Galileo Open Service Navigation Message Authentication

Sophie Damy, Matteo Paonni

European Commission, JRC

62nd meeting of the CGSIC

International Information Subcommittee

September 19-20

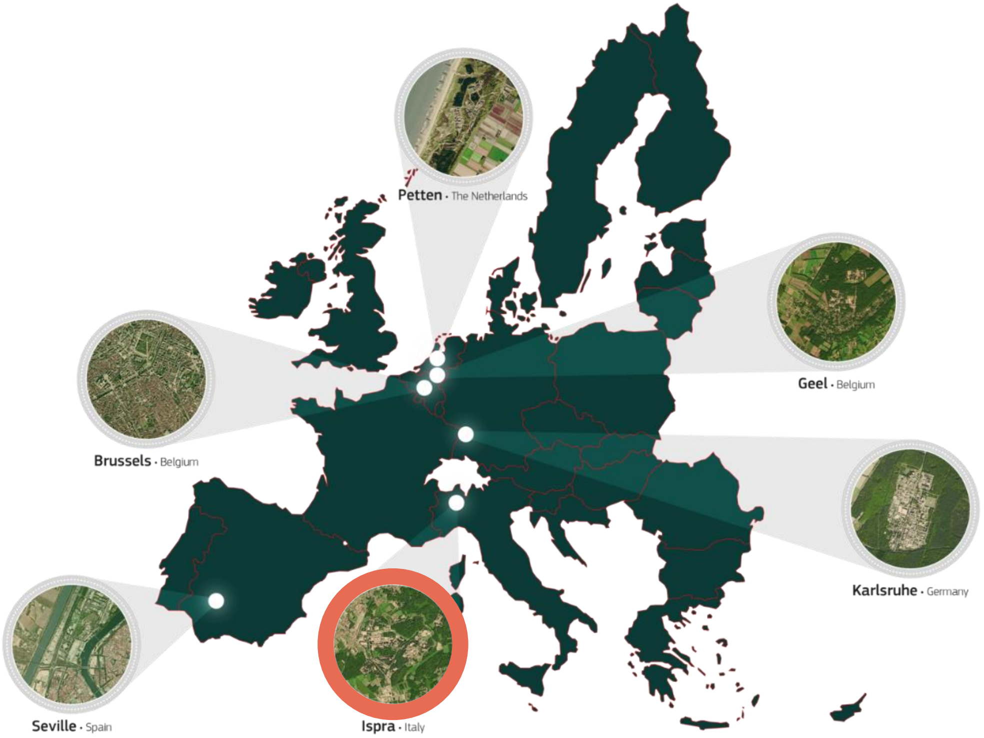
Denver, CO

What is the JRC? What it does for Galileo?

The **Joint Research Centre** (JRC) is the Directorate-General of the **European Commission** in charge of carrying out research to provide independent scientific advice and support to the European Union policy.

JRC developed dedicated capacities (state-of-the-art **laboratories**) for the EU GNSS Programmes, with a specific focus on **user segment** testing and validation.

Scientific and technical support on many areas, including mission and service definition and exploitation, signal design and performance assessment.



European Commission

Presentation Outline

- OSNMA Overview
- OSNMA Principle
- Examples of Application
- Roadmap to service
- Testing Activity within JRC Laboratories
- Authentication at ION GNSS+ 2022

OSNMA overview

- **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
- **No need for dedicated hardware:** capability enabled by means of a GNSS receiver/user terminal enabled with a specific firmware
- Minimal impact on receivers - **computational burden commensurate with low-cost receiver** capabilities
- Added-value brought to a variety of applications

A first degree of protection against data spoofing of the Galileo OS I/NAV

Enhanced confidence at user level

Galileo differentiator with a **more robust and trustworthy** GNSS solution

OSNMA principle (1/3)

- GNSS authentication is achieved by incorporating specific features that **cannot be predicted** or **forged** by malicious actors in the broadcast signals. A receiver enabled for authentication can interpret these features in order to distinguish genuine signals from imitations.

- OSNMA offers authentication at **data level**, enabling the authenticate the broadcast navigation message. It provides receivers with the **assurance that the received Galileo navigation message is coming from the system itself and has not been modified.**

- OSNMA increases the likelihood of detecting spoofing attacks at the data level, contributing to the security of the solution. It should be noted that a PVT computed using non-verified ranging information **cannot be considered authenticated**.

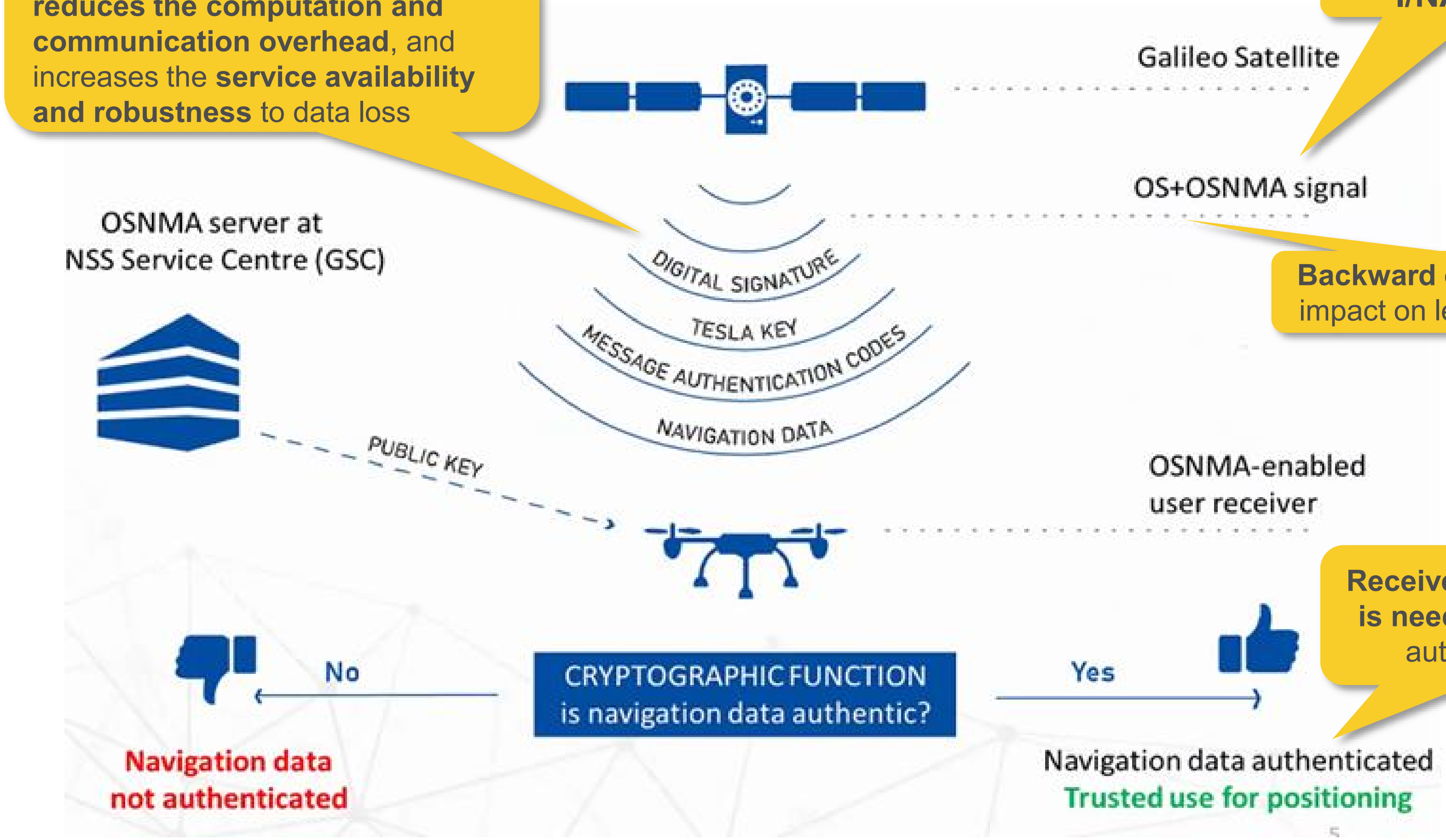
OSNMA principle (2/3)

Use of **TESLA protocol**: compared to other studied protocols, OSNMA **reduces the computation and communication overhead**, and increases the **service availability and robustness** to data loss

Use of **spare bits of the I/NAV message**

Backward compatible: no impact on legacy receivers

Receiver contribution is needed to achieve authentication


Galileo Satellite
OS+OSNMA signal
OSNMA server at NSS 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

OSNMA principle (3/3)

- Based on Time-Efficient Stream Loss-Tolerant Authentication (**TESLA**) protocol, which uses symmetric cryptographic functions to achieve asymmetric properties through **the delayed release of the key**. The keys are part of one-way chain, and missing keys can be recomputed using later values.

- To ensure that the key being retrieved from the SIS is not known to anyone, the receiver is required to be **loosely synchronised to the Galileo System Time** (GST). The protocol support synchronisation within 30 sec and also within 5 min.

- The system also has the possibility to authenticate satellites which do not transmit OSNMA data with the data retrieved from satellites transmitting OSNMA, referred to as **cross-authentication**.

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

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

GIANO

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

ASGARD

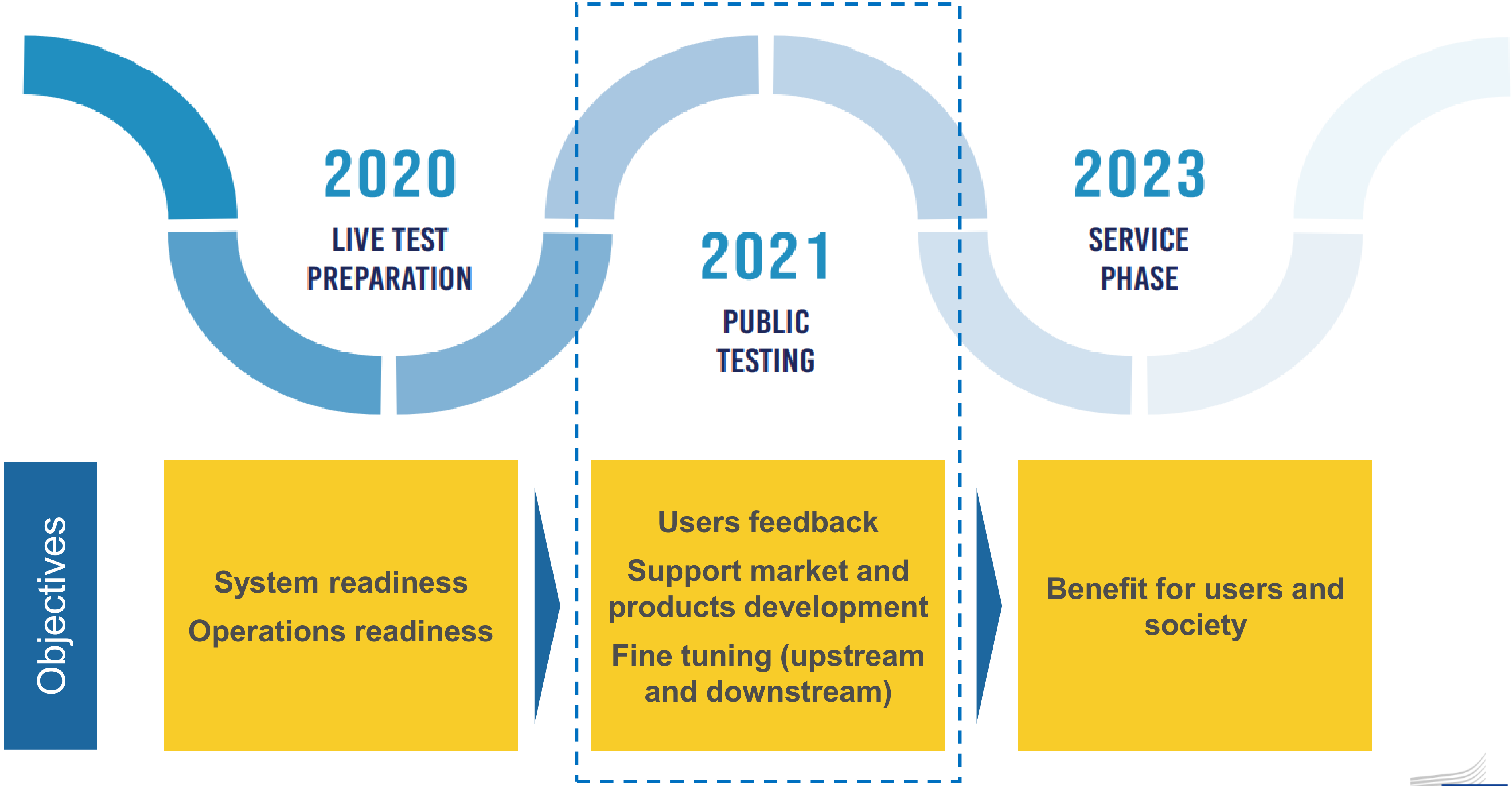
Design, integration and V&V of a shipborne receiver **dual-frequency multi-constellation Galileo OS enabled including OSNMA** and IEC GNSS approval.

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.

Roadmap to service



2020

LIVE TEST PREPARATION

2021

PUBLIC TESTING

2023

SERVICE PHASE

Objectives

System readiness

Operations readiness

Users feedback

Support market and products development

Fine tuning (upstream and downstream)

Benefit for users and society

OSNMA Testing (1/3)

- Public test phase targeting receiver manufacturers, application developers and research institutes started in November 2021.

- The interface to the system for the test phase is described in the OSNMA User ICD and the user requirements are captured in the OSNMA Receiver Guidelines for the Test Phase, both available to the users.

- Test vectors will soon be published to support developers with the implementation of the protocol.

- Users are already implementing the protocol and using the new Galileo feature.

GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OSNMA)

INFO NOTE

EUSPA

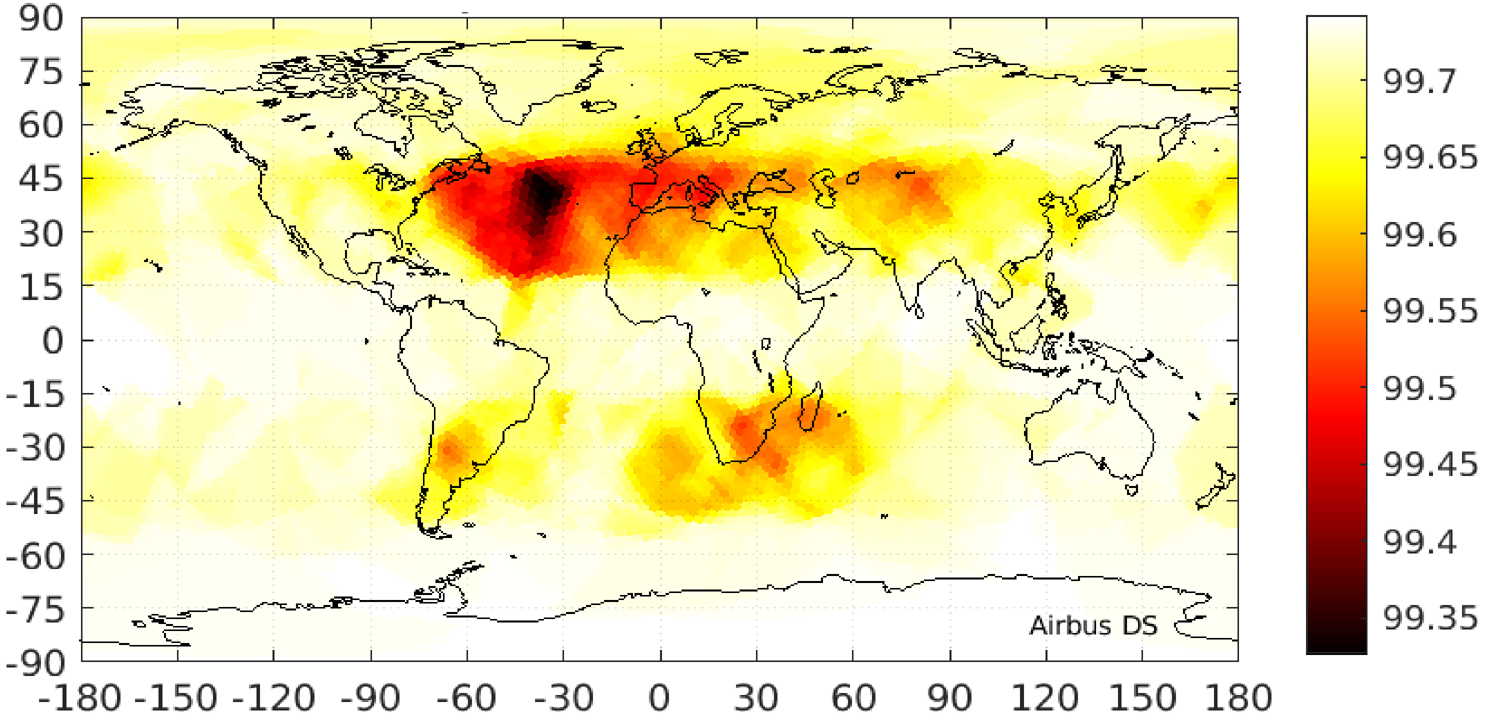
EUSPA

AIRBUS

OSNMA Typical Performance

OSNMA Testing (2/3)

Availability of tags for Galileo I/NAV orbit & clock data (ADKD0) for at least 4 satellites in view, within a period of 120 sec.



Source: Galileo Services Monthly Performance Report – July 2022, EUSPA

OSNMA Testing (3/3)

- JRC developed a set of testing capabilities related to OSNMA: we have the capability to provide OSNMA relevant scenarios and to carry out comparative analysis with reference OSNMA implementations.
- Multiple testing strategies:
  - static and dynamic testing,
  - capacity to post-process both replayed RF signals and navigation data,
  - capacity to simulate RF signals with OSNMA.
- Work was also done on the definition of KPIs for functional, performance and robustness testing.

Conclusion

- OSNMA is the first contribution of a GNSS open service to increase the robustness of the information it broadcasts.

- The public testing phase offers a great opportunity for users to understand OSNMA potential and consider implementation aspects

  ✓ Several GNSS receivers are now OSNMA-ready.

- The initial service phase is expected to start next year (2023) and is planned to be complemented in future with other authentication functions (including ranging).

What to look for at ION GNSS+ 2022?

- Session B1: System Status Update
- Session A1: Augmentation Services, Integrity and Authentication
- Session B4: Trends in Future Satellite Navigation Technology, System and Services
  - *Impact of OSNMA Configurations, Operations and User’s Strategies on Receiver Performance*
  - *Receiver Testing for Galileo E1 OSNMA and I/NAV Improvements*
- Session F3: GNSS Authentication and Anti-Spoofing

Thank you

European Commission

Keep in touch

EU Science Hub: ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub – Joint Research Centre

EU Science, Research and Innovation

Eu Science Hub