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

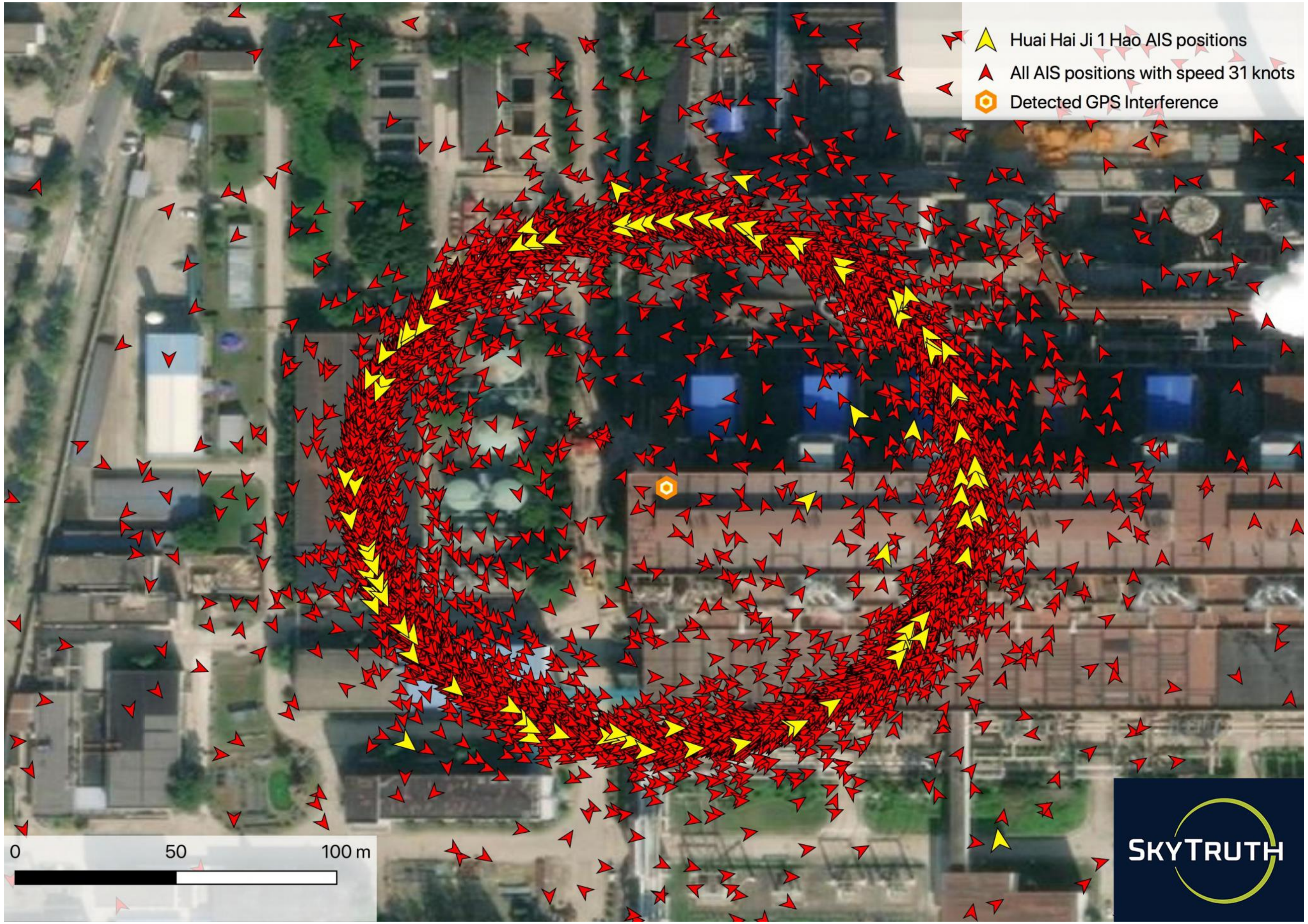
- **What is Galileo OSNMA**
- Current status
- Performance
- Next steps

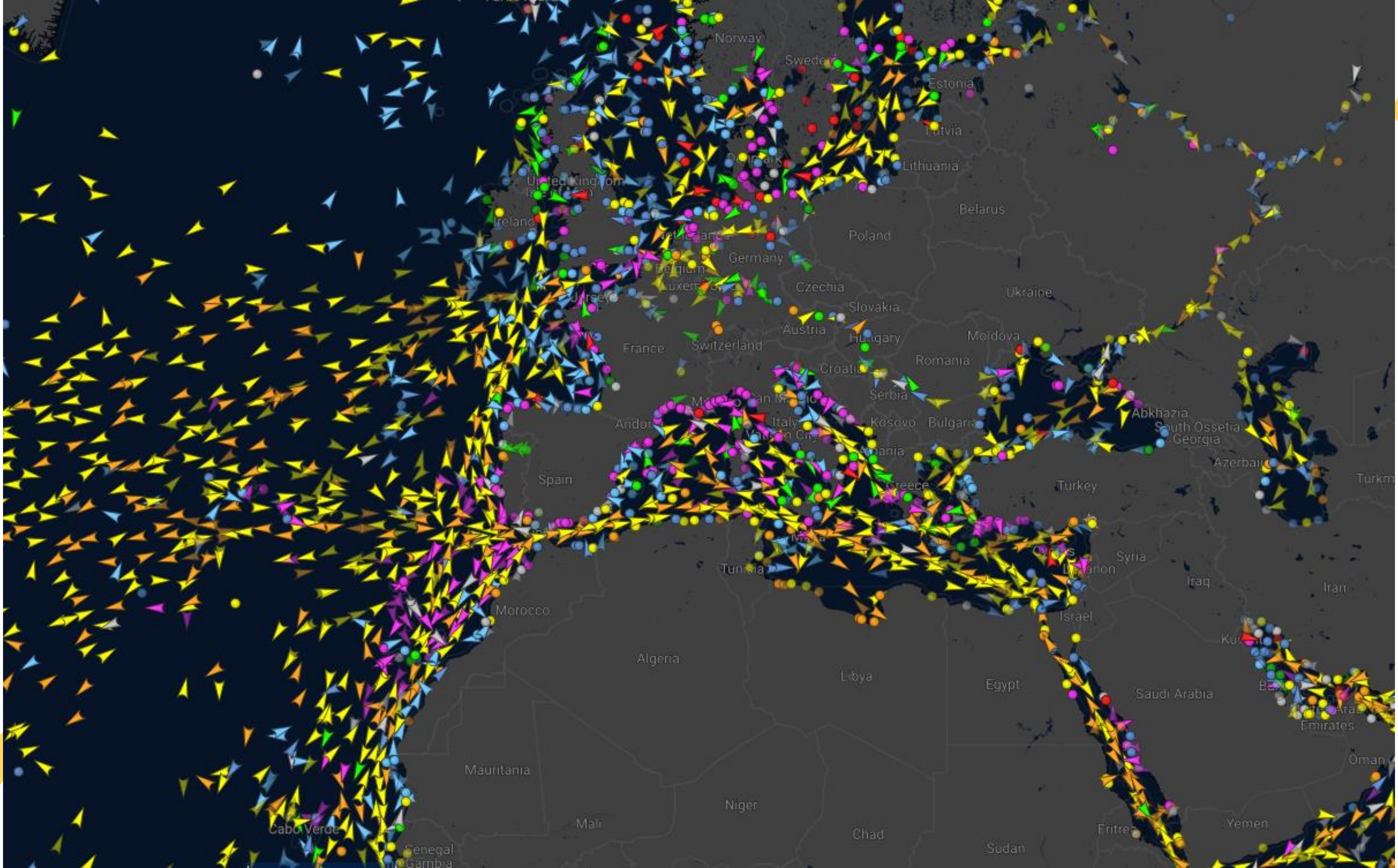
What is Galileo OSNMA

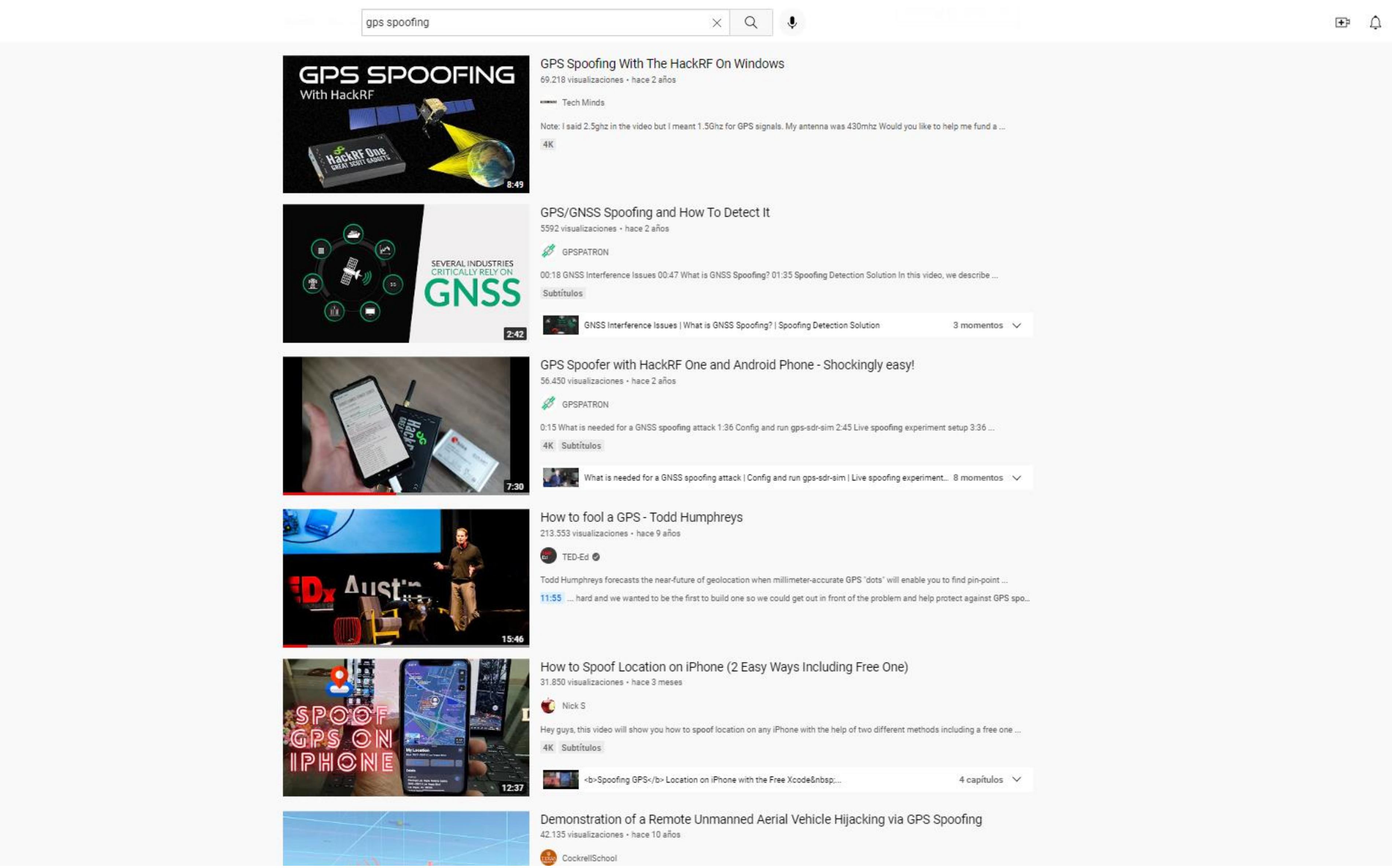
- What is Galileo OSNMA?
  - Stands for Open Service Navigation Message Authentication
  - Mechanism to authenticate the Galileo data used to calculate a position: satellite orbits and clock corrections, satellite status flags, time…
  - Equivalent to a Galileo “digital signature”
  - Transmitted in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

Galileo

- Why OSNMA?


Huai Hai Ji 1 Hao AIS positions
All AIS positions with speed 31 knots
Detected GPS Interference
0
50
100 m
SKYTRUTH


Norway
Sweden
Estonia
Latvia
Denmark
Lithuania
United Kingdom
Ireland
Belarus
Netherlands
Poland
Germany
Belgium
Luxembourg
Jersey
Czechia
Ukraine
Slovakia
Austria
Hungary
Moldova
France
Switzerland
Romania
Croatia
Serbia
Monaco
San Marino
Italy
Vatican City
Kosovo
Bulgaria
Andorra
Albania
Abkhazia
South Ossetia
Georgia
Azerbaijan
Spain
Greece
Turkey
Turkm
Malta
Tunisia
Cyprus
Syria
Lebanon
Iraq
Iran
Israel
Morocco
Algeria
Libya
Egypt
Kuwait
Saudi Arabia
United Arab Emirates
Mauritania
Oman
Niger
Mali
Chad
Eritrea
Yemen
Cabo Verde
Senegal
Gambia
Sudan



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

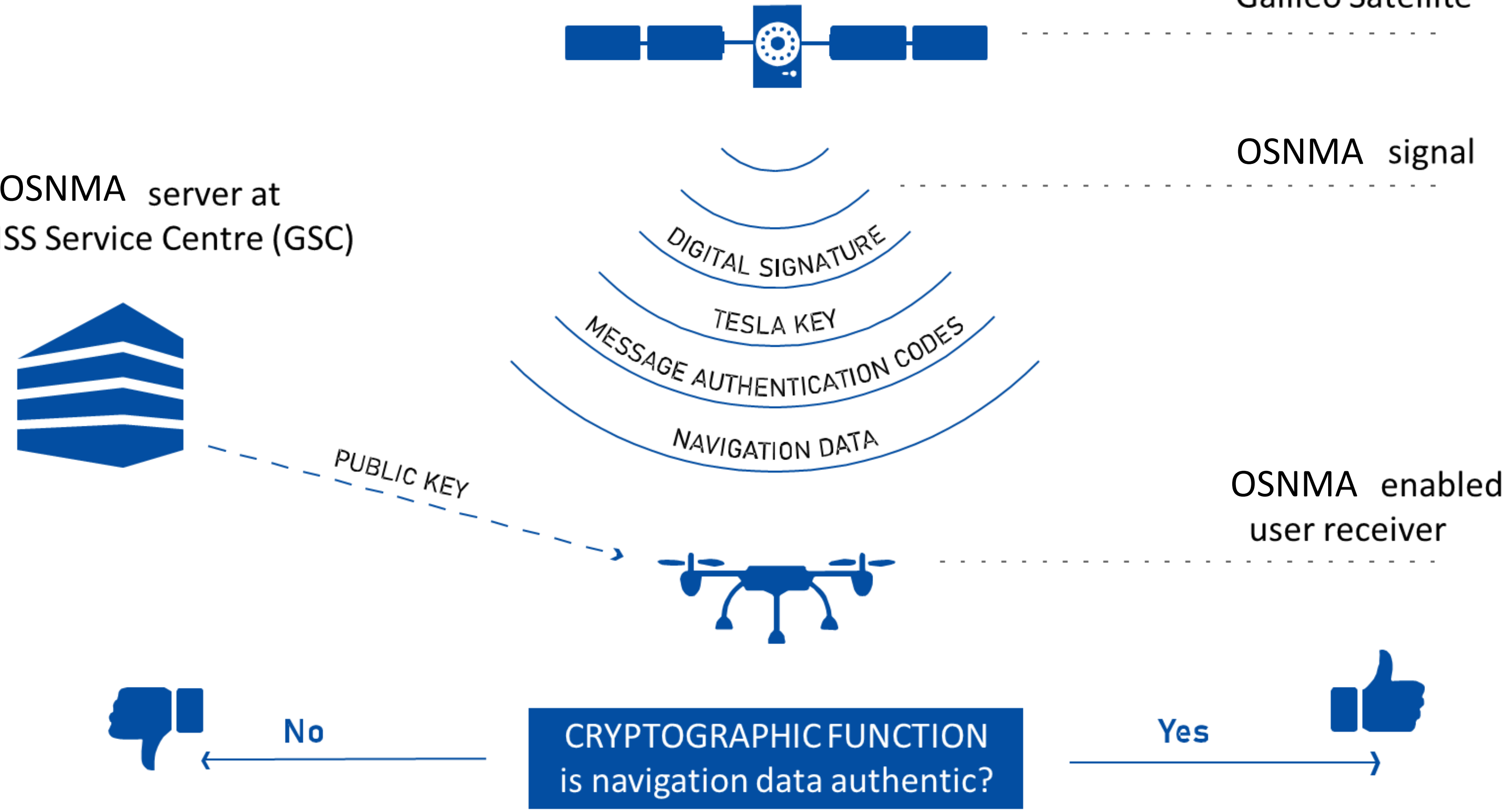
GPS Spoofer with HackRF One and Android Phone - Shockingly easy!
56.450 visualizaciones • hace 2 años
GPSPATRON
0:15 What is needed for a GNSS **spoofing** attack 1:36 Config and run gps-sdr-sim 2:45 Live **spoofing** experiment setup 3:36 ...
4K Subtítulos
What is needed for a GNSS spoofing attack | 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
<b>Spoofing GPS</b> 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



Galileo Satellite

OSNMA signal

OSNMA server at
GNSS Service Centre (GSC)

OSNMA enabled
user receiver

CRYPTOGRAPHIC FUNCTION
is navigation data authentic?

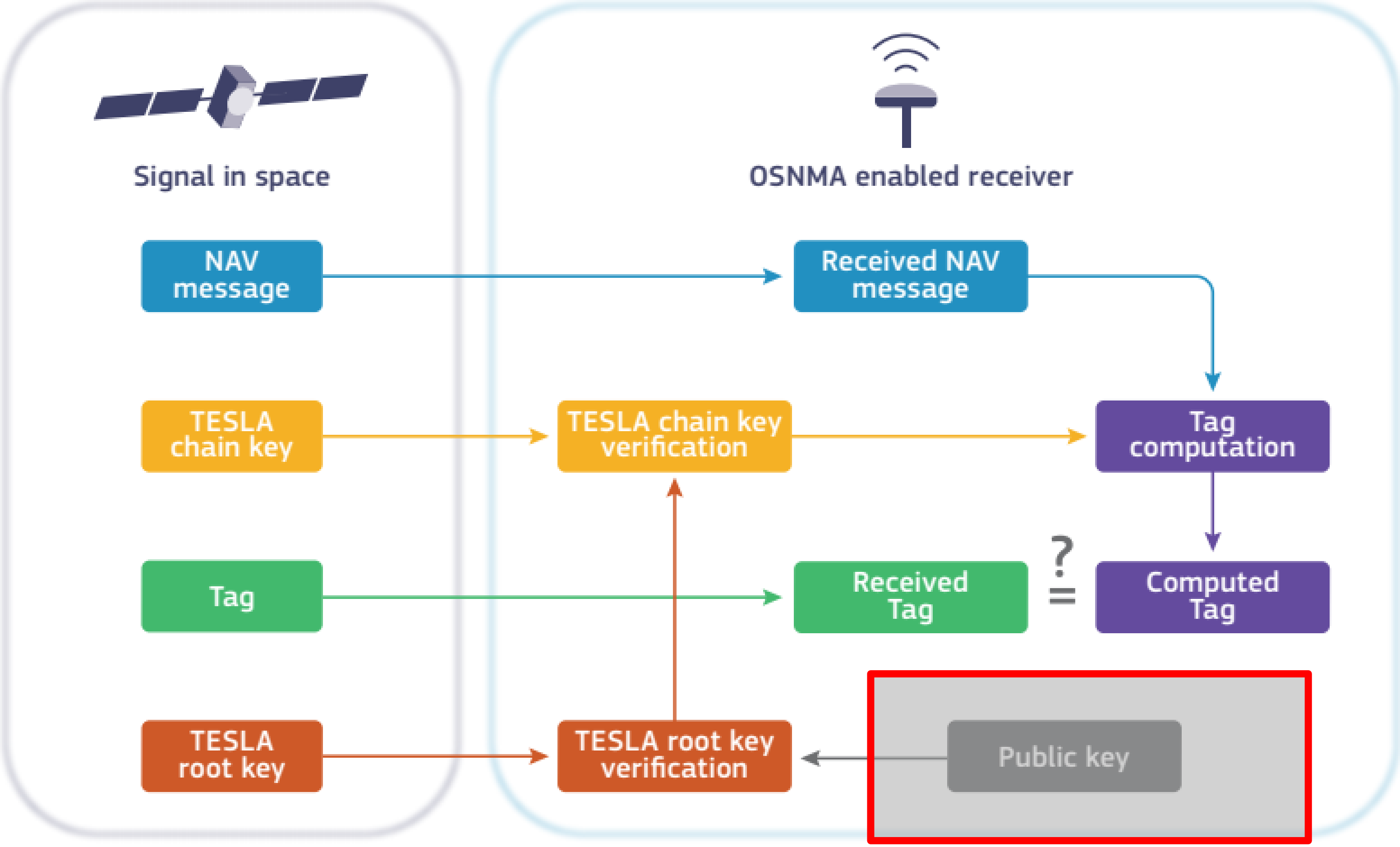
No

Navigation data
not authenticated

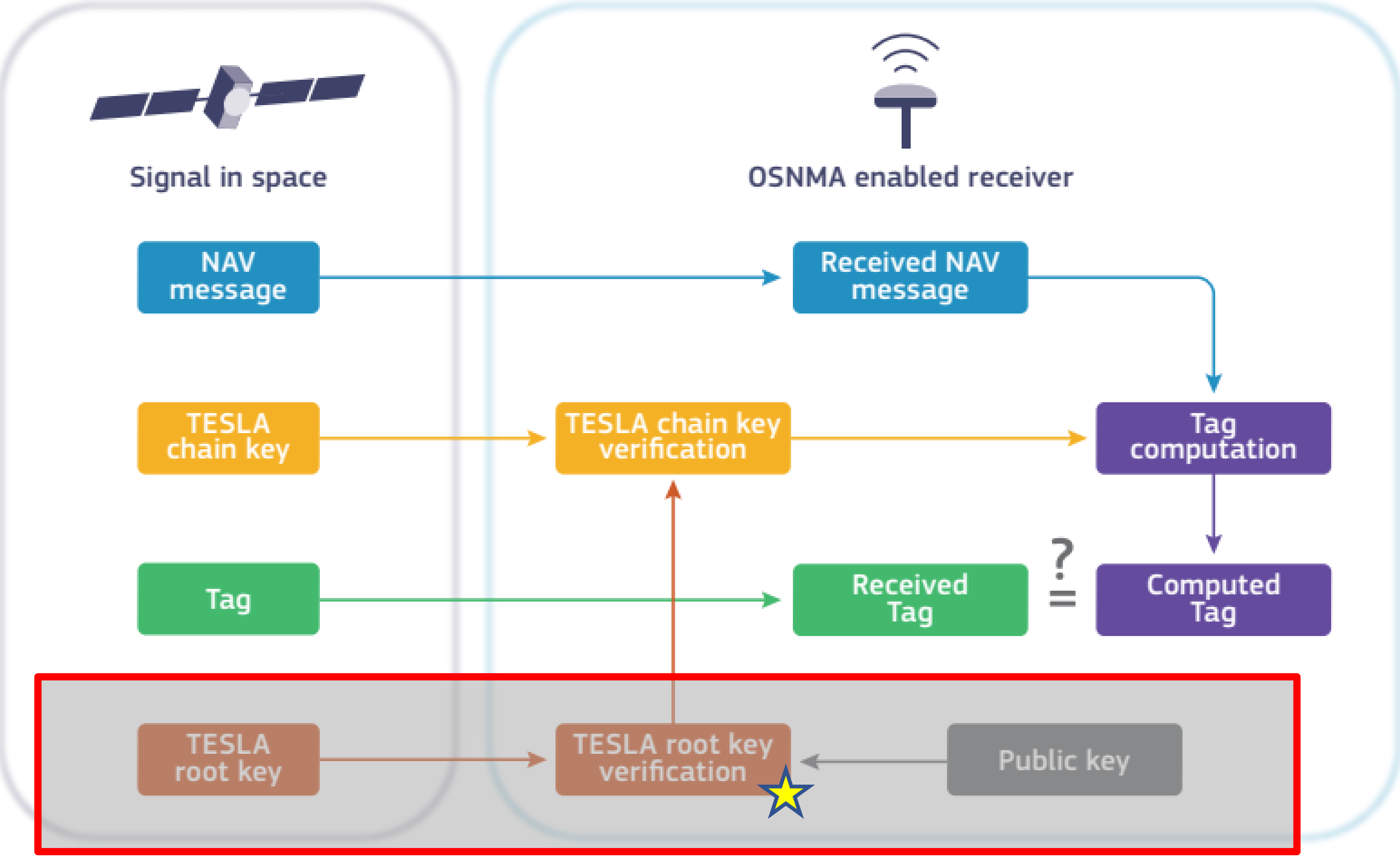
Yes

Navigation data authenticated
Trusted use for positioning

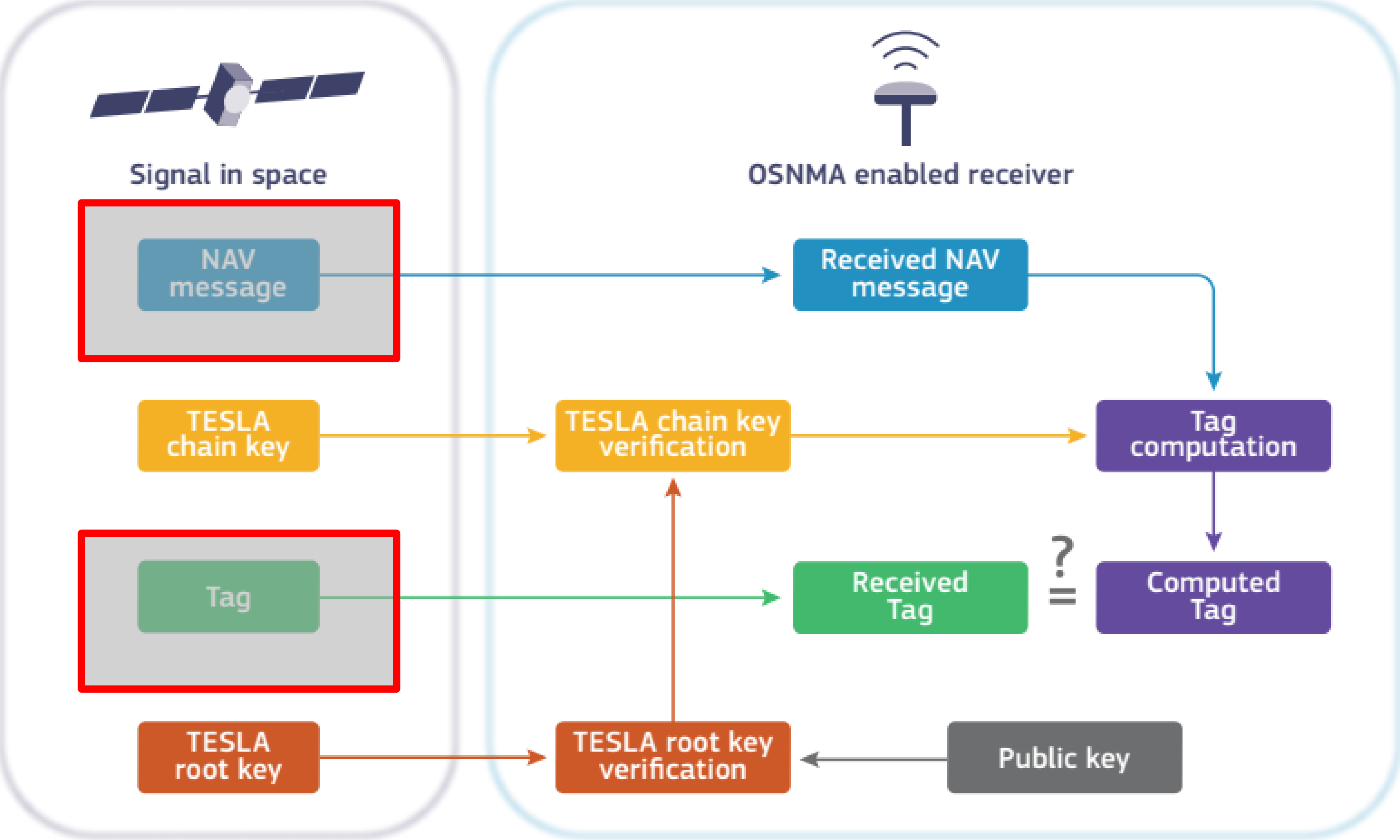
OSNMA Receiver processing logic



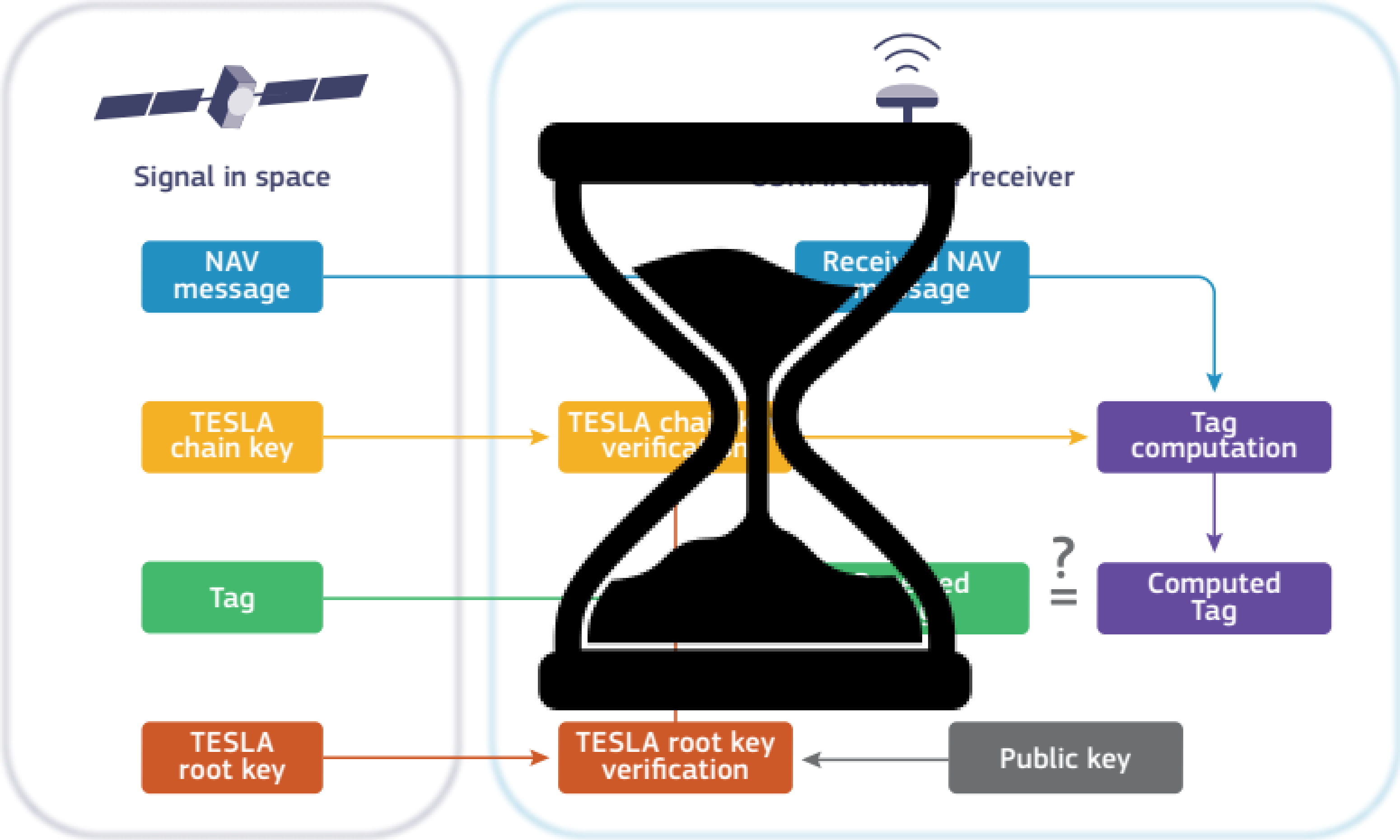
OSNMA Receiver processing logic



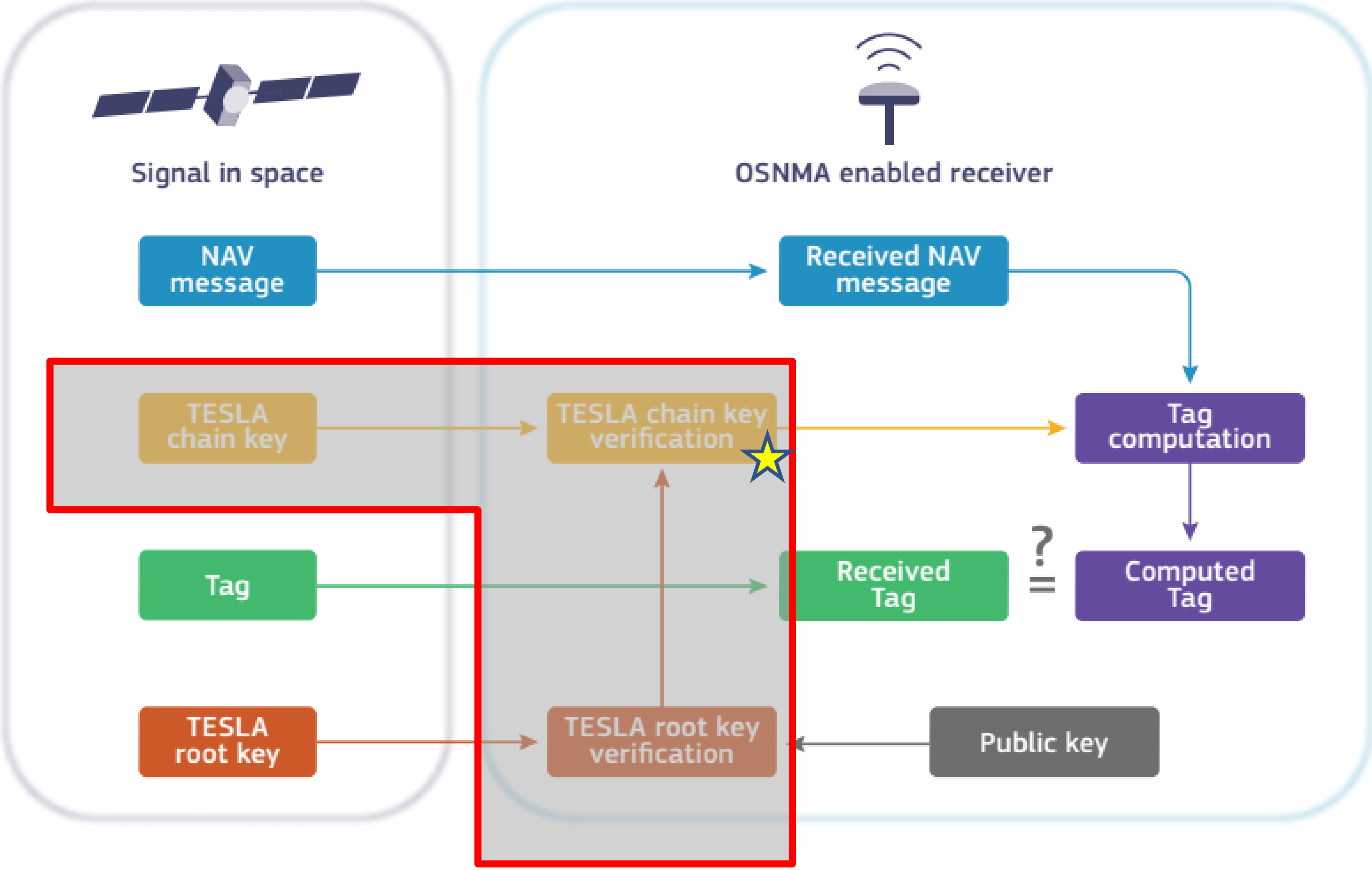
OSNMA Receiver processing logic



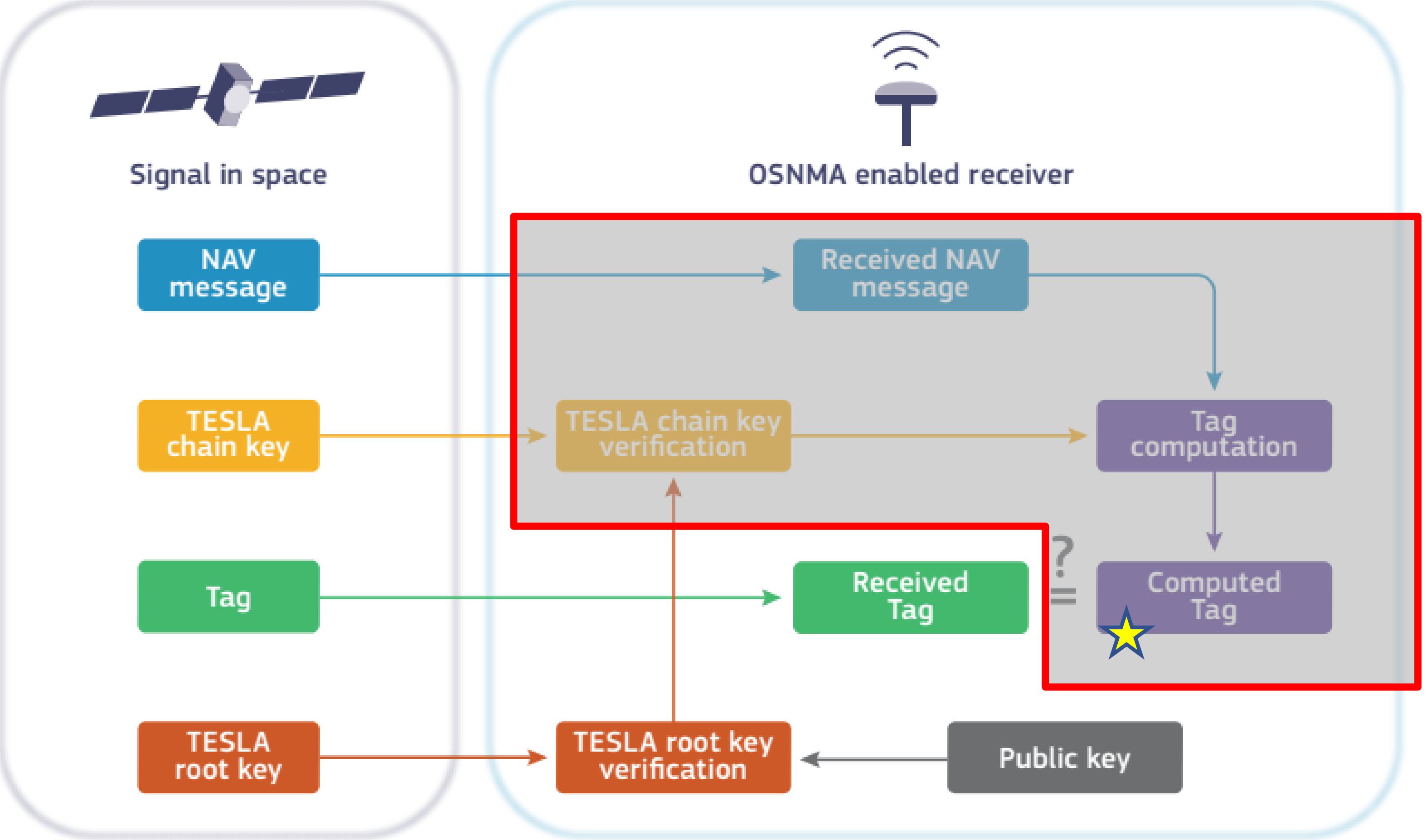
OSNMA Receiver processing logic



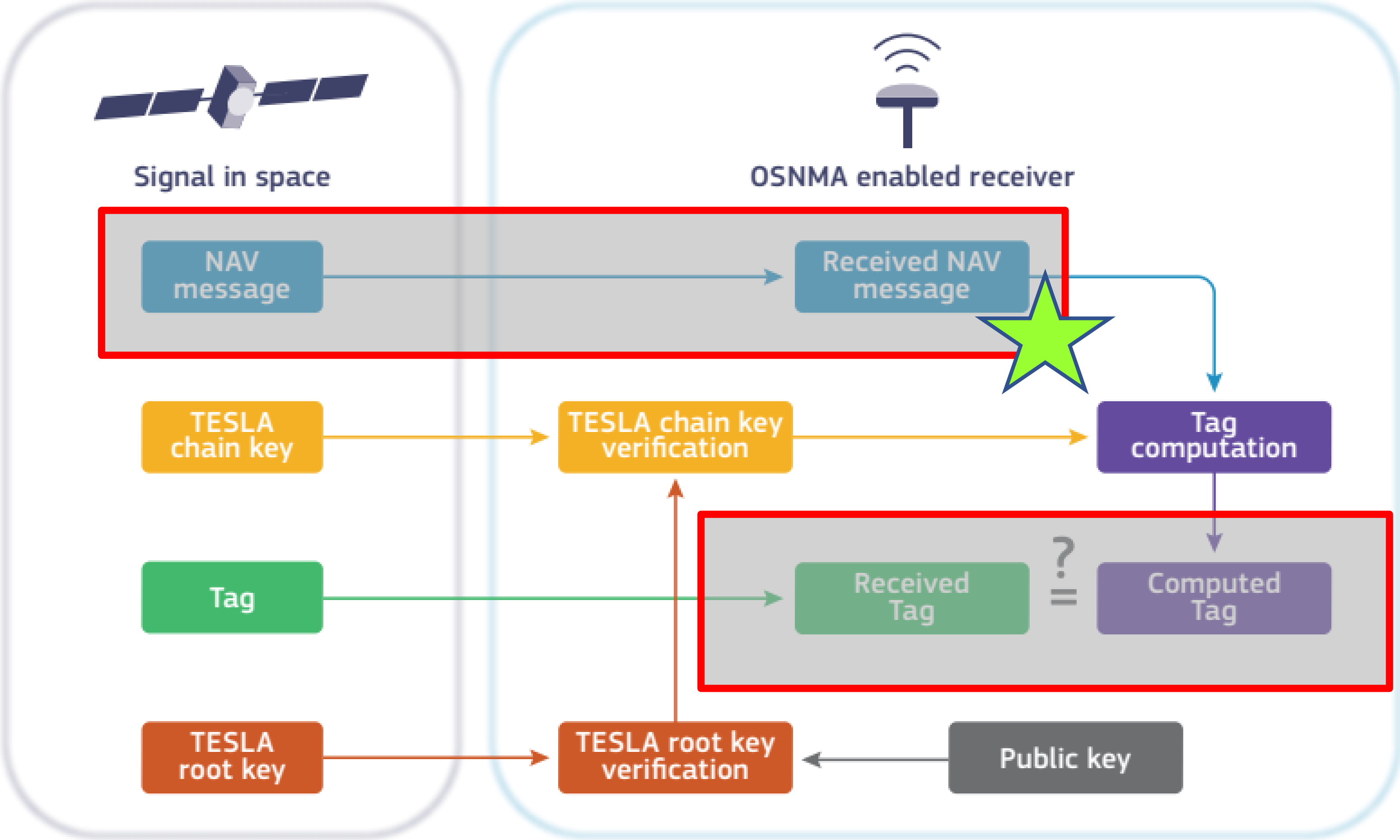
OSNMA Receiver processing logic



OSNMA Receiver processing logic

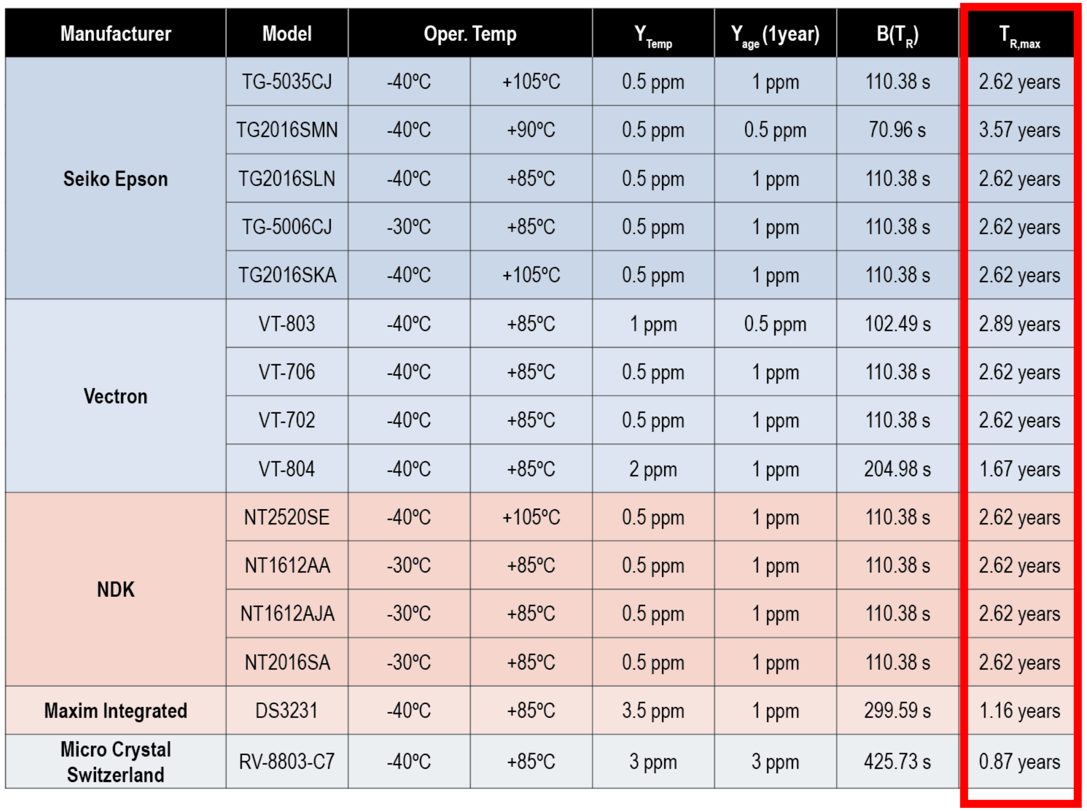


OSNMA Receiver processing logic

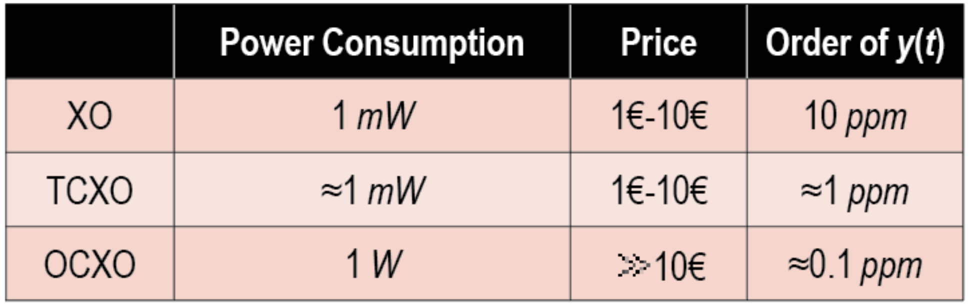


Loose time synchronization

- 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)



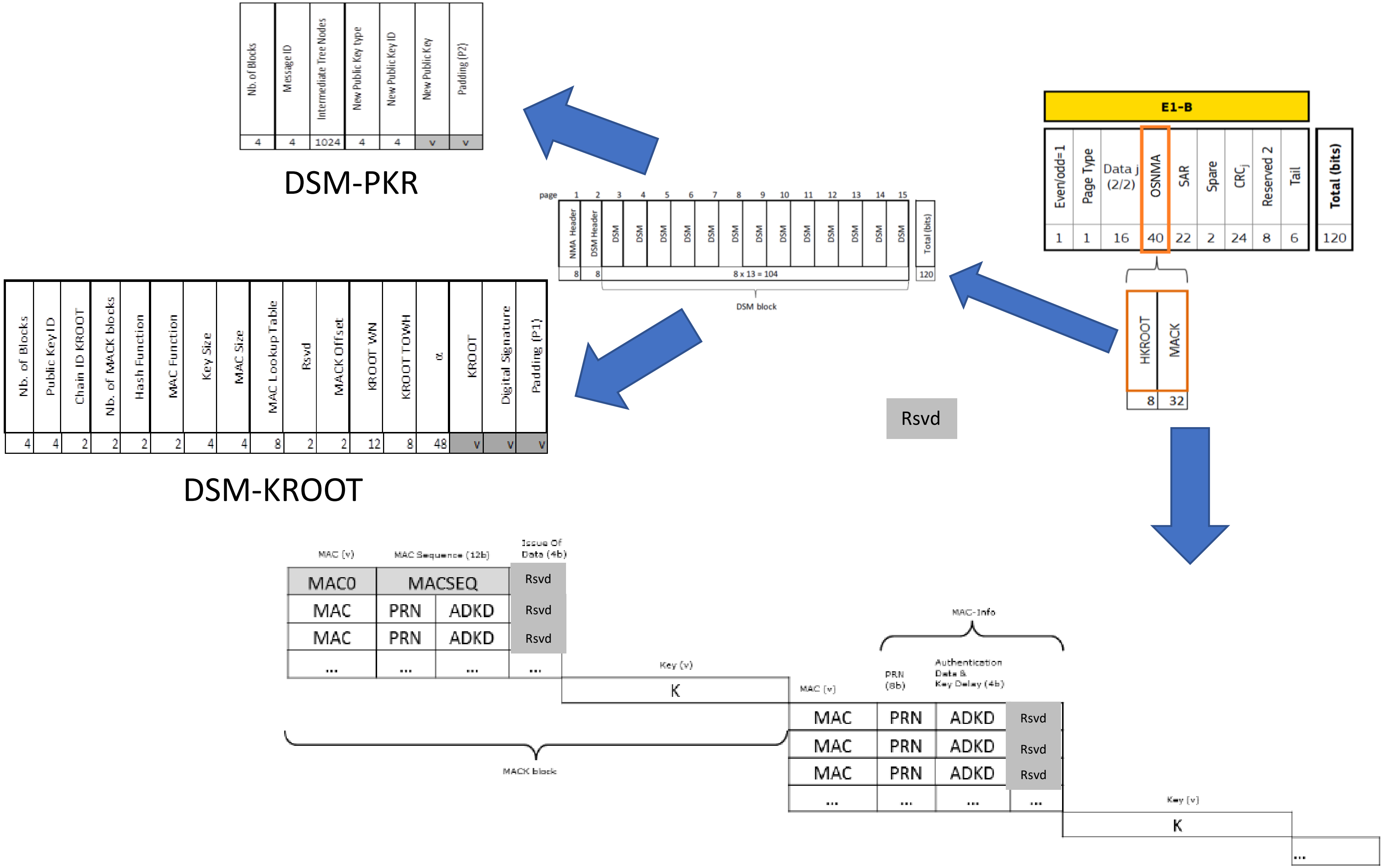
Manufacturer	Model	Oper. Temp		Y_{Temp}	Y_{age} (1year)	$B(T_R)$	$T_{R,max}$
Seiko Epson	TG-5035CJ	-40ºC	+105ºC	0.5 ppm	1 ppm	110.38 s	2.62 years
	TG2016SMN	-40ºC	+90ºC	0.5 ppm	0.5 ppm	70.96 s	3.57 years
	TG2016SLN	-40ºC	+85ºC	0.5 ppm	1 ppm	110.38 s	2.62 years
	TG-5006CJ	-30ºC	+85ºC	0.5 ppm	1 ppm	110.38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

https://www.gpsworld.com/its-galileo-time-options-for-crystal-oscillators-in-osnma-enabled-receivers/

Galileo OSNMA protocol



Nb. of Blocks	Message ID	Intermediate Tree Nodes	New Public Key type	New Public Key ID	New Public Key	Padding (P2)
4	4	1024	4	4	v	v

DSM-PKR

page	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
	NMA Header	DSM Header	DSM	DSM	DSM	DSM	DSM	DSM	DSM	DSM	DSM	DSM	DSM	DSM	DSM	Total (bits)
	8	8	8 x 13 = 104													120

DSM block

E1-B									
Even/odd=1	Page Type	Data j (2/2)	OSNMA	SAR	Spare	CRC_j	Reserved 2	Tail	**Total (bits)**
1	1	16	40	22	2	24	8	6	120

HKROOT	MACK
8	32

Nb. of Blocks	Public Key ID	Chain ID KROOT	Nb. of MACK blocks	Hash Function	MAC Function	Key Size	MAC Size	MAC Lookup Table	Rsvd	MACK Offset	KROOT WN	KROOT TOWH	α	KROOT	Digital Signature	Padding (P1)
4	4	2	2	2	2	4	4	8	2	2	12	8	48	v	v	v

DSM-KROOT

Rsvd

MAC (v)	MAC Sequence (12b)		Issue Of Data (4b)
MAC0	MACSEQ		Rsvd
MAC	PRN	ADKD	Rsvd
MAC	PRN	ADKD	Rsvd
...	...	...	...

Key (v)
K

	MAC-Info		
MAC (v)	PRN (8b)	Authentication Data & Key Delay (4b)	
MAC	PRN	ADKD	Rsvd
MAC	PRN	ADKD	Rsvd
MAC	PRN	ADKD	Rsvd
...	...	...	...

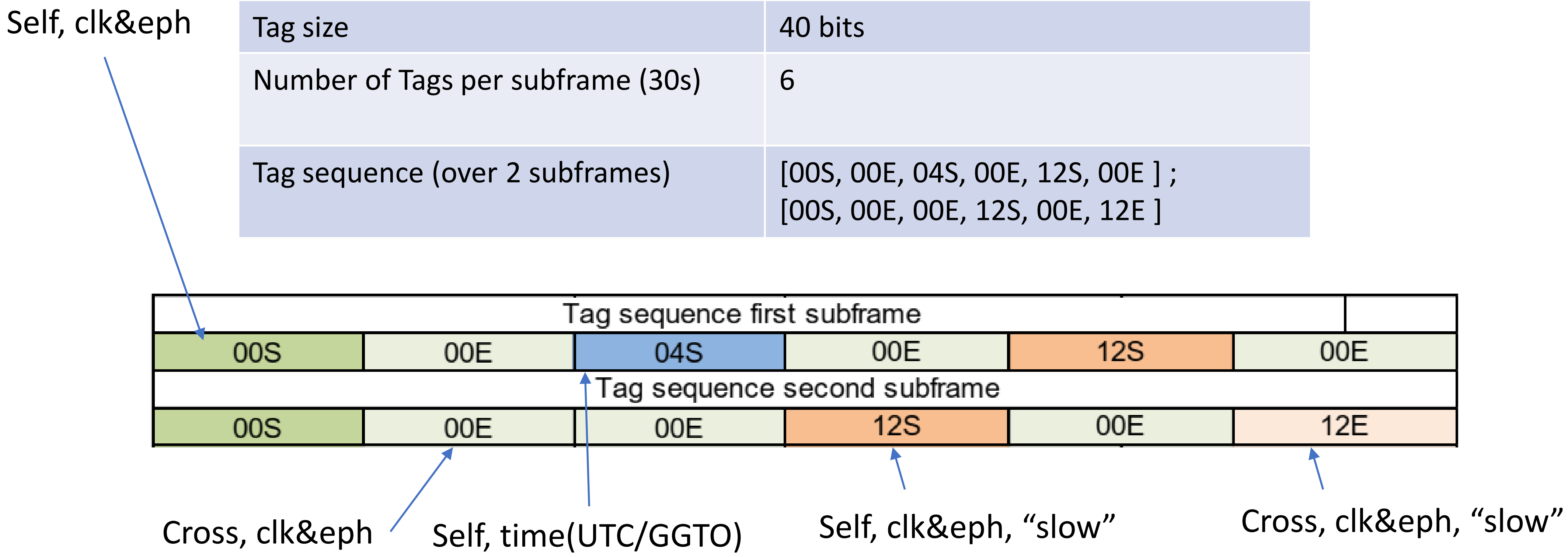
MACK block

Key (v)
K

...

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]



Tag sequence first subframe					
00S	00E	04S	00E	12S	00E
Tag sequence second subframe					
00S	00E	00E	12S	00E	12E

Self, clk&eph

Cross, clk&eph

Self, time(UTC/GGTO)

Self, clk&eph, “slow”

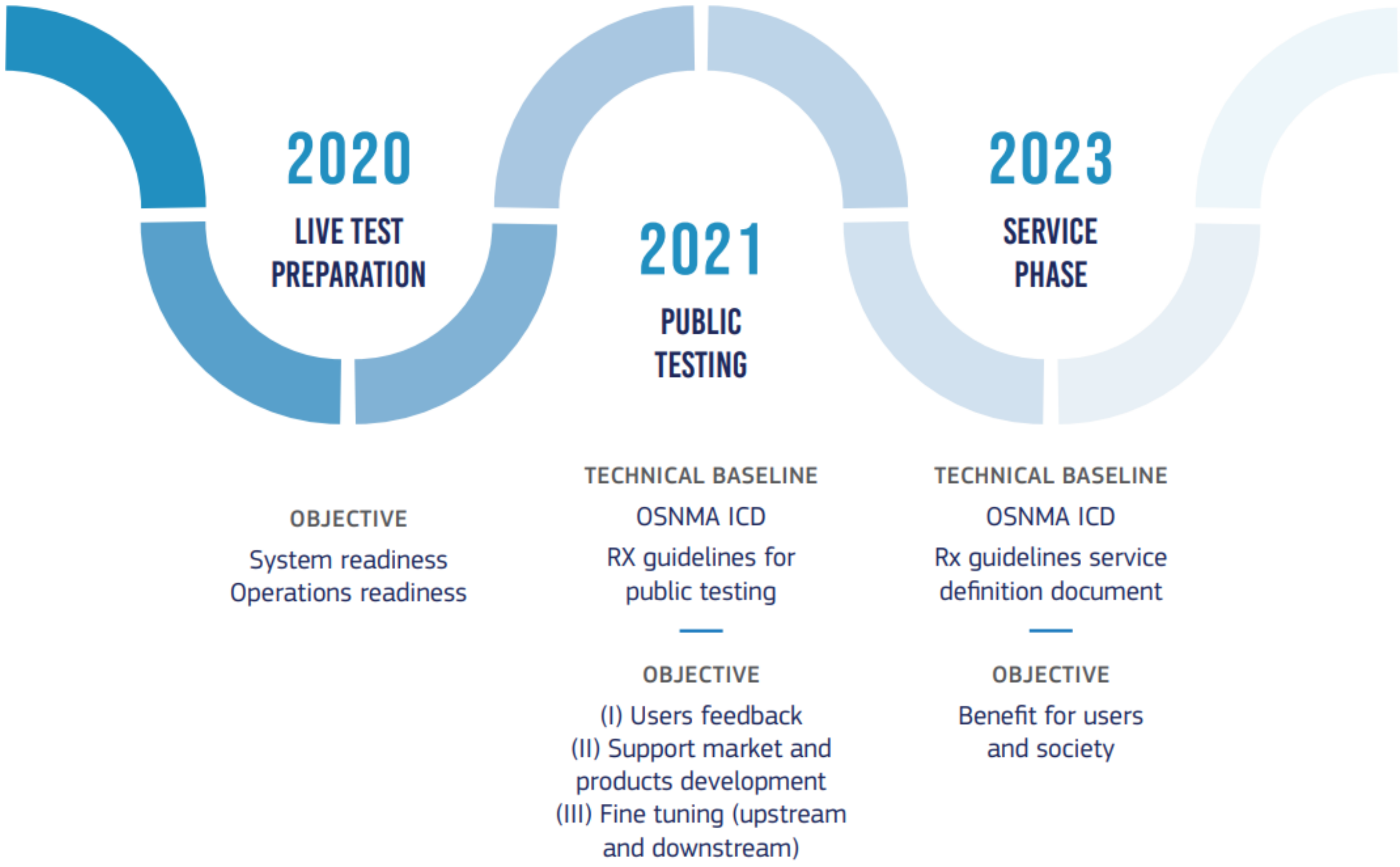
Cross, clk&eph, “slow”

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’)



2020

LIVE TEST PREPARATION

OBJECTIVE

System readiness
Operations readiness

2021

PUBLIC TESTING

TECHNICAL BASELINE

OSNMA ICD

RX guidelines for public testing

OBJECTIVE

(I) Users feedback
(II) Support market and products development
(III) Fine tuning (upstream and downstream)

2023

SERVICE PHASE

TECHNICAL BASELINE

OSNMA ICD

Rx guidelines service definition document

OBJECTIVE

Benefit for users and society

- 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

OSNMA

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

GIANO

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

ASGARD

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

ROOT

Rolling Out OSNMA for the securesynchronization of Telecom networks

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

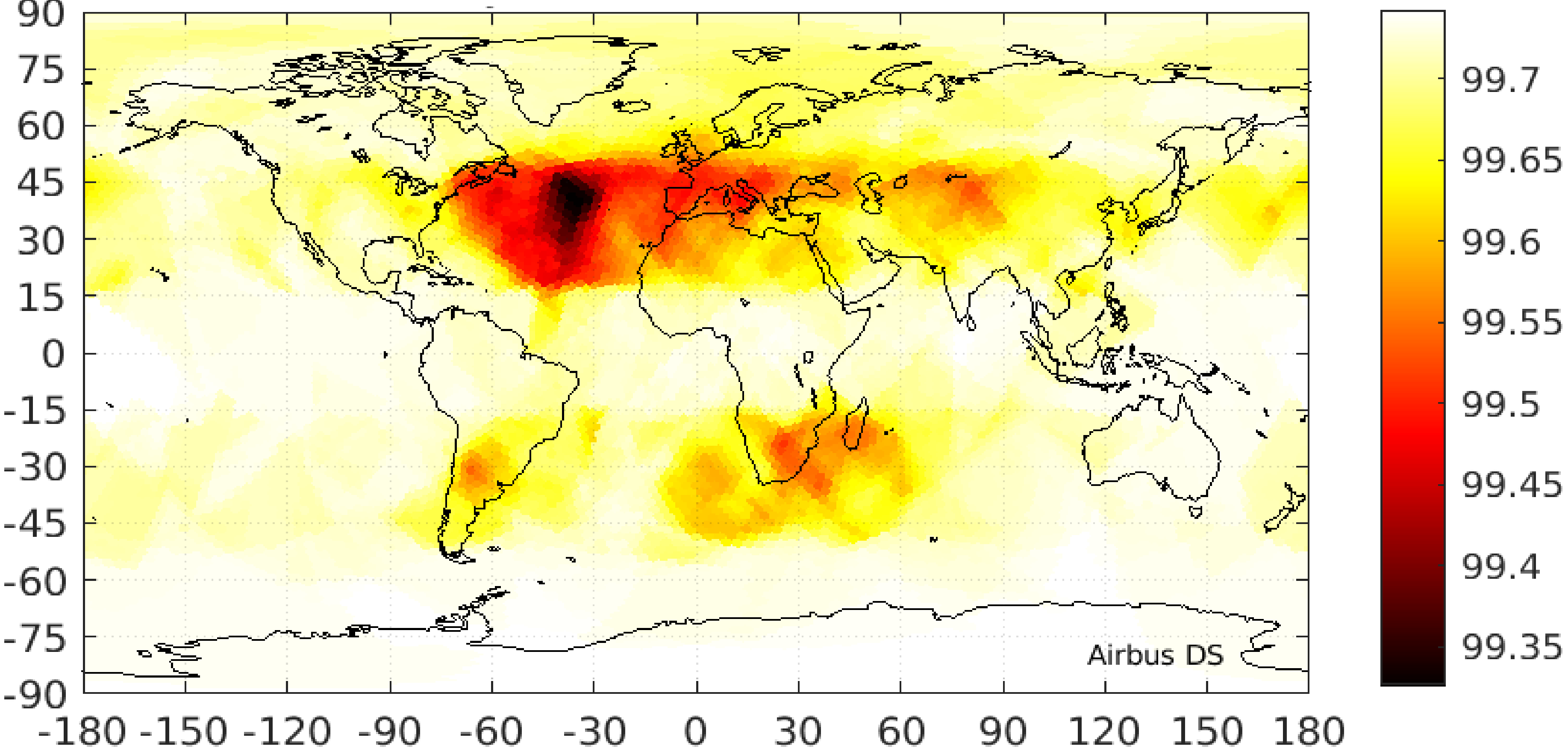
Open-source OSNMA library: https://github.com/Algafix/OSNMA

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)

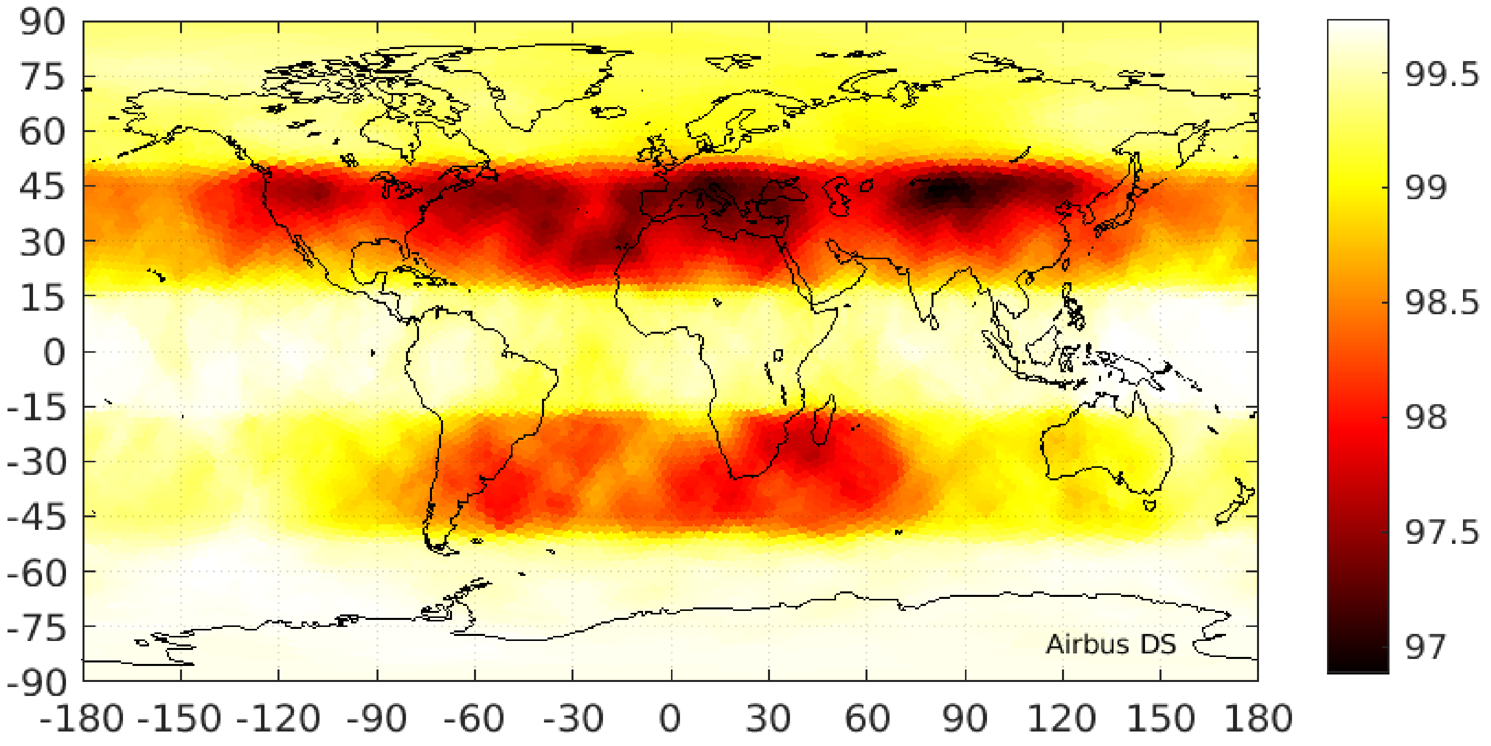


Min: 99.33% - Mean: 99.69% - Max: 99.74%

Source: ADS/EUSPA

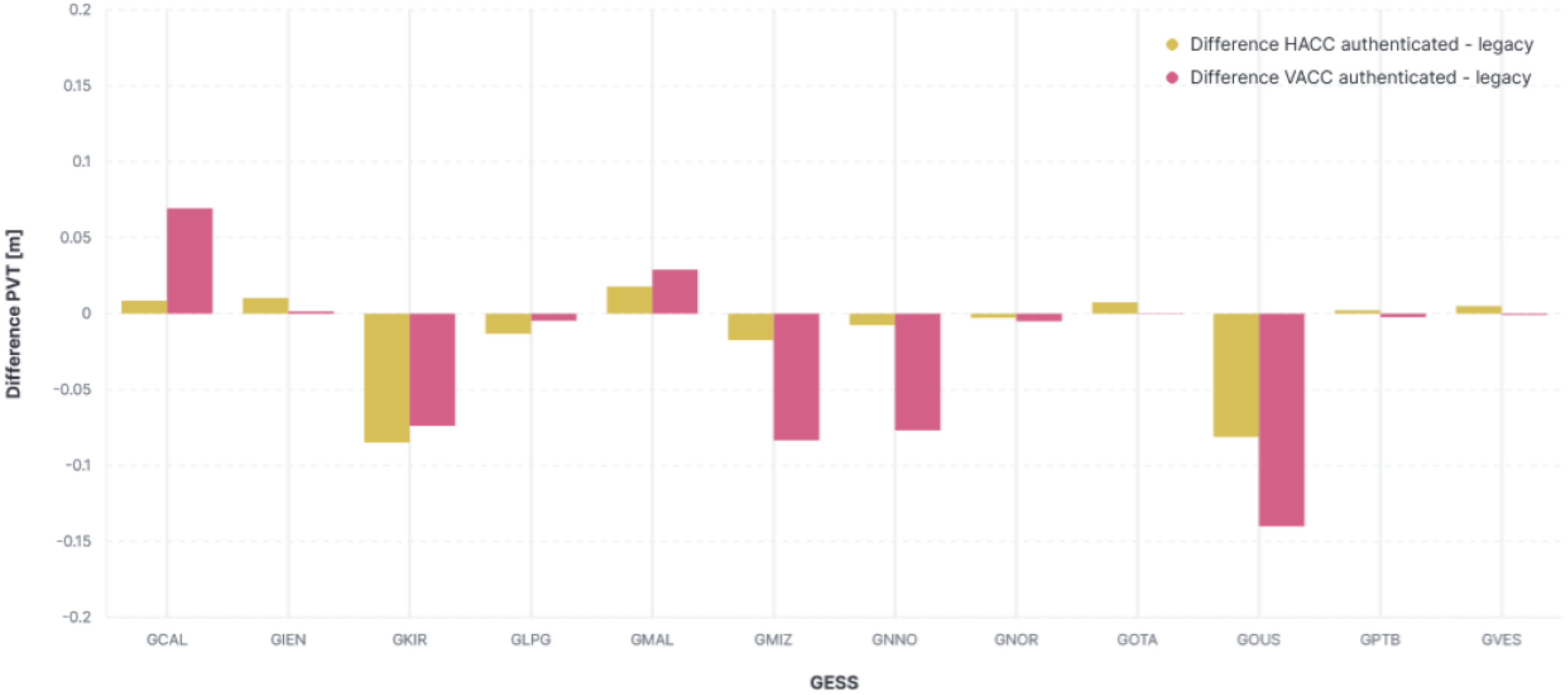
OSNMA availability

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)



Min: 96.88% - Mean: 99.01% - Max: 99.74%

OSNMA accuracy



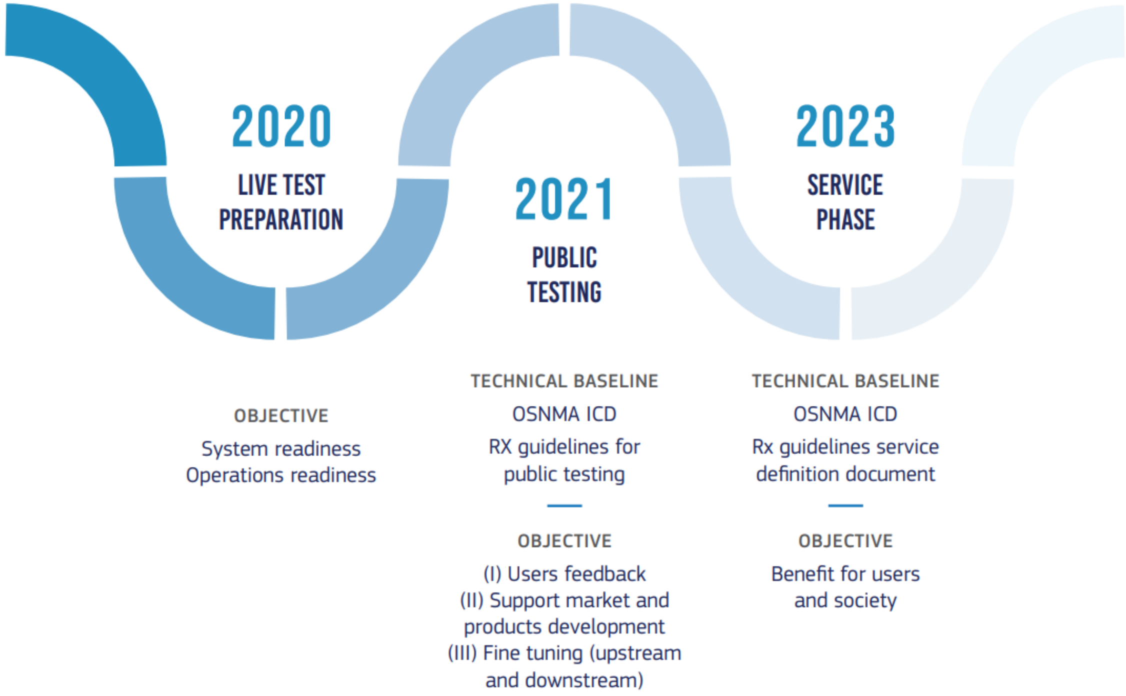
Average difference between legacy and OSNMA vertical and horizontal position accuracy (95%) measured at each TGVFx GESS from 1st May until 30th June 2022

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 1st Generation, then ranging authentication in all frequencies in Galileo 2nd Generation



2020

LIVE TEST PREPARATION

OBJECTIVE

System readiness
Operations readiness

2021

PUBLIC TESTING

TECHNICAL BASELINE

OSNMA ICD

RX guidelines for public testing

OBJECTIVE

(I) Users feedback
(II) Support market and products development
(III) Fine tuning (upstream and downstream)

2023

SERVICE PHASE

TECHNICAL BASELINE

OSNMA ICD

Rx guidelines service definition document

OBJECTIVE

Benefit for users and society

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)

Thank you for your attention!

Galileo
OSNMA

Ignacio Fernández Hernández
European Commission

Acknowledgements: JRC, ESA, EUSPA/ADS