GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OSNMA)

INFO NOTE

GALILEO EGNOS
NAVIGATION MADE IN EUROPE

EUSPA
European Union Agency for the Space Programme

Table 1: Reference Documents

REFERENCE DOCUMENTS

TYPE	Title	Reference
[RD1]	European Commission, COMMISSION IMPLEMENTING DECISION (CS Implementing Act).	(EU)2017/224, 8 February 2017
[RD2]	European Commission, COMMISSION IMPLEMENTING DECISION amending Implementing Decision (EU) 2017/224 (CS Implementing Act).	(EU)2018/321, 2 March 2018
[RD3]	GSA User Technology Report	Issue 3 Oct. 2020

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1 BENEFITS OF AUTHENTICATION

Position, Velocity and Timing (PVT) based on GNSS, and in particular on Galileo, is used by many *critical* applications in transportation, finance, telecommunications, information technology, energy, utilities, manufacturing, health services, emergency services, defence and law enforcement.

However, accessibility to spoofing and jamming and relevant knowledge is increasing, resulting in disruption or denial incidents being more frequently observed.

GNSS jamming incidents are reported in very large numbers, the vast majority of them caused by so-called "privacy protection devices" (illegal in most countries).

GNSS spoofing (including meaconing) incidents are less frequently reported, but they are increasing in number. A possible explanation for the lower numbers is that successful (covert) spoofing attacks are not detected or not reported by their victims for security reasons.

While jamming and detected spoofing events can have negative consequences, these incidents typically result in a partial or total interruption of the GNSS services and, for critical applications, one can expect that a fall-back solution is in place and will be used.

Authentication is set to further strengthen system robustness by increasing the capability of detecting spoofing events. However, it should be kept in mind that authentication does not prevent the occurrence of such event, and does not protect against jamming. Nonetheless, this added layer of protection proposes to be one step ahead of evolving technological trends by amplifying the system's overall robustness and resilience.

1.2 LOCATION AND TIMING AUTHENTICATION VS. GNSS AUTHENTICATION

GNSS vulnerabilities are now commonly acknowledged and widely described in the relevant literature, such as in GSA User Technology Report ([RD3]). However, when safety and security are concerned, the trust in the PNT goes beyond GNSS and must encompass the end-to-end-application, which is only as safe or secure as its weakest component. This need for an overall "trust perimeter" is schematically described in Figure 1.

Indeed, the trust perimeter of a typical application contains many interconnected building blocks. Every block and connection is contributing to the overall security, or lack thereof.

Several actors are involved in the process:

- The GNSS service provider
- The augmentation service provider if different
- The terminal manufacturer
- The data communication provider
- The application service provider

GNSS authentication – or Galileo authentication - is one important contributor to the desired overall security of the application. However, the Application Service Provider builds the overall system, or application, and is ultimately responsible for its overall security, including the choice of technical solutions contributing to it.

1.3 OSNMA VALUE PROPOSITION

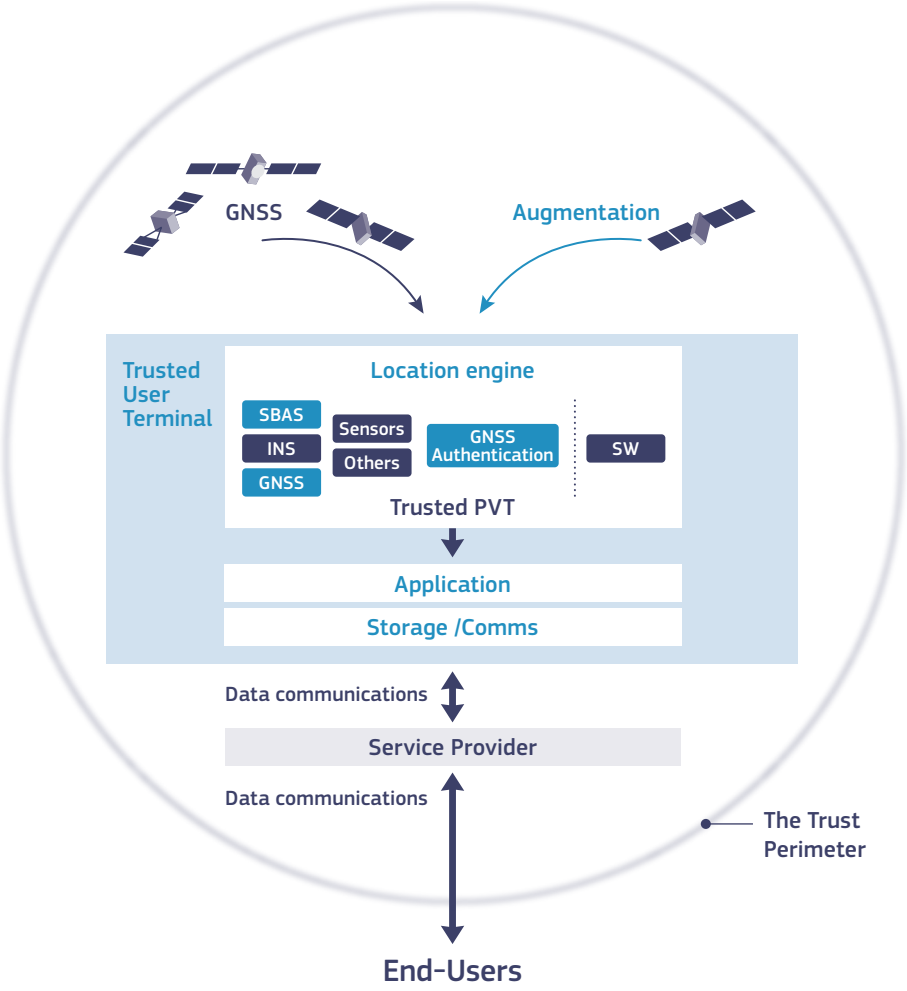
DOWNSTREAM, UPSTREAM OR TERMINAL VULNERABILITIES

Focussing on the security of GNSS derived information, potential spoofing attacks may occur upstream (prior to the receiver input), at the terminal itself, and downstream (after the terminal output).

- Downstream (i.e. at the output of the receiver or the channel over which it reports the position of its antenna, known as "Impersonating the receiver"), typically include general cyber security issues fully independent of the use of GNSS and totally out the reach of the Galileo programme, therefore excluded from this note.

- Vulnerabilities at terminal-level should be prevented or detected by the terminal/receiver design. Similarly to downstream attacks above, these are out the reach of

Figure 1: The trust perimeter



the Galileo programme, and under the sole responsibility of the terminal manufacturer. Note however that regulations or standards, up to the certification of products, can be a way to increase robustness to this type of attacks when justified by the application objectives.

- Upstream (i.e. on signals arriving at the receiver antenna) are those that Galileo can contribute to fight against, by means of signal authentication.

RANGE VS. DATA AUTHENTICATION

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. This can be done at two complementary levels: at the *data level*, to authenticate the broadcast navigation messages; and at the *range level*, to authenticate the measured ranges to the satellites. The combination of both data and range authentication allows the computation of an authenticated PVT solution.

Open Service Navigation Message Authentication (OSNMA) is a data authentication function for the Galileo Open Service worldwide users, freely accessible to all and with no impact on the OS users and performance. A brief description of OSNMA is provided in chapter 2 of this note, and the detailed implementation is described in relevant documentation specified in chapter 5.

OSNMA provides receivers with the assurance that the received Galileo navigation message is coming from the system itself and has not been modified, thus increasing the likelihood of detecting spoofing attacks at the data level and significantly contributing to the security of the solution, given that the receiver fulfils a set of requirements (see section 2.3).

OSNMA will be complemented by the Commercial Authentication Service (CAS), which will offer range authentication in the E6 frequency band (out of scope of this document). The OSNMA bits, which are mostly unpredictable, can be also exploited by receivers to provide some level of protection against signal replay attacks.

2. OSNMA SERVICE CHARACTERISATION

2.1 OVERALL DESCRIPTION

OSNMA is an integral function of the Galileo Open Service, providing data authentication to all enabled receivers.

OSNMA is authenticating data for geolocation information from the Open Service through the Navigation Message (I/NAV) broadcast on the E1B signal component. This is realised by transmitting authentication specific data in previously reserved fields of the E1 I/NAV message.

OSNMA adapts an existing standard lightweight broadcast authentication protocol named TESLA (Timed-Efficient Stream Loss-Tolerant Authentication) for optimal transmission through Galileo. This optimization includes the use of a shared one-way chain by Galileo satellites, and the possibility to authenticate satellites which do not transmit OSNMA data with the data retrieved from satellites transmitting OSNMA, referred to as *cross-authentication*. Compared to other studied protocols, OSNMA reduces the computation and communication overhead, and increases the service availability and robustness to data loss.

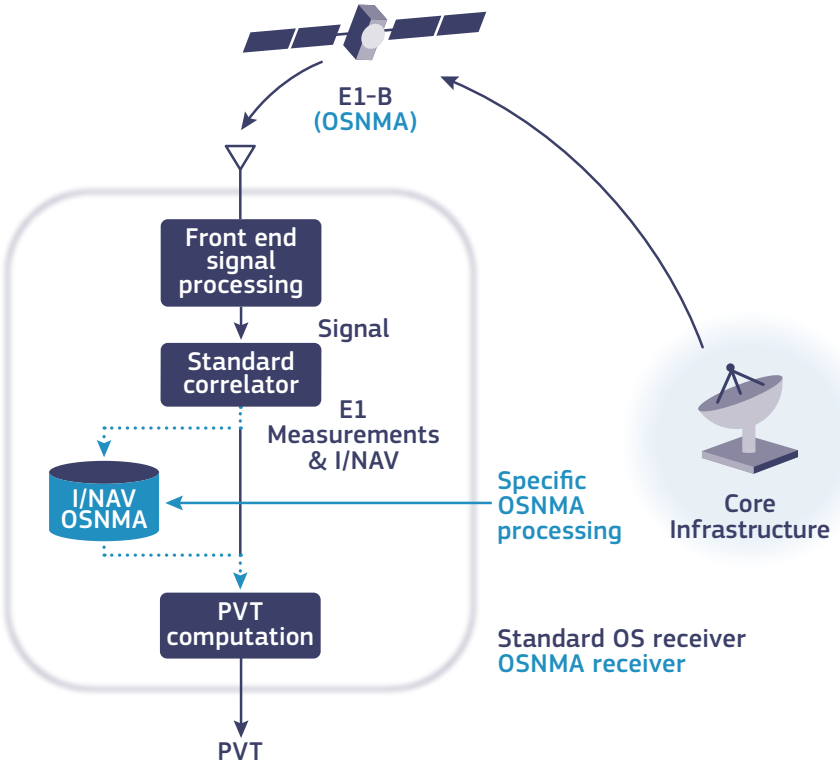
Using previously reserved fields of the I/NAV message, OSNMA does not introduce any overlay to the system, thus the OS navigation performance remains untouched. Furthermore, this design ensures full backward compatibility, and standard OS receivers can continue ignoring the OSNMA dedicated fields of I/NAV and keep functioning with the same performance level. Only OSNMA ready receivers will decode these fields and be able to authenticate Galileo navigation data.

As depicted in Figure 2, an OSNMA capable receiver differs from a generic OS receiver by the additional firmware/software required to:

1. Retrieve the OSNMA dedicated fields in the navigation message;

2. Process these data to confirm whether data is authentic.

Figure 2: OSNMA Scheme



In addition, for a secure implementation of the TESLA protocol, OSNMA receivers require at start-up *loose time synchronization* with time reference with an accuracy between 18 seconds and five minutes, depending on the mode of operation. Sources of the loose reference time can be e.g. an internal real-time clock or a secure network connection with time transfer capability.

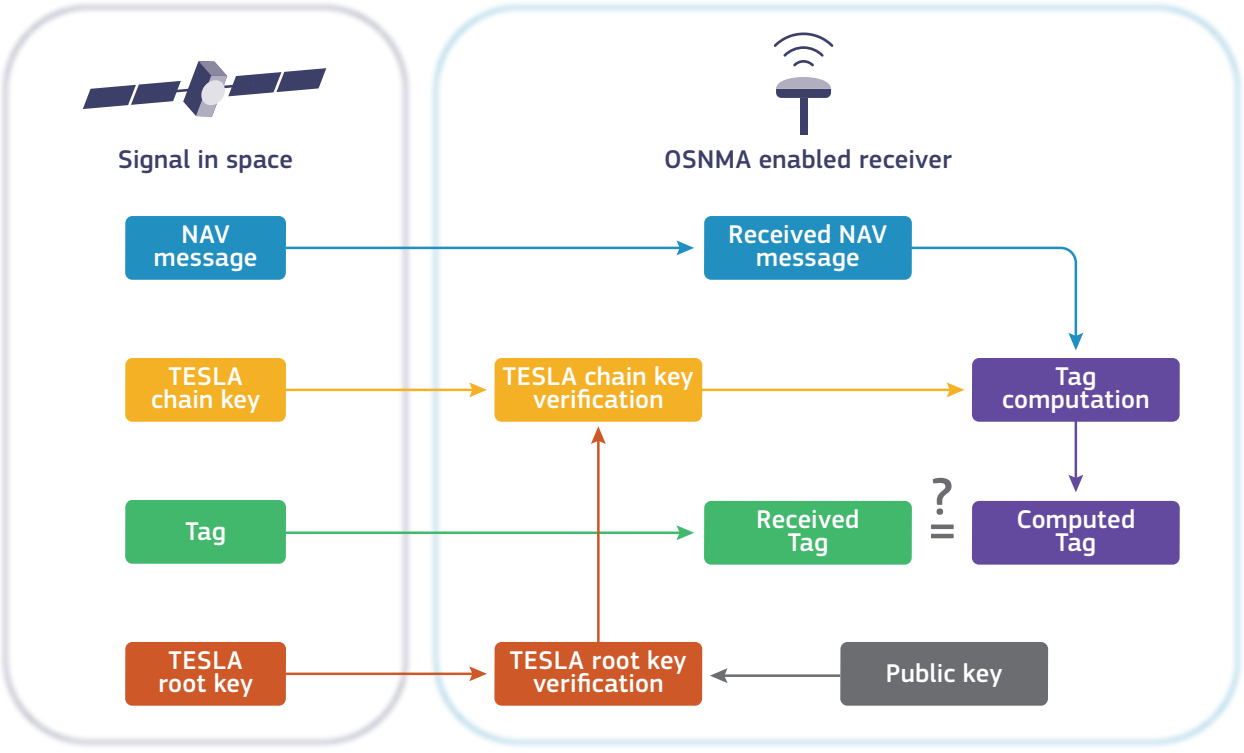
From a receiver perspective, the process of the OS NMA data can be described at a high level by the following steps, illustrated in Figure 3.

- The receiver receives the **navigation data** and the corresponding OS NMA data (**tag**, **TESLA chain key** and **TESLA root key**). The **tag** authenticates the **navigation data** transmitted before the **tag** and is received before its associated **TESLA chain key**.
- The **TESLA root key** is authenticated by means of its digital signature using a **public key** that shall be available at the receiver.
- The receiver authenticates the **TESLA chain key** with the **TESLA root key** or with a previously authenticated key from the TESLA chain.
- The receiver re-generates locally the **tag** with the verified **TESLA chain key** and the **data**, and checks whether it coincides with the received **tag**.

If the result of all these steps is successful the user shall consider the **navigation data** as authentic.

Further details will be provided in the OSNMA ICD and receiver guidelines.

Figure 3: OSNMA processing logic



2.2 FUNCTIONAL COVERAGE

OSNMA provides a means to authenticate navigation data, which is in turn used to compute a PVT.

It should be noted though, that if/when this PVT is computed using non-verified ranging information, it cannot be considered authenticated.

OSNMA enables the detection of certain spoofing attacks on the navigation message. Due to the distribution mechanism of the authentication material, the navigation data is authenticated with a latency that can vary between one and few minutes depending on the reception conditions.

OSNMA does not require any network connectivity[1], however a receiver connected to the European GNSS Service Centre (GSC) will be able to retrieve some of the cryptographic material (see section 2.4.1).

OSNMA works in standalone mode: when assistance and/or augmentation data are used instead of (or to modify) the broadcast Galileo navigation messages, it is the data used for the PVT computation that should be trusted. In such a case, OSNMA cannot be used directly at receiver level, although it can indeed be leveraged by the service provider to generate more trustable assistance/augmentation products.

2.3 OSNMA HARDWARE REQUIREMENTS AND RECEIVER COMPATIBILITY

OSNMA introduction has a minimal impact on receivers, and the extra computational burden needed to handle the cryptographic functions remains commensurate with low-cost receiver capabilities.

The impact is limited to few constraints on:

- The availability of a trustable knowledge of time[2]
- The capability to store and ensure the integrity of a public key, which can be updated if and when necessary through an OTAR (Over The Air Rekeying) mechanism.

OSNMA is in principle compatible with all types of receivers decoding the E1B signal component, therefore can bring navigation data authentication in all application domains.

In order to achieve data authentication at user level, the receiver OSNMA implementation shall be fully compliant with the requirements provided in the OSNMA receiver guidelines (see chapter 5 for a list of relevant documentation).

OSNMA is conceived to support standalone users. Therefore, users of Assisted GNSS or of duty cycling techniques, i.e. typically receivers used in LBS or IoT applications, in order to benefit from OSNMA, may develop other concept of operations/service provision schemes. For example, it is noticeable that some recent Android smartphones chipsets can be configured in a “forced tracking” mode, thus allowing continuous bit level decoding of the I/NAV message and subsequent OSNMA processing. Applications developers can leverage this possibility and experiment the OSNMA benefits already today.

2.4 OSNMA USER SEGMENT INTERFACE

2.4.1 EUROPEAN GNSS SERVICE CENTRE (GSC)

The GSC plays a central role in interfacing with the OSNMA user community beyond the satellite signals. In particular, it is responsible for the following main functions:

- Publication of the OSNMA public keys, crypto material and associated certificates in a way that can be accessible to, and trusted by, end user communities.
- General interaction, notifications, and information updates on the OSNMA service status for all user communities.
- Publication of NAGUs and Service Notices about planned public key renewal, unplanned public key revocation, planned key chain renewal and unplanned key chain revocation and any service incident.
- Helpdesk function related to OSNMA user communities.

For the service provision phase, a Public Key Infrastructure (PKI) will be deployed supporting the authenticity of the NMA data downloaded by the user segment via the GSC interface.

1 For the sake of the one-off receiver initialisation, the manufacturers are expected to connect one time to the GSC, see section 2.4 for further information.

2 To ensure the security of the TESLA protocol and guarantee the authenticity of the data, the receiver must ensure it has received the navigation data and associated tag before the corresponding TESLA chain key is disclosed by the system.

As described in section 2.4.2, end users will generally not have to interface to the GSC, except advanced users willing to receive OSNMA Service notifications and NAGUs. Such users, including receiver manufacturers and dedicated entities (e.g. entities involved in Research and Development activities) will be able to connect to the GSC web server in order to perform initialisation or update of the certified cryptographic material for their receiver fleet.

2.4.2 KEY MANAGEMENT

To benefit from the OSNMA, the receiver must be able to perform the following operations:

1 Installing and storing the certified public key in the user receiver 2 Updating the public key stored in the receiver	*Described in this section*	Interface through the European GNSS Service Centre (GSC) Interface through the signal in space (SIS) or the European GNSS Service Centre (GSC)
3 Reception of the I/NAV and authentication data 4 Verification of the digital signature which signs the root key of the applicable TESLA key chain and the applicable OSNMA configuration parameters 5 Authentication of the Navigation data	*Described in section 2.1*	Interface through the signal in space (SIS), detailed in the OSNMA ICD The receiver cryptographic operations, detailed in the OSNMA receiver guidelines

Point 1 above is also known as "receiver initialisation" and consists in installing and storing in the receiver the certified cryptographic material required to access OSNMA. This is a one-off operation, requiring a connection to the GSC that will supply the necessary material.

It is anticipated that this operation will only be performed by the receiver manufacturers and advanced users such as application developers, but will remain invisible to "standard" end users.

Point 2 consists in renewing or updating the public key stored in the receiver. This operation may happen several times in the receiver lifetime (yet remain infrequent[3]) e.g. when public keys have been revoked, expired, or otherwise regenerated, requiring re-installation to the user receiver.

There are two methods to perform this operation:

1. Through over-the-air rekeying (OTAR) transmitted as part of the SIS authentication data. This will be the nominal procedure, ensuring no required intervention and no service interruption for end users. In addition to this OTAR procedure, it is planned to broadcast the active public key with a low frequency, even when it is not renewed or revoked.

2. Through contacting the OSNMA server in GSC, which will keep the history of the public keys status (this method is to be used only by receiver manufacturers or advanced users, e.g. for preparation of firmware updates).

The details regarding the key generation, signing and sharing can be found in the OSNMA ICD. This document provides the Galileo OSNMA bit-level specification. In addition, the details regarding the processing the receiver cryptographic operations are provided in the OSNMA receiver guidelines.

3 In the order of once every year or every few years.

2.5 SUMMARY OF OSNMA CAPABILITIES

Table 2: Overview of OSNMA features

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[4]
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[5]

4 Except for the one-off initialisation of the receiver, performed by manufacturers (see section 2.4).
5 In the order of 18 s under nominal conditions.

3. TARGET MARKETS

As authentication has not existed in the civil GNSS domain so far, there is a rather theoretical market awareness and only initial concrete feedbacks to validate (or otherwise) the findings of the analysis presented in this section. To ensure both completeness and validity of the following market demand assessment, EUSPA is regularly engaged in industry and end user consultations and has added the authentication topic (and relevant performance parameters) to its User Requirements consultations, including but not limited to the 2020 Users Consultation Platform.

The table below elaborates on the applications that are expected to benefit the most from the use of authentication and as such are considered candidate use cases for Galileo authentication features, including but not limited to the OSNMA.

In addition, it presents the relevant technology currently used in User Terminals and identifies the future trends in that respect, also highlighting the potential role of OSNMA for each analysed application. Indeed, as discussed in sections 1.2 and 1.3, OSNMA is one important contributor to the desired overall security of the application, but it is anticipated that in most use cases it will be used in synergy with other receiver based or external techniques to reduce the likelihood of success of a spoofing attack and therefore increase the overall security at PNT level.

By providing this context, Table 4 allows to identify applications where OSNMA appears most relevant and likely to be rapidly adopted, such as:

- Smart Digital Tachograph
- Logistics
- Mobile Payments
- Insurance Telematics
- Autonomous Driving
- Fleet Management & Dangerous Good Transports
- Road User Charging (RUC)
- Internet of Things
- Drones navigation, identification and traffic management
- Timing & Synchronisation (e.g. Energy, Finance, Telecom, DVB, etc.)
- (Manned) Aviation navigation
- Fishing Vessel monitoring
- ADS-B
- Cadastral Surveying
- And more… including support to CAP policy in the Agriculture domain

The market data represents the current best estimate for an innovative GNSS capability which is set to be provided by Galileo as clear differentiator to any other GNSS system. For this reason the market information is expected to evolve as the users will start using this capability and the availability of OSNMA will undoubtedly modify the market perception and maturity. It will also be for the Member States to decide on the applications development.

On this basis, it is anticipated that such initial forecasts will be modified in the coming years.

Table 3: Summary of authentication needs and future trends for target applications

MARKET SEGMENT	APPLICATIONS	BRIEF DESCRIPTION	AUTHENTICATION REQUIREMENTS
 AGRICULTURE	**AUTOMATIC STEERING & AUTONOMOUS MACHINERY**	This application, in the frame of Precision Agriculture, allows the partial or complete take-over of the steering of the farm equipment by the driver allowing the operator to engage in core agricultural tasks.	• Automation requires a high level of resilience to spoofing, in addition to integrity. • GNSS security is a concern. Researches and industry consultations have demonstrated the need for authentication and anti-spoofing measures. Positioning is based on fusion of different sensors (GNSS+INS; Cameras, LIDAR, radar, etc.) in case of autonomous machinery.
	GEOTAGGING PHOTO APPLICATION WITHIN CAP	In the EU, GNSS-based operations using EGNOS and Galileo support a system of area-based subsidies for farmers within the Common Agricultural Policy. Use of geotagged photographs in CAP defines data security measures to be implemented within geotagging application, including the detection of fake position and future use of OSNMA.	• Support to EU Common Agricultural Policy. • Both single and dual-frequency phones are used, utilising either internal PVT or advanced techniques via GNSS raw measurements. Gradual penetration of Galileo/ multi-constellation phones. • Interest in GNSS authentication that contributes to the increased robustness. JRC Technical Report - Use of geotagged photographs (JRC 120223) in CAP - defines data security measures to be implemented within geotagging application, including the detection of fake position and future use of OSNMA.
	AGRI-LOGISTICS, *(I.E. ASSET MANAGEMENT, MACHINERY MONITORING AND GEO-TRACEABILITY)*	This application includes: • Farm machinery monitoring, with location monitoring and status of the mechanical equipment; and • Asset management, by means of efficient workflow management. Geo-traceability enhances the effectiveness of food, animal and product traceability by using transponders on animals and vehicle GNSS trackers, as well as by geo-referencing location and size of land parcels.	• Asset value can justify higher resilience to spoofing. • High crop value and possible impact of non-traceability. • No authentication currently. • “Farm2Fork” and the transparency of agriculture production request documentation including also position and time. Authentication might be relevant.

TECHNOLOGICAL ENVIRONMENT	RECENT TECHNOLOGY TRENDS	POTENTIAL ROLE OF OSNMA
• RTK or PPP-RTK combined with other sensors. • Dual GNSS smart antennas. • High-accuracy corrections redundancy for autonomous machinery. • Integrity for high-accuracy GNSS correction service. • 5G [potential].	• Connectivity. • Resilience. • Anti-spoofing and anti-jamming.	OSNMA has a role in synergy with additional technologies.
• GNSS + other techniques that increase the robustness (cell-ID, wi-fi, etc.). • Artificial Intelligence to detect fake images [potential].	• Dual-frequency and multi-constellation phones. • Use of high-accuracy corrections/ advanced positioning techniques. • 5G.	OSNMA has a role in synergy with additional security measures.
• GNSS tracker. • Comparison of communication network node position with GNSS. • 5G [potential].	• Connectivity. • Anti-spoofing and anti-jamming.	OSNMA has a role in synergy with additional technologies.

MARKET SEGMENT	APPLICATIONS	BRIEF DESCRIPTION	AUTHENTICATION REQUIREMENTS
 CIVIL AVIATION (MANNED)	**NAVIGATION FOR COMMERCIAL REGIONAL, GENERAL & BUSINESS AVIATION**	This application allows performance based navigation (PBN) by which an aircraft follows a specific procedure or route with a prescribed margin of error.	• All applications in the aviation domain are safety critical (SoL), furthermore, if GNSS is used to support automated operations a very high level of resilience to spoofing is required, in addition to integrity. • GNSS Authentication is not part of the current aviation standards. • Main focus is on availability and integrity. • GNSS will become the primary navigation technology by 2030. • International organizations (ICAO, RTCA, FAA...) are issuing recommendation to integrate interference and spoofing mitigation mechanisms.
	TRAFFIC MANAGEMENT (ADS-B) FOR MANNED AVIATION	This application includes Automatic Depended Surveillance Broadcast (ADS-B). It allows aircrafts to automatically report their position to air traffic controllers on the ground and other aircrafts equipped with receivers.	• All applications in the aviation domain are safety critical (SoL), furthermore if GNSS is used to support automated operations a very high level of resilience to spoofing is required, in addition to integrity. • There is currently no Authentication. • Potential Authentication Service required is Location authentication for aircrafts traffic monitoring.
 DRONES	**NAVIGATION AND TRAFFIC MANAGEMENT FOR UAVS**	This application includes both safe Navigation and Traffic management of drones. It allows the development of Drones applications, while safely sharing the airspace with manned aviation.	• Safety critical platform in need of resilience to spoofing, whatever the application domain. • Regulation currently not fully available. • Need for Navigation Robustness / Redundancy. • Potential Authentication Service required is Signal/ Message Authentication for UAV GNSS receivers and Location authentication for the UAV traffic monitoring systems.

TECHNOLOGICAL ENVIRONMENT	RECENT TECHNOLOGY TRENDS	POTENTIAL ROLE OF OSNMA
• Consistency Check with other navigation systems to be implemented on-board. • Redundancy based on Dual Frequency / Dual Constellation [potential]. • Consistency Checks with other systems (A-PNT) to be implemented on-board [potential].	• Receiver based Spoofing detection methods. • Cross check with other Navigation system such as INU (Inertial Navigation Unit). • Advanced Receiver Autonomous Integrity Monitoring (ARAIM).	OSNMA has a potential role in synergy with other technologies. It shall be noted that the OSNMA uptake would be subject to a prior recognition by official certification and standardisation bodies (FAA, RTCA, Eurocontrol etc.).
• Secure Location Verification based on multilateration. • Related to Aviation technology [potential].	• Secure Broadcast Authentication (various schemes that apply asymmetric properties (cryptographic and non- cryptographic) to directly authenticate broadcast communication). • Secure Location Verification (several different methods that seek to verify the authenticity of location claims made by aircraft and other ADS-B participants).	ADS-B growth could be one additional driver for the introduction of OSNMA in the aviation market, even if it is not a primary GNSS application. As for navigation the OSNMA uptake would be subject to a prior recognition by official certification and standardisation bodies.
• Fusion with external sensor mainly for navigation availability. • Fusion with external sensors (GNSS, IMU, Map data, Vision, Lidar, Radar, Ultrasonic…) for authentication [potential].	• Lidar. • Synthetic Aperture Radar (SAR), Image Processing. • Signal of Opportunity Navigation (LTE, 5G).	OSNMA has a potential role in synergy with additional receiver / external sensor technologies.

MARKET SEGMENT	APPLICATIONS	BRIEF DESCRIPTION	AUTHENTICATION REQUIREMENTS
 LOCATION BASED SERVICES	**SAFETY**	Allows the reporting of critical situations, or the dissemination of safety / security warnings using smartphones as the terminal / user interface.	• Safety warnings received on a smartphone must come from a trusted source. • Position accuracy is the main requirement. Position authentication is currently not required.
	GAMES AND AUGMENTED REALITY	Leverage GNSS as it enables a wide range of location-based games, including augmented reality, on smartphones and tablets (Phones, Tablets, Mobile computers).	• Gaming was the first widespread GNSS (self) spoofing attack reported worldwide. • Position authentication is required by different applications. • GNSS authentication can contribute but the challenging environment shall be considered.
	SPORTS	Allows the monitoring of users' performance through a variety of fitness applications (smartphones, wearables).	• Depending on the specific application, authentication could prevent damages or issues arising from a spoofing attempt. • GNSS used for tracking of the athletes and statistics. • GNSS authentication will likely not be required.
	MOBILE PAYMENTS AND E-COMMERCE	Allowing consumers to use their smartphone instead of their debit or credit card, or to perform payment on eCommerce sites. In both cases the debit / credit card is not present (no PIN code validation).	• Such payments require a security level at least equivalent to the payment card system they replace. • Economic and liability impact associated to commercial transactions. • User authentication and authorization are critical controls, especially for "Card Not Present" payments. • GNSS authentication potentially useful. Position availability is required on demand and in challenging environment.
	NAVIGATION	Enables route planning and turn-by-turn instructions based on GNSS support for both pedestrian and road navigation (Phones, PNDs, some IVS).	• Misleading turn by turn instructions may distract the driver's attention and create hazards. • Widely popular LBS. Location based on smartphone hybrid position + map matching.
	MAPPING AND GIS	Empowers users to become map creators thanks to the democratization of digital mapping (Phones, Tablets, Mobile computers).	• Quality assurance for crowd sourcing, potential liabilities depending on use case of maps. • GNSS used as the main source of absolute "accurate" position. • Potential use of Authentication, to decentralise this function at the data collection level.

TECHNOLOGICAL ENVIRONMENT	RECENT TECHNOLOGY TRENDS	POTENTIAL ROLE OF OSNMA
• Cellular network localisation (e.g. Cell ID). • Techniques available in COTS GNSS receivers [potential].	• LTE, 5G.	OSNMA may have an added value in reducing the likelihood of spoofing, since the application has legal implications.
• Operative system APIs: combination of GNSS, Wi-Fi and cellular network localisation. • Position falsification detection at software level. • Software/Firmware tampering detection [potential].	• Software/Firmware tampering detection.	OSNMA may mitigate the risk of spoofing, including self-spoofing.
• Image processing. • RFID.	• No trend Identified.	Application with very low GNSS maturity. No major concerns on GNSS authentication.
• Combined use of GNSS, Cellular Networks signal and Wi-Fi. • NFC. • IP localisation. • Techniques available in COTS terminals [potential]. • Blockchain [potential].	• Generic Hardware/Software security. • Signal of Opportunity positioning (LTE,5G).	Galileo OSNMA service may contribute to the overall mobile payment system protection against fraud.
• Combined use of GNSS, Cellular Networks signal and Wi-Fi, integrated with map matching.	• No trend Identified.	OSNMA may mitigate the risk of spoofing.
• Combined use of GNSS, Cellular Networks signal and Wi-Fi. • Carrier based positioning (e.g. PPP techniques) to improve accuracy [potential].	• No trend Identified.	OSNMA can be useful to enable more trustable decentralised data collection.

MARKET SEGMENT	APPLICATIONS	BRIEF DESCRIPTION	AUTHENTICATION REQUIREMENTS
	mHEALTH	Where GNSS enables, in combination with other technologies, a vast array of applications from patient monitoring to guidance systems for the visually impaired (Phones, wearables).	• Sensitivity of the application due to the vulnerability of the relevant users. • Mobile phone API location (including GNSS) used for positioning. • Authentication potentially useful for increased trustability of the users location.
	GEO-MARKETING AND ADVERTISING	Allows to combine consumer preferences with positioning data to provide personalized offers to potential customers (Phones, wearables).	• The associated commercial and economic impact makes this application exposed to spoofing threats. • Mobile phone API location (including GNSS) used for positioning.
	ENTERPRISE APPLICATIONS	Support companies to improve productivity by use of mobile workforce management and tracking solutions (Phones, Tablets, Mobile computers).	• Depending on the specific application authentication can prevent damages or issues arising from a spoofing attempt. • Mobile phone API location (including GNSS) or GNSS tracker used for positioning.
	SOCIAL NETWORKING	Through the use of Friend locators, embedded in social networks, it leverages GNSS to help keeping in touch and sharing travel information (Phones, Tablets, Mobile computers).	• Similarly to gaming, it might be exposed to self-spoofing. • User Authentication and authorization are critical controls for every mobile payment.
	PERSONAL TRACKING	This application uses positioning, for example to automatically control the blades and buckets of construction equipment based on information provided by 3D digital design.	• Security (e.g. children locator) or value (e.g. asset trackers) justify higher resilience to spoofing. • Authentication is critical for asset tracking, including persons.
 GEOMATICS	**CADASTRAL SURVEYING**	This application specialises in the establishment and re-establishment of real property boundaries. Fiscal policies such as land taxation rely widely on cadastral surveying.	• Economic relevance and legal value make this application exposed to potential spoofing. • Typically RTK dual-frequency employed for cm-level positioning, with gradual penetration of multi-constellation and multi-frequency over Europe while other techniques such as PPP or PPP-RTK has emerged in areas with no RTK infrastructure. • Potential Authentication Service required is Signal/ Message Authentication for determination of surveying points position and distances.

TECHNOLOGICAL ENVIRONMENT	RECENT TECHNOLOGY TRENDS	POTENTIAL ROLE OF OSNMA
• Combined use of GNSS, Cellular Networks signal and Wi-Fi.	• No trend Identified.	OSNMA may contribute to higher trustability of the applications.
• Combined use of GNSS, Cellular Networks signal and Wi-Fi. • Bluetooth, NFC, etc.	• No trend Identified.	OSNMA may contribute to higher trustability of the applications.
• Combined use of GNSS, Cellular Networks signal and Wi-Fi. • IoT type GNSS trackers.	• No trend Identified.	OSNMA may mitigate the risk of spoofing, including self-spoofing.
• Combined use of GNSS, Cellular Networks signal and Wi-Fi.	• No trend Identified.	OSNMA may mitigate the risk of spoofing, including self-spoofing.
• Combined use of GNSS, Cellular Networks signal and Wi-Fi.	• No trend Identified.	OSNMA may contribute to higher trustability of the applications.
• Observations Redundancy. • Equipment Validation (geodetic points).	• Use of Drones and associated technologies (in countries with less stringent accuracy requirements). • Combination of different techniques or corrections (RTK, PPP-RTK, etc.) in one solution to ensure cm-level seamless positioning if one technique fails.	OSNMA may have an added value in reducing the likelihood of spoofing, since the application has liability and legal implications.

MARKET SEGMENT	APPLICATIONS	BRIEF DESCRIPTION	AUTHENTICATION REQUIREMENTS
	MACHINE CONTROL AND AUTONOMOUS MACHINERY IN CONSTRUCTION AND MINING	This application uses positioning, for example to automatically control the blades and buckets of construction equipment based on information provided by 3D digital design.	• Automation requires a high level of resilience to spoofing, in addition to integrity. • GNSS security is a concern. Researches and industry consultations have demonstrated the need for authentication and anti-spoofing measures. Positioning is based on fusion of different sensors (GNSS+INS; Cameras, LIDAR, radar, etc.) in case of autonomous machinery.
 MARITIME	**NAVIGATION FOR SOLAS & NON-SOLAS VESSELS, OCEANIC TO IWW**	This application safe navigation for all types of vessels (SOLAS and non SOLAS) in all phases, ranging from inland waterways and restricted waters to oceanic.	• All applications in the maritime domain are safety critical (SoL), furthermore if GNSS is used to support automated operations a very high level of resilience to spoofing is required, in addition to integrity. • High economic relevance of merchant navigation. • IMO and IALA are promoting the e-Navigation and the resilient PNT that requires collaborative use of navigation system. • Currently no authentication, but Location authentication may be required in the future.
	MARINE ENGINEERING AND SURVEYING	This application supports marine engineering activities (e.g. dredging and construction, pipeline and cable laying, support to offshore Oil & Gas exploration and Production, etc). Surveying covers a wide range of activities (e.g. seabed exploration, tide and current estimation, offshore surveying, etc.) and their outcomes are important for engineering activities but also for maritime navigation.	• (Very) high asset value and costs of operation in hostile environment, as well as economic relevance, justify increased resilience to spoofing. • IMO and IALA are promoting the e-Navigation and the resilient PNT that requires collaborative use of navigation system. • Potential Location authentication required.

TECHNOLOGICAL ENVIRONMENT	RECENT TECHNOLOGY TRENDS	POTENTIAL ROLE OF OSNMA
• RTK or PPP-RTK combined with other sensors. • Dual GNSS smart antennas. • High-accuracy corrections redundancy in autonomous mode. • Integrity for high-accuracy GNSS correction service. • 5G [potential].	• Connectivity. • Resilience. • Anti-spoofing and anti-jamming.	OSNMA has a role in synergy with additional technologies.
• No use of authentication mechanisms. • Consistency Checks with CORS, LORAN, Radars [potential]. • Integration with Inertial Sensor [potential]. • GNSS Receivers redundancy [potential].	• Multiconstellation and Multifrequency redundancy. • Big Data techniques (mainly for increased traffic efficiency). • Receiver Based and multi- antenna spoofing detection techniques. • Automation / Unmanned vessels.	OSNMA has a role in synergy with additional technologies.
• No use of authentication mechanisms. • Consistency Checks with CORS, LORAN, Radars. • Integration with Inertial Sensor. • GNSS Receivers redundancy. • Multiple independent augmentation systems.	• Multiconstellation and Multifrequency redundancy. • Receiver Based and multi- antenna spoofing detection techniques. • Automation / Unmanned vessels.	OSNMA has a role in synergy with additional technologies.

MARKET SEGMENT	APPLICATIONS	BRIEF DESCRIPTION	AUTHENTICATION REQUIREMENTS
	PORT OPERATIONS	This application covers Port operations applications whereby transit progress, docking and loading-unloading operations are monitored through GNSS based technologies.	• Safety critical applications. High impact economic and safety impact of disruption. • IMO and IALA are promoting the e-Navigation and the resilient PNT that requires collaborative use of navigation system. • Potential Authentication Service required is Signal/ Message Authentication for maritime GNSS receivers.
	SURVEILLANCE OF FISHING VESSEL	This application covers vessel monitoring systems allowing to check the position of the vessel as well as the time spent in international and foreign waters, protected areas, etc.	• Potential self-spoofing of fishing vessels to escape reporting to fisheries monitoring system. • Potential impact of spoofing on nearby vessels. • IMO and IALA are promoting the e-Navigation and the resilient PNT that requires collaborative use of navigation system. • Potential Location authentication required.
	TRAFFIC INFORMATION AND MANAGEMENT (AIS / LRIT) OCEANIC TO IWW	This application includes Traffic management and surveillance of vessels, as well as situational awareness enabled by ship to ship, ship to shore and shore to ship automated communications. GNSS-based systems include Automatic Identification System and Long-Range Identification and Tracking (LRIT).	• All applications in the maritime domain are safety critical (SoL), furthermore if GNSS is used to support automated operations a very high level of resilience to spoofing is required, in addition to integrity. • High economic impact in case of disruption. • IMO and IALA are promoting the e-Navigation and the resilient PNT that requires collaborative use of navigation system. • Location authentication will potentially be required.
 RAIL	**SIGNALLING AND TRAIN CONTROL APPLICATIONS (HD CSS & LD CSS)**	This application includes Command & Control Systems applications (main lines and low-density lines) by providing positioning as well enhancing odometry in European Train Control Systems or to support Positive Train Control.	• Safety critical applications require a high level of resilience to spoofing, in addition to integrity. • GNSS has a primary role in ERTMS platform designed to operate with virtual balise. • Integrity and Safety are the main Rail requirements. • GNSS security is a concern. • GNSS authentication measures will be required.
	ASSET MANAGEMENT	This application comprises functions as fleet management, need-based maintenance, infrastructure charges and inter-modal transfers. GNSS is increasingly seen as a standard source of positioning and timing information in these systems.	• Economic impact of a potential disruption can justify higher resilience of the solution. • GNSS used for positioning and timestamping of diagnostic information. • GNSS security is a concern. • GNSS authentication measures will be required.

TECHNOLOGICAL ENVIRONMENT	RECENT TECHNOLOGY TRENDS	POTENTIAL ROLE OF OSNMA
• No use of authentication mechanisms. • Consistency Checks with CORS, LORAN, Radars [potential]. • Integration with Inertial Sensor [potential]. • GNSS Receivers redundancy [potential].	• Multiconstellation and Multifrequency redundancy. • Big Data techniques (mainly for increased traffic efficiency). • Receiver Based and multi- antenna spoofing detection techniques. • RFID.	OSNMA has a role in synergy with additional receiver / external sensor technologies.
• No use of authentication mechanisms. • Consistency Checks with CORS, LORAN, Radars [potential]. • Integration with Inertial Sensor [potential]. • GNSS Receivers redundancy [potential].	• Multiconstellation and Multifrequency redundancy. • Receiver Based and multi- antenna spoofing detection techniques.	OSNMA is important as this application has liability implications.
• No use of authentication mechanisms. • Consistency Checks with CORS, LORAN, Radars [potential]. • Integration with Inertial Sensor [potential]. • GNSS Receivers redundancy [potential].	• Multiconstellation and Multifrequency redundancy. • Big Data techniques (mainly for increased traffic efficiency). • Receiver Based and multi- antenna spoofing detection techniques.	OSNMA has a role in synergy with additional receiver / external sensor technologies.
• Physical Balise. • A-GNSS (data) [potential]. • Integration with IMU or Train speed data – (Odometer) [potential]. • Multiconstellation / Multifrequency redundancy [potential]. • RAIM [potential].	• CRPA / Digital Beamforming. • Receiver Based Antispoofing. • Location database or Map.	OSNMA may have a role in synergy with additional receiver / external sensor technologies.
• Multiconstellation / Multifrequency redundancy [potential].	• No trend Identified.	OSNMA could provide an added value in providing authenticated location.

MARKET SEGMENT	APPLICATIONS	BRIEF DESCRIPTION	AUTHENTICATION REQUIREMENTS
 ROAD & LOGISTICS	**ROAD USER CHARGING (RUC)**	This application enables toll operators to charge a user (i.e., vehicle) based on its reported position, for the use of the roads and for traffic and congestion control.	• Liability critical application. Proof of fair charging. Potential self-spoofing. • Development of GNSS based Road User Charging schemes is ongoing, currently not requiring GNSS authentication. • GNSS positioning is a liability risk in case of falsification of the signal. Authentication will provide benefits.
	SMART DIGITAL TACHOGRAPH	This application leverages GNSS positioning to support road enforcers, by recording the position of the vehicle at different points during the working day.	• Regulated application, use of authenticated GNSS and its authentication capability is compulsory, when available. • EU Regulation 2016/799 foresee that GNSS receiver shall have the capability to support Authentication on the Open Service of Galileo. • GNSS authentication will be adopted.
	INSURANCE TELEMATICS	This application uses GNSS data, transmitted to the "black box", to increase the fairness of motor insurance for both insurers and subscribers in the frame of Usage-based Insurance i.e. Pay as you drive (PAYD).	• Liability critical application. Proof of fair charging. Potential self-spoofing. • GNSS position authenticity and the robustness to interference are fundamental. • GNSS authentication has a potential use, as the application has liability and legal implications.
	FLEET MANAGEMENT & GOOD TRANSPORTS	This application leverage On Board Units (OBUs) to transmit positioning information through telematics to support transport operators in monitoring their fleet. For goods, reports may include other information about the status of the cargo.	• Asset value can justify higher security. • GNSS-based fleet management systems are used to locate vehicles (e.g. trucks, buses, emergency vehicles, taxis) in order to optimize resource management, reduce travel time, increase security and reduce fuel consumption. • GNSS authentication might provide an added value mainly for vehicle transporting valuable goods.
	AUTONOMOUS DRIVING	This application is covering ADAS levels 3-5 (partial to full vehicle autonomy), removing the driver from the driving seat and having a set of technologies including GNSS to guide and operate the vehicle.	• Automation requires a high level of resilience to spoofing, in addition to integrity. • GNSS security is a concern. Researches have demonstrated the need for authentication and anti-spoofing measures.

TECHNOLOGICAL ENVIRONMENT	RECENT TECHNOLOGY TRENDS	POTENTIAL ROLE OF OSNMA
• Integration of GNSS with INS and CAN BUS interface. • DSRC/Balise. • Integration with other sensors [potential]. • Techniques available in COTS GNSS receivers [potential].	• No trend Identified.	OSNMA is considered as key contributor for GNSS based tolling as this application has economic and liability implications.
• Internal or external GNSS device with anti-tamper detection. • ITS Interface [potential].	• Integration with other sensors. • Data manipulation detection.	OSNMA is already part of the regulation and is set to contribute increasing safety in EU roads.
• Integration of GNSS with INS and CAN BUS interface. • Cellular network.	• No trend Identified.	OSNMA is important as this application has liability /legal implications.
• Integration of GNSS with INS. • Cellular network.	• No trend Identified.	OSNMA is important as this application has liability /legal implications.
• GNSS + INS device. • Lidar. • Computer Vision. • RTK Technology. • Precise Point Positioning.	• Lidar.	OSNMA has a role in synergy with additional receiver / external sensor technologies.

MARKET SEGMENT	APPLICATIONS	BRIEF DESCRIPTION	AUTHENTICATION REQUIREMENTS
	COMMERCIAL LOGISTICS	This application is similar to fleet management; however it focusses on the cargo rather than on the carrier. It covers the whole terrestrial logistic chain (road, rail, and interconnection nodes). It uses GNSS trackers attached to the cargo (e.g. container) rather than carrier OBUs.	• Cargo value can justify higher security. • Proof of delivery in logistics and e-Documents for transport. • Proof of delivery is critical for the correct operations, reducing claims and liabilities through all the supply chain. • GNSS authentication could be used for proof of delivery, in combination with other technologies (e.g. images). • GNSS authentication could contribute to increase security in the increased automated logistics.
 TIMING	**TELECOM**	This application allows telco operators to have accurate and consistent time and frequency at distant points of their network to face increasingly demanding broadband requirements.	• Spoofing attack could cause extended problems and damages. • Reliance on GNSS and atomic clocks for synchronisation. • Clear interest on GNSS authentication confirmed during the 2nd UCP in 2018 and 3rd UCP in Dec 2020.
	ENERGY	This application enables energy operators to monitor the energy flow of their network by delivering an accurate time source.	• Spoofing attack could cause extended problems and damages. • Reliance on GNSS for synchronisation requires increased robustness against Jamming and Spoofing. • Clear interest on GNSS authentication confirmed during the 2nd UCP in 2018 and 3rd UCP in Dec 2020.
	FINANCE	This application empowers financial institutions to trace operations with a consistent and accurate time scale. It is complementary to other sources.	• Spoofing attack could cause extended problems and damages. • Reliance on GNSS for synchronisation. • EU and US finance has started moving toward the new regulations. Each transaction shall be timestamped. • Clear interest on GNSS authentication confirmed during the 2nd UCP in 2018 and 3rd UCP in Dec 2020.
	GROUND INFRASTRUC-TURE FOR NAVIGATIONAL AIDS AND TRAFFIC MANAGEMENT, AVIATION AND MARITIME	Infrastructure enabling or contributing to the provision of Safety of Life services, including GBAS and DGNSS reference and monitoring stations, AIS / VDL shore stations, airports A-SMGCS, and others.	• Infrastructures supporting safety critical (SoL) applications. • Spoofing attack could cause extended damages. • Reliance on GNSS for synchronisation and positioning. • Current focus on integrity, no specific anti-spoofing measure. • Anti-spoofing will become more critical, possibly mandated.

TECHNOLOGICAL ENVIRONMENT	RECENT TECHNOLOGY TRENDS	POTENTIAL ROLE OF OSNMA
• Single packages are tracked using bar codes and RFIDs.	• Sensor for real time monitoring. • Use of smartphones and BYOD (Bring Your Own Devices) to reduce costs. • Low cost sensors. • Proof position may include digital cameras. • 5G.	OSNMA could be used for proof of delivery, in combination with other technologies (e.g. images).
• Dedicated Atomic Clocks; • Network Synchronisation protocols: NTP/PTP.	• Secure PTP evolutions. • Iridium, eLoran, White Rabbit.	OSNMA has an added value for this application.
• Network Synchronisation protocols: NTP/PTP.	• Secure PTP evolutions. • Iridium, eLoran, White Rabbit.	OSNMA can play a role in synergy with other technologies.
• Dedicated Atomic Clocks. • GNSS-disciplined oscillators. • Network Synchronisation protocols: NTP/PTP. • Alternative: Iridium, eLoran…[potential].	• Optical Links. • Iridium, eLoran, White Rabbit.	OSNMA has an added value for this application in particular for securing time transfer.
• GNSS-disciplined oscillators. • Monitoring stations supporting real time integrity. • Redundancy (multiple station coverage). • Alternative PNT solutions [potential].	• No trend Identified.	OSNMA can play a role in synergy with other technologies.

MARKET SEGMENT	APPLICATIONS	BRIEF DESCRIPTION	AUTHENTICATION REQUIREMENTS
 SPACE	**PRECISE ORBIT DETERMINATION ON LOW EARTH ORBIT**	In this application GNSS is used as a source of position for different operations (e.g. formation flying or autonomous navigation).	• Space mission operations need the position to be reliable at all time. • LEO is particularly suitable for spoofing attacks due to the relatively reduced distance from the Earth's surface meaning that an attacker would need a relatively modest power to reach satellites operating there. • GNSS services are available for 95% of satellites in Low Earth Orbit (as a general rule, that availability degrades as the orbit's altitude increases requiring the use of a multi-GNSS solutions). • Precise orbit determination is a driver for several types of future space applications GNSS used in many space applications. • Industry manifests great interest in authentication due to the high value of the missions involved. • Space cyberattacks is an increasing trend therefore GNSS robustness and security will be a need.
	LAUNCHERS	GNSS can be useful as a complementary solution to inertial units. It can also be used to detect deviations from nominal trajectory and triggering emergency procedures.	• Critical application where spoofing can have dramatic consequences by providing the onboard navigation systems false information leading to the destruction of the launcher. • Most launchers use GNSS with the notable exception of the European family (Ariane 5, 6 and Vega). • Space cyberattacks is an increasing threat therefore GNSS robustness and security will be a need.

MARKET SEGMENT	APPLICATIONS	BRIEF DESCRIPTION
 SAR	**MARITIME (EPIRBS)**	This application includes sub-set of GNSS enabled applications i.e.: • Ship and person-registered beacons, namely the Emergency Position Indicating Radio Beacons (EPIRBs) and Personal Locator Beacons (PLBs) that once activated allow to transmit the necessary information for rescue to authorities via satellite communication; and • Automatic Identification System - Search and Rescue Transponders (AIS-SART) and Automatic Identification System - Man Overboard (AIS-MOB) for continuous transmission of alert message including ID number and GNSS-based location which triggers an alarm on all AIS equipped vessels within Very High Frequency Range.
	AVIATION (ELTS AND PLBS)	• This application enables Emergency Locator Transmitters (ELTs) and Personal Locator Beacons (PLBs), in case of accident to utilize GNSS to report their position when triggered.

TECHNOLOGICAL ENVIRONMENT	RECENT TECHNOLOGY TRENDS	POTENTIAL ROLE OF OSNMA
• Military satellites use GNSS receivers with security modules for the encrypted signals. • Radiation hardened components. • Software radio receivers. • Star trackers. • Ground-based tracking. • Technologies for interference detection and mitigation [potential]. • Low-latency authentication is highly expected [potential].	• Interference detection and mitigation and anti-spoofing technologies will be embedded in Space GNSS Receivers.	High expectation for OSNMA and CAS for secure Satellite Tracking and Orbit Determination.
• Inertial systems. • Technologies for interference detection and mitigation [potential]. • Integration of GNSS and IMU [potential].	• Interference detection and mitigation and anti-spoofing technologies, resilient to high-dynamics environments (in particular, high vibration) will be embedded in Space GNSS Receivers.	Interest in OSNMA for trajectory monitoring for emergency self-destruction and tracking of Launchers on re-entering Spacecraft in synergy with other technologies.

AUTHENTICATION REQUIREMENTS
• Safety critical applications require a high level of resilience to spoofing, in addition to integrity. • Galileo RLS operational since 2020. No authentication currently foreseen. • Remote activation may require authentication.
• Safety critical applications require a high level of resilience to spoofing, in addition to integrity. • Remote activation of SAR beacons requires higher resilience to spoofing. • Galileo RLS operational since 2020. No authentication currently foreseen. • Remote activation may require authentication.

4. OSNMA ROADMAP

Despite the high level of maturity of the concept and technical readiness achieved thanks to dedicated Research and Innovation projects (see **Annex I – OSNMA Research and Development**) and close interactions with the industry, an extensive end-to-end testing phase is necessary in order to validate this new function of Galileo "in the field", identify and address any remaining area of improvement and fine tune some parameters in order to best match the users expectations.

A public testing phase is planned to start in 2021 and will last until the start of the service provision (see Chapter 4 for the roadmap to OSNMA).

During that period, OSNMA will be broadcast by Galileo satellites following the OSNMA ICD specifications, thus allowing participants to test and validate their implementation of this function, as well its performance and overall interest for their application(s).

When the testing phase will be launched, all interested parties are welcome to participate in these tests: chipset and terminal manufacturers, integrators, service providers, application developer and end users will have the chance to directly take part into the test campaign and provide their views to the programme.

The relevant documentation (see section 5.1.2) will be made available online for public use on the European GNSS Service Centre (GSC) web site (www.gsc-europa.eu) and will be freely accessible to all users. Support and interactions will also be managed through the GSC, as is the case for other Galileo services. This will also include the supply and management of the cryptographic material necessary to access and process OSNMA (see section 2.4).

Testers will be invited to join and provide feedback, comments and suggestions toEUSPA, by contacting us through electronic mail: MARKET@euspa.europa.eu.

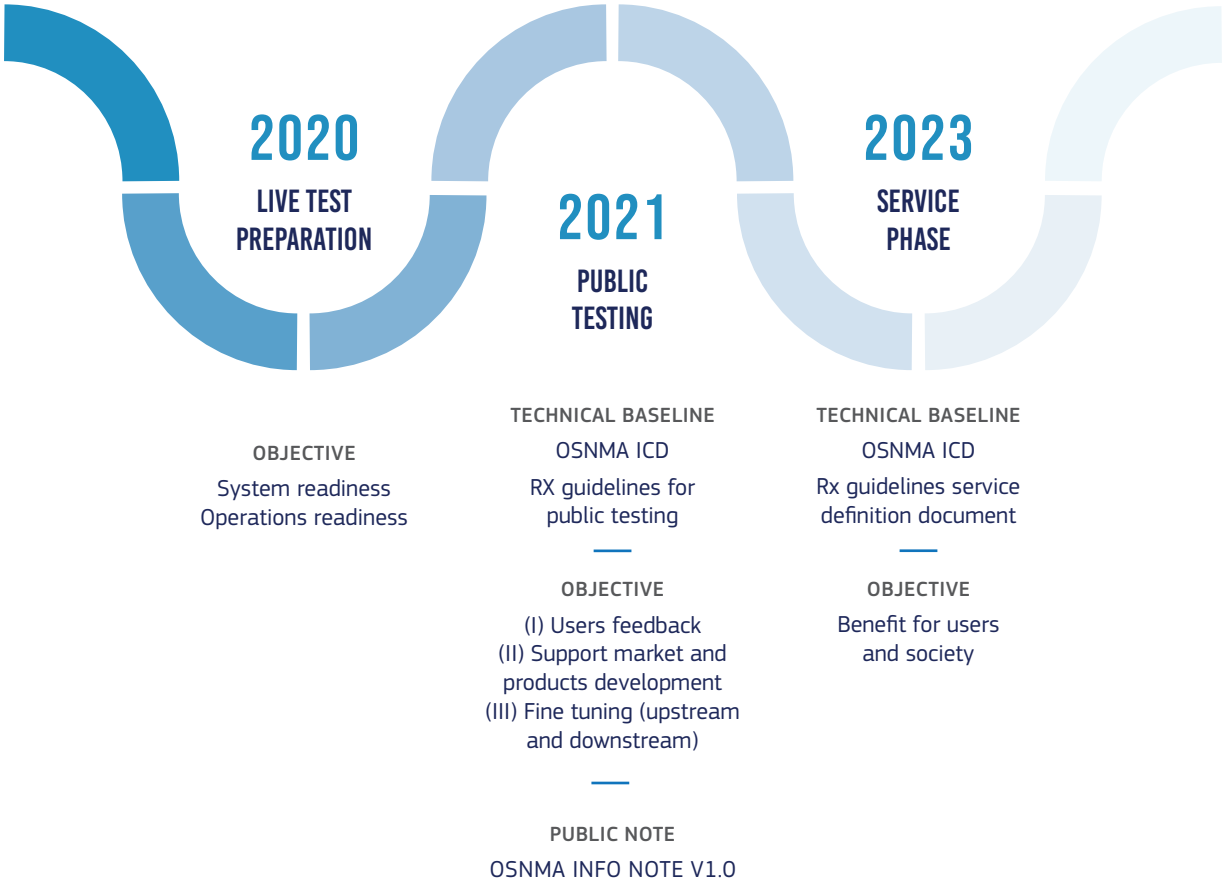
EUSPA will collect users' comments, suggestions and overall response as part of its continuous user and industry consultation activities, e.g. through the User Consultation Platform or via dedicated workshops.

Relevant suggestions will be considered for implementation either for the first service provision phase, or for future evolutions depending upon their feasibility and associated technical and security constraints.

Such user feedback is essential for the Galileo programme to get a wider and more concrete perspective of the future OSNMA market, and will allow to fine tune the OSNMA service provision scheme to best match user needs.

The OSNMA capability will be deployed following the roadmap presented in Figure 4:

Figure 4: The OSNMA Roadmap



The coming public testing phase of this roadmap is of particular interest, which will allow participants to test and validate their implementation of OSNMA and enable EUSPA to finalise the preparation of the subsequent service phase.

5. OSNMA RELEVANT DOCUMENTATION

5.1 DOCUMENTATION

To support the testing (pre-operational) and the operational phases of OSNMA, the following information will be made publicly available on the European GNSS Service Centre (GSC) web site:

5.1.1 PREPARATION PHASE

- OSNMA Information Note (this document)

5.1.2 TESTING PHASE

- OSNMA ICD for the Test Phase
- OSNMA Receiver Guidelines for the Test Phase, including a set of test vectors

5.1.3 SERVICE PHASE

- OSNMA ICD (consolidated after test phase)
- OSNMA Receiver Guidelines including a set of test vectors (consolidated after test phase)
- OS SDD updated to include OSNMA

6. SUMMARY

Open Service Navigation Message Authentication (OSNMA) is a Galileo differentiator which aims to answer a clear user need for a more robust and trustworthy GNSS solution that will bring benefit to a variety of applications. OSNMA will allow users to verify whether the navigation message is actually received by a genuine Galileo satellite or by a potentially malicious source.

Galileo OSNMA is set to be an innovative feature embedded in the Open Service freely accessible to worldwide users, and with no impact on the current Open Service users and performance.

Users will benefit from this enhanced Galileo capability by means of a GNSS receiver or user terminal enabled with a specific firmware without any need for dedicated hardware (as specified in section 2.3).

OSNMA is being implemented in a stepwise approach. Currently, the system is getting ready for a first public testing phase, which will start in the course of 2021. The testing phase will be open to every interested party, who will have the opportunity to implement the algorithm, test it in the field and eventually provide a user feedback to the programme. EUSPA will collect such responses as described in section 4 and as part of its continuous user and industry consultation activities, through the User Consultation Platform or via dedicated workshops. Such feedback will be taken in due consideration for the service consolidation and for future evolutions of the Galileo authentication capabilities, including Galileo 2nd Generation (G2G) OSNMA.

ANNEX I – OSNMA RESEARCH AND DEVELOPMENT

For several years, many activities have been carried out by EUSPA to increase the awareness and foster the implementation of the Galileo Open Service Navigation Message Authentication (OSNMA), and overall to support the GNSS industry with the assessment of the benefits enabled by OSNMA.

These activities encompass the development of applications and the prototyping of close-to-market OSNMA enabled GNSS terminals and have typically been supported by EU funding, through the Horizon 2020 and Fundamental Elements mechanisms. Furthermore it is also noticeable that, well ahead of the actual service declaration, some major industrial stakeholders entirely invested their own resources to prototype and experiment the OSNMA to be ready with innovative products enabled with this technology for their customers, demonstrating great market interest over this GNSS differentiator.

A list of such projects, either directly focussed on OSNMA or which benefitted from OSNMA is given below.

These listed projects are meant to provide visibility on the range of existing prototypes and therefore potential upcoming commercial products enabled with OSNMA capability.

PROJECT NAME	PROJECT DESCRIPTION AND LINK
AALECS: Authentic and Accurate Location Experimentation with the (Galileo) Commercial Service	Development of the platform that confirmed the feasibility of Galileo message authentication. The project implemented the first OSNMA receiver prototype and data generator and also evaluated the first OSNMA performances.
PATROL: Position Authenticated Tachograph foR OSNMA Launch	Development, supply and testing of an OSNMA User Terminal for a Smart Tachograph with a specific focus on the assessment of OSNMA and additional anti-spoofing countermeasures. https://www.patrol-osnma.eu/
INDRIVE: Automotive European GNSS Receiver for High Integrity Applications on the Drive	Development of a robust GNSS solution for automated manoeuvres in automotive applications to be used to estimate the level of confidence of the position. https://www.euspa.europa.eu/indrive-galileo-european-project
ESCAPE: European Safety Critical Applications Positioning Engine	Development of a GNSS-based highly automated positioning engine (L4) suitable for autonomous driving application, building on high accuracy and sensor fusion and leveraging OSNMA to cope with crypto-security aspects. https://www.euspa.europa.eu/newsroom/news/escape-project-launches-positioning-module-autonomous-driving
EGNSS4CAP	Mobile phone application for Android that digitises procedures for farmers in the European Union to satisfy their reporting requirements under the current and post-2020 Common Agricultural Policy (CAP) reform, including authenticated geo-tagging of pictures. https://www.egnss4cap.eu/
FANTASTIC: Field Aware Navigation and Timing Authentication Sensor for Timing Infrastructure and Centimeter level positioning	Development of a professional GNSS receiver in which OSNMA is used to implement time authentication as well as spoofing detection and mitigation algorithms for ensuring the correct functioning of critical infrastructures.

PROJECT NAME	PROJECT DESCRIPTION AND LINK
PRoPART: Precise and Robust Positioning for Automated Road Transports	Development of a GNSS On-Board Unit aimed at enhancing road safety in autonomous trucks driving by exploiting a RTK (Real Time Kinematic) software solution and also exploiting OSNMA. http://propart-project.eu/
TransSec: Autonomous emergency manoeuvring and movement monitoring for road transport security	Development of autonomous systems able to avoid the occurrence of terrorist attacks (mis)employing trucks. http://www.transsec.eu/
ENSPACE: Enhanced Navigation in Space	Development of an innovative software application for enhanced space navigation, positioning, and time to support future space missions (LEO, MEO, GEO/IGSO orbits, interplanetary missions and launchers). http://www.enspace-gnss.eu/
GOEASY: Galileo-based trusted applications for health and Sustainability	Development of mass market solutions aimed at improving citizen well-being; expected to be tested in medium-scale pilots in Torino (Italy) and Stockholm (Sweden). https://goeasyproject.eu/
PREParE SHIPS: PREdicted Positioning based on Egnss for SHIPS	Development and demonstration of a collaborative resilient navigation solution combining distinguished features of different sensor and signal sources. https://prepare-ships.eu/
DELOREAN: Drones and Egnss for LOw aiRspacE urbAN mobility	Development of navigation and positioning requirements for the challenging urban air services, and demonstration of EGNSS as an enabler of this future city sky. https://www.euspa.europa.eu/drones-and-egnss-low-airspace-urban-mobility
GEARS: GalilEo Authenticated Robust timing System	Development of a prototype that aims to provide a Galileo-based timing receiver for Critical Infrastructures for the provision of authenticated time stamping traceability. https://gears-gsa-project.eu
GIANO: Galileo-based tIming receiver for criticAl iNfrastructure rObustness	Increase robustness of critical infrastructure against interference, jamming and spoofing by implementing the two different Galileo authentication solutions. https://gianoproject.eu/
GALIRUMI: Galileo-assisted robot to tackle the weed Rumex obtusifolius and increase the profitability and sustainability of dairy farming	Delivery of robot weeding for herbicide-free weed control in dairy farming. https://www.euspa.europa.eu/galileo-assisted-robot-tackle-weed-rumex-obtusifolius-and-increase-profitability-and-sustainability
GAUSS: Galileo-EGNOS as an Asset for UTM Safety and Security	Development of a high performance positioning system for drones within the U-Space framework focusing on VLL (Very Low Level) and UAS (Unmanned Aircraft System) operations. https://projectgauss.eu/

PROJECT NAME	PROJECT DESCRIPTION AND LINK
ERASMO and **ACCURATE**	Development of an innovative positioning On-Board-Unit (OBU) suitable for fully automated driving, integrating a GNSS receiver together with additional sensors and a communication channel to enable the target applications' performance in the SAE levels 4/5.
ARGOS	Development of a low-cost GNSS based solution to achieve high-level anti-theft protection, adaptable to different types of operations and users from yachts to bikes, from trucks to earth moving vehicles.
OSNMA+	Providing of more robust consumer solutions through the development of the OSNMA+ Service, Software Application, and Receiver connected services.
ROOT: Rolling Out OSNMA for the secure synchronization of Telecom networks	Assess the benefits introduced by Galileo OSNMA in the specific context of telecommunication network synchronization applications, in particular 5G. https://www.gnss-root.eu/

Beyond this already significant effort, EUSPA intends to continue supporting the OSNMA adoption by funding relevant projects through the tools offered by the upcoming Framework Programme Horizon Europe, with the aim to support the downstream sector benefitting from this innovative technology, including the development of innovative use cases and relevant concepts of use leveraging OSNMA.

ANNEX II – ACRONYMS AND ABBREVIATIONS

Table 4: Abbreviations

ABBREVIATION	DEFINITION
3GPP	3rd Generation Partnership Project
5G	5th Generation (3GPP standard)
A-GNSS	Assisted GNSS
AIS-SART	Automatic Identification System - Search and Rescue Transponders
AIS-MOB	Automatic Identification System - Man Overboard
ADS-B	Automatic Dependent Surveillance-Broadcast
API	Application Programming Interface
APNT	Alternative PNT
ARAIM	Advanced Receiver Autonomous Integrity Monitoring
CAN (bus)	Controller Area Network (bus)
CAP	Common Agricultural Policy
CAS	Commercial Authentication Service
CED	Clock and Ephemeris Data
ConOps	Concept of Operations
CORS	Continuously Operating Reference Station
COTS	Commercial Off The Shelf
CRPA	Controlled Radiation Pattern Antenna
CS	(Galileo) Commercial Service
CSAC	Chip Scale Atomic Clock
DSRC	Dedicated Short Range Communication
DVB	Digital Video Broadcast
(Geo) DRM	(Geographical) Digital Rights Management
EC	European Commission
EDBS	External Data Broadcast Service
EGNOS	European Geostationary Navigation Overlay Service
EGNSS	European GNSS
ELT	Emergency Locator Transmitter
EPIRB	Emergency Position Indicating Radio Beacons
ERTMS	European Rail Traffic Management System
EU	European Union
EUSPA	European Union Agency for the Space Programme (before GSA)
FAA	Federal Aviation Authority
FE	Fundamental Elements
G2G	Galileo 2nd Generation
GEO	Geostationary Orbit (or Geosynchronous Equatorial Orbit)
GIS	Geographical Information System
GNSS	Global Navigation Satellite System (e.g. GPS, Galileo, GLONASS etc.)
GSC	European GNSS Service Centre
H2020	Horizon 2020

ABBREVIATION	DEFINITION
IALA	International Association of Marine Aids to Navigation and Lighthouse Authorities
ICAO	International Civil Aviation Organisation
ICD	Interface Control Document
IGSO	Inclined Geosynchronous Orbit
IMO	International Maritime Organisation
IMU	Inertial Measurement Unit
INS / INU	Inertial Navigation System / Inertial Navigation Unit
IoT	Internet of Things
IP (address)	Internet Protocol (address)
ITS	Intelligent Transport System
LBS	Location Based Services
LEO	Low Earth Orbit
LTE	Long Term Evolution (3GPP standard)
MEO	Medium Earth Orbit
N/A	Not Available
NFC	Near Field Communication
NTP	Network Time Protocol
OBU	On Board Unit
OCXO	Oven Controlled X-tal (Crystal) Oscillator
OS	(Galileo) Open Service
OSNMA	Open Service Navigation Message Authentication
OTAR	Over The Air Rekeying
PKI	Public Key Infrastructure
PLB	Personal Locator Beacon
PNT	Position Navigation and Timing
PPP	Precise Point Positioning
PTP	Precision Time Protocol
PVT	Position Velocity and Time
RAIM	Receiver Autonomous Integrity Monitoring
RCA	Root Certificate Authority
RFID	Radio Frequency Identification
RTCA	Radio Technical Commission for Aeronautics (now RTCA, Inc.)
RTK	Real Time Kinematic
RUC	Road User Charging
SAE	Society of Automotive Engineers
SAR	Synthetic Aperture Radar
SDD	Service Definition Document
SIS	Signal In Space
T/S	Timing and Synchronisation
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UTM	Unmanned aerial system Traffic Management
VLL	Very Low Level
VRT	Variable Rate Technology

TS-02-21-688-EN-N

The European Union Agency for the Space Programme

The European Union Agency for the Space Programme (EUSPA) provides safe and secure European satellite navigation services, promotes the commercialization of Galileo, EGNOS, and Copernicus data and services and coordinates the EU's forthcoming governmental satellite communications programme GOVSATCOM. EUSPA is responsible for the security accreditation of all the EU Space Programme components. By fostering the development of an innovative and competitive space sector and engaging with the entire EU Space community, EUSPA contributes to the European Green Deal and digital transition, the safety and security of the Union and its citizens, while reinforcing its autonomy and resilience.

Galileo

Galileo is the European Union's Global Satellite Navigation System (GNSS) that provides accurate positioning and timing information. Galileo is a programme under civilian control and its services can be used for a broad range of applications. It is autonomous but also interoperable with existing satellite navigation systems.

On 15 December 2016, the Declaration of Initial Services marked the beginning of Galileo's operational phase. This means that anyone with a Galileo-enabled device is now, in combination with other GNSS systems, able to use signals provided by Galileo's global satellite constellation for positioning, navigation and timing.

The fully deployed Galileo system will provide five different services:

- Open Service (OS) that targets the mass market. The OS offers either single (E1) or dual frequency (E1 and E5) and will be the first to broadcast authentication data through its Navigation Message Authentication (OS NMA).
- HAS (High Accuracy Service) will complement the OS and provide a higher positioning accuracy being broadcast on the E6-B signal component.
- CAS (Commercial Authentication Service) will make it possible to authenticate signals, by giving access to the E6 signal pilot component (E6-C) codes, which will be encrypted.[6]
- Public Regulated Service (PRS) will be dedicated to government-authorised users. It will be encrypted and secured against jamming and spoofing.
- Search and Rescue (SAR) service will allow near real time alert localisation and message detection, higher beacon localisation accuracy, high availability and global satellite coverage. It will have a return link, which is unique to Galileo, and will reduce the rate of false alerts.

useGALILEO.eu

Devices containing a Galileo-enabled chipset, such as smartphones or vehicle navigation devices, can use Galileo signals for positioning, navigation and timing. The www.useGALILEO.eu tool helps you find Galileo-enabled chipsets, smartphones, wearables and tracking devices.

6 According to the Commission Implementing Decision (EU) 2017/224 of 8 February 2017 setting out the technical and operational specifications allowing the commercial service offered by the system established under the Galileo programme to fulfil the function referred to in Article 2(4)(c) of Regulation (EU) No 1285/2013 of the European Parliament and of the Council CS comprises two major improvements – the High Accuracy Service and Commercial Authentication Service.

www.euspa.europa.eu

EU4Space

EU4Space

EUSPA

EUSPA

Space4EU

ISBN 978-92-9206-052-7
doi:10.2878/49446