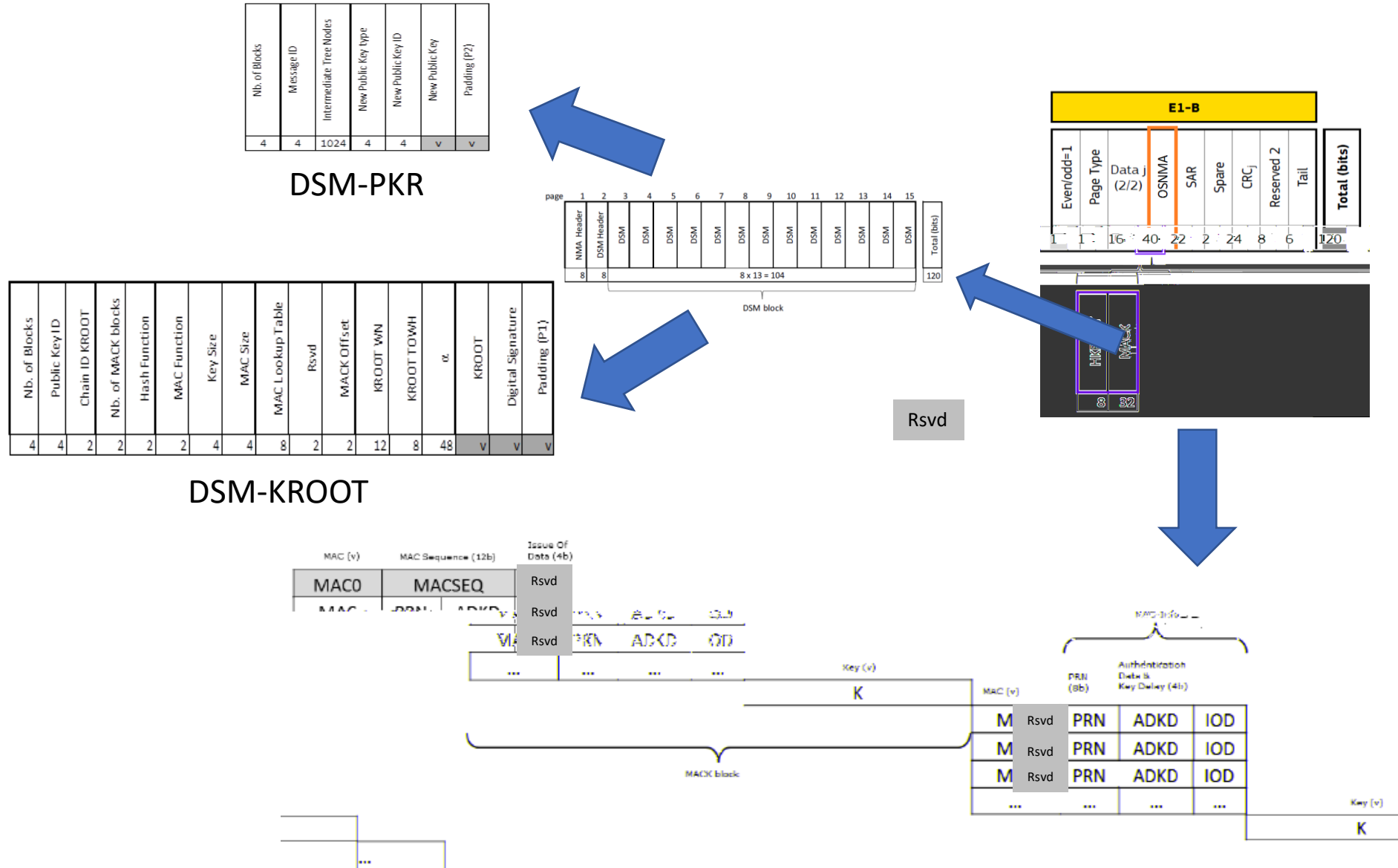
- OSNMA requires a “loose time” reference independent from the signal to (data-)authenticate
  - If ensures signal is not delayed > 30s -> nominal mode (ADKD0)
  - If ensures signal is not delayed > 330s -> “slow MAC” mode (ADKD12)

Manufacturer	Model	Oper. Temp		$Y_{Temp}$	$Y_{age}$ (1year)	$B(T_R)$	$T_{R,max}$
Seiko Epson	TG-5035CJ	-40°C	+105°C	0.5 ppm	1 ppm	110.38 s	2.62 years
	TG2016SMN	-40°C	+90°C	0.5 ppm	0.5 ppm	70.96 s	3.57 years
	TG2016SLN	-40°C	+85°C	0.5 ppm	1 ppm	110.38 s	2.62 years
	TG-5006CJ	-30°C	+85°C	0.5 ppm	1 ppm	110.38 s	2.62 years
	TG2016SKA	-40°C	+105°C	0.5 ppm	1 ppm	110.38 s	2.62 years
Vectron	VT-803	-40°C	+85°C	1 ppm	0.5 ppm	102.49 s	2.89 years
	VT-706	-40°C	+85°C	0.5 ppm	1 ppm	110.38 s	2.62 years
	VT-702	-40°C	+85°C	0.5 ppm	1 ppm	110.38 s	2.62 years
	VT-804	-40°C	+85°C	2 ppm	1 ppm	204.98 s	1.67 years
NDK	NT2520SE	-40°C	+105°C	0.5 ppm	1 ppm	110.38 s	2.62 years
	NT1612AA	-30°C	+85°C	0.5 ppm	1 ppm	110.38 s	2.62 years
	NT1612AJA	-30°C	+85°C	0.5 ppm	1 ppm	110.38 s	2.62 years
	NT2016SA	-30°C	+85°C	0.5 ppm	1 ppm	110.38 s	2.62 years
Maxim Integrated	DS3231	-40°C	+85°C	3.5 ppm	1 ppm	299.59 s	1.16 years
Micro Crystal Switzerland	RV-8803-C7	-40°C	+85°C	3 ppm	3 ppm	425.73 s	0.87 years



	Power Consumption	Price	Order of $y(t)$
XO	1 mW	1€-10€	10 ppm
TCXO	≈1 mW	1€-10€	≈1 ppm
OCXO	1 W	≫10€	≈0.1 ppm

# Galileo OSNMA protocol

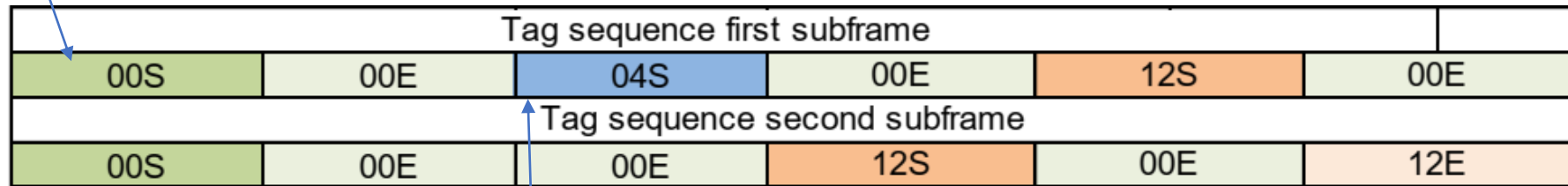




# OSNMA SIS configuration (example)

OSNMA SiS Parameter	Configuration
Digital signature	ECDSA P-256
Hash function for TESLA chain	SHA-256
Key size	128 bits
MAC function	HMAC-SHA-256
Tag size	40 bits
Number of Tags per subframe (30s)	6
Tag sequence (over 2 subframes)	[00S, 00E, 04S, 00E, 12S, 00E ] ; [00S, 00E, 00E, 12S, 00E, 12E ]

Self, clk&eph



Cross, clk&eph

Self, time(UTC/GGTO)

Self, clk&eph, "slow"

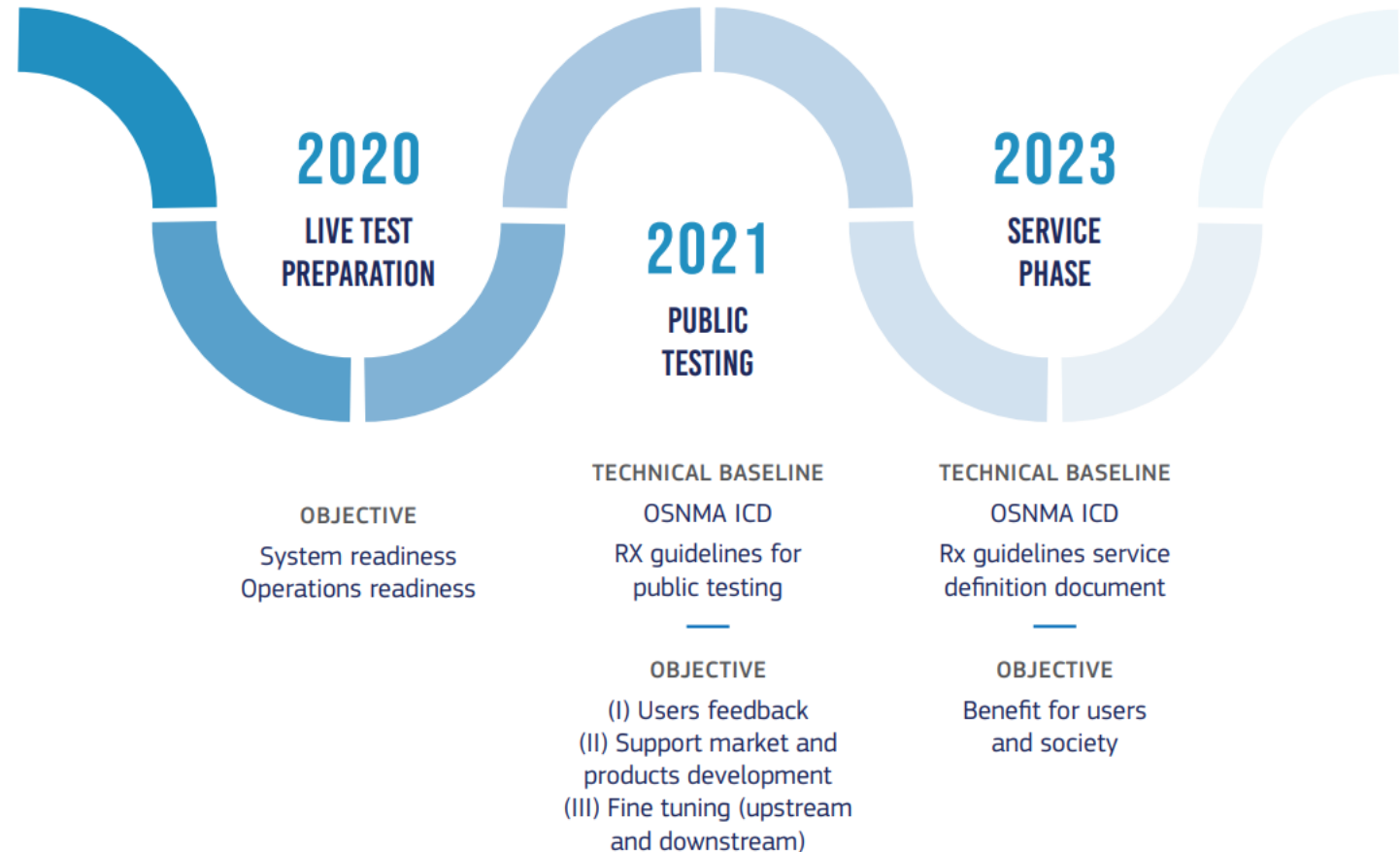
Cross, clk&eph, "slow"

# Table of contents

- What is Galileo OSNMA
- **Current status**
- Performance
- Next steps

# OSNMA current status

- **2014-2020: Studies, design, devpt**
  - **2021-2022: Public testing**
  - **2023: Service declaration (OSNMA status switch from 'test' to 'operational')**
- 
- **SIS ICD (test phase), "Info note" and guidelines published\***
  - **SIS reliably transmitted worldwide for almost two years, 1+ year publicly**



\*<https://www.gsc-europa.eu/electronic-library/programme-reference-documents#OSNMA>

# Examples of OSNMA applications



**Safety-Critical Applications:** OSNMA-secured GNSS positioning to support safety-critical applications, such as in the automotive sector

→ OSNMA included in the EU Digital Tachograph regulation



**Telecom:** to allow telecom operators to have accurate and consistent time and frequency at distant points of network.

→ Clear interest on GNSS authentication



**Insurance telematics:** use of GNSS data to increase the fairness of motor insurance for both insurers and subscribers in the frame of usage-based insurance.

→ Liability critical application

More applications can be found in '*Galileo Open Service Navigation Message Authentication (OSNMA) Info Note*', European Union Agency for the Space Programme (EUSPA), 2021.

# Some EU projects exploiting OSNMA



PATROL: Development, supply and testing of an **OSNMA user terminal** for **smart tachographs**.



**Galileo-based timing platform** (TRL7), using OSNMA and EGNOS corrections.



Design, integration and V&V of a shipborne receiver **dual-frequency multi-constellation Galileo OS enabled including OSNMA** and IEC GNSS approval.



Assessment of the benefits introduced by **Galileo authenticated signals** (OSNMA) in the specific context of **synchronisation of 5G telecommunication networks**.

Python 3.8 passing Python 3.9 passing Python 3.10 passing

OSNMAlib

Open-source OSNMA library: <https://github.com/Algafix/OSNMA>

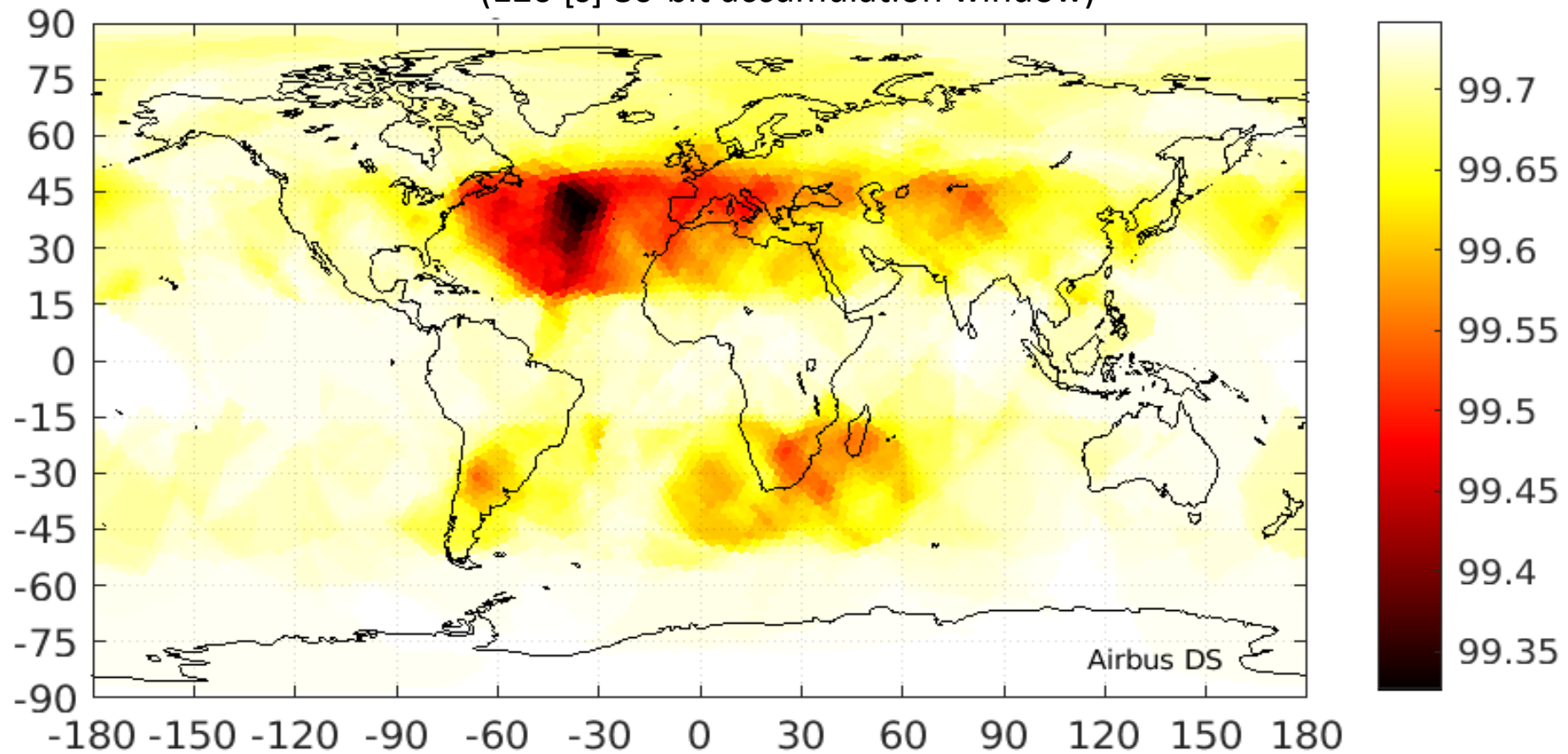


# Table of contents

- What is Galileo OSNMA
- Current status
- **Performance**
- Next steps

# OSNMA availability

Availability of Tags for Galileo I/NAV orbit & clock data (ADKD0), for target security level and for at least 4 SV in view  
(120 [s] 80-bit accumulation window)



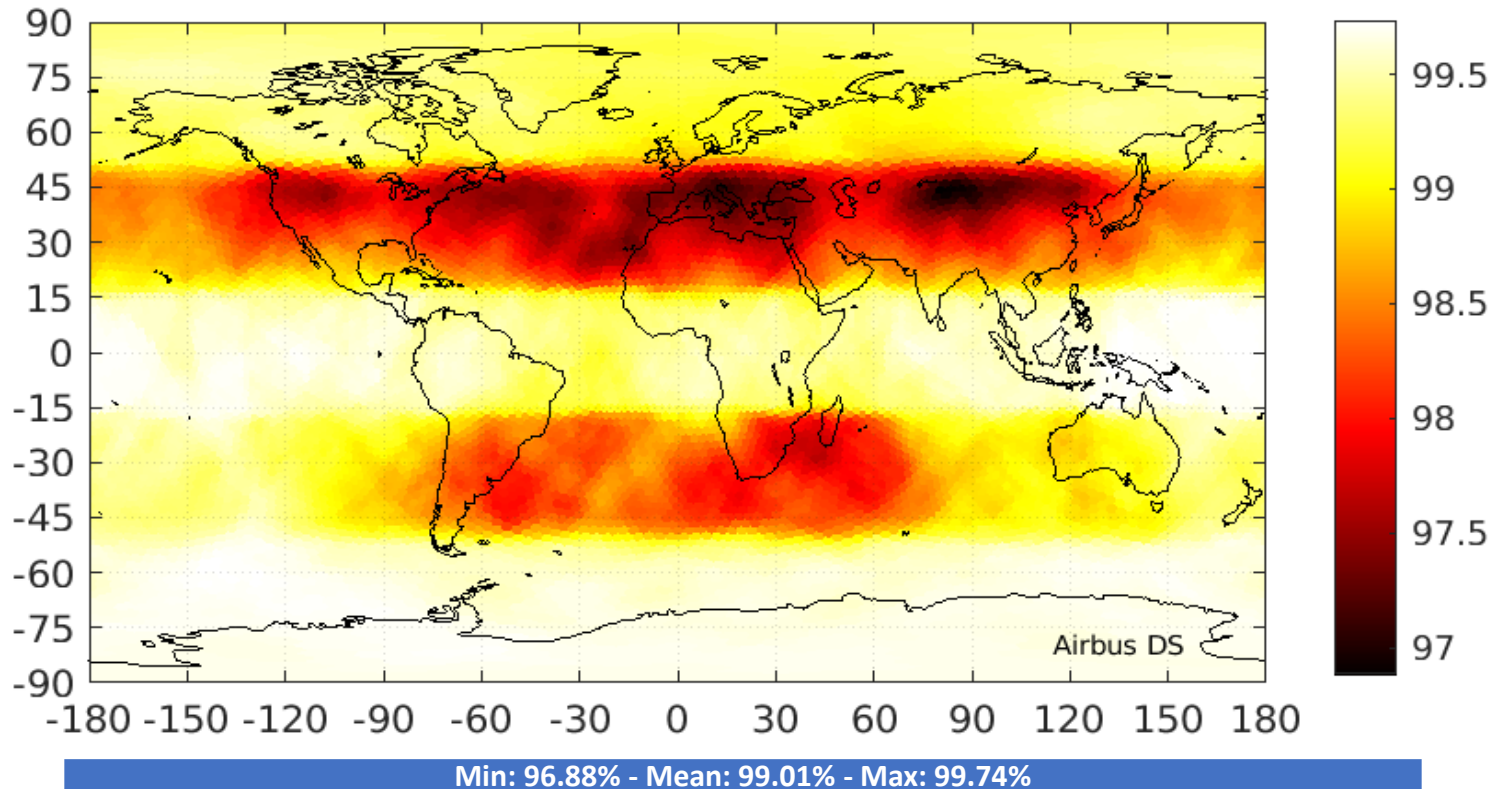
Min: 99.33% - Mean: 99.69% - Max: 99.74%

Source: ADS/EUSPA

# OSNMA availability



Availability of Tags for Galileo I/NAV orbit & clock data (ADKD12), for target security level and for 4 SV in view (240 [s] 80-bit accumulation window)



# OSNMA accuracy



Average difference between legacy and OSNMA vertical and horizontal position accuracy (95%) measured at each TGVPx GESS from 1<sup>st</sup> May until 30<sup>th</sup> June 2022

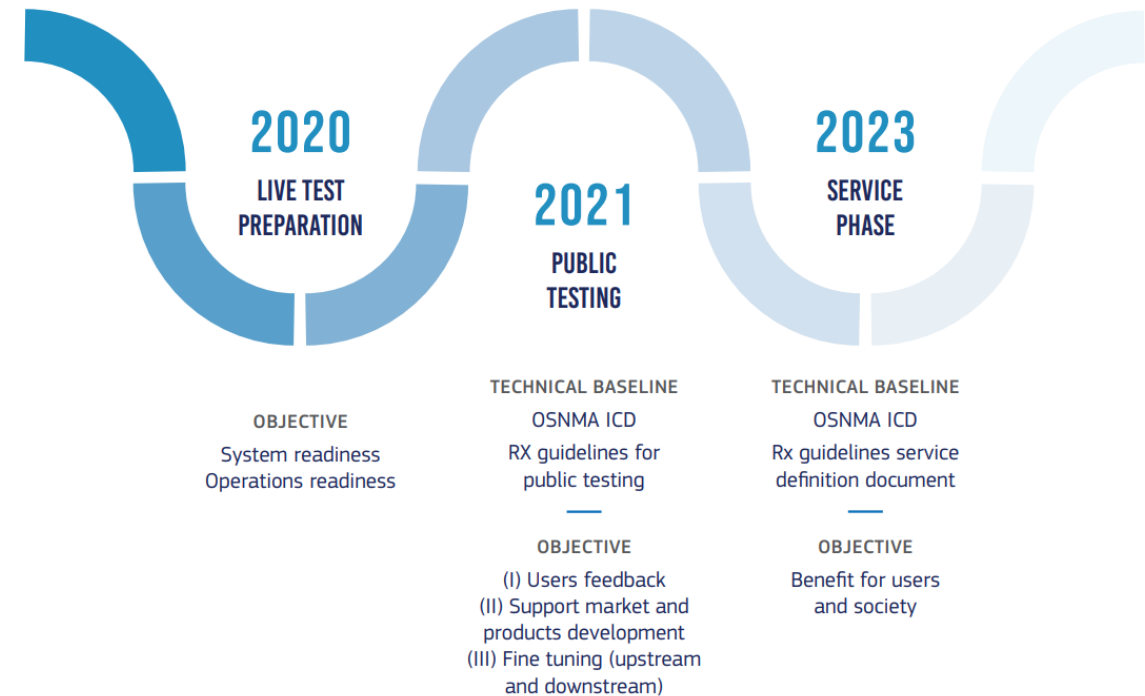
# Table of contents

- What is Galileo OSNMA
- Current status
- Performance
- **Next steps**



# Next Steps

- Continue public testing
- Publication of Service ICD (Q4'22/Q1'23). Mostly compatible with current (test) ICD
- Publication of operational cryptographic data to be installed in receivers for the operational phase
- Operational service declaration: 2023 (date TBC EUSPA)
- To be complemented by signal authentication (ACAS) and HAS data authentication in Galileo 1<sup>st</sup> Generation, then ranging authentication in all frequencies in Galileo 2<sup>nd</sup> Generation



# Conclusion

- OSNMA is a pioneering data authentication service offered freely and worldwide by Galileo
- Very reliable and stable signal, as per 1+ year of public testing. Can be used now already!
- Initial service to start next year (2023)



EU SPACE



Thank you for your attention!  
Galileo  
OSNMA

Ignacio Fernández Hernández  
European Commission

Acknowledgements: JRC, ESA, EUSPA/ADS