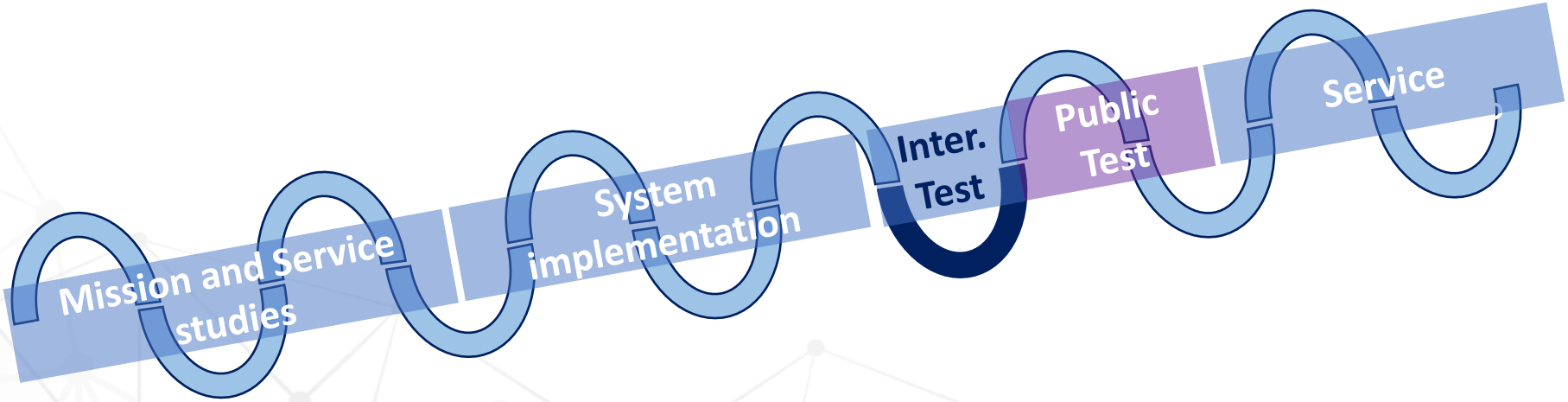
OSNMA Public Testing

EUSPA Receiver Manufactures Info Day

Javier Simon. Service Design Engineer
@EUSPA

EUSPA
European Union Agency for the Space Programme

- February 8th, 2017 – Commission implementing decision (EU) 2017/224
- November 18th, 2020 – First broadcast of OSNMA data. First OS PVT with authenticated data
- End 2021 – Start of the OSNMA public Test Phase



Galileo OSNMA is here!

GNSS has become a ubiquitous technology

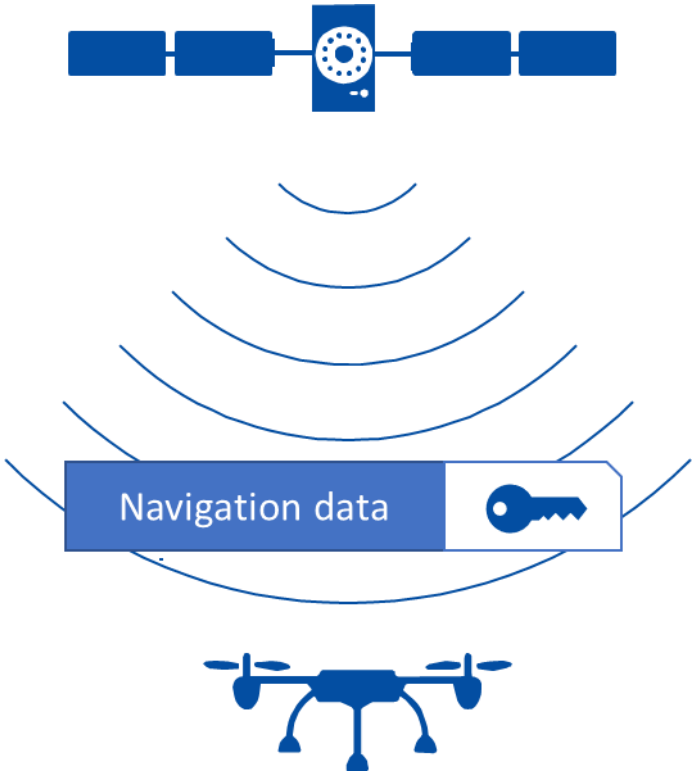
Users, applications and services relay more and more on GNSS ($$$)

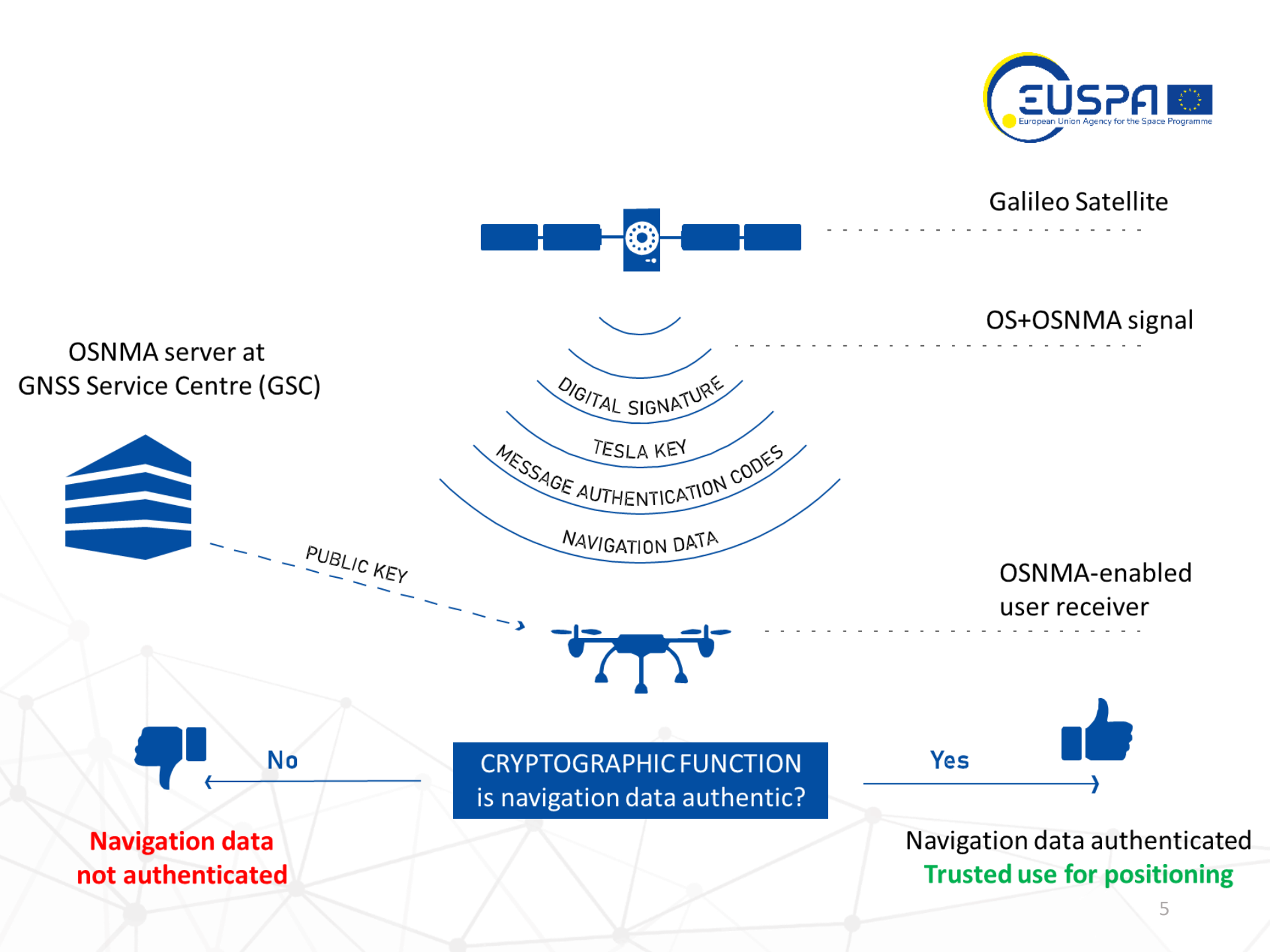
Spoofing is the generation and transmission of fake GNSS signals modifying receiver behaviour

…(usually) with the purpose to obtain an advantage

Need for a robust GNSS positioning for civil users

First step from the Galileo program to increase the robustness of the user navigation solution for open access signals

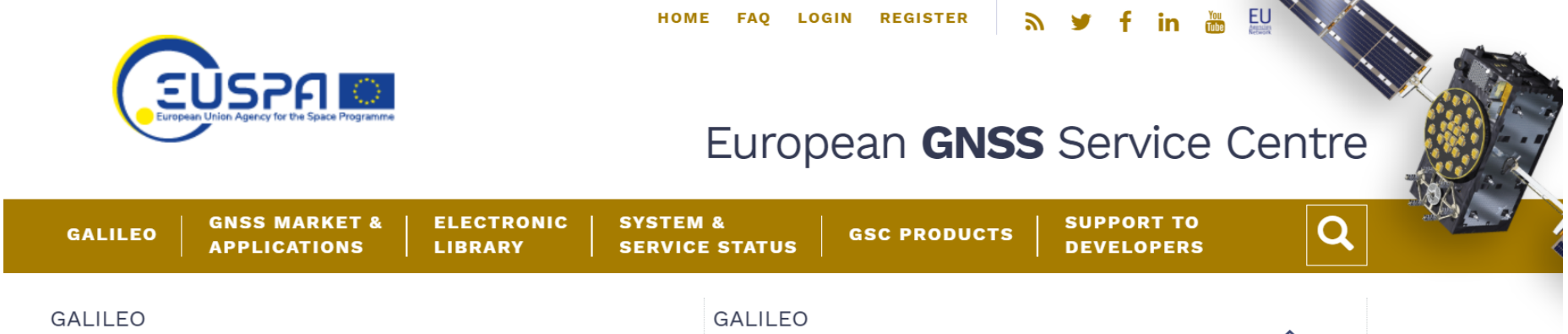



Galileo Satellite
OS+OSNMA signal
OSNMA server at
GNSS Service Centre (GSC)
DIGITAL SIGNATURE
TESLA KEY
MESSAGE AUTHENTICATION CODES
NAVIGATION DATA
PUBLIC KEY
OSNMA-enabled
user receiver
No
CRYPTOGRAPHIC FUNCTION
is navigation data authentic?
Yes
Navigation data
not authenticated
Navigation data authenticated
Trusted use for positioning

Where are we now?

- OSNMA test signal, global coverage.
- Open access (following registration process at GSC to get access to key material)
- Continuous signal provision

* Highest quality of test signal will be pursued, without associated commitments



Step 1:

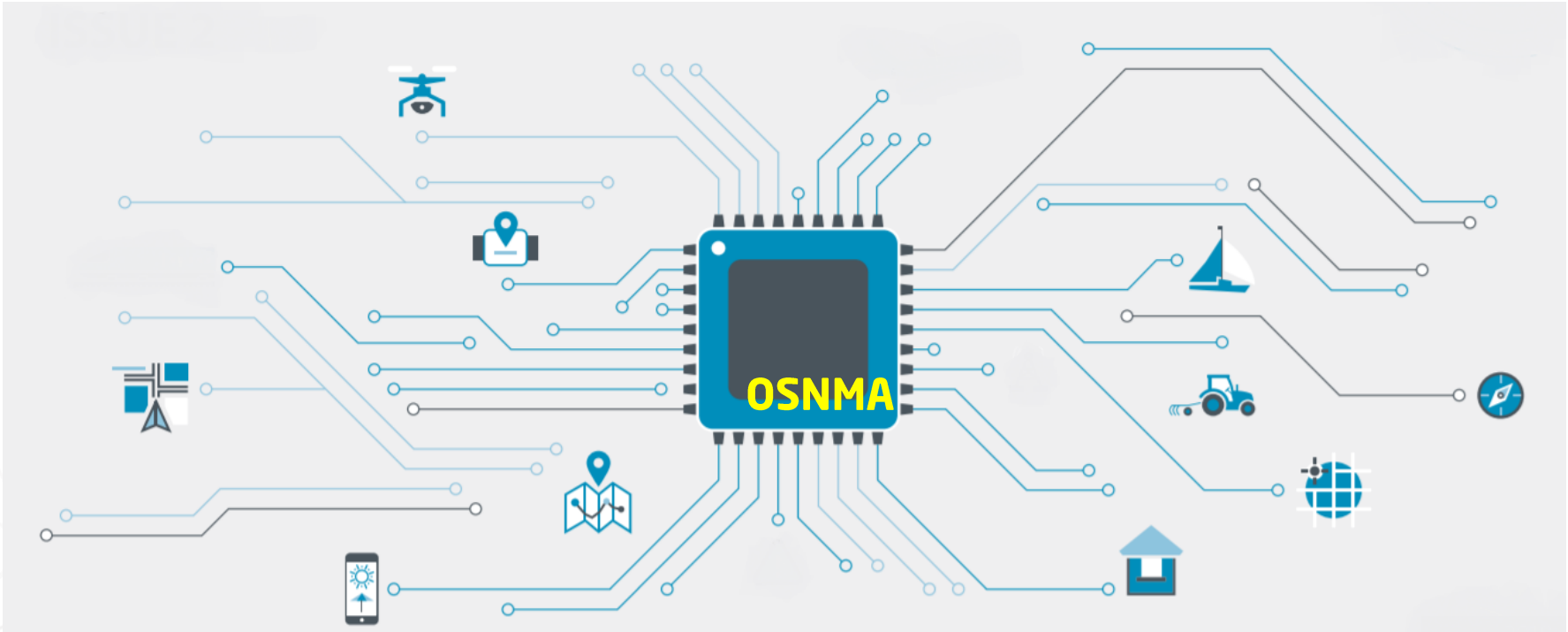
- Galileo OSNMA Info Note
- GSC web section (FAQ)

Step2:

Service Notice with start date for Test Phase

Step 3 (opening day)

- GSC news, banners
- GSC email notification to newsletters registered users
- GSC web update
  - OSNMA User ICD for Test Phase
  - OSNMA Receiver Guidelines for Test Phase
  - OSNMA Typical Performance presentation
  - User registration form to participate on Test Phase (access to key material)


OSNMA

OSNMA Test SiS structure

OSNMA Receiver Requirements

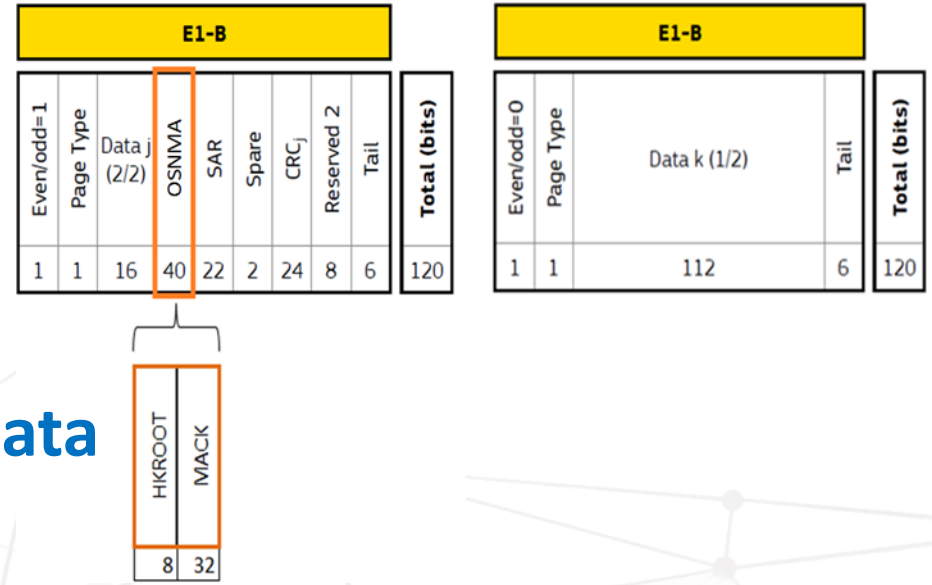
OSNMA Receiver processing logic

OSNMA Test SiS configuration and performance

DISCLAIMER: please refer to OSNMA User ICD for Test Phase and OSNMA Receiver Guidelines for Test Phase

OSNMA Test SiS structure

- Use of spare bits of I/NAV E1-B
- HKROOT section:
  - NMA header, including status flags (SiS in TEST Mode)
  - **Digital signature for Tesla Root key (K0)** and associated parameters
  - *Public key rekeying*
- MACK section
  - **Tags**
  - **TESLA chain keys**
- **Authenticated navigation data**



OSNMA Test SiS structure

- TESLA protocol (**Timed** Efficient Stream Loss-Tolerant Authentication) adapted to Galileo
- TESLA keys belong to a 1-way function

- Tag_N = trunc (MAC_function (TESLA key_N, Nav Data, other)
- Tags/TESLA keys data broadcast order within MACK section

- How user can trust a received TESLA key:
  - Received OSNMA SiS is not delayed. **Synchronization sender/receiver**
  - TESLA key is verified versus TESLA Root Key (K0) or previously verified key (hashing process)

OSNMA Test SiS structure

Authenticated navigation data (ADKD Tags types)

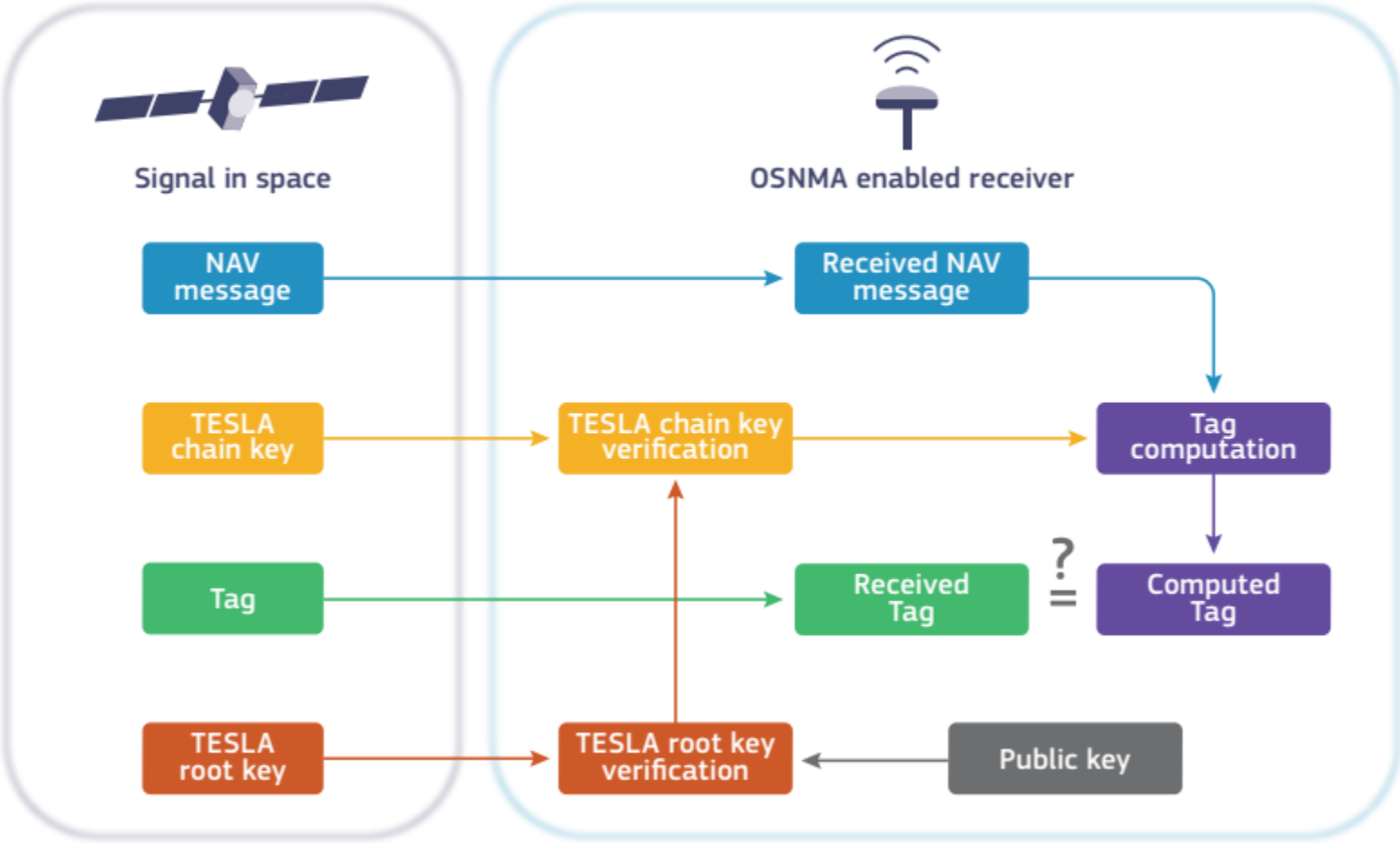
1. Galileo I/NAV Ephemeris, Clock and Status (ADKD=0 and ADKD=12)

data from Word Type 1					data from Word Type 2					data from Word Type 3								data from Word Type 4								data from Word Type 5														
	Ephemeris (1/4)					Ephemeris (2/4)					Ephemeris (3/4)									Ephemeris (4/4)		Clock Correction				Ionospheric correction													
IOD_{nav}	t_{0e}	M_0	e	$A^{1/2}$	IOD_{nav}	Ω_0	i_0	ω	$\dot{i}$	IOD_{nav}	$\dot{\Omega}$	Δn	C_{UC}	C_{US}	C_{RC}	C_{RS}	SISA(E1,E5b)	IOD_{nav}	SVID	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	BGD(E1,E5a)	BGD(E1,E5b)	$E5b_{HS}$	$E1B_{HS}$	$E5b_{DVS}$	$E1B_{DVS}$	**Total (bits)**
10	14	32	32	32	10	32	32	32	14	10	24	16	16	16	16	16	8	10	6	16	16	14	31	21	6	11	11	14	1	1	1	1	1	10	10	2	2	1	1	**549**

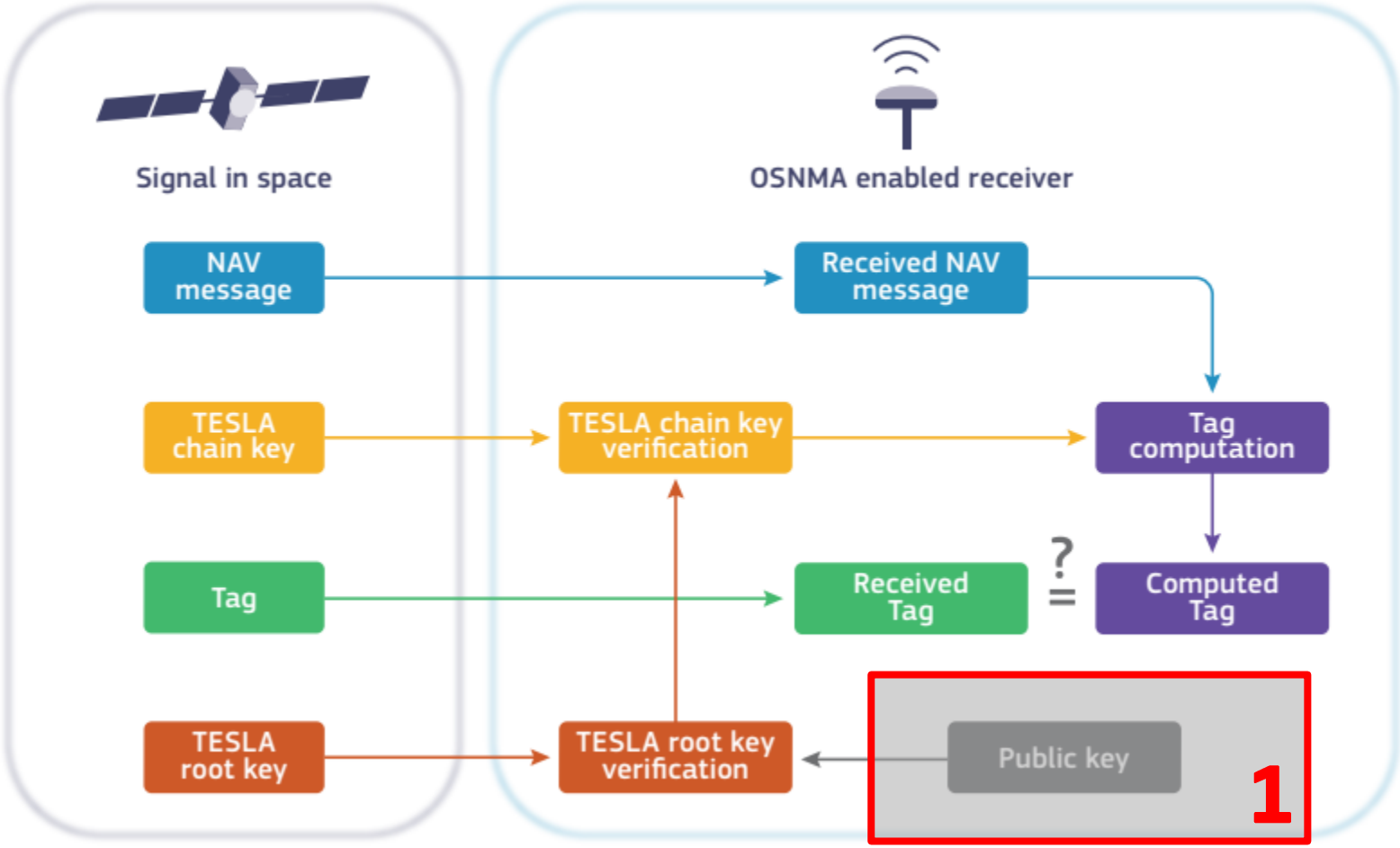
2. Galileo I/NAV Timing Parameters (ADKD=4)

data from Word Type 6									data from Word Type 10				
GST-UTC conversion parameters									GST-GPS conversion parameters				
A_0	A_1	Δt_{LS}	t_{ot}	WN_{0t}	WN_{LSF}	DN	Δt_{LSF}	TOW	A_{0G}	A_{1G}	t_{0G}	WN_{0G}	**Total (bits)**
32	24	8	8	8	8	3	8	20	16	12	8	6	**161**

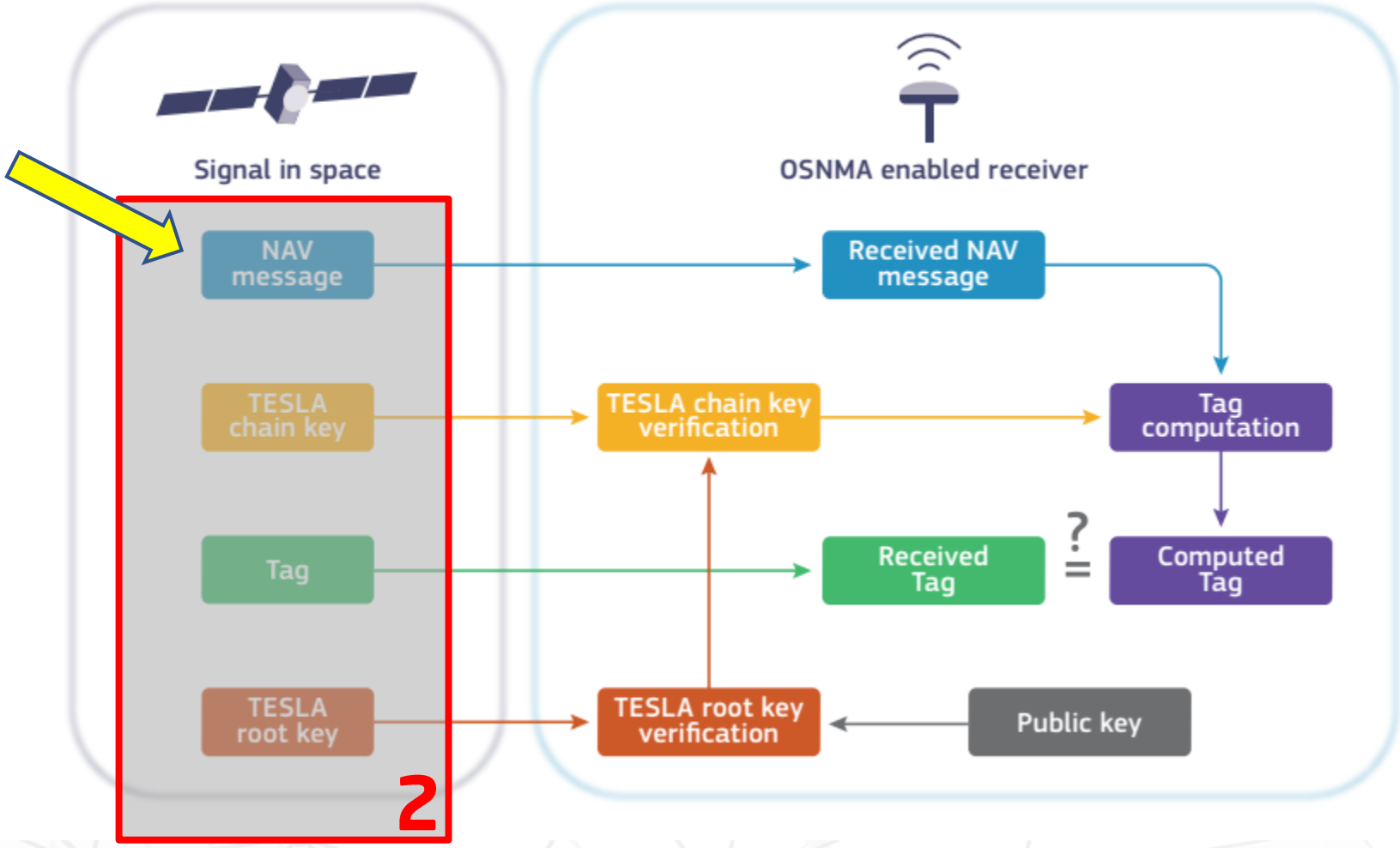
OSNMA Receiver processing logic



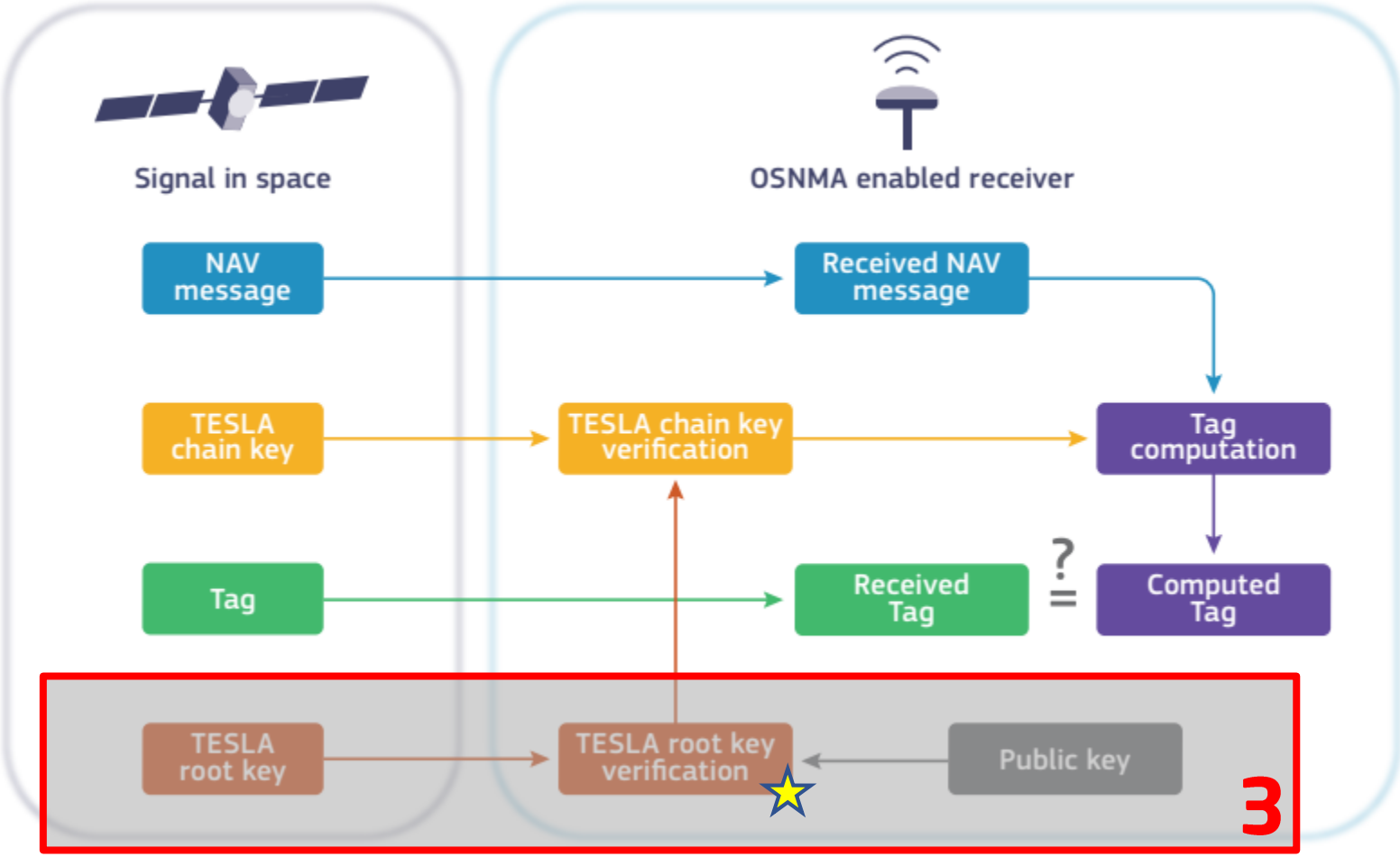
OSNMA Receiver processing logic



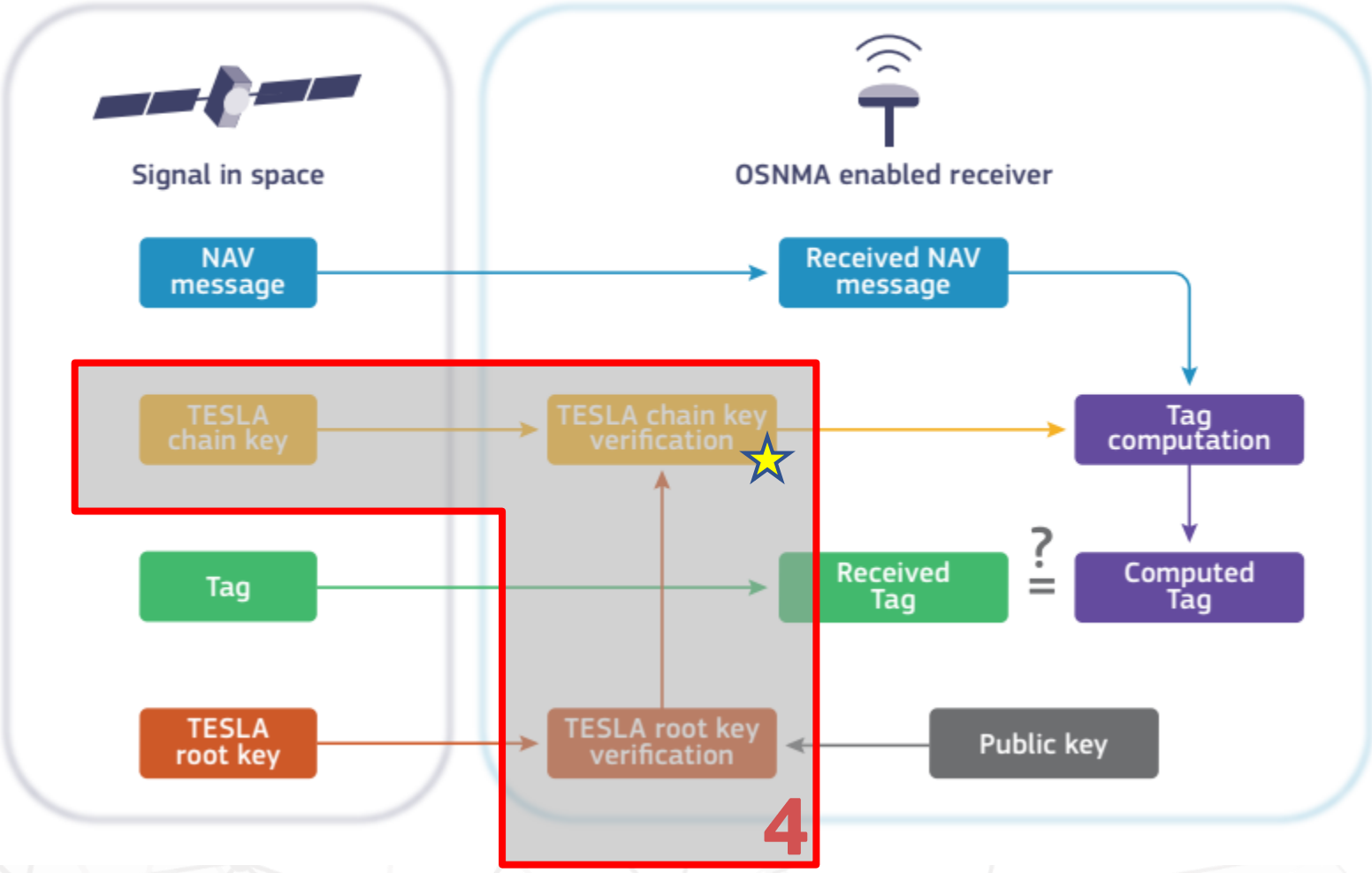
OSNMA Receiver processing logic



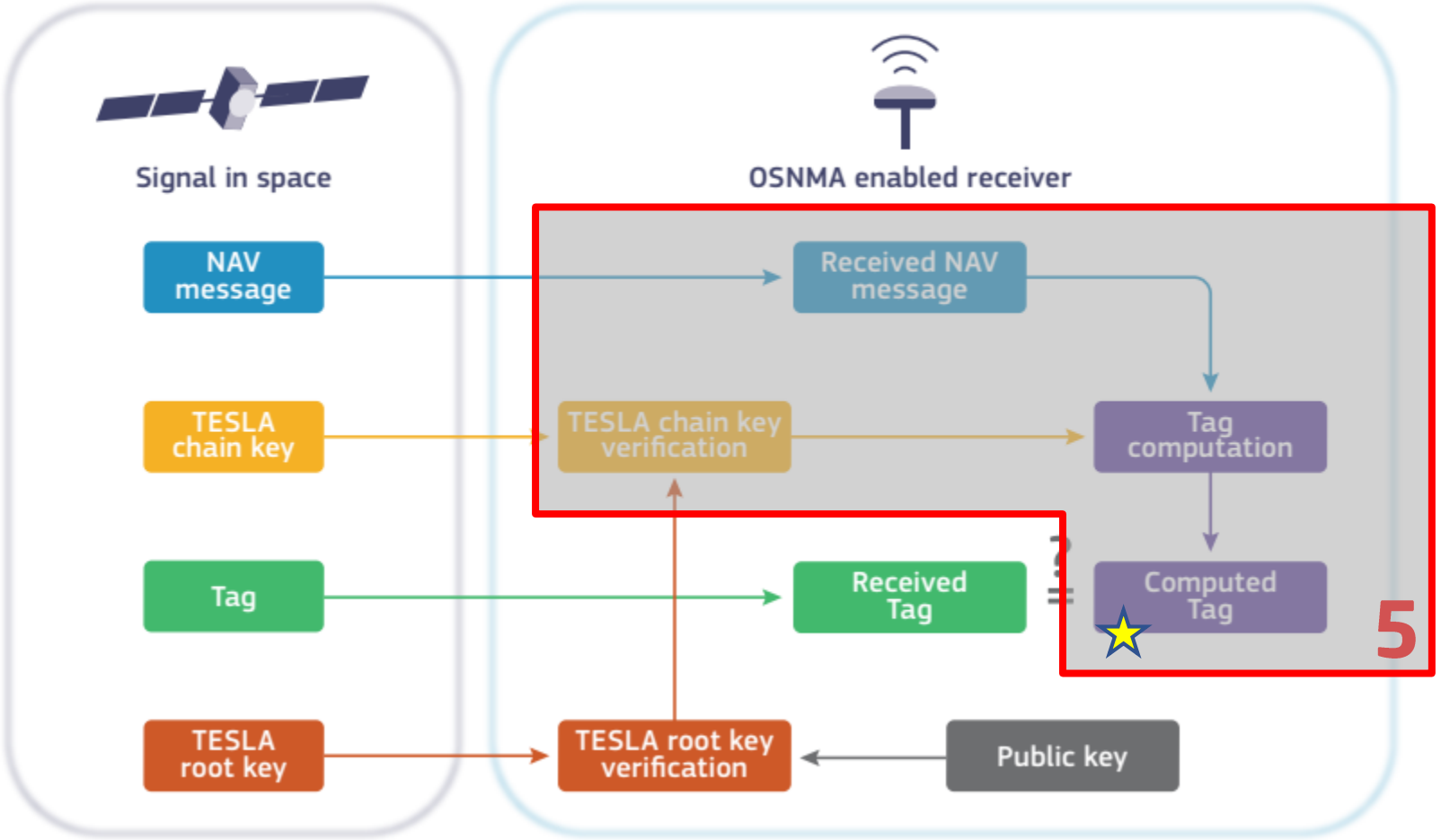
OSNMA Receiver processing logic



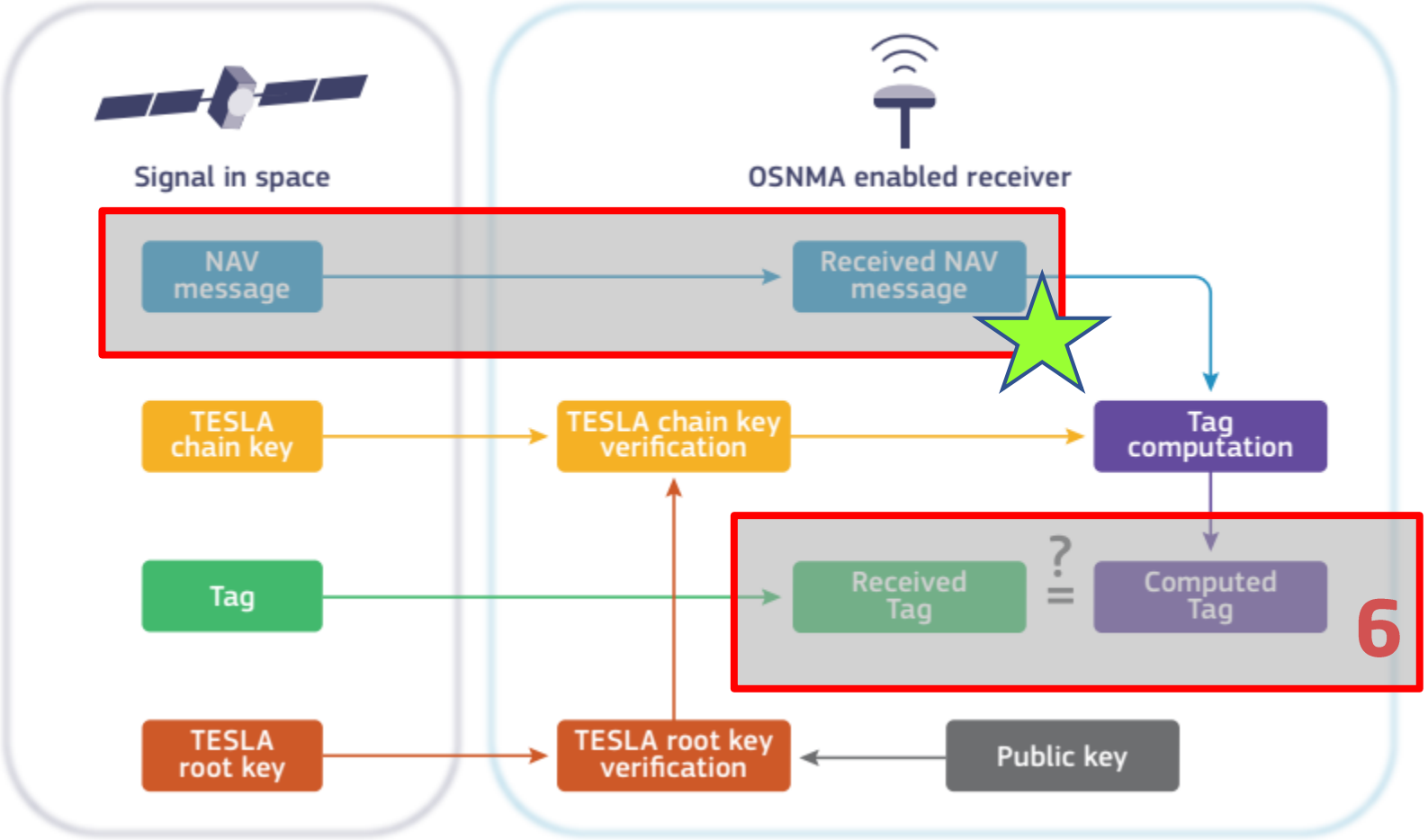
OSNMA Receiver processing logic



OSNMA Receiver processing logic



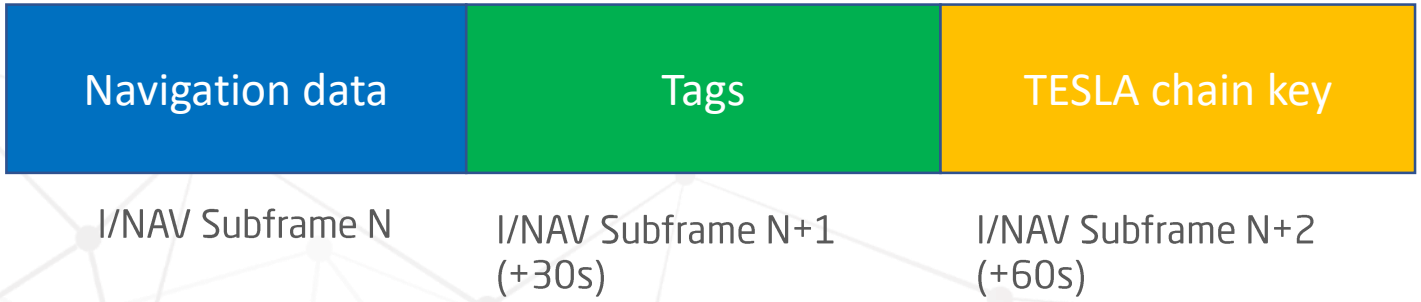
OSNMA Receiver processing logic



OSNMA Receiver processing logic

Important steps:

- Verification of OSNMA status flags
- GST Retrieval and Verification from the SIS. User shall verify that received OSNMA SiS is not delayed. Retrieved value (GST SiS) shall be verified against the receiver local realization (GST Rx)
- OSNMA and navigation data retrieval for authentication. IOD aiding for navigation data retrieval. Extended TESLA chain key delay for ADKD#12 Tags



- Tag accumulation to reach minimum tag length for authentication (80 bits)

OSNMA Receiver Requirements

- Time synchronization requirement (set and maintain GST Rx)
- Cryptographic Functions (SHA-256, SHA3-256, HMAC-SHA-256, CMAC-AES, ECDSA P-256/SHA-256, ECDSA P-521/SHA-512)
- Integrity of the stored cryptographic material and functions
- Interfaces. OSNMA SiS (+GSC)

Receiver contribution is <u>needed</u> to achieve authentication. Please check OSNMA Receiver Guidelines for Test Phase

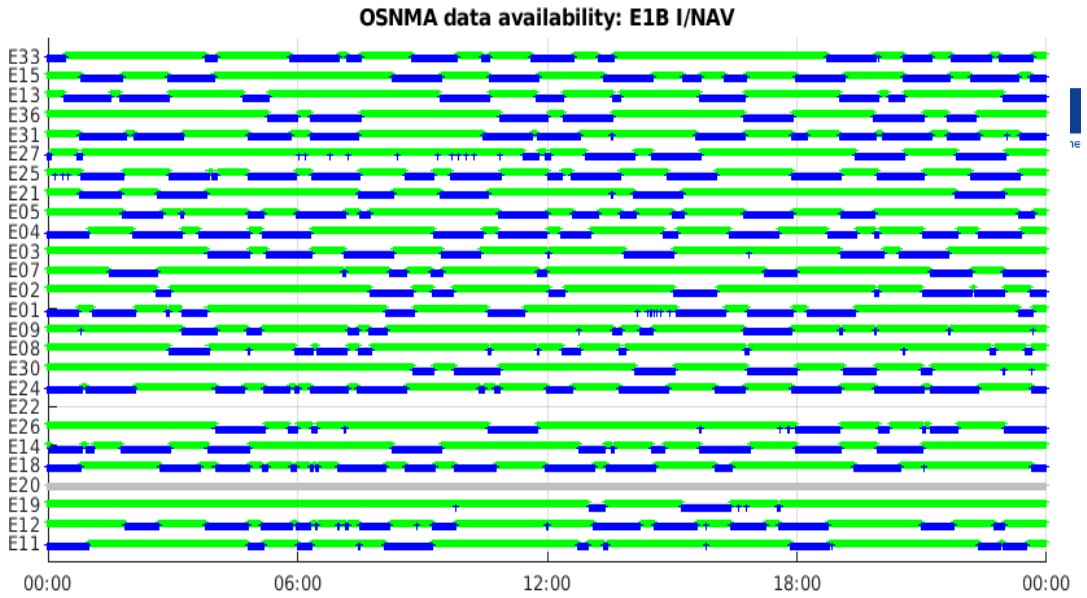
OSNMA Test SiS configuration and performance

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 (target security level 80 bits)
Number of Tags per subframe	6
Tag sequence (over 2 subframes)	[00S, 00E, 04S, 00E, 12S, 00E] ; [00S, 00E, 00E, 12S, 00E, 12E]

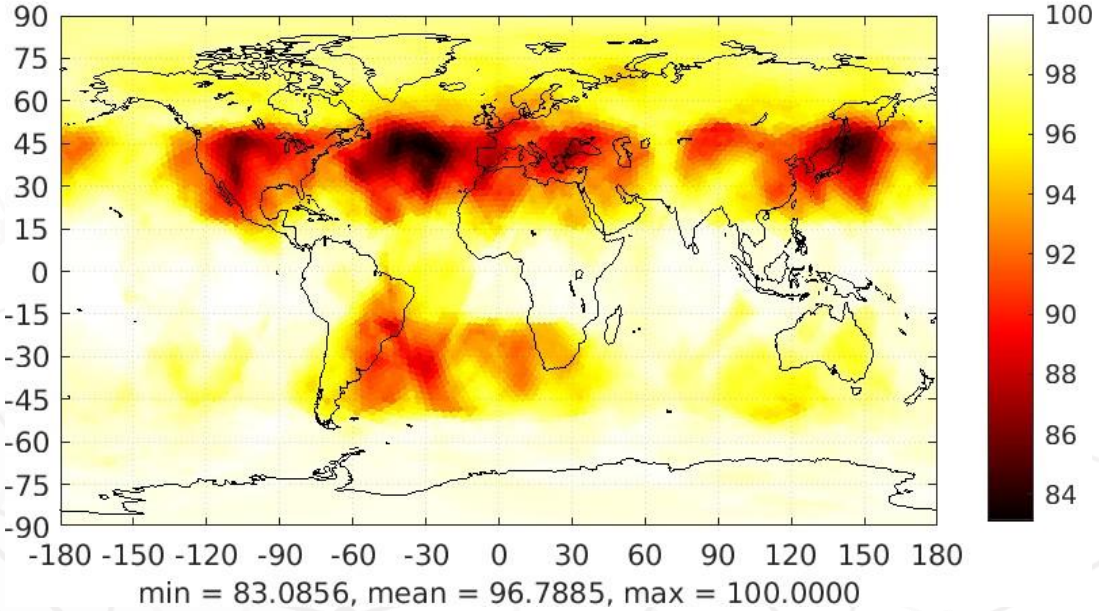
Tag sequence first subframe					
00S	00E	04S	00E	12S	00E
Tag sequence second subframe					
00S	00E	00E	12S	00E	12E

OSNMA SiS configuration and performance

OSNMA data broadcast from Galileo satellites is not continuous



Green: OSNMA data available. Blue: No OSNMA data



OSNMA data availability from at least 4 SV > 5°

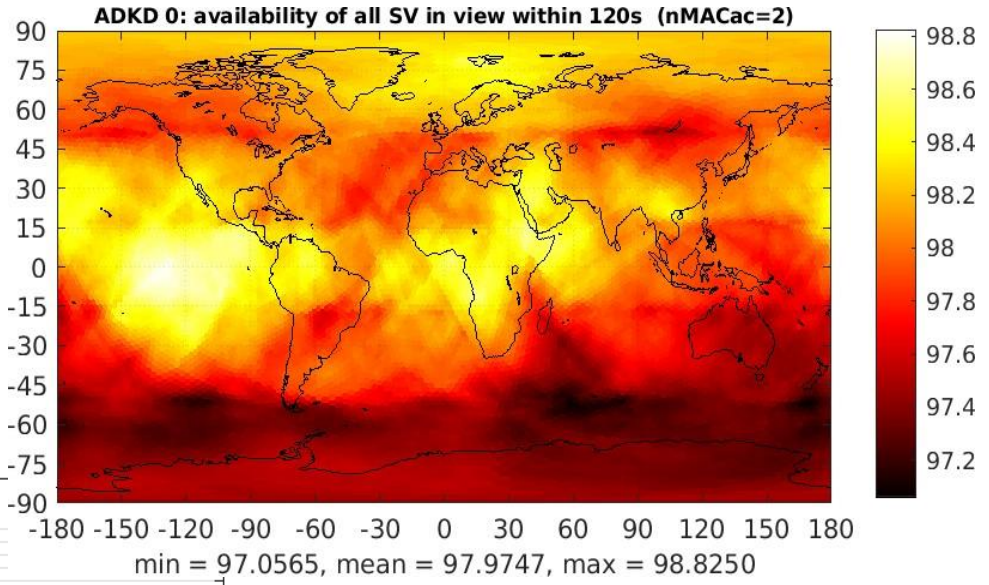
OSNMA SiS configuration and performance

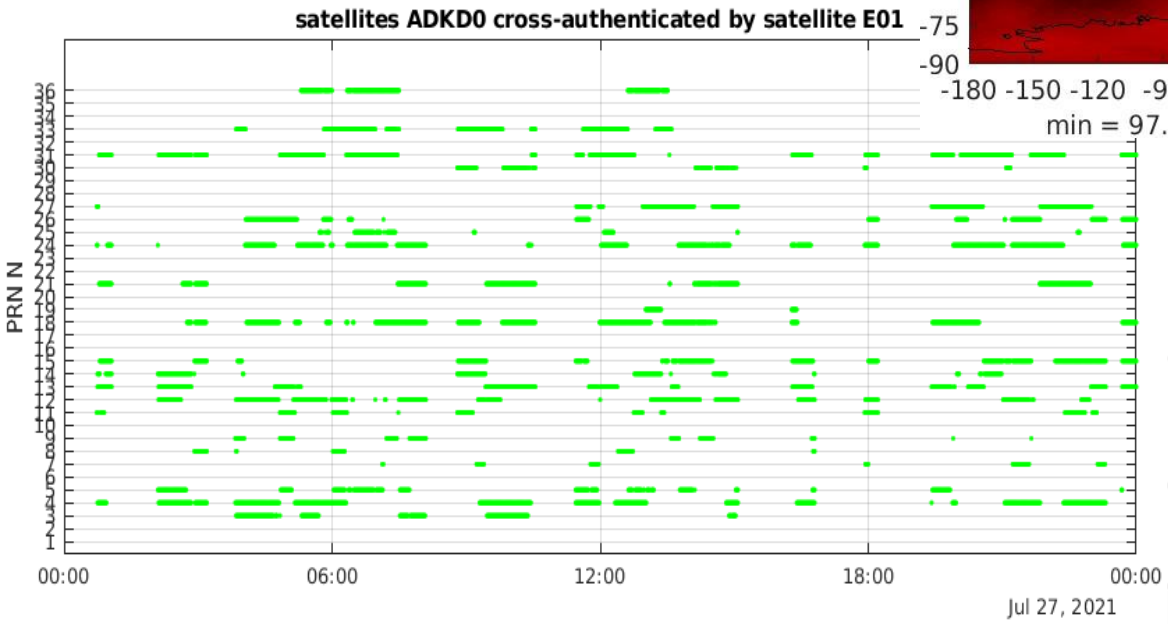
Tags for I/NAV ephemeris and clock correction for all SV in view (every 120 sec), August 2021

“cross-authentication” feature to increase the availability of tags at user level

Ultimate target is to provide authentication for every visible satellite at user level, and do it frequently

Residual Tag verification failure rate to be expected during the Test Phase

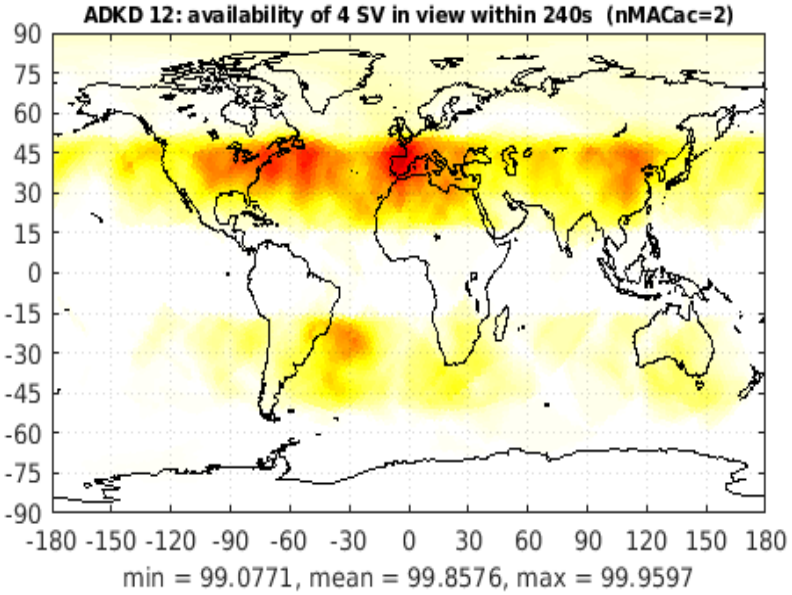




WUL: 97.06%
AUL: 97.97%
BUL: 98.82%

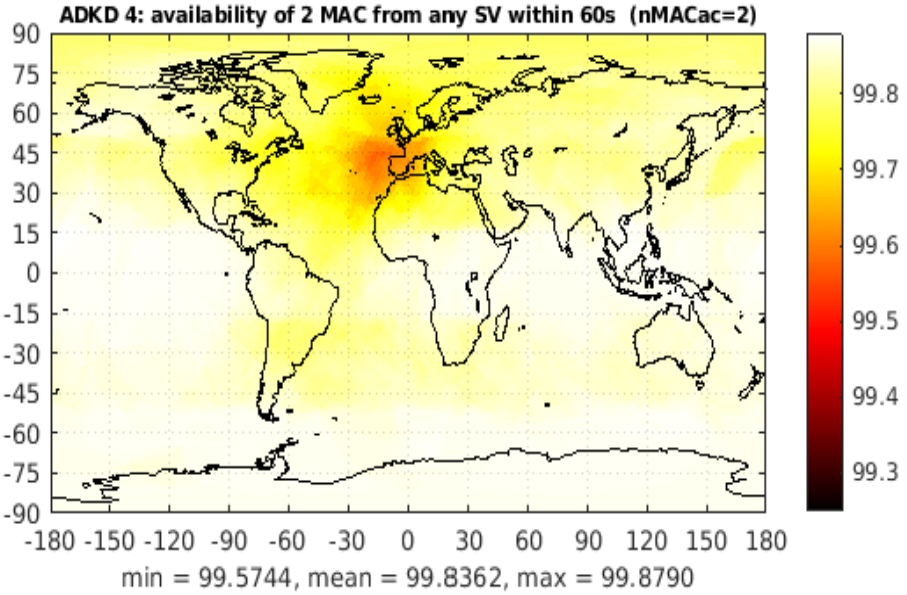
OSNMA SiS configuration and performance

Tags for I/NAV ephemeris and clock correction (ADKD#12) for at least 4 SV in view (every 240 secs), August 2021



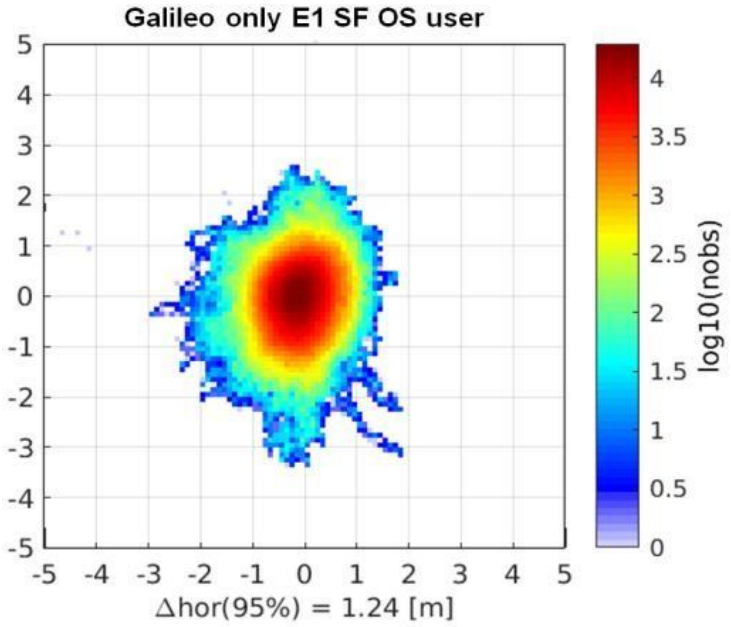
WUL: 99.08%
AUL: 99.86%
BUL: 99.96%

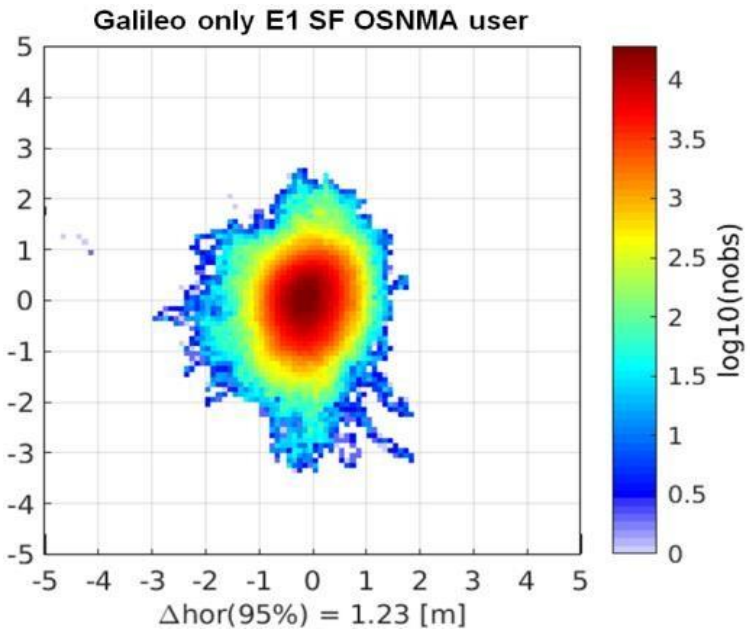
Tags for timing parameters from at least 1 SV in view (every 60 secs), August 2021



WUL: 99.57%
AUL: 99.84%
BUL: 99.88%

OSNMA SiS configuration and performance





H: 1.24m (95%)
V: 1.83m (95%)

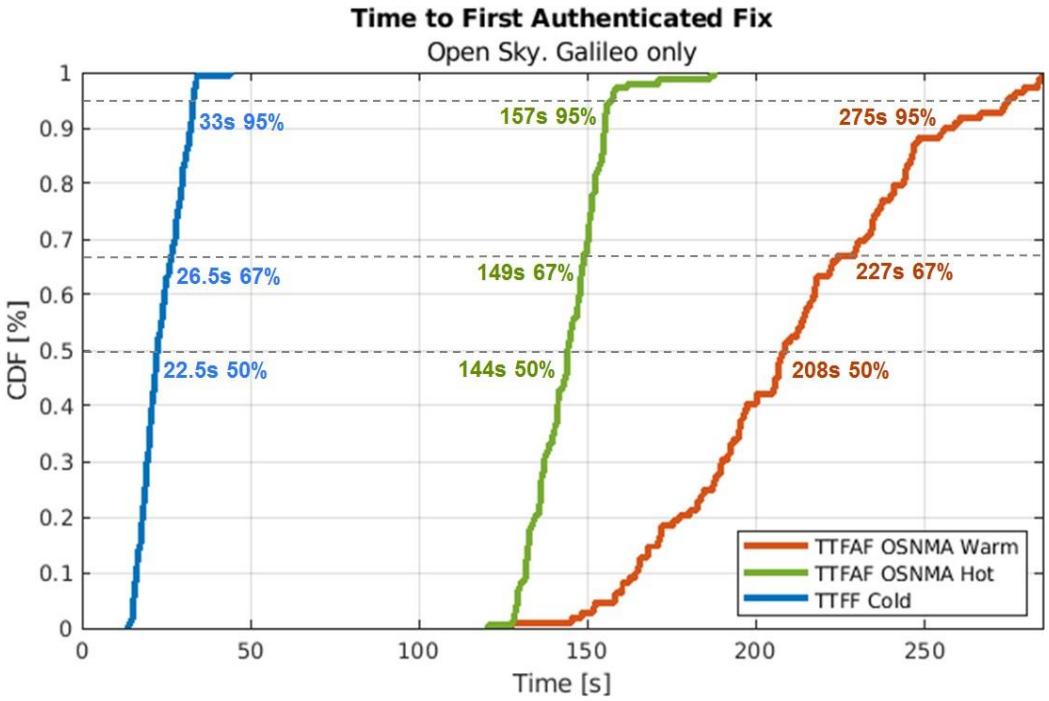
Standard OS user

H: 1.23m (95%)
V: 1.82m (95%)

OSNMA user

E1 Single Freq OS/OSNMA user, open sky, fixed antenna, Airbus premises Munich, July 2021

OSNMA SiS configuration and performance



Startup conditions for OSNMA:

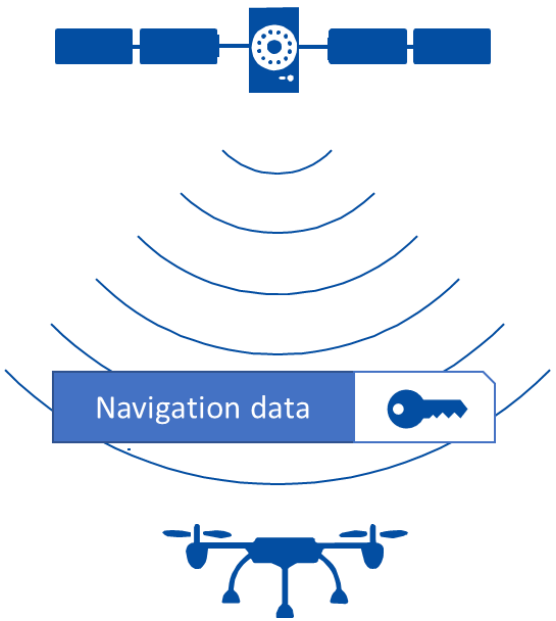
- OSNMA Warm Start: Public Key available; TESLA Root Key not-available at startup
- OSNMA Hot Start: Public Key and Root Key available at startup

OSNMA Test SiS structure

- Evolutions of the OSNMA Test SiS are already identified. Basic structure and principles unmodified.
  - Reserved fields in Tag section will be defined to provide unambiguous link between Tag and authenticated navigation data
  - Navigation data mask for ADKD 4 Tag (Timing Parameter) will be redefined to remove TOW
  - Regular transmission of Public Key via SIS

- Flexible implementation to be able to accommodate evolutions

- OSNMA Test Signal is (almost) there. Relevant documentation is about to be published. Follow GSC web portal updates.
- Please implement! And give us feedback! Galileo GSC helpdesk
- Work continues towards future service declaration



Linking space to user needs

Get in touch with us

www.euspa.europa.eu

EU4Space | EUSPA | @EU4Space | @space4eu | EUSPA