

Galileo OSNMA:

Join the Public
Observation Test
Phase and share
your feedback!



EUSPA Webinar – 2nd February 2022



House rules:

The session is not recorded, the slides/link to slides will be provided in a separate communication after the webinar

Ahead of us: series of presentations; after each short Q/A, last 30 min the general Q/A

Interaction:

Q/A panel – we will do our best to address the questions on spot, in case some are left unaddressed/ require longer elaboration or additional checking, we will revert to you by e-mail

Informative session – no possibility to network

By default, no possibility to unmute or share video; however should you wish to speak, please raise hand or write in the Q/A to the panellists and we will make it possible

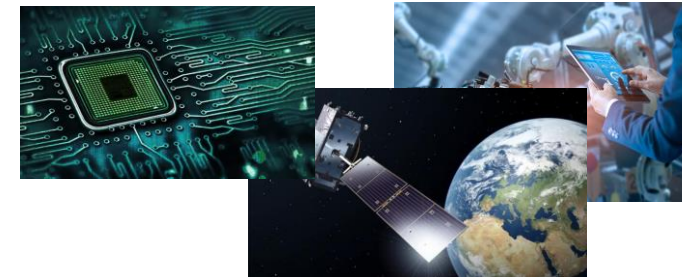
In case of technical issues, please write directly to the host in the Q/A



Galileo OSNMA: Join the Public Observation Test Phase and share your feedback!



Application developers



Receiver manufacturers

Galileo OSNMA: Join the Public Observation Test phase and share your feedback!

1 Welcome & Introduction

- EUSPA & OSNMA team introduction
- Objective of the webinar



10 min

2 Galileo OSNMA

- GNSS Authentication & the Galileo solution: OSNMA
- OSNMA Service and Roadmap



20 min

3 Public Observation Phase

- How to benefit from it
- Guidelines for testing & feedback



55 min

4 Q&A



35 min



Galileo OSNMA: Join the Public Observation Test phase and share your feedback!

1 Welcome & Introduction

- EUSPA & OSNMA team introduction
- Objective of the webinar



10 min

2 Galileo OSNMA

- GNSS Authentication & the Galileo solution: OSNMA
- OSNMA Service and Roadmap



20 min

3 Public Observation Phase

- How to benefit from it
- Guidelines for testing & feedback



55 min

4 Q&A



35 min



1

2

3

4

Welcome & Introduction

Speakers



Flavio Sbardellati

Head of Governmental Market and
downstream R&I, EUSPA



Javier Simon

Galileo Service Design Engineer,
EUSPA



Sophie Damy

Scientific officer, JRC



Ernst Phillip Mrohs

Head of Laboratory, NavCert GmbH



**OSNMA
Public
Observation
Phase**



Application developers

Receiver manufacturers



Support



Galileo OSNMA: Join the Public Observation Test phase and share your feedback!

1 Welcome & Introduction

- EUSPA & OSNMA team introduction
- Objective of the webinar



10 min

2 Galileo OSNMA

- GNSS Authentication & the Galileo solution: OSNMA
- OSNMA Service and Roadmap



20 min

3 Public Observation Phase

- How to benefit from it
- Guidelines for testing & feedback



55 min

4 Q&A



35 min



Increasing incidence of spoofing attacks is driven by growing awareness and availability of illegal disruption equipment



What is GNSS spoofing?

- Spoofing is the generation and transmission of **counterfeit GNSS signals** modifying receiver behaviour
- **Estimated cost¹** of possible GNSS outage caused by various attacks, including spoofing, is over **€ 1 bi /day**
- Range of attack can be wide and create **collateral damage**
- Receivers and GNSS-dependent systems may be **vulnerable**
- **Need for robust functionality** for civil users



¹ Based on a study estimating cost of GNSS outage. Source: RTI International (2019)

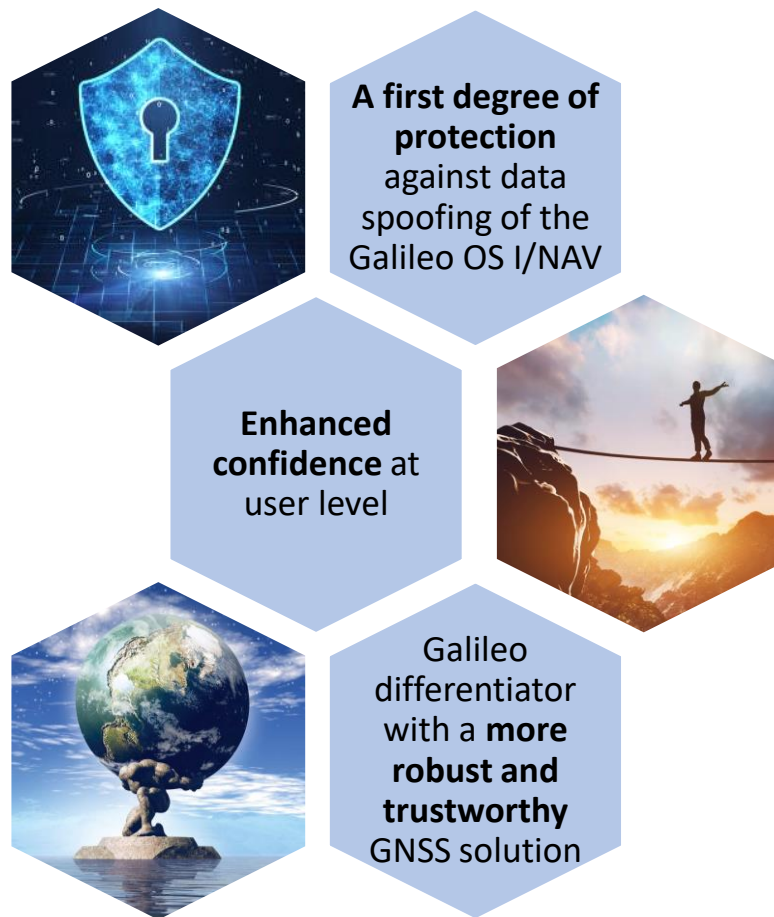
OSNMA contributes to the overall robustness of the application against certain types of spoofing attacks

OSNMA: Open Service Navigation Message Authentication

- **Authentication of Galileo Navigation Message**
- **Freely** accessible to **worldwide** users
- **First of its kind for open GNSS signals**
- **Full backward compatible:** performance levels of standard OS receivers remain untouched
- **Limited hardware impact:**
 - Trustable knowledge of time
 - Store and ensure the integrity of a public key
- Minimal impact on receivers - **computational burden commensurate with low-cost receiver capabilities**
- Added-value brought to a **variety of applications**

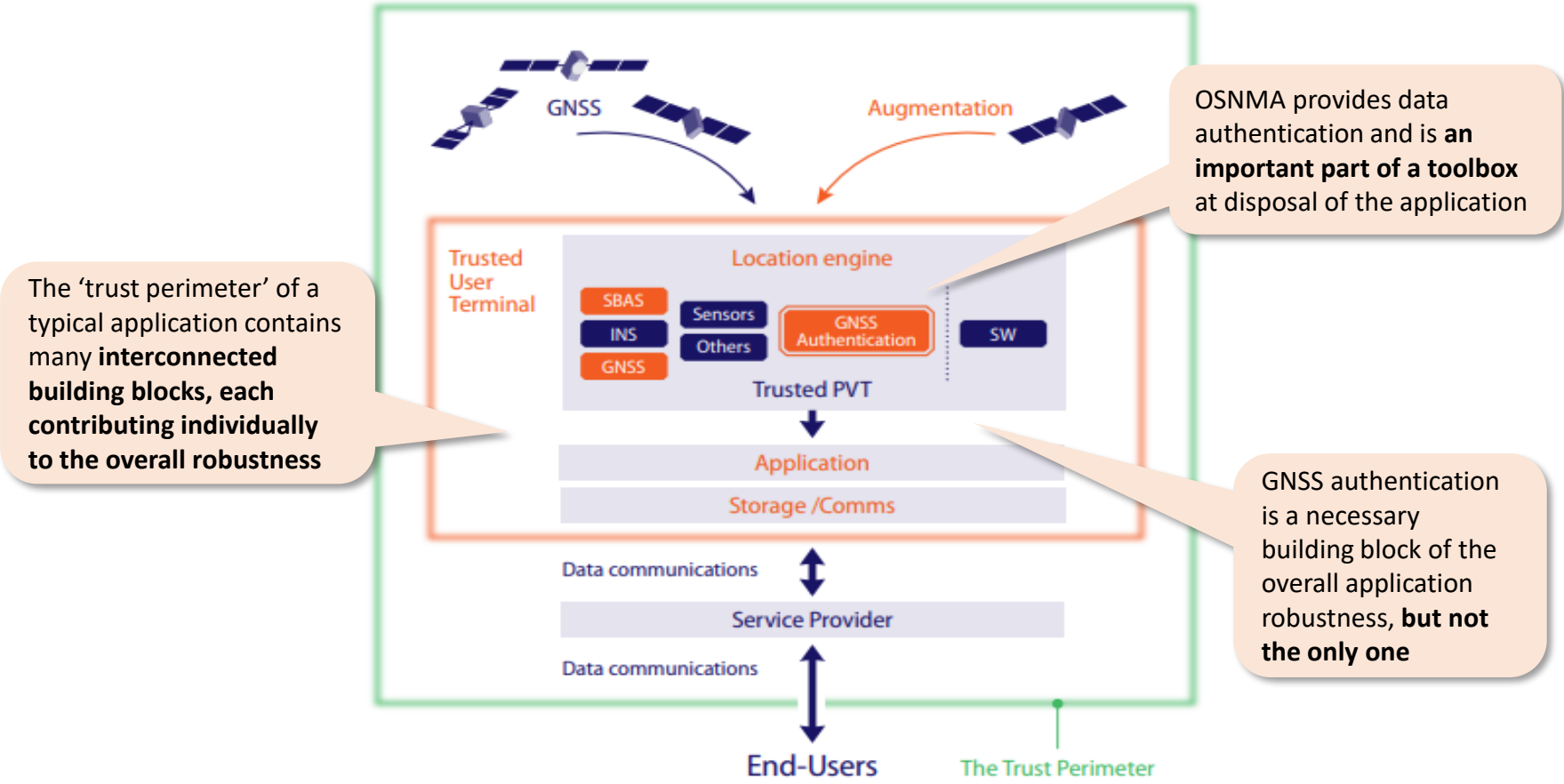


Benefits and added value



- 1
- 2
- 3
- 4

OSNMA is an essential part of the application's robustness within the Trust Perimeter



Despite the improvement provided, other building blocks are required for end-to-end authentication



OSNMA has high market potential for many applications in various segments

Examples of application to benefit from OSNMA

Market potential is constrained by relevant **certification/regulatory frameworks**

Asset management

OSNMA enables product differentiation as **asset value** justify higher robustness

Drones

OSNMA to contribute on navigation robustness for **safely sharing the airspace**

Proof of Delivery

OSNMA adds value in B2B and B2C dispatches through **last mile position authentication**

Smart Tachograph

OSNMA supports road enforcers and simplifies **regulation compliance**

Mobile Payments

OSNMA **reinforces required robustness** of commercial transactions

Check the **complete list of targeted applications** on the [OSNMA Info Note](#)

https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_Info_Note.pdf



1

2

3

4

OSNMA has been successfully tested in several projects



... and many others!



PATROL involves the development, supply and testing of an **OSNMA user terminal** for **smart tachographs**



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



Development of a low-cost GNSS based solution to achieve **high-level antitheft protection**, adaptable to different types of operations and users



Development of an innovative positioning On-Board-Unit suitable for **fully automated driving** to enable the target applications' performance in the SAE levels 4/5



Development of a **high performance positioning system for drones** within the U-Space framework focusing on Very Low Level and UAS operations



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

Check the **complete list of OSNMA-related projects** on the [OSNMA Info Note](#)

1

2

3

4

Summary of OSNMA Capabilities

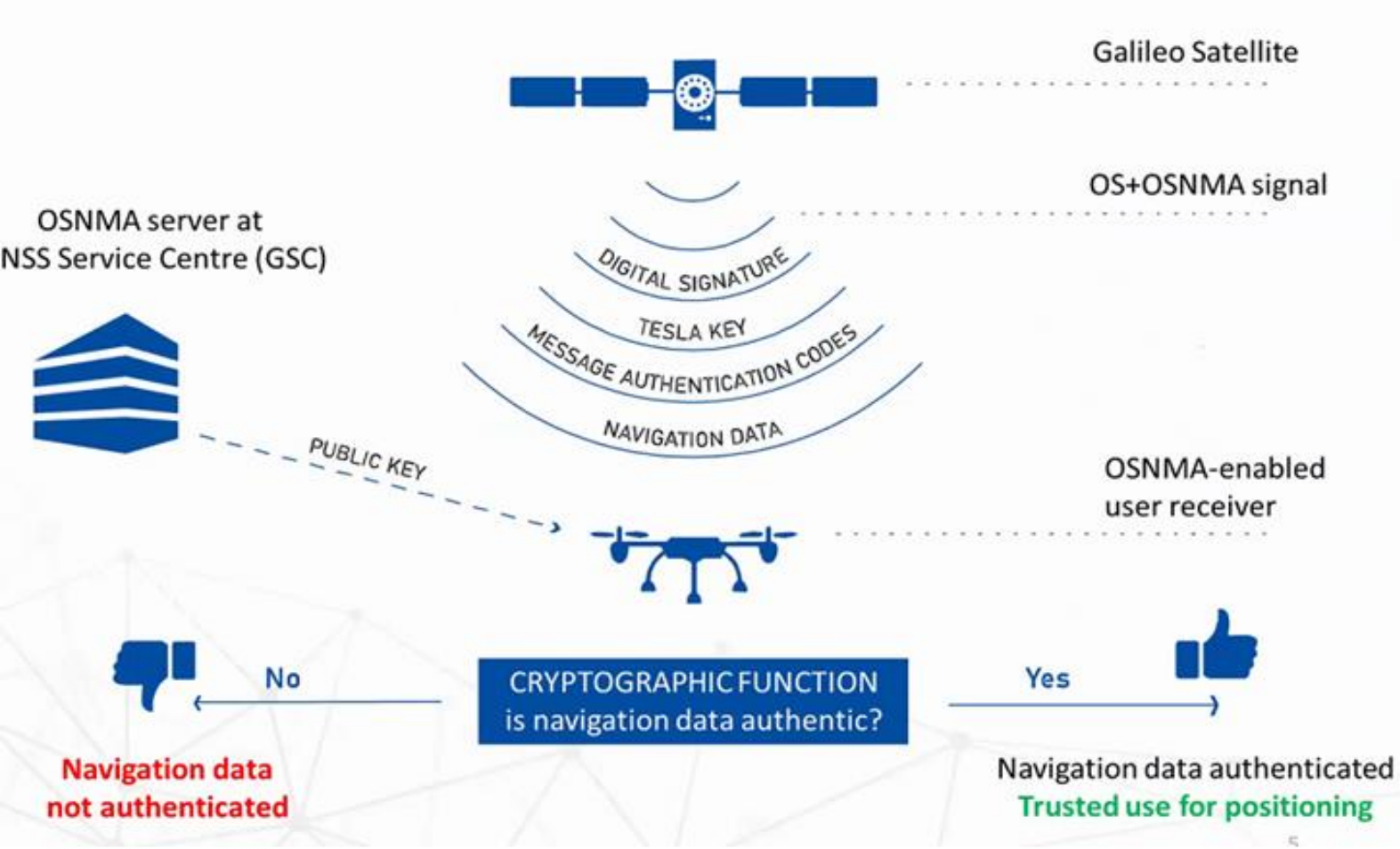
CHARACTERISTIC	OSNMA
GNSS Receiver Minimal Capabilities	Single frequency E1
Object Of Authentication	Nav Data (E1B I/Nav and E5b I/Nav and capability for E5a F/Nav if required)
Required Components	E1B
Need Of Raw GNSS Signal Storage At Receiver Side	No
Navigation Signals Decryption By GNSS Receiver	No
Need Of A Network Connection	No
Authentication	Clock & Ephemeris Data (CED) and timing parameters (GGTO and UTC), delayed
Time To First Authentication	One to few minutes
Authentication Availability	High, expected above 95%
Anti-tampering Features	Light, as the receiver only stores a public key. To be considered depending on the specific application threats
Other Requirements	Time synchronisation

Few constraints on receivers enable a broader range of potential applications



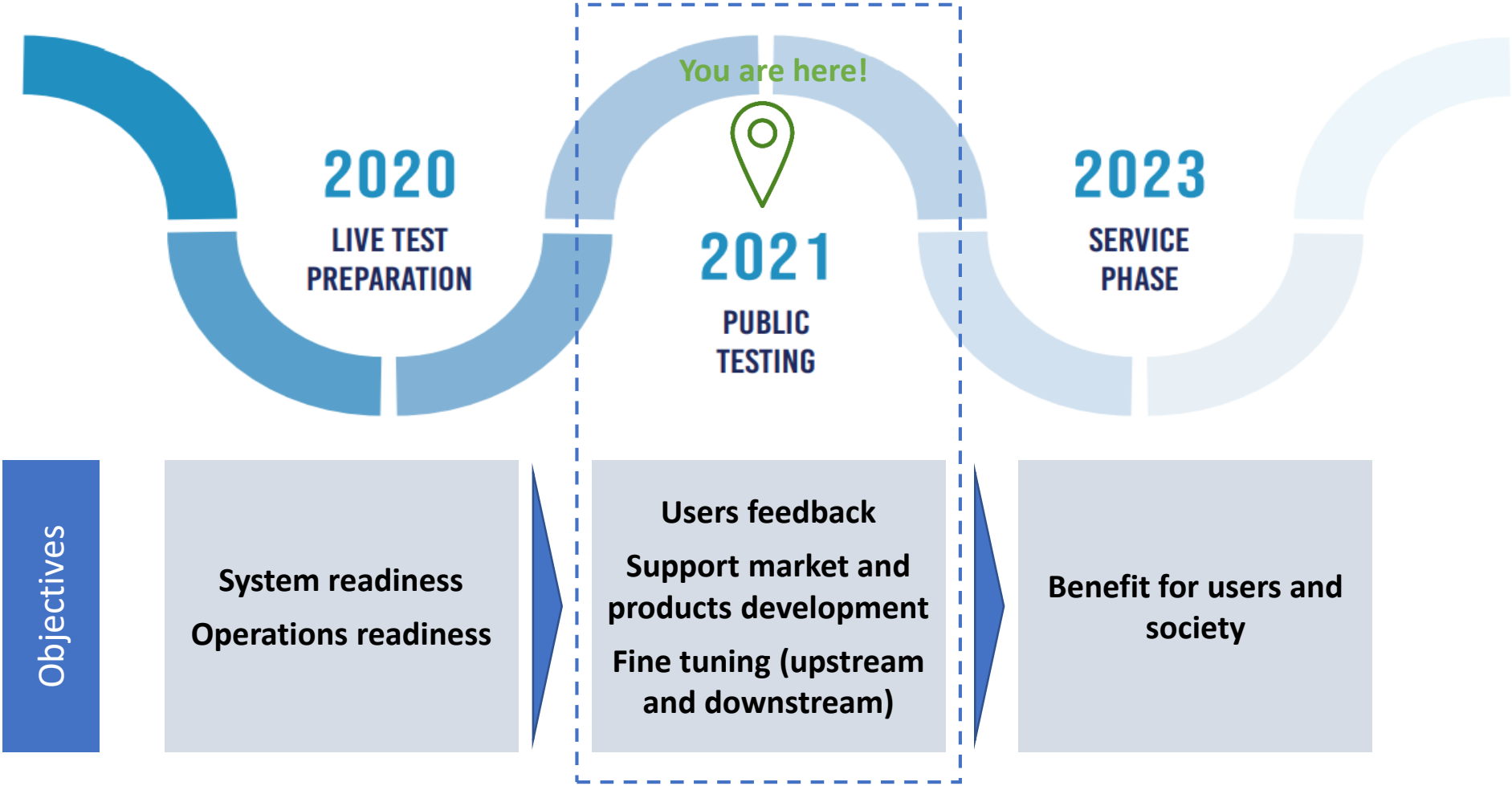
- 1
- 2
- 3
- 4

An OSNMA-enabled receiver can verify if the navigation message originates from a genuine Galileo satellite



- 1
- 2
- 3
- 4

The OSNMA Roadmap: the stepstones on the way to full service provision



Galileo OSNMA: Join the Public Observation Test phase and share your feedback!

1 Welcome & Introduction

- EUSPA & OSNMA team introduction
- Objective of the webinar



10 min

2 Galileo OSNMA

- GNSS Authentication & the Galileo solution: OSNMA
- OSNMA Service and Roadmap



20 min

3 Public Observation Phase

- How to benefit from it
- Guidelines for testing & feedback



55 min

4 Q&A



35 min

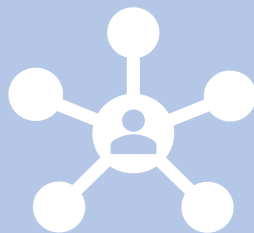


Objectives of the OSNMA test phase

OBJECTIVES



- Validation of critical OSNMA service elements (ICD).
- Complementary performance characterization



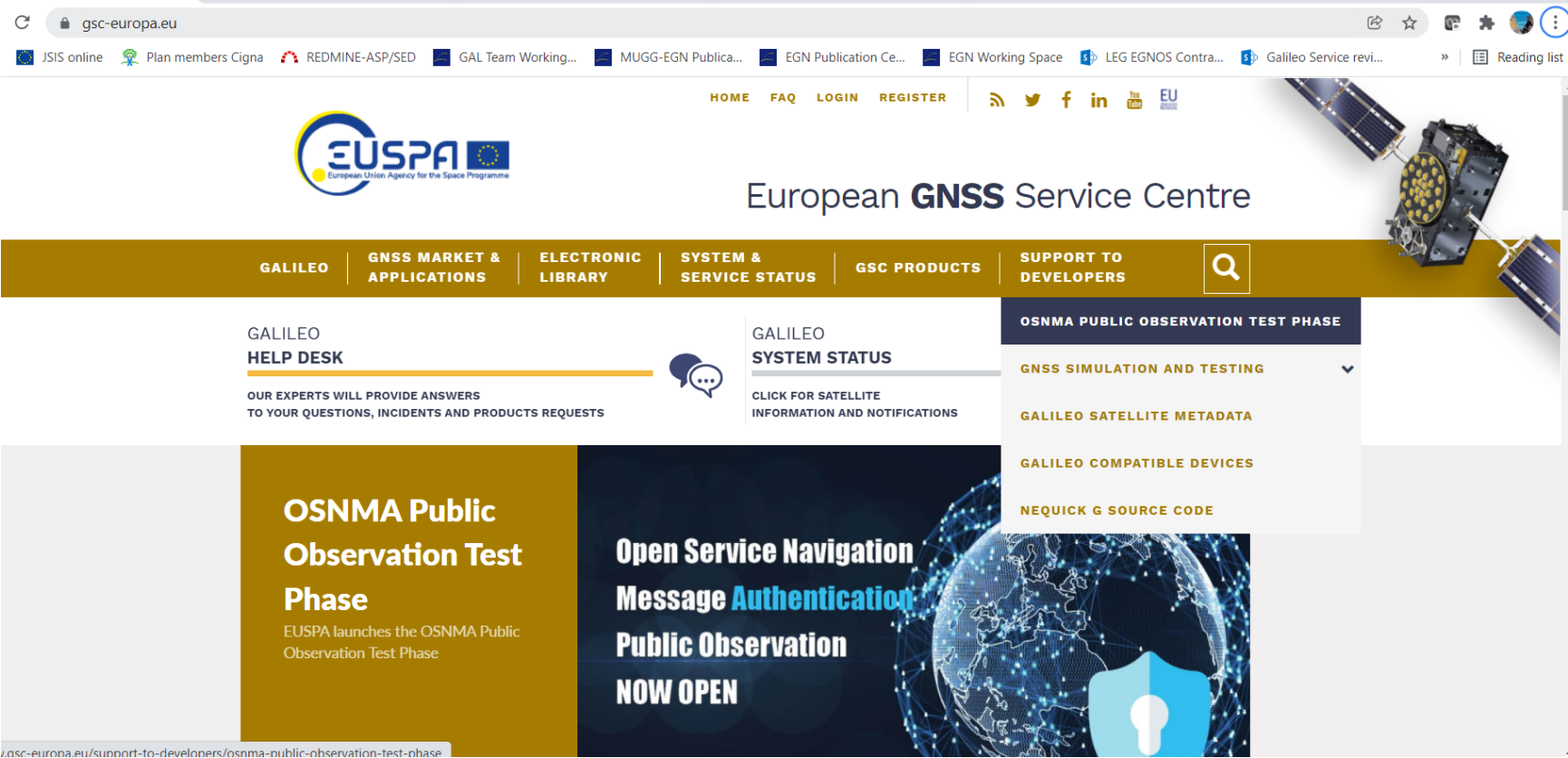
- Engage stakeholders
- Build a strong relationships with future OSNMA users
- Foster OSNMA adoption



- Gather lessons learned and recommendations towards OSNMA service provision

- 1
- 2
- 3
- 4

How to join the OSNMA test phase



The target users are receiver manufacturers, application developers, members of research institutions, or similar.



Extensive documentation provides details on OSNMA implementation, user interface and crypto material

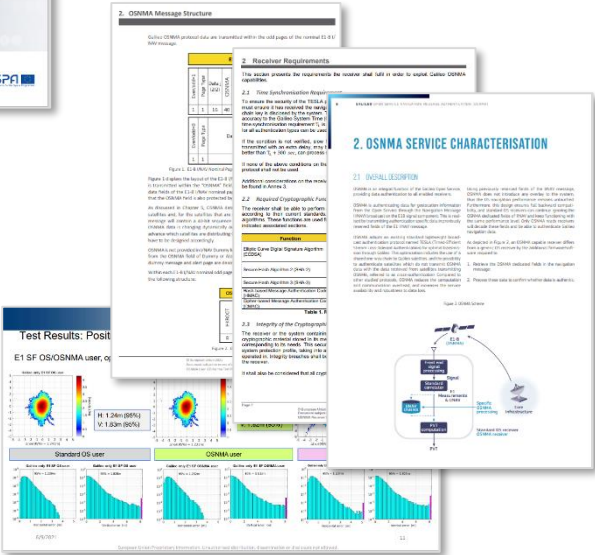
Available documents

- [Galileo OSNMA User Interface Control Document \(ICD\) for the Test Phase](#)
Specifies the interface between the Galileo Space Segment and the Galileo User Segment and crypto material retrieval
- [Galileo OSNMA Receiver Guidelines for the Test Phase](#)
Instructions for the user segment implementation of the OSNMA functionality, including requirements, interfaces, and steps to be followed
- [Technical presentation](#)
OSNMA Typical Performance and foreseen changes to the Galileo OSNMA User ICD for Service provision phase
- [OSNMA Info Note](#)
Description for the Service provision phase, including high-level details about the keys' authentication process, receiver compatibility, user interface and target markets

Multiple documents and presentations available

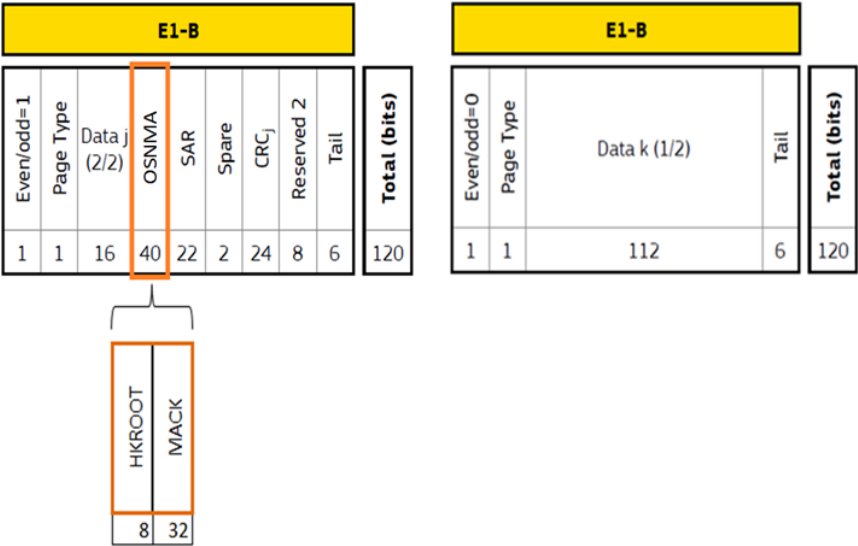


Detailed information on OSNMA capabilities



Recap of OSNMA Test SiS structure

- Use of spare bits of OS I/NAV E1-B
- HKROOT section:
 - OSNMA 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**



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



Recap of OSNMA Test SiS structure

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



- How user can trust a received TESLA key:
 - Received OSNMA SiS is not delayed. **Receiver to GST synchronization**
 - TESLA key is verified versus TESLA Root Key (K_0) or previously verified key (hashing process)

OSNMA Receiver Requirements

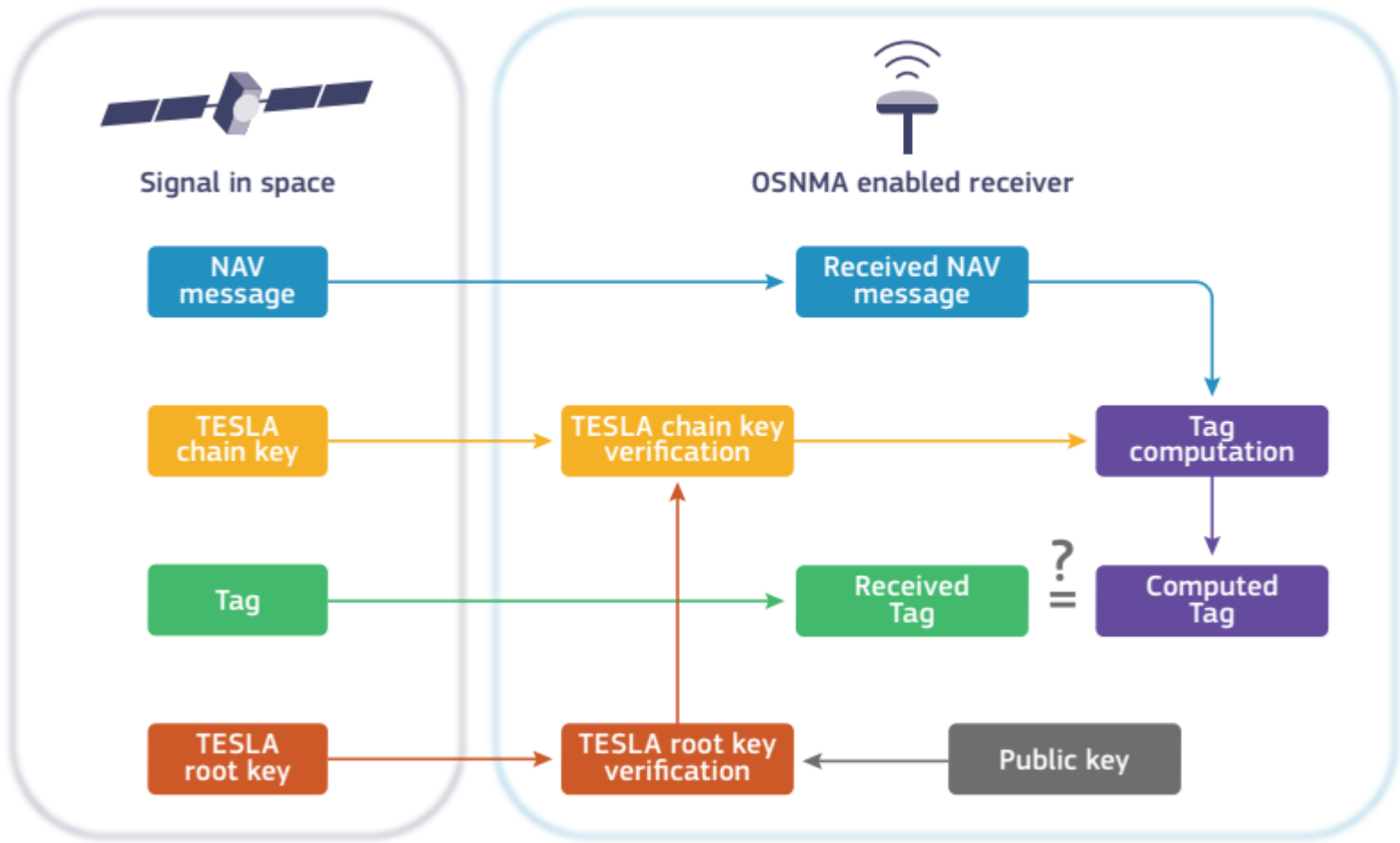
- Time synchronization requirement (**set and maintain GST Rx**)
- Cryptographic Functions (SHA-256, SHA3-256, HMAC-SHA-256, CMAC-AES, ECDSA P-256/SHA-256, ECDSA P-521/SHA-512)
- Integrity of the stored cryptographic material and functions
- Interfaces. OSNMA SiS (+GSC)

Receiver contribution is needed to achieve authentication. Please check OSNMA Receiver Guidelines for Test Phase



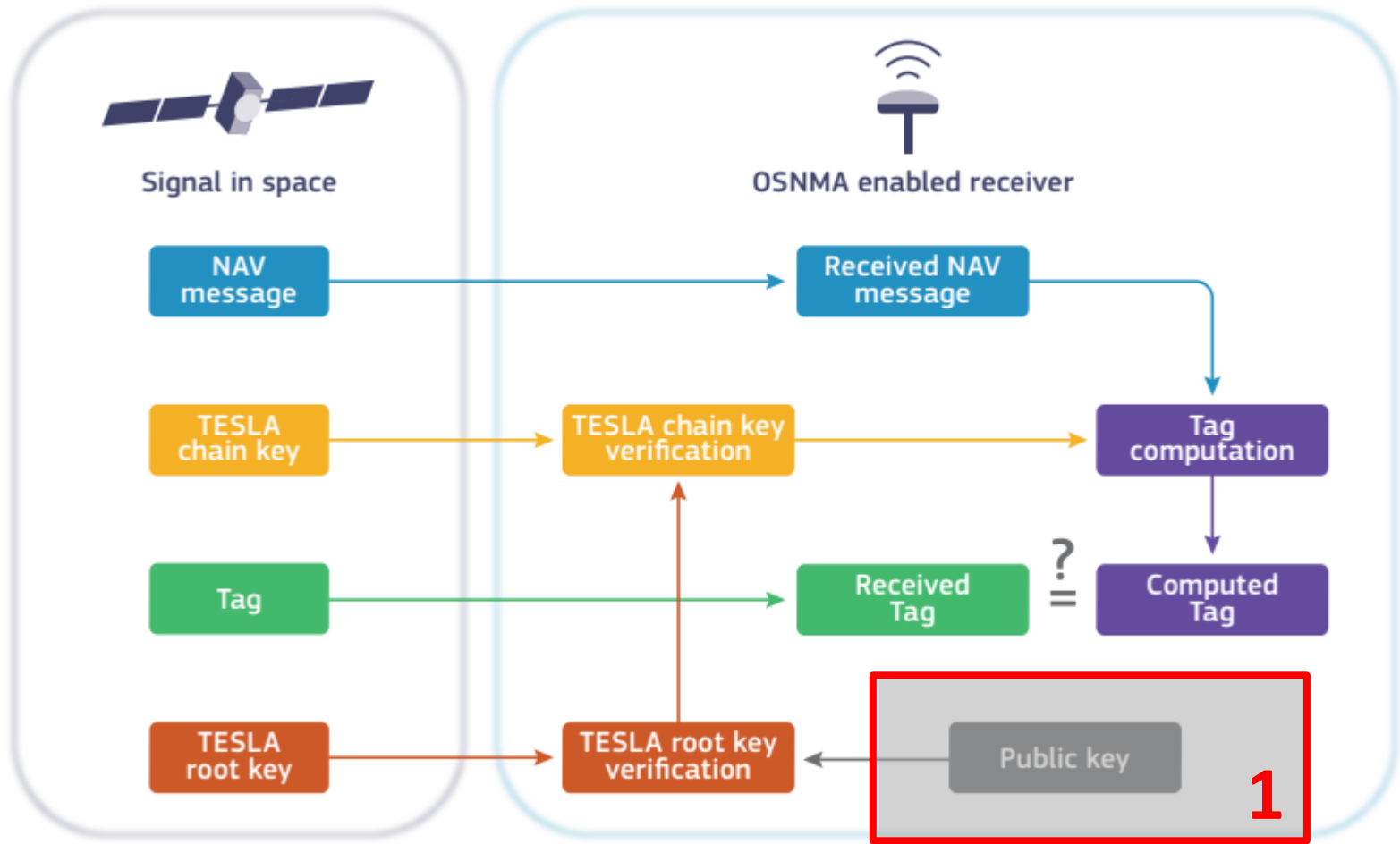
- 1
- 2
- 3
- 4

OSNMA Receiver Processing logic



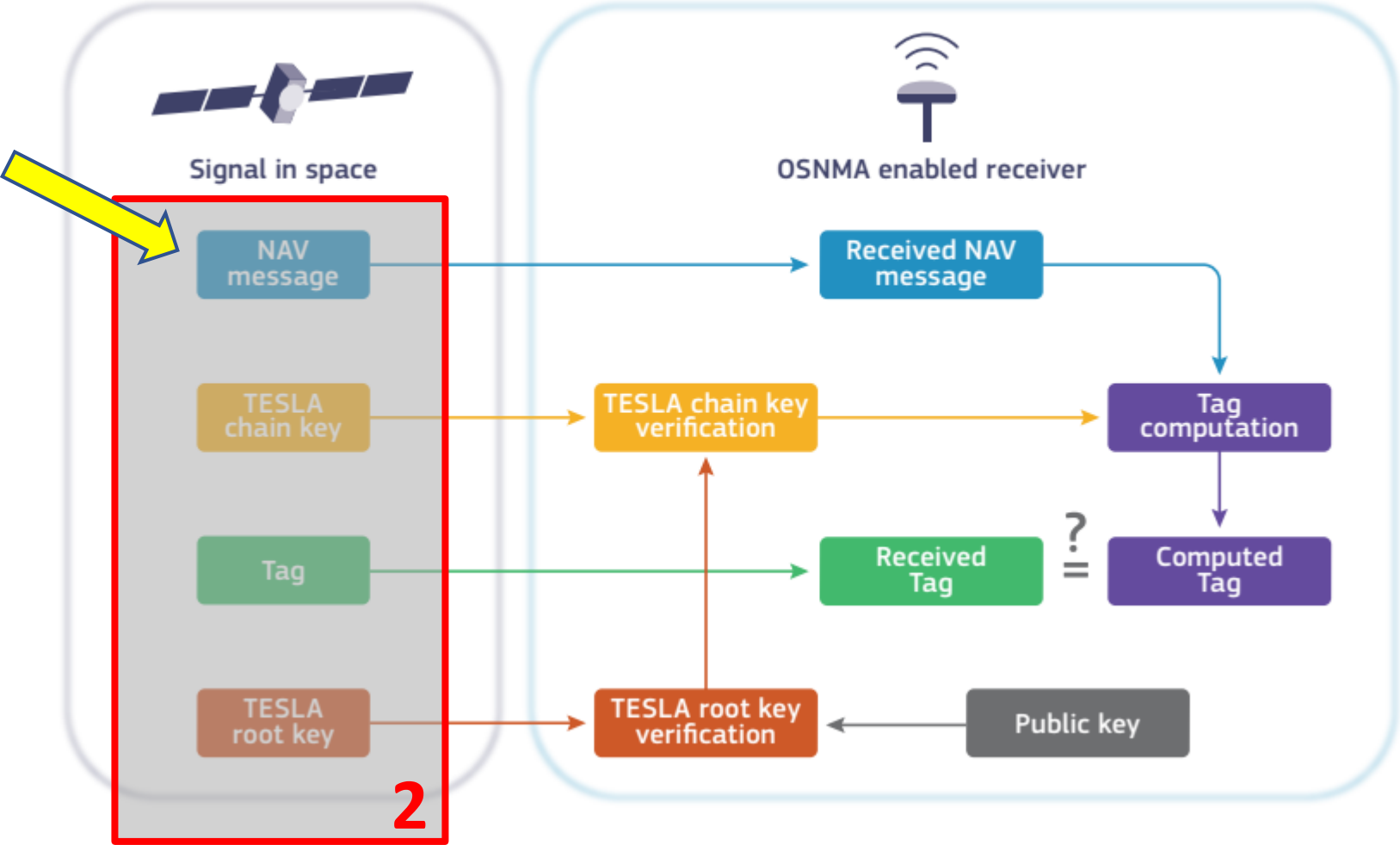
- 1
- 2
- 3
- 4

OSNMA Receiver Processing logic



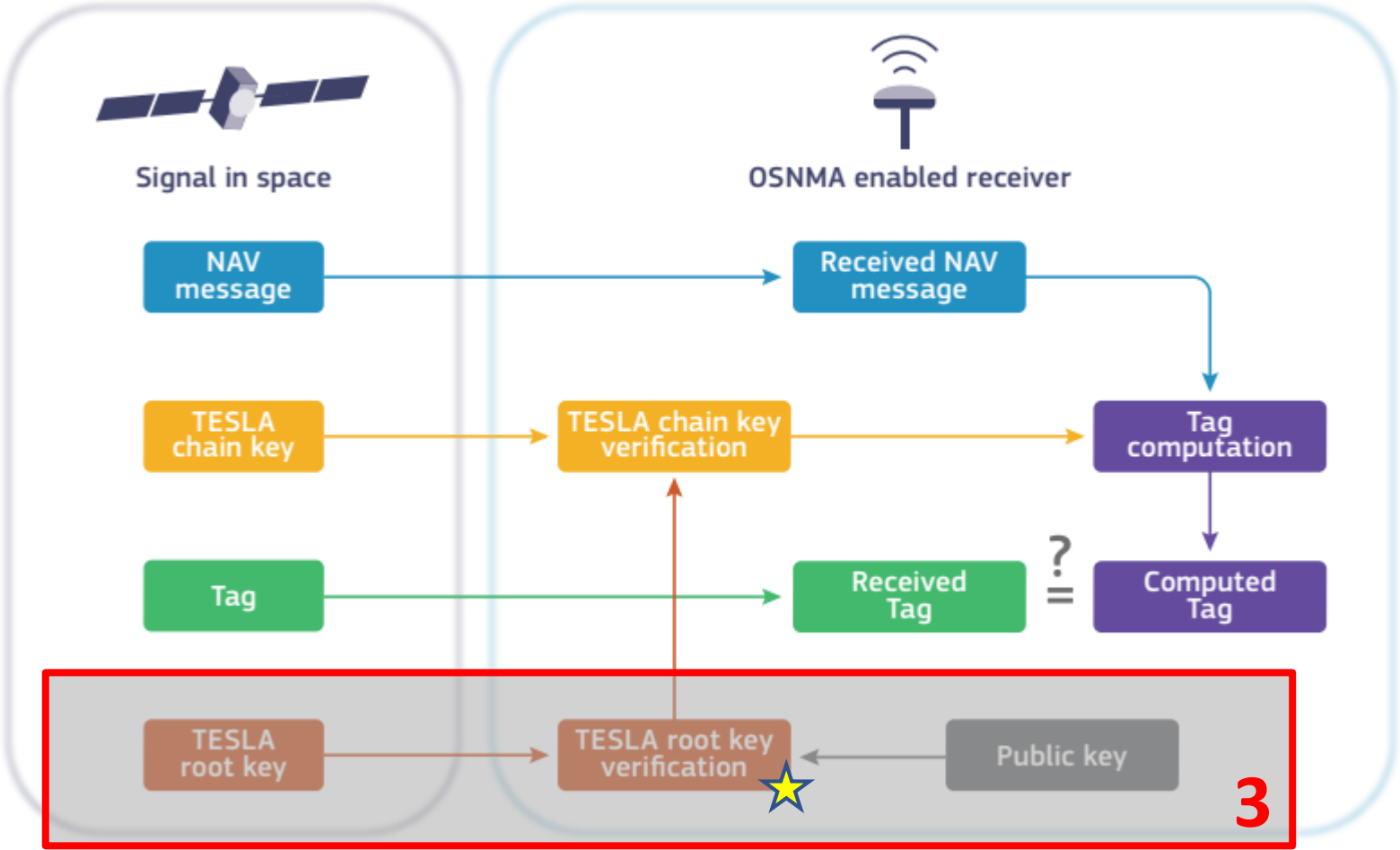
- 1
- 2
- 3
- 4

OSNMA Receiver Processing logic



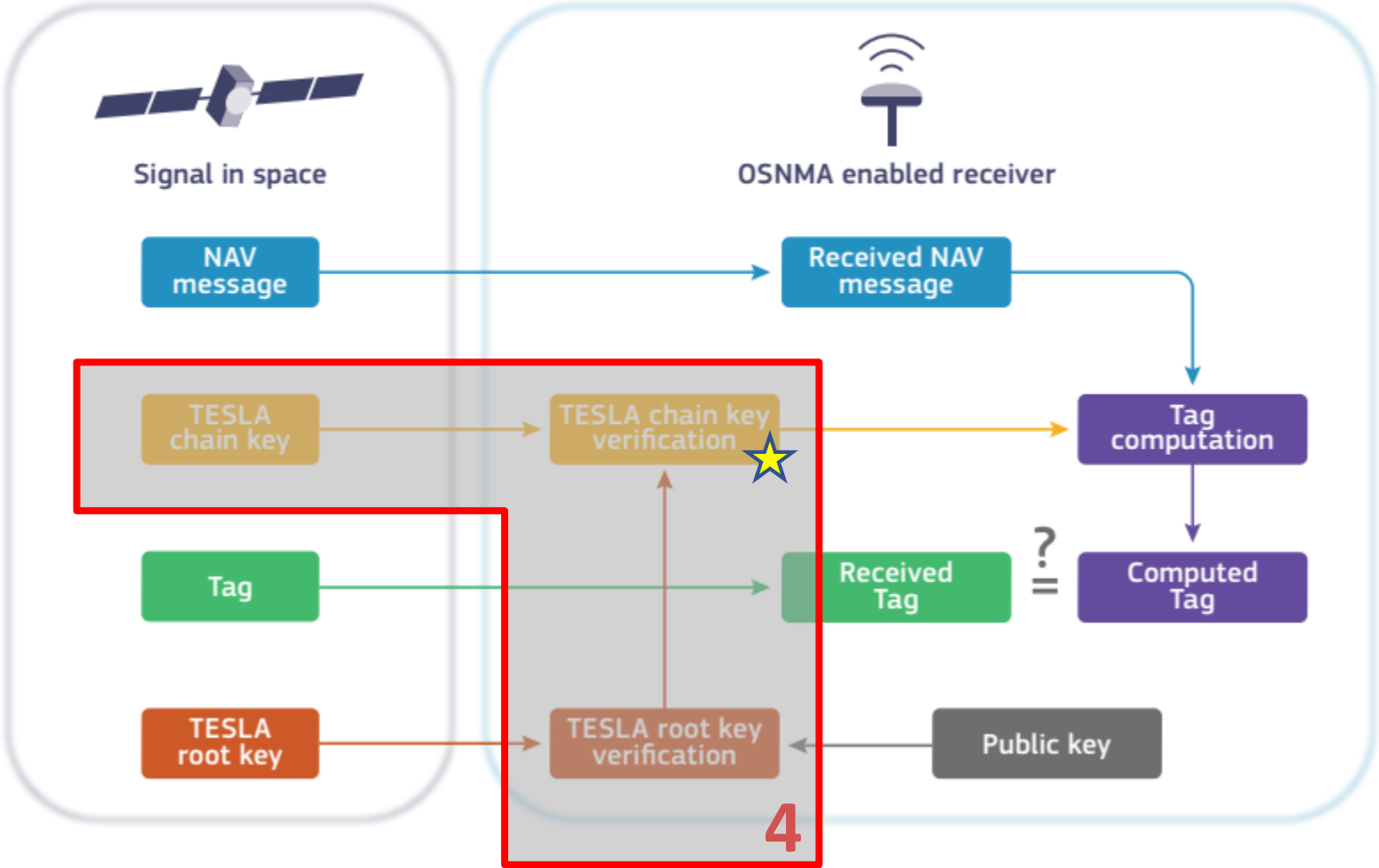
- 1
- 2
- 3
- 4

OSNMA Receiver Processing logic



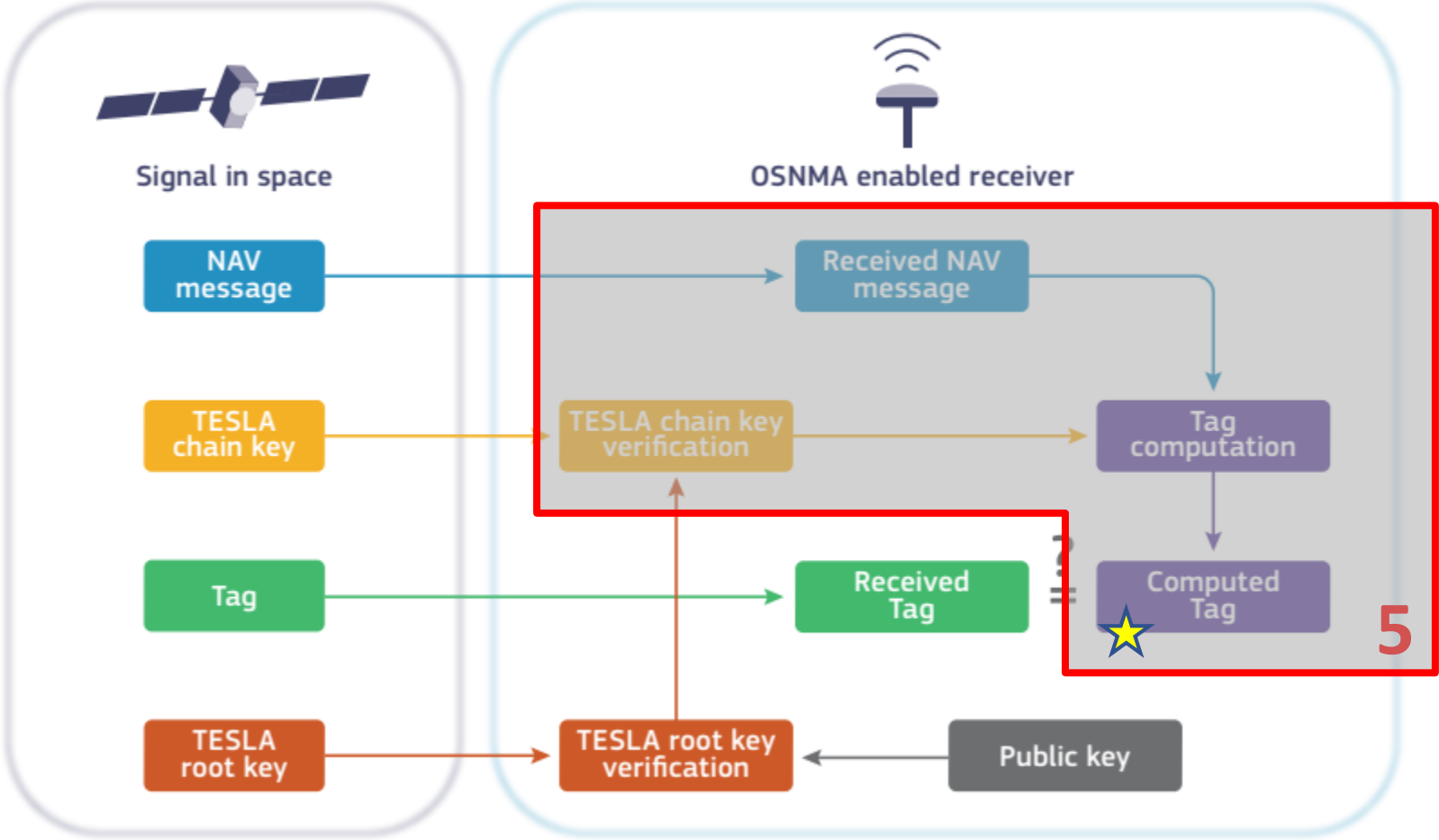
- 1
- 2
- 3
- 4

OSNMA Receiver Processing logic



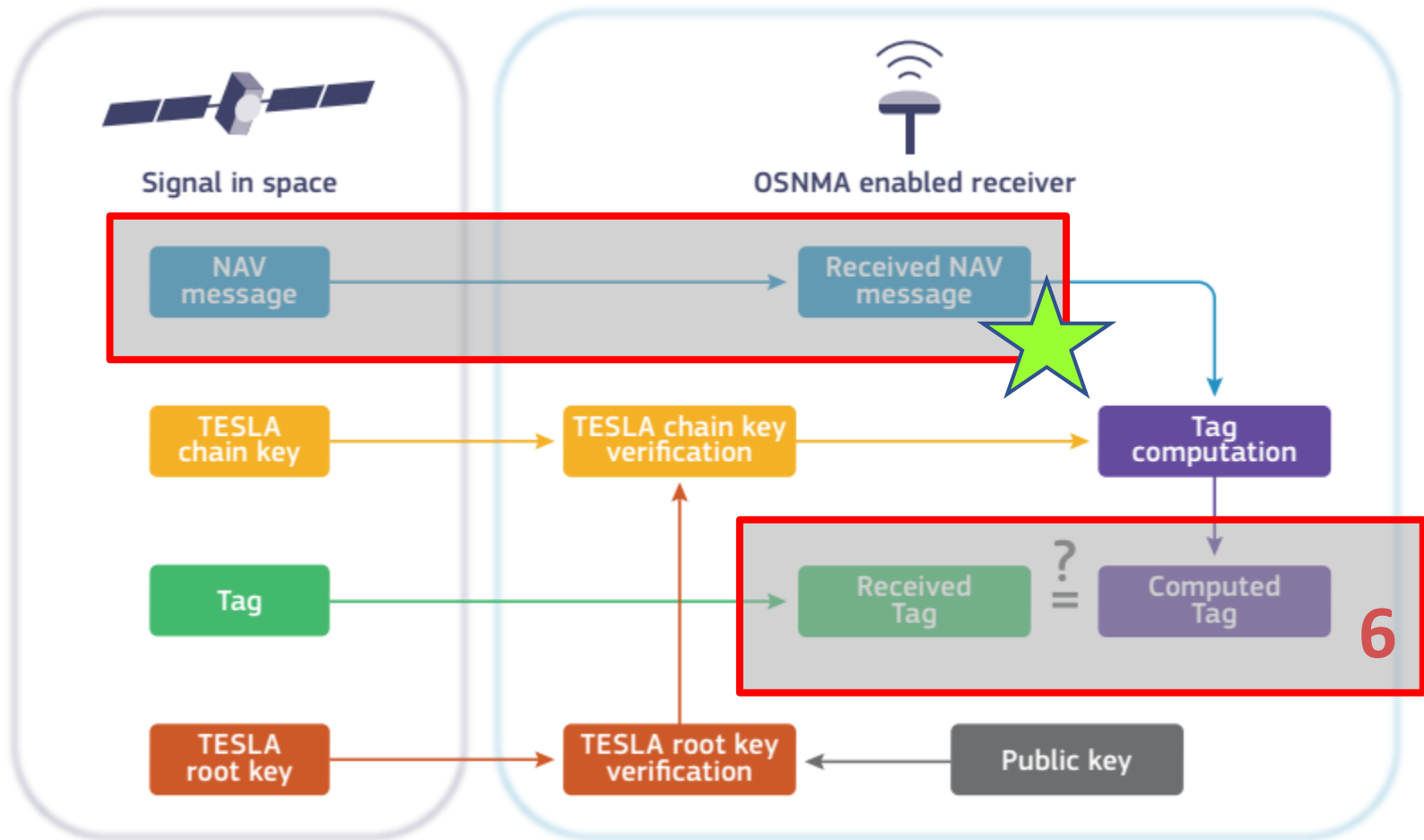
- 1
- 2
- 3
- 4

OSNMA Receiver Processing logic



- 1
- 2
- 3
- 4

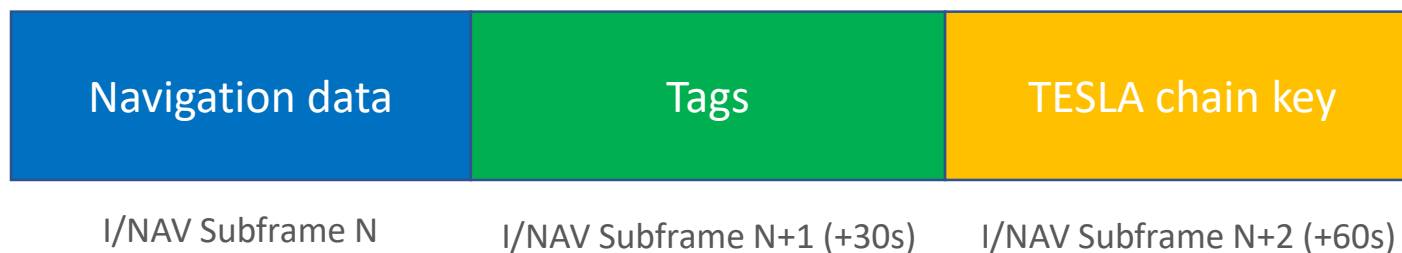
OSNMA Receiver Processing logic



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. Extended TESLA chain key delay for ADKD#12 Tags



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

OSNMA Typical performance

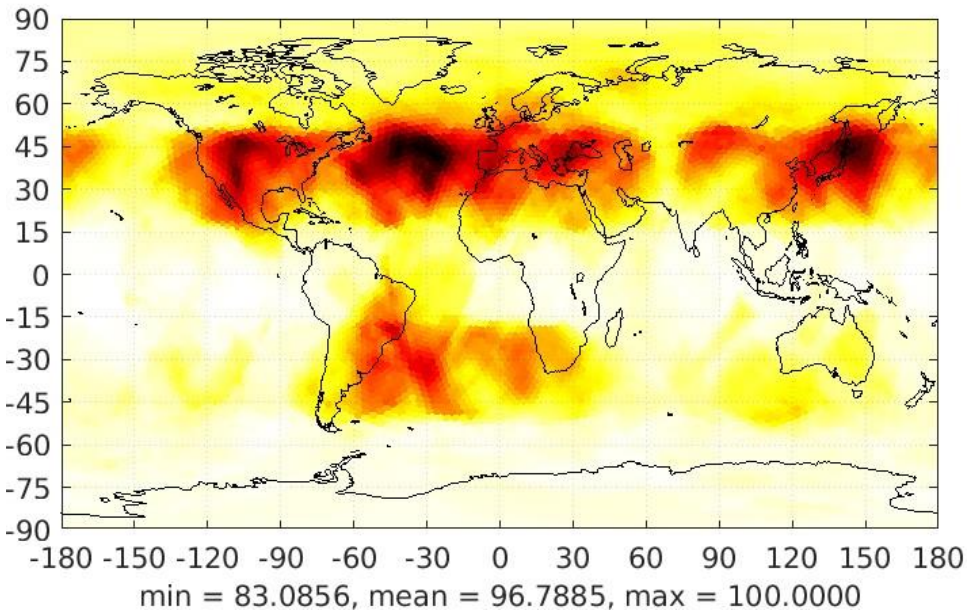
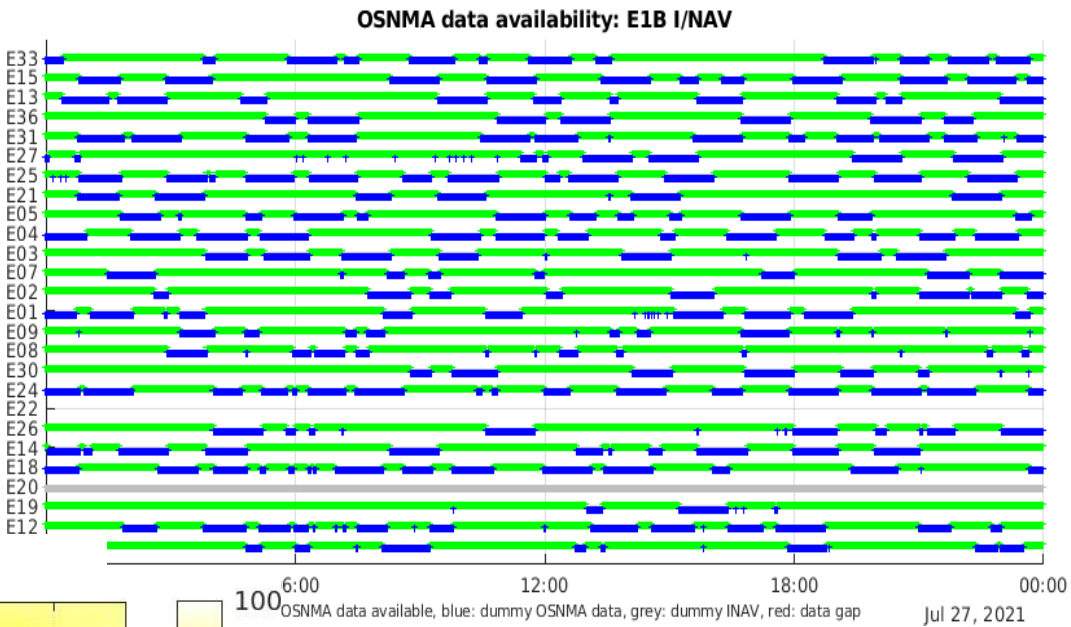
OSNMA SiS Parameter	Configuration
Digital signature	ECDSA P-256
Hash function for TESLA chain	SHA-256
Key size	128 bits
MAC function	HMAC-SHA-256
Tag size	40 bits (target security level 80 bits)
Number of Tags per subframe	6
Tag sequence (over 2 subframes)	[00S, 00E, 04S, 00E, 12S, 00E] ; [00S, 00E, 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 Typical performance

OSNMA data
broadcast from
Galileo satellites is
not continuous



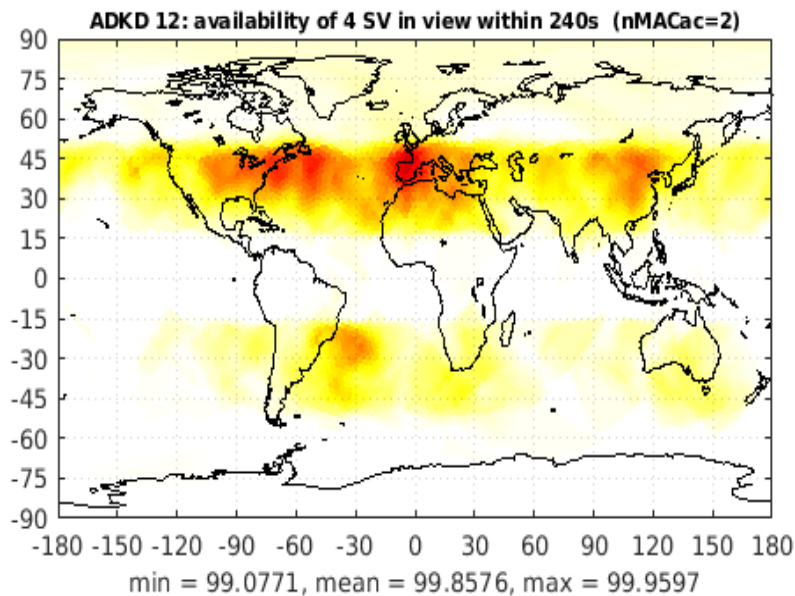
Green: OSNMA data available.
Blue: No OSNMA data



- 1
- 2
- 3
- 4

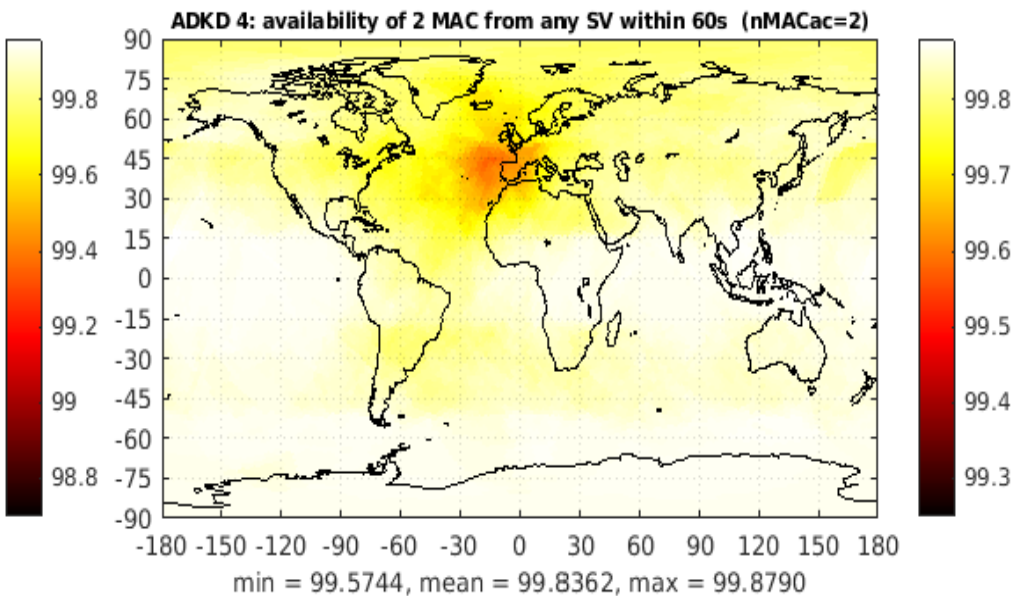
OSNMA Typical performance

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

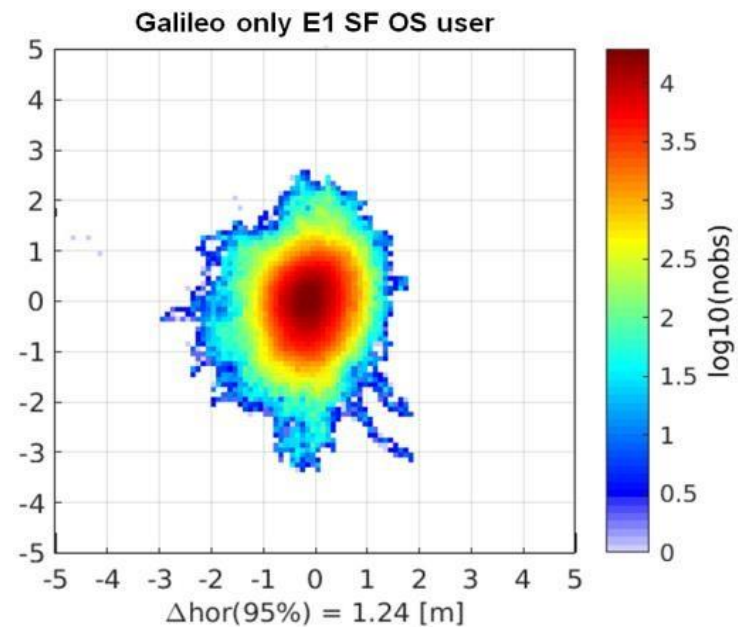


WUL: 99.57%
AUL: 99.84%
BUL: 99.88%



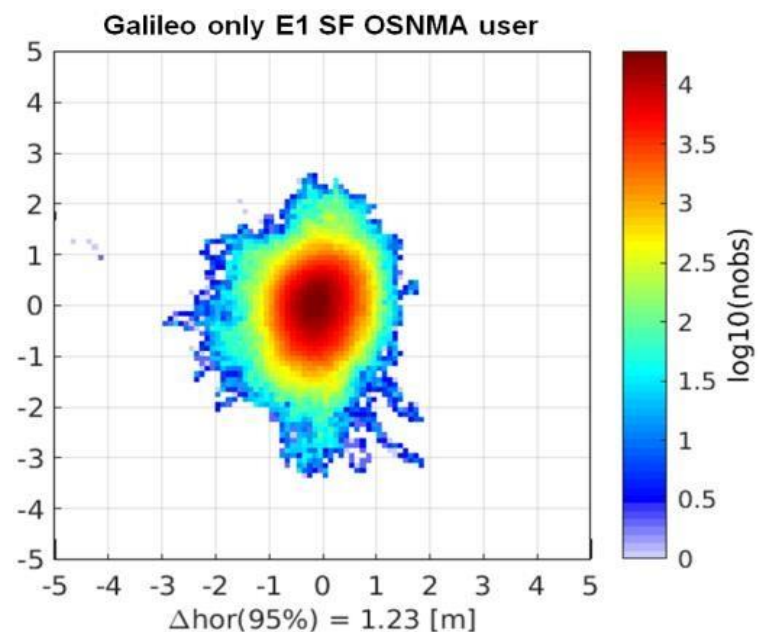
- 1
- 2
- 3
- 4

OSNMA Typical performance



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

Standard OS user



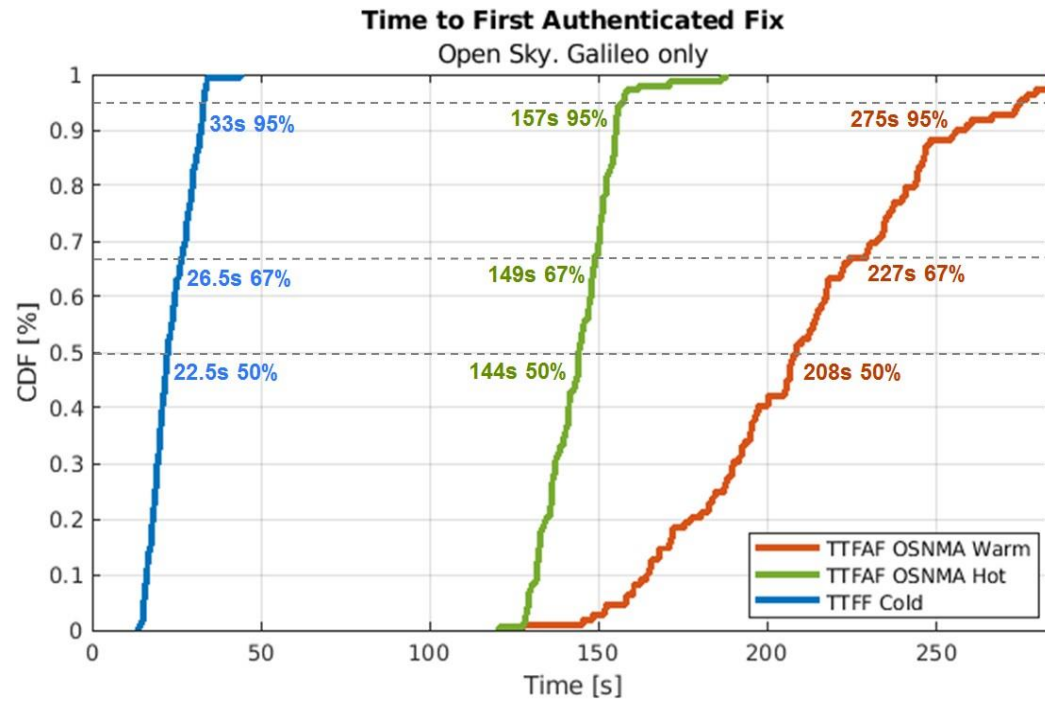
H: 1.23m (95%)
V: 1.82m (95%)

OSNMA user

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



OSNMA Typical 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




Different OSNMA testing configurations will be addressed separately

The testing phase will consist of:

Part 1: OSNMA test via Signal in the Space

- To be conducted by receiver manufacturers and application developers
- Representing their **target use cases/applications**
- **Free choice of scenarios** in terms of:
 - Movement pattern : Static, dynamic
 - Environment: urban, rural, asymmetric
- Performance assessed in terms of OSNMA **accuracy, availability and time to first authenticated fix (TTFAF)**



Share the outcome according to feedback characterization

Support provided by EUSPA in collaboration with JRC



Part 2: Corner test cases

- Specific capabilities devised by EUSPA, with the **support of EC Joint Research Centre**
- Testing of **scenarios not accessible via SiS** such as other NMA configurations, key revocation, etc



Participants are invited to share their experience with OSNMA in various forms profiting from exclusive benefits

Share your feedback!

Participants will directly benefit from:

- Inclusion in a **dedicated “OSNMA tested”** area to be created in the EUSPA managed website:
<https://www.usegalileo.eu/>
- **Visibility** of the tested OSNMA-enabled solution on the **two foreseen OSNMA workshops** including individual invitation to share user experience
- Support for a **correct OSNMA algorithm implementation**
- Provide your results by sending it directly to EUSPA Market Development team:
MARKET@euspa.europa.eu

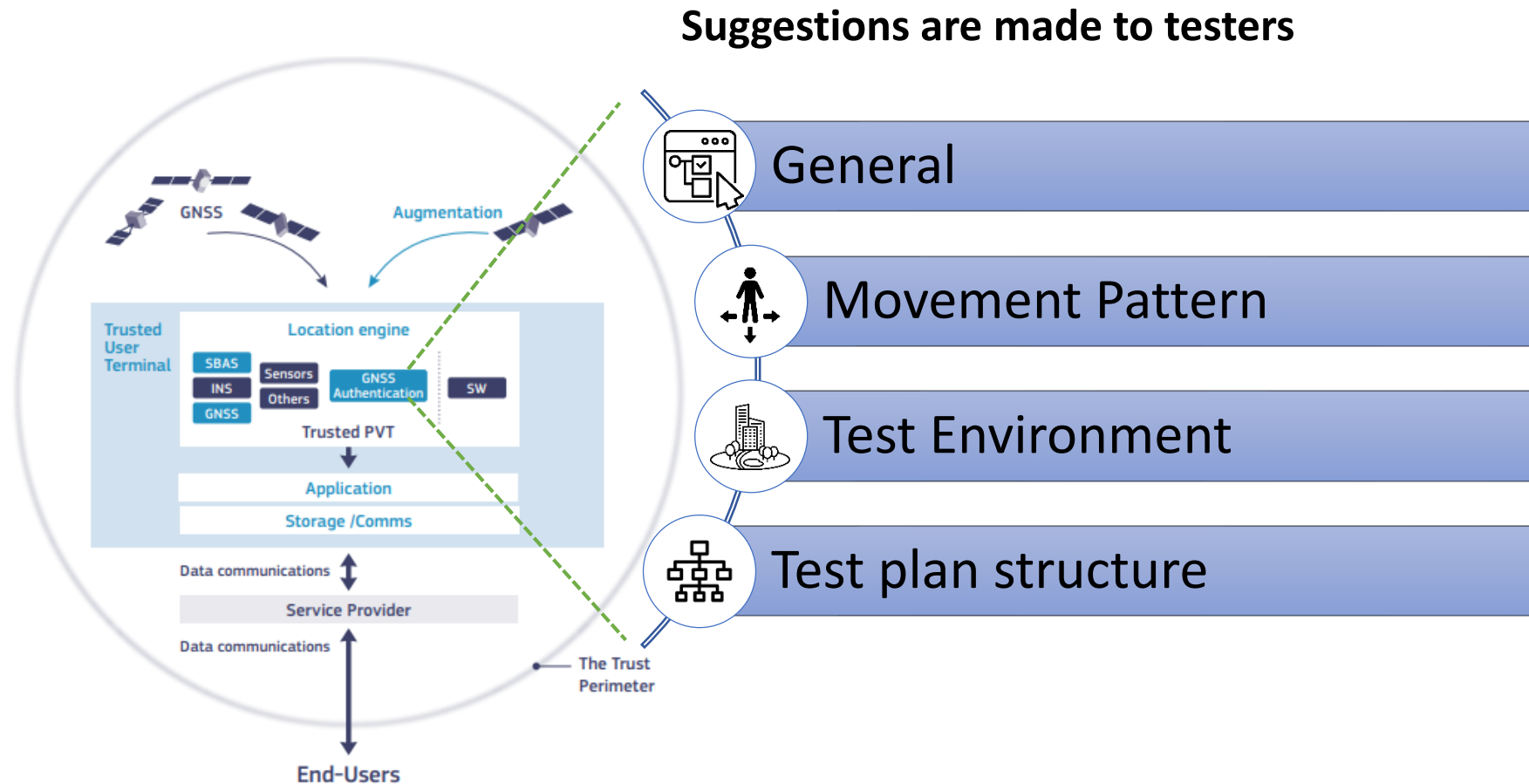


Part 1: OSNMA test via Signal in the Space



1
2
3
4

The OSNMA SiS Test Phase will be conducted by participants representing their target applications



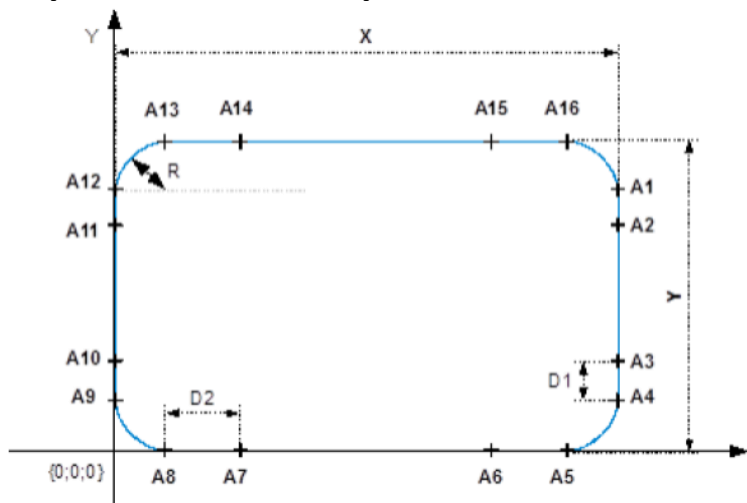
Source: EUSPA- GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OSNMA)- 2021



Dedicated test scenarios (field tests)

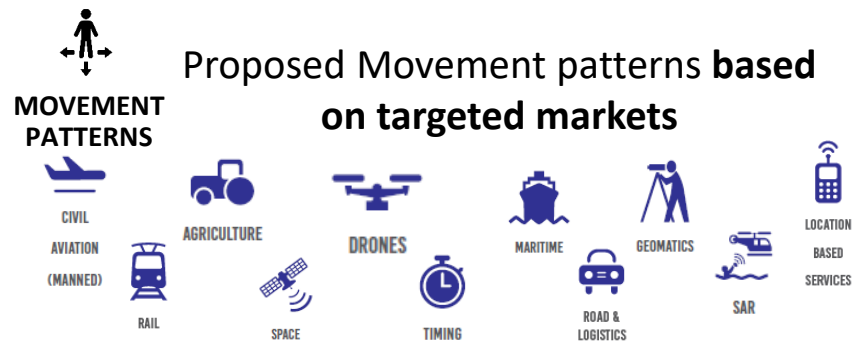
- Inspired by ISO 17025 requirements
- Based on the available OSNMA documents

Example of movement patterns



Source: ETSI- ETSI TS 103 246-3 V1.3.1 (2020-10)

Proposed Movement patterns based on targeted markets



Static

- Cadastral Surveying
- GIS
-

Dynamic

- Agriculture- Automatic Steering
- Automotive- Smart digital tachograph
- UAS- Navigation and traffic management for UAVS
-

- Any specified land point

- Pedestrian
- Automotive
- UAS

Other dynamics can be chosen

Tests can be conducted in any environment

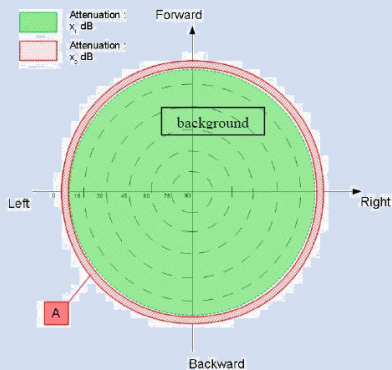


TEST
ENVIRONMENT

Three representative scenarios, depending on target applications (examples only):

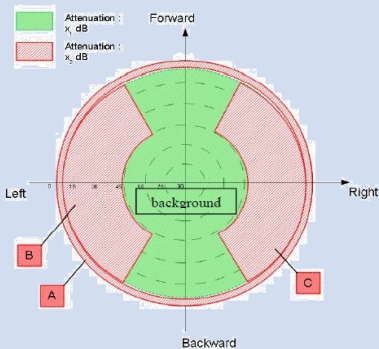
Rural

Typical open view to sky
without disruption



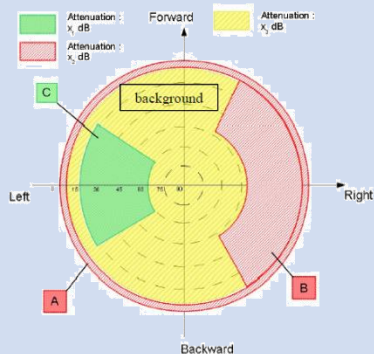
Urban

Obstructions on both sides
(buildings or other objects)

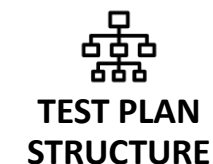


Asymmetric

All further environments



General KPIs are suggested as possibilities for the performance assessment of their implementations



Field tests-General KPIs- Part 1

OSNMA accuracy

- OSNMA Position accuracy

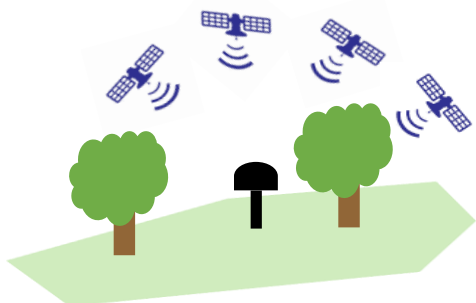
Characterized as the difference between the position from a selected reference and the position output using only data-authenticated satellites provided by the OSNMA receiver at a given time.

The OSNMA position accuracy may be used for **static and mobile user scenarios**.

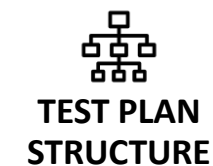
- OSNMA Velocity accuracy

Characterized as the difference between the velocity from a selected reference and the velocity output using only data-authenticated satellites provided by the OSNMA receiver at a given time.

Velocity accuracy is **only in the scope of mobile user** scenarios.



General KPIs are suggested as possibilities for the performance assessment of their implementations



Field tests-General KPIs- Part 2

OSNMA availability

Duration in Warm and Hot start scenario till

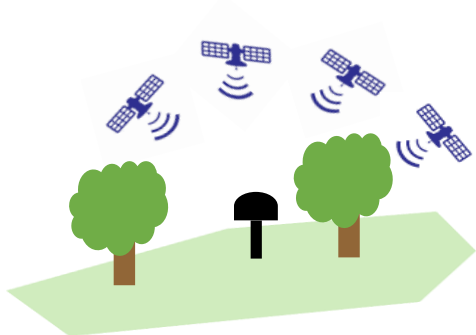
- First Availability of authenticated output
- Availability of authentication of all SV in view

Warm start

The receiver possesses the public key and can retrieve the DSM-KROOT to verify the tesla root key and proceed with the mack verifications

Hot start

The receiver already possesses a verified tesla root key, so its does not need to retrieve and verify again the DSM-KROOT and can start processing the MACK section



General KPIs are suggested as possibilities for the performance assessment of their implementations



Field tests-General KPIs-Part 3

OSNMA availability

Duration in Warm and Hot start scenario till

- First Availability of authenticated output

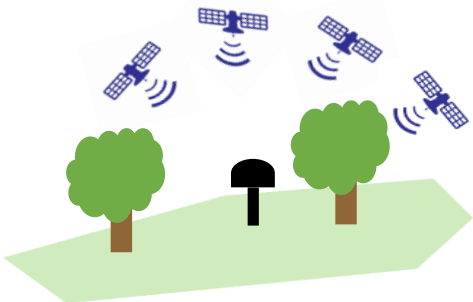
Time to first authenticated fix

Characterized by the time required for OSNMA receiver to acquire the satellite signals, navigation data, to authenticate navigation message, calculate and to output the first position solution using only the authenticated navigation parameters.

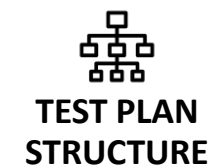
- Availability of authentication of all SV in view

OSNMA navigation solution availability

Characterized as the percentage of time that a navigation solution using only data-authenticated satellites is obtained in comparison to the complete time with available position output.

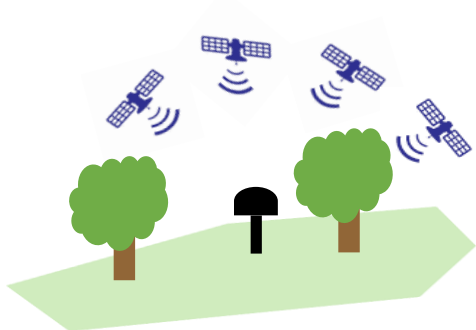


General KPIs are suggested as possibilities for the performance assessment of their implementations



Field tests-General KPIs- Part 4

- **OSNMA availability**
 - Continuity of OSNMA supported output with a defined output rate



Time between authentications

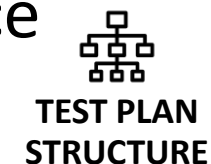
At satellite level

characterized as time between consecutive authentications for a satellite that is used in the navigation solution.

At navigation solution level:

- characterized as time between computation of navigation solutions with renewed authenticated navigation data for at least 4 satellites used in the navigation solution.
- Same metrics can be reported as well for the computation of navigation solutions with renewed authenticated navigation data for all the satellites used in the navigation solution.

Participants are encouraged to share the performance statistics of their implementations



Field tests metrics

- **OSNMA accuracy:**
 - 50th, 75th, 95th percentile of calculated **position / speed** error
- **Time to first authenticated fix:**
 - 50th, 75th, 95th percentile for warm and hot start condition
- **OSNMA availability:**
 - Navigation solution availability value
 - 50th, 75th, 95th percentile of the calculated distribution of the time between authentications

Proposed reference in field

- **Static**
 - Timing reference: time output of the receiver via NMEA or an independent clock
 - Position reference: premeasured point
- **Dynamic**
 - Timing reference and position: Independent GNSS based PVT-system

Testers are encouraged to provide the following data:

- Used receiver (low grade (e.g. smartphone), standard (e.g. automotive), high grade (e.g. geodetic))
- Specification of used environment
- Specification of used dynamics
- Recorded trajectory data, max. Yaw-rate, maximum horizontal speed,
- Proposed: Receiver output (NMEA v4.x) of receiver under test and for reference and separate document regarding the comments

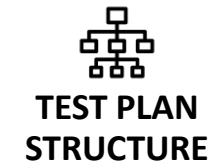
1

2

3

4

Qualitative and quantitative feedback on various OSNMA aspects are welcome



Participants' feedback on tests as questions and comments

- Covering feedback from the participants regarding the content and outcome of the tests, e.g.:

The test covered the expectations



☐ Full coverage

☐ No coverage

☐ Comments

The outcome of the test



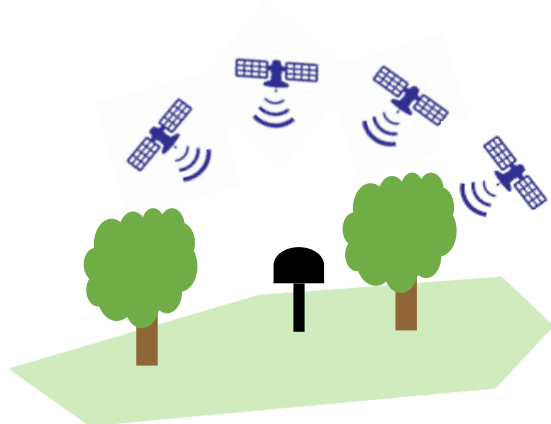
☐ Exceeded the expectations

☐ Met the expectations

☐ Didn't meet the expectations

☐ Comments

....



General feedback on documentation

- Covering feedback from the participants regarding the content of the available documents, e.g.:

Clarity of the document:

Any specific information missing?



☐ No

☐ Yes

☐ Comments

Any unclear section/information?



☐ No

☐ Yes

☐ Comments

Which difficulties/issues were identified?



☐ Comments

How grave were/are these difficulties/issues?



☐ Comments

Improvements/modifications:

Improvements/modifications needed?



☐ No

☐ Yes, needed

☐ Yes, suggested

In which area modifications are proposed? Which? Why?



☐ (Multiselect)

☐ Comments



Part 2: OSNMA corner test cases



OSNMA Functional Testing

In addition to the SiS, **test vectors** will be made available to support OSNMA functional testing. In order to use these test vectors, **the receiver will have to pass the time synchronisation check**, despite the test vector being set in the past.



A mean to set the internal time (GST realization) used by the receiver within the OSNMA protocol shall be in place for the testing.

- No test vector can be provided to verify the *time synchronisation check*. Its correct implementation shall be verified through the offsetting the receiver internal time by a value larger than the requirement.
- The *time synchronisation mechanism* (used to align the receiver internal time with GST) can be verified through the recording and delayed replay of the SiS (support from JRC available).

OSNMA Functional Testing

The test vectors provided will cover:

- The receiver capabilities to support different OSNMA configurations:
 - Tag length
 - Key length
 - Cryptographic functions
- The public key and TESLA chain management, as such operations are not part of the public testing phase
 - Public key renewal
 - Public key revocation
 - TESLA chain renewal
 - OSNMA Alert Message



OSNMA Functional Testing

Additional scenarios being considered for possible further support:

- TESLA chain revocation
- Inclusion of flexible tags (FLX)
- NMA status set to Operational
- Inclusion of additional cryptographic functions (CMAC, SHA3-256)



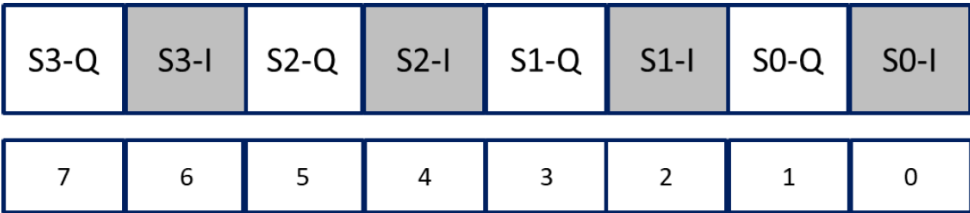
OSNMA Functional Testing

These test vectors may be provided in different format:

- I/NAV data stream (specific format might change)

```
01 432000 02140082D65809F49F4A0000000000800040000000002AAAAA78943B0800041401000000007
02 432000 02140082D65809F49F4A0000000000800040000000002AAAAA78943B0800041402000000007
03 432000 02140082D65809F49F4A0000000000800040000000002AAAAA78943B08C0041403000000007
04 432000 02140082D65809F49F4A0000000000800040000000002AAAAA78943B08C0041404000000007
05 432000 02140082D65809F49F4A0000000000800040000000002AAAAA78943B0940041405000000007
06 432000 02140082D65809F49F4A0000000000800040000000002AAAAA78943B0940041406000000007
```

- Sampled signals (specific format might change)
 - IF: 0
 - Sampling frequency: 50 Msps
 - Quantisation: 1 bit
 - Format: interleaved I/Q format



OSNMA Functional Testing

For each test scenario, a description will be provided that contains:

- the configuration used, to be used to ensure the correct parsing of the data retrieved.

Parameters	Values
Tag length	40 bits
Key length	128 bits
Nb. of tags per MACK message	6
Digital Signature	ECDSA P-256
Nb. of blocks in DSM-KROOT	8
MAC function	HMAC-SHA-256
MACLT ID	33
ADKD sequence	[00S, 00E, 04S, 00E, 12S, 00E] [00S, 00E, 00E, 12S, 00E, 12E]

- the time stamps of the different events/steps, to ensure the correct implementation of the protocol logic during renewal and revocation events.



Join the Public Observation Test Phase and share your feedback!

- **Register to the OSNMA Public Observation Test Phase** and profit from a series of exclusive features and benefits;
- **Take the chance** to participate on the testing phase of a long-awaited service that will **differentiate Galileo from any other GNSS system**.
- **Test a one-of-a-kind service** with support on the correct implementation and many opportunities for exchange and discussions;
- **Conduct the tests** according to the conditions and environment that are **most suitable to your applications**;
- If you wish so, be ready **to discuss your experience** on exclusive workshops and profit from the visibility of your OSNMA-enabled solution on a dedicated section on the [Use Galileo website](#).



Galileo OSNMA: Join the Public Observation Test phase and share your feedback!

1 Welcome & Introduction

- EUSPA & OSNMA team introduction
- Objective of the webinar



10 min

2 Galileo OSNMA

- GNSS Authentication & the Galileo solution: OSNMA
- OSNMA Service and Roadmap



20 min

3 Public Observation Phase

- How to benefit from it
- Guidelines for testing & feedback



55 min

4 Q&A



35 min

