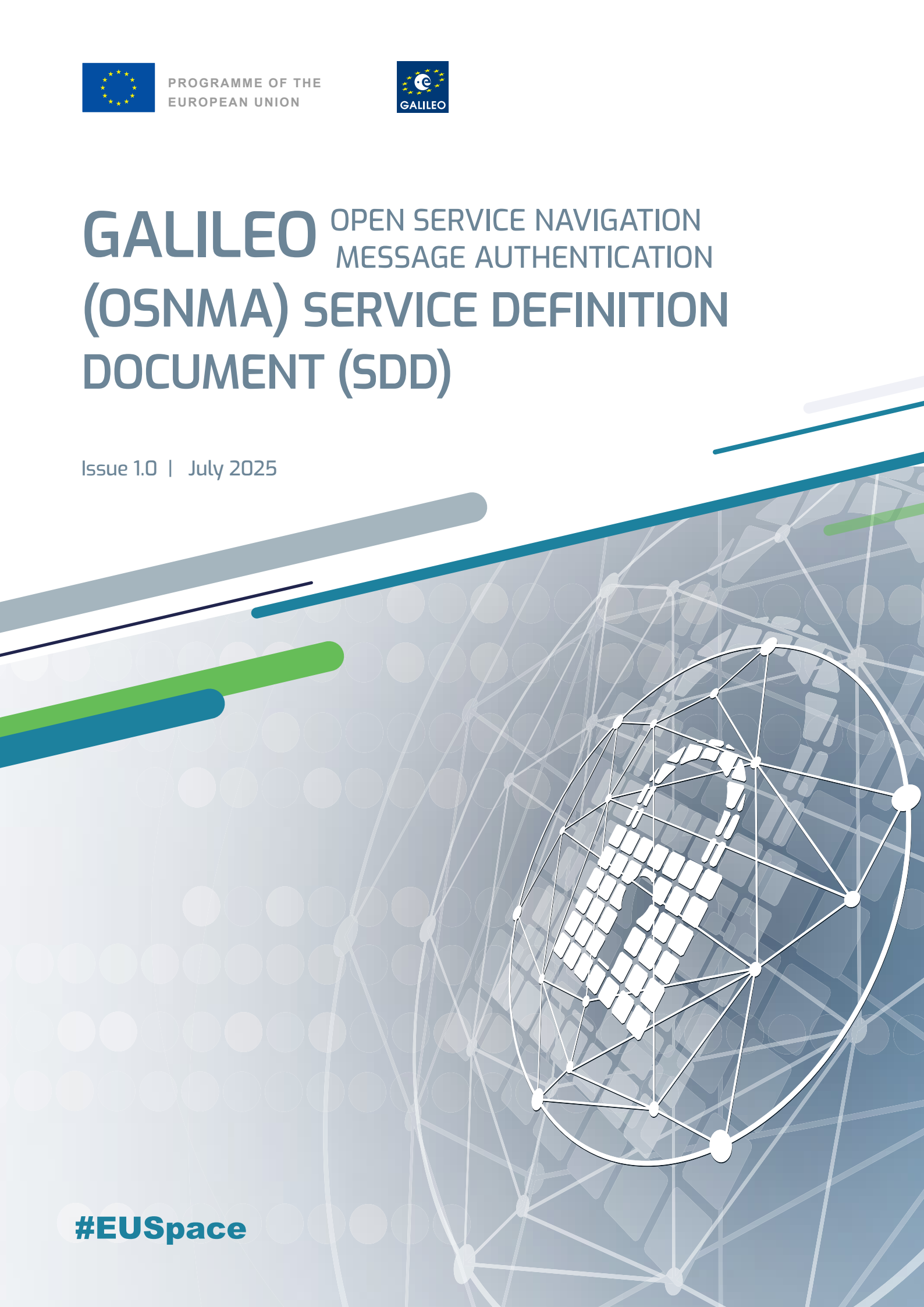
PROGRAMME OF THE EUROPEAN UNION

GALILEO

GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OSNMA) SERVICE DEFINITION DOCUMENT (SDD)

Issue 1.0 | July 2025



#EUSpace

TERMS OF USE AND DISCLAIMERS

The Galileo Open Service Navigation Message Authentication (OSNMA) service, unless complemented by certified or otherwise legally approved dedicated systems designed to this effect, has been designed and can only be used for non-safety critical purposes, i.e. purposes that have no impact on the safety of human life and where an underperformance in availability, continuity, accuracy and/or integrity of the Galileo Signal in Space (SIS) or the data provision through the Internet Data Distribution interface, could not cause any kind of direct or indirect personal damage, including bodily injuries or death.

Scope of Galileo OSNMA Service Commitment

Although care has been taken in designing, implementing, and operating the system, as well as in providing the Galileo OSNMA service, the Galileo OSNMA service is not meant to offer any service guarantee to the users.

The minimum level of performance against which the system has been validated and is operated, as well as data of actual performance of the Galileo OSNMA service are expressed in statistical values that are valid under assumptions described in this document, **the Galileo OSNMA SDD**. The European Commission reserves the right to revise the Galileo OSNMA SDD should these assumptions change or to reflect changes in performance during the deployment of the Galileo infrastructure. This commitment regarding the minimum level of performance shall be without prejudice to the disclaimer of liability below, measures potentially affecting service availability that may be taken either by the Security Accreditation Board, or according to the Council decision 2021/698/CSFP, or in the interests of Member States' national security.

The European Union plans to take all necessary measures for the foreseeable future to maintain or exceed the minimum levels of the Galileo OSNMA service performance described herein.

The minimum level of performance of the Galileo OSNMA service, as specified in the Galileo OSNMA SDD, may be obtained under the condition that the user equipment processes the health and status flags as described in the section 2.1.4 below. The users are also advised to check the Galileo notices (Notice Advisory to Galileo Users (NAGUs), and Service Notices), which are published through the EGNSS Service Centre for planning the use of the Galileo OSNMA service for any purpose.

User responsibilities

The user retains the responsibility to exercise a level of care appropriate with respect to the uses she/he intends to make of the Galileo OSNMA service, under the considerations outlined above.

The users are reminded that the authentication performance they will experience is also driven by other parameters outside the control of the Galileo OSNMA service provider (e.g., signal propagation errors or user receiver induced errors), which must be considered when deciding to use the Galileo OSNMA service for a given purpose.

Before any use of the Galileo OSNMA service, users should study this document to understand how they can use the service, as well as to familiarise themselves with the performance level and other aspects of the service they can rely on.

In case of doubt, the users and other parties should contact the Galileo helpdesk (see section 1.6.1 for contact details) and their user equipment manufacturer.

Disclaimer of liability

As the owner of the Galileo system, the European Union - including any of its institutions, offices or agencies, such as the European Commission, the European Union Agency for the Space Programme (EUSPA), and other entities acting on the basis of a contract or agreement with the European Union involved in the Galileo OSNMA service provision - does not offer any warranties of any kind (whether expressed or implied) with respect to the Galileo OSNMA service, including, but not limited to, the warranties regarding availability, authenticity of any navigation solution provided by a compatible receiver[1], continuity, accuracy, integrity, reliability and fitness for a particular purpose or meeting the users' requirements. No advice or information, whether oral or written, obtained from the European Union - including any of its institutions, offices, or agencies, such as the European Commission, the European Union Agency for the Space Programme (EUSPA), and other entities acting on the basis of a contract or agreement with the European Union involved in the Galileo OSNMA service provision - shall create any such warranty.

By using the Galileo OSNMA service, the user accepts and agrees that the European Union - including any of its institutions, offices or agencies, such as the European Commission, the European Union Agency for the Space Programme (EUSPA), and other entities acting on the basis of a contract or agreement with the European Union involved in the Galileo OSNMA service provision - shall not be held responsible or liable for any damages resulting from the use of, misuse of, or the inability to use the Galileo OSNMA service, including, but not limited to, direct, indirect, special or consequential damages, including, but not limited to, damages for interruption of business, loss of profits, goodwill or other intangible losses, other than in accordance with Article 340 of the Treaty on the Functioning of the European Union.

ISBN: 978-92-9206-080-0

doi: 10.2878/485549

[1] It shall be noted that the Galileo OSNMA Service provides security mechanisms for the authentication of the OS Navigation Message but does not guarantee by itself the authenticity of a navigation solution computed with Galileo, as this depends on the user equipment implementation which is the responsibility of the manufacturers. At this stage, Galileo does not intend to develop certification schemes for the implementation of the OSNMA Service in user equipment.

DOCUMENT CHANGE RECORD

REASON FOR CHANGE	ISSUE	REVISION	DATE
First version of the document	1	0	July 2025

FOREWORD

This OSNMA SDD defines the Minimum Performance Levels (MPLs) of the Galileo OSNMA.

The document will be updated in the future to reflect further changes and improvements of the Galileo OSNMA and/or inclusion of new Galileo Authentication Services.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 THE GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION

Galileo is the European Global Navigation Satellite System (EGNSS), under civil control, that provides satellite positioning services to European citizens and worldwide.

Position, Velocity and Timing (PVT) based on GNSS is used by many applications in transportation, finance, telecommunications, information technology, energy, utilities, manufacturing, health services, emergency services, defence, and law enforcement. However, GNSS signals are vulnerable to interferences or intentional attacks such as spoofing[2].

Improving robustness against GNSS spoofing has become a priority for most GNSS stakeholders. On the GNSS providers side, the Galileo Programme has been a pioneer in the field by including a portfolio of authentication capabilities within Galileo starting with OSNMA and PRS[3] that will be expanded in the future with further services (see section 1.5 for details).

With OSNMA, Galileo provides Navigation Message Authentication (NMA) for relevant elements of the broadcast OS navigation data. Subject to the terms and conditions of the present document, this gives the OSNMA enabled receivers 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 data level and significantly contributing to the security of the solution.

In order to successfully authenticate the Open Service navigation data, the user must extract the relevant OSNMA protocol elements from the SIS and the IDD (Internet Data Distribution) interfaces (see section 2 of this document) and follow the processing steps described in the OSNMA Receiver Guidelines document (see [RD-03]).

This SDD describes the terms and conditions in which the Galileo OSNMA Initial Service is provided. Future releases of this document will be issued to consider further evolutions of OSNMA (i.e., authenticating other navigation data types) and/or to include new Galileo Authentication Services as per section 1.5 (excluding PRS).

1.1 PURPOSE OF THE DOCUMENT

The purpose of this Galileo OSNMA Service Definition Document is to describe the characteristics and performance of the Galileo OSNMA. This version presents the Minimum Performance Levels (MPLs) targeted for the OSNMA Initial Service and defines the conditions under which such MPLs can be reached.

This document consists of a main body and four annexes comprising the following sections:

- Section 1: Introduction to OSNMA, future Galileo Authentication services and High-Level description of the Galileo System
- Section 2: The Galileo OSNMA characteristics and MPLs
    - Section 2.1: OSNMA Characteristics and Minimum Usage Assumptions
    - Section 2.2: OSNMA Minimum Performance Levels

[2] Spoofing of GNSS signals is the broadcast of false signals with the intent that the victim's receiver will misinterpret them as authentic signals. The victim might deduce a false position fix, a false clock offset, or both.

[3] The PRS is outside the scope of this document, and it is presented here for information only. More details on the difference between PRS, OSNMA and future authentication services can be found in section 1.5.

- Annex A Reference Documents
- Annex B Abbreviations and Acronyms
- Annex C Description of Advisory Notice to Galileo Users
- Annex D Time to First Fix with Authenticated Data

1.2 SCOPE OF THE DOCUMENT

The Galileo OSNMA SDD applies to the OSNMA service as provided at the time of its publication. This SDD belongs to the series of Galileo Programme Reference Documents published for the benefit of Galileo users, to present and explain various aspects of the EGNSS concerning the Galileo OSNMA. The other Programme Reference Documents currently linked to OSNMA are:

- The European GNSS (Galileo) – Open Service Navigation Message Authentication Signal-In-Space Interface Control Document.

  Describing the interface between the Galileo Space Segment and the Galileo User Segment for the Navigation Message Authentication capabilities.
- The European GNSS (Galileo) – Open Service Navigation Message Authentication User Receiver Guidelines.

  Providing the requirements and steps to be followed by the user segment for the secure processing of the broadcast Navigation Message Authentication data to achieve the authentication capabilities.
- The European GNSS (Galileo) – Open Service Navigation Message Authentication Internet Data Distribution Interface Control Document.

  Describing the interface between the OSNMA data provided through the Internet and the Galileo User Segment.
- The European GNSS (Galileo) Open Service – Service Definition Document.

  Describing the Galileo Open Service, providing an overview of the OS SIS and presenting the Minimum Performance Levels for the OS.

All public Galileo Programme Reference Documents are made available to users through the web portal of the European GNSS Service Centre (http://www.gsc- europa.eu).

1.3 TERMS AND CONDITIONS OF USE

The terms and conditions of use of the Galileo OSNMA are described at the beginning of this document.

1.4 ACRONYMS AND ABBREVIATIONS

Abbreviations and acronyms used in this document are provided in Annex B

1.5 FUTURE GALILEO AUTHENTICATION SERVICE DEFINITION AND MAIN CHARACTERISTICS

With the new Open Service Navigation Message Authentication (OSNMA), Galileo introduces for the first time a data authentication feature in its Open Service (OS) signals openly accessible to the public. This

feature is intended to be exploited by receivers to verify the signals' data authenticity. Galileo OSNMA is expected to be followed in the coming years by new features designed to offer additional protection barriers. When fully implemented, Galileo will deliver the following authentication services:

- OSNMA: A service transmitted in the E1-B component of Galileo 1st Generation signals and authenticating Galileo Open Service data.
- Open Service – Authentication (OS-A): A service to be transmitted in Galileo 2nd Generation signals and authenticating Galileo Open Service signals and data.
- Signal Authentication Service (SAS): A service based on the encrypted E6-C component of Galileo 1st Generation signals and authenticating the E6-C signal.

Such new services are intended for consumer and professional applications, with the specific characteristics provided in Table 1 below. It is remarked that the level of protection for OSNMA, OS-A and SAS is considered below governmental standards and needs, but sufficient for consumer and professional applications.

It shall be noted that the Galileo services above provide security mechanisms but do not guarantee by themselves the authenticity of a navigation solution computed with Galileo, as this depends on the user equipment implementation which is the responsibility of the manufacturers. At this stage, Galileo does not intend to develop certification schemes for user equipment.

Galileo also provides the Public Regulated Service (PRS) that addresses governmental applications requiring higher levels of protection in terms of confidentiality, integrity, availability, authenticity, and non-repudiation, and including defence applications. Top security standards apply to the development of PRS user equipment. PRS is therefore the Galileo service providing the strongest protection against security threats and increased robustness against interference. Governmental users requiring access to PRS shall contact their national Competent PRS Authority. It is important to highlight that PRS will remain outside the scope of this document, and it is provided here only for information.

Table 1 - Summary of the Galileo Authentication Services main characteristics

		OSNMA	OS-A	SAS	PRS[4]
ACCESS		PUBLIC	PUBLIC	PUBLIC	GOVERNMENTAL
CONFIDENTIALITY		NO	NO	NO	YES
AUTHENTICATION	Data	YES	YES	YES	YES
	Ranging	NO	YES	YES	YES
	Real time	NO	NO	NO	YES
	Bands used	E1	E1, E5	E6	E1, E6
	Authentication key protection	Public/ Commercial	Public/ Commercial	Public/ Commercial	Governmental
CRYPTOGRAPHIC ALGORITHMS		PUBLIC	PUBLIC	PUBLIC	GOVERNMENTAL
RECEIVER CERTIFICATION		NO	NO	NO	YES
APPLICATIONS		PUBLIC	PUBLIC	PUBLIC	GOVERNMENTAL (requiring higher levels of protection)

1.6 GALILEO SYSTEM OVERVIEW

The Galileo OSNMA is provided through the current Galileo 1st Generation System.

[4] The PRS will remain outside the scope of this document, and it is provided here for information only.

The Galileo system is composed of a Core Infrastructure and several Service Facilities. The Core Infrastructure, in turn, comprises a Space Segment and a Ground Segment.

Further details on the Galileo System are provided in [RD-04].

The elements of the Galileo System related to the provision of OSNMA are described in the following sub-sections.

1.6.1 THE EUROPEAN GNSS SERVICE CENTRE (GSC)

The European GNSS Service Centre (GSC), part of the European GNSS infrastructure, provides the single centralised ground interface between the Galileo user communities (for OS, OSNMA, High Accuracy Service and the future Signal Authentication Service) and the Galileo system infrastructure and operator, for the provision of specific services beyond the SIS transmitted by the Galileo satellites. It is accessible through its web portal www.gsc-europa.eu.

The GSC plays a central role in the provision of the Galileo OSNMA as it hosts the OSNMA module in charge of generating the necessary elements to perform the authentication of the Navigation Messages (see section 2.1.1).

The functionality and services covered by the GSC towards the OSNMA users are:

- Helpdesk support: For answering general queries and incident notifications from users on Galileo SIS and specific queries from Galileo receiver and application developers on the official Galileo user documents. In addition, registered users can subscribe to be informed in real time about events affecting the Galileo services.
- Information on Galileo system status: Publication of Galileo almanacs and ephemeris data, of constellation status and provision of Galileo Service Notices.
- Reports on the Galileo Open Service navigation key performance indicators and on the GSC performance itself are also published for the users' information.
- Electronic Library, including Programme Reference documentation and general information.
- Support to GNSS developers, including the GNSS Simulation and Testing infrastructure (GSTI).
- Interface with other GNSS Service Providers.
- Galileo user satisfaction monitoring, including customised performance assessment, reporting and forecasts for specific communities, and support to the Galileo services development for each community or domain.
- Interfaces for OSNMA key management towards users (in complement to the Signal in Space capabilities) can be found in the GSC web portal. See section 2.1.3 for further information.

The GSC is responsible for the publication of Notice Advisory to Galileo Users (NAGU) messages. NAGUs are used to notify Galileo OSNMA users about planned and unplanned outages/degradations.

Different kinds of NAGUs are issued depending on the specific event to be communicated. The description of the structure and content of the NAGUs for OSNMA is provided in Annex C . This information, together with the list of active and archived NAGUs can be also found in the GSC web portal, www.gsc-europa.eu, under “System Status”. Users have the possibility to subscribe to the automatic notification of NAGUs via e-mail.

Minimum Performance Levels for the timely publication of NAGUs for both unplanned and planned outages events are reported in Section 2.2.3.

Further details on the GSC are provided in [RD-04].

2 GALILEO OSNMA CHARACTERISTICS AND MPLS

This section starts by providing an overview of the Galileo OSNMA processing logic at user level and SIS/Internet interfaces characteristics, along with the performance characteristics and the minimum usage assumptions for the users of the Galileo OSNMA. This short description is given for information purposes. The user shall always refer to the OSNMA SIS ICD [RD-01], the OSNMA IDD ICD [RD-02] and the OSNMA Receiver Guidelines [RD-03] for details of the Galileo OSNMA protocol and the different interfaces characteristics.

A description is then provided of the different Minimum Performance Levels (MPLs) with the associated justification and together with the target values.

2.1 OSNMA CHARACTERISTICS AND MINIMUM USAGE ASSUMPTIONS

This section provides a high-level description of the OSNMA processing logic at user level. A brief description of the relevant Galileo signals and the SIS interface with the OSNMA protocol is also described. High-level information is then provided on the OSNMA data that is accessible via the Internet Data Distribution interface. The section then provides the performance characteristics and the minimum usage assumptions that condition the use of the OSNMA service and the achievement of the MPL targets.

2.1.1 GALILEO OSNMA PROCESSING LOGIC AT USER LEVEL

The processing logic of OSNMA at receiver level is depicted in Figure 1.

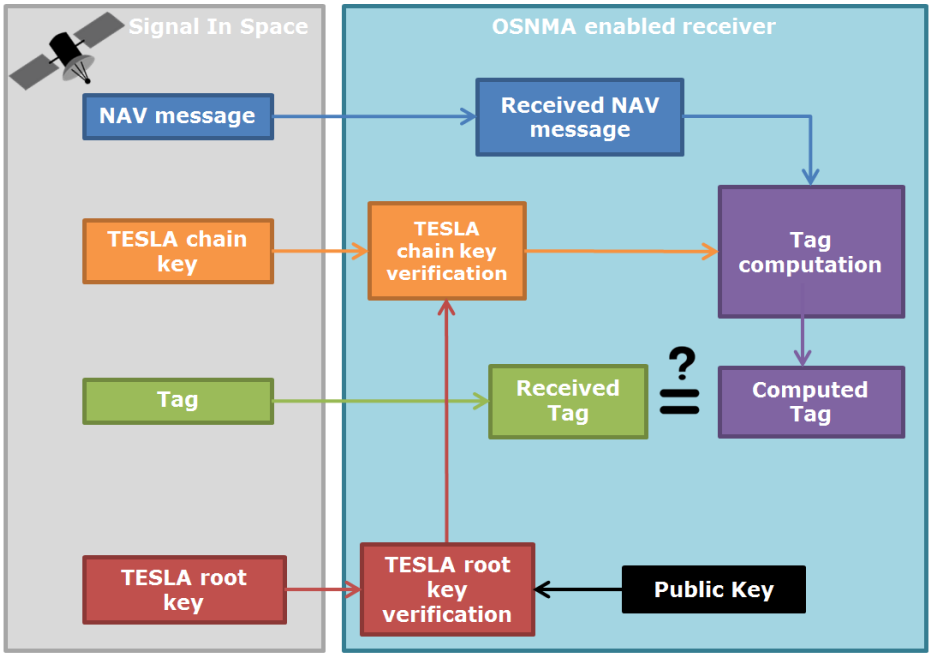


Figure 1 - OSNMA processing logic

To validate the authenticity of the navigation message received on the L-band, the OSNMA receiver has to perform a Digital Signature verification, a TESLA chain key verification, and a Message Authentication Code (MAC[5]) verification. Firstly, the TESLA root key signature verification is done using the Public Key (PK) received from the GSC User Interface or the SIS. Then, the TESLA key contained in the received E1/NAV message can be verified with this TESLA root key. In this way, the receiver can proceed to compute the local MAC, by means of the received NAV message, and the TESLA key earlier verified. In the case that the computed MAC matches the received one, then the navigation message is validated, otherwise the verification fails. Full details on the OSNMA processing logic at receiver level can be found in [RD-03].

In order to verify the authenticity of additional elements provided through the OSNMA SIS, as new Public Keys or the OSNMA Alert Message, the user receiver must also store the Merkle Tree root (see sections 2.1.3 and 2.1.4).

It is to be noted that OSNMA data are distributed only by a subset of Galileo satellites. The satellites distributing the OSNMA are changing dynamically over time. The OSNMA protocol is built such that, even if OSNMA data are transmitted only by a subset of the satellites of the Galileo constellation, the data from all satellites can be authenticated. This is realised by means of the so-called cross-authentication: the satellites transmitting OSNMA data can distribute MACs authenticating the navigation data from other satellites.

2.1.2 SIGNAL IN SPACE

2.1.2.1 RELEVANT SIS INTERFACE CONTROL DOCUMENTS

The OSNMA SIS is compliant to the technical requirements related to the interface between the Space Segment and the OSNMA receivers as established by the OSNMA SIS ICD [RD-01].

2.1.2.2 RELEVANT GALILEO SIGNALS FOR OSNMA

Galileo transmits several signals and codes on four different carrier frequencies within the 1.1 to 1.6 GHz band, namely:

- E1, centred at 1575.42 MHz;
- E5a and E5b, at 1176.45 MHz and 1207.14 MHz respectively, multiplexed together through an AltBOC scheme and transmitted at the E5 carrier frequency centred at 1191.795 MHz;
- E6, centred at 1278.75 MHz.

A complete representation of the Galileo signal baseline is provided in Figure 2.

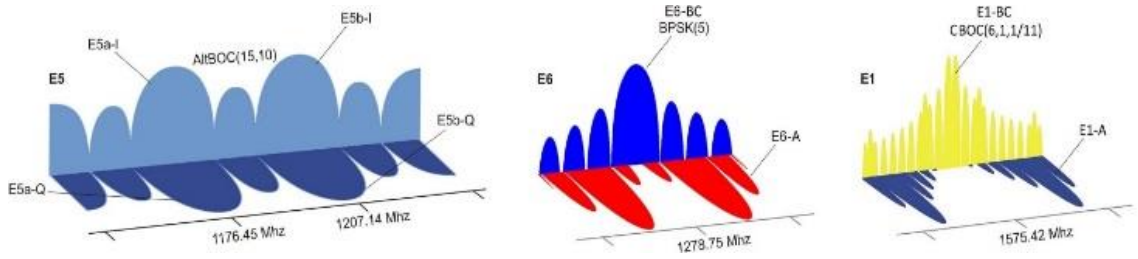


Figure 2 - Signals transmitted by Galileo satellites

The Galileo SF (Single Frequency) OS is provided by each of the three signals: E1, E5a and E5b, whereas the Galileo DF (Dual Frequency) OS is provided by each of the following signal combinations broadcast by the same satellite:

- E1 and E5a.

[5] Also referred to as “tag”.

- E1 and E5b.

The signals relevant for the OSNMA service are presented in Table 2 with more detailed information.

Table 2 - Galileo Services channels relevant for OSNMA

Band	Carrier freq. (MHz)	Signal Component	Modulation Type	Code rate (Mcps)	Data rate (bps)	Services
E1	1575.420	E1-B data	CBOC (6,1,1/11)	1.023	125	OS, OSNMA
		E1-C pilot			-	
E5b	1207.140	E5b-I data	BPSK (10)	10.23	125	OS
		E5b-Q pilot			-	

The OSNMA data is transmitted on E1-B and authenticate the I/NAV data transmitted on E1-B and E5b-I.

2.1.2.3 OSNMA MESSAGE STRUCTURE

Galileo OSNMA protocol data are transmitted within the odd pages of the nominal E1-B I/NAV message.

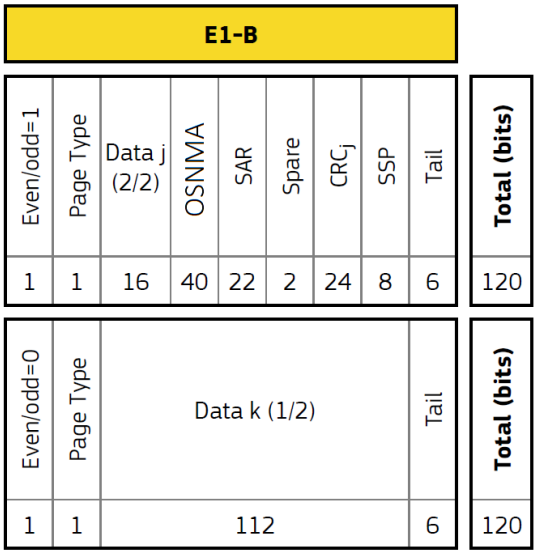


Figure 3 - E1-B I/NAV Nominal Page with bits allocation, including OSNMA data

Figure 3 displays the layout of the E1-B I/NAV nominal page, as described in [RD-01] and [RD-05]. The OSNMA data is transmitted within the "OSNMA" field. It is important to recall that the OSNMA field is also protected by the CRC, as described below.

OSNMA is not provided in I/NAV Dummy Messages or in I/NAV Alert Pages. Any data retrieved from the OSNMA field of Dummy or Alert Pages shall be therefore discarded. Both I/NAV dummy message and alert page are described in [RD-05].

Within each E1-B I/NAV nominal odd page part, including pages used to transmit the I/NAV Spare Words, an OSNMA message is transmitted. The OSNMA field has the following structure:

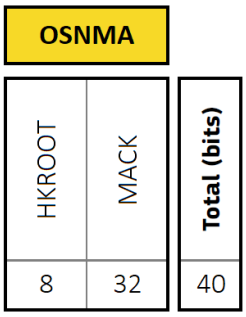


Figure 4 - OSNMA data message

Two sections compose the OSNMA message: the HKROOT section (first 8 bits) and MACK section (next 32 bits).

- HKROOT section provides:
  - NMA header with the different flags indicating the NMA status (see section 2.1.4)
  - DSM field transmitting the TESLA root key and the Public Key
- MACK section provides:
  - MAC
  - TESLA key chain

As stated in section 2.1.1, the OSNMA data are distributed only by a subset of Galileo satellites. It is to be noted that when a satellite is not transmitting OSNMA data, the I/NAV OSNMA message transmitted will contain a 40-bit sequence of zeros.

Full details of the HKROOT and the MACK messages are described in [RD-01], where a description of the message structure and the message data contents is provided, including semantics, formats, and specific characteristics.

Within an E1-B I/NAV nominal sub-frame, 15 pages are transmitted every 30 seconds, with the OSNMA data message included within the odd part of the page. This means that 15 OSNMA data messages as the one represented in Figure 4 are transmitted over 30 seconds. Therefore, a 120-bit HKROOT message and a 480-bit MACK message are transmitted every 30 seconds. Both HKROOT and MACK messages are split into 15 portions of equal size (8 or 32 bits) and transmitted within each 40-bit OSNMA data message.

To detect corruption of the received data, a checksum is used by the Galileo navigation message, employing a CRC technique. The detailed description of this checksum is provided in the OS SIS ICD [RD-05]. It is important to recall that the OSNMA message is also protected by this CRC.

The CRC is not used to indicate any problem at satellite level, but on the receiver side. The CRC checksum is related exclusively to the errorless reception of the transmitted bits, i.e., to the transmission channel, not to the correctness of the structure or the contents of the message as transmitted by the Galileo system. The CRC within the navigation message of Galileo is therefore not involved in the definition of the SIS Status.

If the CRC checksum is not passed successfully, the respective data must be rejected. Once a navigation message is received with a successful CRC, the user can then proceed to the SIS Status determination, as described in section 2.1.4, and eventually to the utilisation of such SIS.

2.1.3 THE INTERNET DATA DISTRIBUTION (IDD) INTERFACE

The OSNMA IDD interface provides the users with the Public Key, the Merkle Tree root and the associated PKI (Public Key Infrastructure) certificates, that are required for the processing of the OSNMA SIS.

A high-level description of the IDD interface is provided in this section. Full details on how to access and use the cryptographic material and certificates provided via the IDD interface can be found in the Galileo OSNMA IDD ICD [RD-02].

2.1.3.1 PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATES

A PKI is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke certificates. The purpose of a PKI is to make sure that the certificate can be trusted.

A digital certificate is an electronic data structure that binds an entity, being an institution, a person, a computer program, a web address, etc., to its public key. Digital certificates are used for secure communication, using public key cryptography and digital signatures.

Within the scope of the OSNMA, the PKI provides the OSNMA users with digital certificates organised hierarchically that allow to verify the authenticity of the public cryptographic material provided through the GSC interface (see section 2.1.3.2 and 2.1.3.3) that is needed to authenticate the OSNMA data coming from the SIS. This is the so-called chain of trust, and it is represented in Figure 5.

The boxes in blue, RCA (Root Certificate Authority) and SCA (Subordinate Certificate Authority) correspond to the higher hierarchical elements of the PKI that are associated to the European Space Programme and the Galileo Programme respectively. The green boxes represent the elements of the PKI that are exclusively linked to the OSNMA service.

A more detailed description of the PKI and specific information on how to access and use the PKI certificates can be found in the Galileo OSNMA IDD ICD [RD-02].

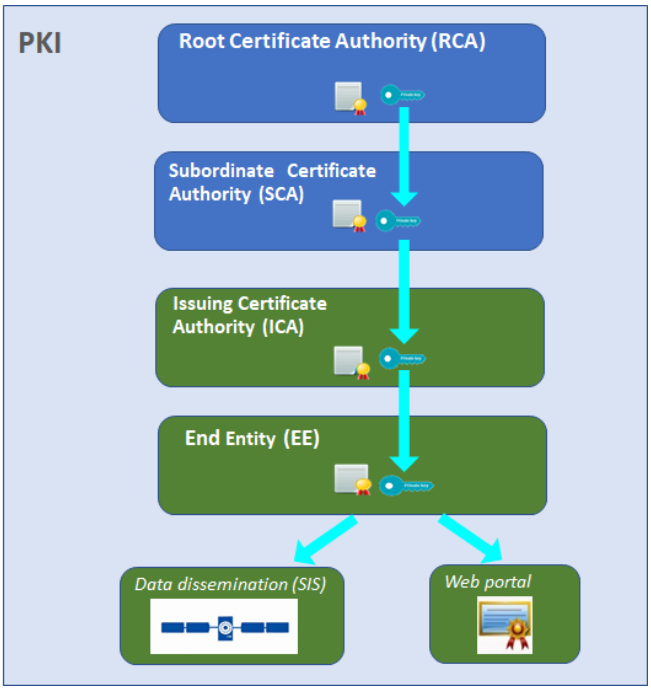


Figure 5 - PKI chain of trust

2.1.3.2 PUBLIC KEY PRODUCT

The receiver shall have a Public Key, with its associated ID and signature algorithm, in order to process the OSNMA SIS. This information can be retrieved from:

- The SIS where the Public Key is transmitted at defined time intervals (see [RD-01]) or during renewal and revocation processes.
- The GSC interface.

The users can check the parameters of the Public Key currently in force and download the following elements from the GSC user interface:

- Public Key in XML format.

- Public Key Certificate embedding the ICA (Issuing Certificate Authority) and EE (End Entity) certificates shown in Figure 5.
- Public Key Certificate Revocation List (CRL).
- Certificate Policy and Certification Practice Statement (CP/CPS).

The user can also check in the GSC user interface the future Public Key that will be applicable after a renewal process and can download the associated files (Public Key, Public Key Certificate and Public Key CRL).

Finally, the user can check in the historical record of the GSC user interface the past Public Keys that are no longer applicable.

2.1.3.3 MERKLE TREE PRODUCT

In order to verify new Public Keys retrieved from the SIS, as well as the authenticity of the OSNMA Alert Message, the user must have the root node of the Merkle Tree (see [RD-01] and [RD-03]). This information can only be loaded in the receiver after being retrieved from the GSC user interface.

The users can check the parameters of the Merkle Tree currently in force and download the following elements from the GSC user interface:

- Partial Merkle Tree in XML format including the root node of the Merkle Tree[6] .
- The Merkle Tree Certificate embedding the ICA and EE certificates shown in Figure 5.
- Merkle Tree Certificate Revocation List (CRL).

The user can also check and download the future Merkle Tree that will be applicable after a renewal process. It is to be noted that the renewal of the Merkle Tree is expected to take place very rarely, typically after more than 10 years as stated in [RD-01] and that the future Merkle Tree root will be available on the GSC user interface at least two years before the planned renewal.

Finally, the user can also review the list of previous Merkle Trees (if any) in the historical record.

2.1.4 OVERVIEW OF OSNMA PERFORMANCE CHARACTERISTICS

The OSNMA protocol is applied to authenticate navigation message parameters of the I/NAV message. The usage assumptions and MPLs regarding the accuracy and validity of the I/NAV navigation message are stated in the Galileo OS SDD [RD-04].

The OSNMA shall authenticate the Galileo nominal and auxiliary satellites as per definitions provided in [RD-04][7], regardless of whether the status of the OS SIS transmitted by the satellite is “Healthy”, “Marginal”, “Unhealthy” or “Extended Operations Mode”. A detailed definition of the OS SIS status can be found in [RD-04].

Users of the Galileo OSNMA can obtain information about the OSNMA status, i.e., about the operational status of the OSNMA through the signals themselves when transmitted (see [RD-01]).

The Galileo OSNMA status can take one of the following three values:

- “Operational”: OSNMA is expected to meet the MPLs described in this document.
- “Test”: OSNMA is provided without any operational guarantees.
- “Don’t use”: the receiver shall not perform authentication of the OS navigation data using the broadcast OSNMA data.

[6] It is remarked that Merkle Tree leaves included in the Partial Merkle Tree are also provided via the OSNMA SIS while the Merkle Tree root node can only be retrieved through the GSC user interface. Full details can be found in the OSNMA IDD ICD [RD-02].

[7] Satellites defined as Not-In-Service or Decommissioned in [RD-04] are not authenticated by OSNMA. Although GSAT0201 (E18) and GSAT0202 (E14) are considered auxiliary satellites, the navigation messages transmitted by these satellites are not authenticated by the OSNMA since they are not used in the provision of the OS service.

The OSNMA status does not affect the status of the OS SIS, and thus, an OS user not implementing OSNMA is not affected by the performance of the latter (see [RD-04]).

The Galileo OSNMA MPLs reported in this document refers exclusively to Operational status. Note that the OSNMA status is a global status and not satellite specific.

The OSNMA status shall be verified before being applied as described in the OSNMA Receiver Guidelines [RD-03].

The OSNMA data includes additional flags informing the user about the status of the relevant cryptographic material, and the need of retrieving new cryptographic material associated to renewal and revocation processes. These flags, including their timely activation and the related user behaviour, are described in OSNMA SIS ICD [RD-01] and OSNMA Receiver Guidelines [RD-03].

The OSNMA protocol aims at achieving successful verification at receiver level when using a non-corrupted navigation message[8] and its corresponding tag[9].

Finally, the OSNMA Alert Message (see [RD-01]) might be broadcast during service provision to identify situations for which specific actions are to be followed. In case such message is broadcast, and its reception and content authenticated, the user shall stop using the OSNMA function and refer to the GSC for specific recovery actions. Please refer to OSNMA Receiver Guidelines [RD-03] and the OSNMA SIS ICD [RD-01] for the processing of OSNMA Alert Message.

2.1.5 USAGE CONDITIONS FOR GALILEO OSNMA SERVICE PERFORMANCE

The MPLs contained in this Galileo OSNMA SDD are conditioned upon certain assumptions regarding the use and processing of the OSNMA broadcast data. Those assumptions are as follows.

2.1.5.1 OSNMA USER RECEIVERS

The MPLs reported in the Galileo OSNMA SDD assume the fulfilment of the technical requirements and the correct implementation of the processing of the broadcast OSNMA by the receiver, as described in the OSNMA Receiver Guidelines [RD-03].

Receiver hardware, software or operation errors are excluded from the MPL computations.

2.1.5.2 MINIMUM EQUIVALENT TAG LENGTH

The minimum equivalent tag length L_t^{min}, corresponding to the minimum number of tag bits to be verified for a given navigation data set, is set to 40 bits for OSNMA Initial Service. Further details on the use of this parameter can be found in the Galileo OSNMA Receiver Guidelines [RD-03].

2.1.5.3 LIMITATIONS ON THE OSNMA FUNCTION

This Galileo OSNMA SDD is conditional upon the use of the OSNMA function when provided in Operational status and the use of the applicable cryptographic material.

[8] Non-corrupted message refers to messages received without any message decoding error.

[9] For the OSNMA Initial Service Phase, in rare cases, the DVS value transmitted on E1 and E5b may differ within the same I/NAV sub-frame. This may lead to an ADKD0 or ADKD12 tag verification failure for the affected satellite and tags broadcast in the following subframe. This implementation will be modified in future evolutions of the service to further limit the impact on user processing. Further details on the DVS flag of the OS SIS can be found in [RD-04] and [RD-05].

2.2 OSNMA MINIMUM PERFORMANCE LEVELS

The performance objectives of the OSNMA service are as follows:

- To provide OSNMA and OS equivalent navigation performance for users with nominal synchronisation capabilities (ADKD0 users). This is achieved by frequently broadcasting authentication tags for all Galileo satellites in view from a user location. This also allows to have frequent re-authentication of the navigation data used for positioning.
- To provide authentication data for at least four satellites in view from a user location for users with nominal and low synchronization capabilities (ADKD0 and ADKD12 users respectively). This ensures the availability of a positioning solution using authenticated data.
- To provide authentication for broadcast timing parameters (ADKD4 users) for at least one satellite in view from a user location.

Further details on the three authentication types can be found in the OSNMA SIS ICD [RD-01].

This section specifies the Galileo OSNMA Service performance in terms of Minimum Performance Levels (MPLs) linked to the service objectives outlined in the bullets above. The Galileo OSNMA performance parameters are divided into the following categories, each described in one of the following subsections:

- MAC availability (see subsection 2.2.1)
- Availability of OS-equivalent OSNMA navigation solution (see subsection 2.2.2)
- Timely publication of OSNMA NAGUs (see subsection 2.2.3)

The MAC availability MPLs are defined to capture the OSNMA performance in terms of authentication data availability, i.e., how often authentication data covering Galileo nominal and auxiliary satellites is provided covering each of the authentication types (ADKD0, ADKD12 and ADKD4). As stated in section 2.1.4, the OSNMA authentication is provided independently of the status of the signal[10] that is transmitted by the satellite. The target is to provide frequent authentications so that the user can authenticate the navigation data for any Galileo nominal or auxiliary satellite. The MAC rate for each authentication type has been chosen considering the characteristics of the use case behind each authentication type, which may evolve in future evolutions of the service. For ADKD0 and ADKD12 users, MAC availability MPLs are defined in order to guarantee that a user will be able to compute a navigation solution with newly authenticated data every 30 and 240 seconds respectively.

Availability of OS-equivalent OSNMA navigation solution MPL is then defined to capture the OSNMA performance in the positioning domain for ADKD0 users; this is, to provide authentication data in such a way that the positioning performance of a user applying OSNMA does not deviate significantly from the performance obtained by the OS user.

The timely communication to the user community of planned and unplanned events is covered by the NAGU publication related MPL.

All MPLs are defined within the service coverage, which for OSNMA is considered worldwide.

The Galileo OSNMA MPLs are expected to be met only if the usage assumptions for OSNMA provided in sections 2.1.4 and 2.1.5 are fulfilled.

The Galileo OSNMA MPLs do not include any contribution that is not under the control of the Galileo system. In particular, atmospheric, local effects and receiver noise contributions or interference are not included in the specifications (see 2.1.5.1).

Besides commitment performance (MPLs), this document provides additional performance characterization for PVT when using OSNMA data in Annex D .

[10] Healthy, marginal, unhealthy or extended operations mode.

2.2.1 MAC AVAILABILITY: DEFINITION AND MPLS

When defining OSNMA availability targets, authentication of a specific navigation data set is achieved when the navigation data set has been verified through a truncated Message Authentication Code (MAC), labelled as 'tag', with a minimum equivalent length of 40 bits (see definition in section 2.1.5.2), following the processing steps from the OSNMA Receiver Guidelines [RD-03].

The OSNMA MAC availability is computed at every user location, and for a given authentication type, as follows:

- Authentication for I/NAV navigation message data of Word Types 1 – 5 (ADKD0 as per OSNMA SIS ICD [RD-01]), for four satellites in view: Percentage of time that authentication tags with an equivalent tag size of at least 40 bits, are broadcast over the user location within a maximum period of 30 sec for at least four Galileo nominal or auxiliary[11] satellites in view, over 5 degrees elevation angle.

  In order to calculate the availability, the condition that tags are broadcast for at least four Galileo nominal or auxiliary satellites over the user location in every 30-second interval is verified. The availability is then computed as the percentage of 30-second intervals in which the condition is verified over a one-year period.

- Authentication for I/NAV navigation message data of Word Types 1 - 5 (ADKD0 as per OSNMA SIS ICD [RD-01]), for all satellites in view: Percentage of time that authentication tags with an equivalent tag size of at least 40 bits, are broadcast over the user location within a maximum period of 600 seconds for all Galileo nominal or auxiliary[11] satellites in view over 5 degrees elevation angle.

  In order to calculate the availability, the condition that tags are broadcast for all Galileo nominal or auxiliary satellites over the user location in every 600-second interval is verified. The availability is then computed as the percentage of 600-second intervals in which the condition is verified over a one-year period.

- Authentication for I/NAV navigation message data of Word Types 1 - 5, for receivers with low synchronization requirements (ADKD12 as per OSNMA SIS ICD [RD-01]): Percentage of time that authentication tags with an equivalent tag size of at least 40 bits, are broadcast over the user location within a maximum period of 240 seconds for at least four Galileo nominal or auxiliary satellites in view, over 5 degrees elevation angle.

  In order to calculate the availability, the condition that tags are broadcast by at least four Galileo nominal or auxiliary satellites over the user location in every 240-second interval is verified. The availability is then computed as the percentage of 240-second intervals in which the condition is verified over a one-year period.

- Authentication for GST-UTC and GST-GPS conversion parameters (ADKD4 as per OSNMA SIS ICD [RD-01]): Percentage of time that authentication tags with an equivalent tag size of at least 40 bits, are broadcast over the user location within a maximum period of 60 seconds for at least one Galileo nominal or auxiliary satellite in view over 5 degrees elevation angle.

  In order to calculate the availability, the condition that tags are broadcast for at least one Galileo nominal or auxiliary satellites over the user location in every 60-second interval is verified. The availability is then computed as the percentage of 60-second intervals in which the condition is verified over a one-year period.

The OSNMA MAC availability MPLs as defined above are specified in Table 3.

[11] Although GSAT0201 (E18) and GSAT0202 (E14) are auxiliary satellites, the navigation messages transmitted by these satellites are not authenticated by the OSNMA since they are not used in the provision of OS service.

Table 3 - MAC Availability MPLs[12]

FIGURE OF MERIT	MPL	CONDITIONS AND CONSTRAINTS	
Availability of OSNMA data (I/NAV navigation message, ADKD0)	≥ 95%	For at least four Galileo nominal or auxiliary satellites in view within a period of 30 seconds	• From any point in the service coverage. • Above a minimum elevation angle of 5 degrees. • Calculated over a one-year period. • Including planned and unplanned outages. • When the data being authenticated is broadcast in the SIS. • Excluding dummy tags[13].
	≥ 80%	For all Galileo nominal or auxiliary satellites in view within a period of 600 seconds	
Availability of OSNMA data (I/NAV navigation message, ADKD12)	≥ 95%	For at least four Galileo nominal or auxiliary satellites in view within a period of 240 seconds	
Availability of OSNMA data (GST-UTC and GGTO parameters, ADKD4)	≥ 97%	For at least one Galileo nominal or auxiliary satellite in view within a period of 60 seconds	

2.2.2 AVAILABILITY OF OS-EQUIVALENT OSNMA NAVIGATION SOLUTION: DEFINITION AND MPL

The availability of OS-equivalent OSNMA navigation solution is defined as the percentage of time in which the OSNMA navigation solution for the ADKD0 user includes the same satellites as the navigation solution for the OS user.

The availability of OS-equivalent OSNMA navigation solution MPL is specified in Table 4.

Note that this MPL is not linked to the reception of tags during a certain period, which is covered in section 2.2.1. Instead, it measures the availability of OSNMA PVT with authenticated navigation data. OSNMA users are expected to retrieve the most recent navigation message parameters relevant to the type of navigation solution to be computed, as broadcast by the Galileo system and authenticated by means of the OSNMA data. Due to the processing latencies inherent to the OSNMA protocol and the OSNMA data broadcast scheme, a navigation message data set may be applied by the OSNMA user for a longer period of time with respect to the standard OS user. During this time, the OSNMA user is expected to continue applying the last authenticated navigation message data set that is still valid under the assumptions described in the Galileo OS SDD [RD-04].

[12] The navigation message transmitted by GSAT0201 (E18) and GSAT0202 (E14) is not authenticated by the OSNMA. However, these satellites can be used to disseminate OSNMA data authenticating other satellites in the constellation, and when doing so, the user is expected to use it to optimize the OSNMA performance. The MPL target values presented in this document are achieved without the contribution of these two satellites to the OSNMA data dissemination.

[13] The dummy tags are indicated by a COP= 0, and although they are still associated with an ADKD, they do not contribute to the service availability since they do not authenticate any data. See [RD-01] for further details on the dummy tags.

Table 4 - Availability of OS-equivalent OSNMA navigation solution MPL

FIGURE OF MERIT	MPL	CONDITIONS AND CONSTRAINTS
MPL of the availability of OS-equivalent OSNMA navigation solution	≥ 95%	• Same satellites used by the OS and the OSNMA user. • From any point in the service coverage. • Above a minimum elevation angle of 5 degrees for PVT calculation[14]. • Calculated over a one-year period. • Including planned and unplanned outages. • Excluding dummy tags[13].

2.2.3 TIMELY PUBLICATION OF OSNMA NAGUS: DEFINITION AND MPL

The Timely publication of OSNMA NAGUs refers to the time intervals within which Galileo NAGUs are published before any planned event or after any unplanned event. The MPL covers the publication as well of NAGUs for cryptographic material updates (renewal/revocation of OSNMA Public key, TESLA key chain or Merkle Tree).

Planned service outages events are anticipated through the publication of a specific NAGU at least 48 hours in advance of the outage event, based on Galileo operations and maintenance plans.

For unforeseen (unplanned) service outage events, the notification through the publication of a specific NAGU is provided not later than 30 hours after the confirmation of the event.

The MPL for the Timely publication of NAGUs for the OSNMA is specified in Table 5.

[14] This value is achieved assuming that the OSNMA data is retrieved as soon as the satellite is tracked above the horizon (0° elevation) so that the satellite can be used in PVT calculation from 5° elevation.

Table 5 - OSNMA timely publication of NAGUs MPL

MPL OF THE TIMELY PUBLICATION OF NAGUs	CONDITIONS AND CONSTRAINTS
≥ 48 hours before the service is affected	• Notification to users of scheduled service outages impacting the OSNMA broadcast, or updates of OSNMA related crypto material (renovation of OSNMA Public key, TESLA key chain or Merkle Tree).
≤ 30 hours after the event affecting the service is confirmed or the OSNMA crypto material is updated	• Notification to users of unscheduled service outages impacting the OSNMA broadcast, or updates of OSNMA related crypto material (revocation of OSNMA Public key or TESLA key chain) or the OAM broadcast.

ANNEX A - REFERENCE DOCUMENTS

Ref.	Title	Issue
RD-01	Galileo Open Service Navigation Message Authentication (OSNMA) Signal-In-Space (SIS) Interface Control Document (SIS ICD).	The most updated issue. (Available on the web page of the Galileo Service Centre)
RD-02	Galileo Open Service Navigation Message Authentication Internet Data Distribution Interface Control Document (OSNMA IDD ICD).	
RD-03	Galileo Open Service Navigation Message Authentication (OSNMA) Receiver Guidelines.	
RD-04	European GNSS (Galileo) Open Service - Service Definition Document (OS SDD).	
RD-05	European GNSS (Galileo) Open Service Signal-In-Space Interface Control Document (OS SIS ICD).	
RD-06	Galileo High Accuracy Service – Service Definition Document (HAS SDD).	

ANNEX B - ABBREVIATIONS AND ACRONYMS

Abbreviation	Definition
AD	Authenticated Data
ADKD	Authentication Data and Key Delay
BID	Block ID
BPSK	Binary Phase Shift Keying
COP	Cut-Off Point
CP/CPS	Certificate Policy/ Certificate Practice Statement
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
DF	Dual Frequency
DSM	Digital Signature Message
EC	European Commission
EGNSS	European Global Navigation Satellite System
EUSPA	European Union Agency for the Space Programme
GGTO	Galileo-GPS Time Offset
GMS	Ground Mission Segment
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSC	Galileo Service Centre
GSS	Galileo Sensor Station
GST	Galileo System Time
GSTI	GNSS Simulation and Testing Tools Infrastructure
HAS	High Accuracy Service
HKROOT	Header and Root Key
ICD	Interface Control Document
IDD	Internet Data Distribution
IOD	Issue of Data
MAC	Message Authentication Code
MACK	MAC and Key
MBOC	Multiplexed Binary Offset Carrier
MPL	Minimum Performance Level
MT	Merkle Tree
NAGU	Notice Advisory to Galileo Users
NMA	Navigation Message Authentication
OAM	OSNMA Alert Message
OS	Open Service

Abbreviation	Definition
OSNMA	Open Service Navigation Message Authentication
PK	Public Key
PKI	Public Key Infrastructure
PRS	Public Regulated Service
PVT	Position, Velocity and Time
RCA	Root Certificate Authority
SAS	Signal Authentication Service
SCA	Subordinate Certificate Authority
SDD	Service Definition Document
SF	Single Frequency
SFTP	Secure File Transfer Protocol
SIS	Signal in SPACE
TAI	International Atomic Time
TBA	Time Between Authentications
TESLA	Time Efficient Stream Loss-Tolerant Authentication
TTFF	Time To First Fix
UTC	Universal Time Coordinated
WT	Word Type
XML	eXtensible Mark-up Language

ANNEX C - DESCRIPTION OF NOTICE ADVISORY TO GALILEO USERS

NAGUs (Notice Advisory to Galileo Users) are used to notify Galileo users about the SIS status of all satellites in the Galileo constellation and the service status. Different categories of NAGUs are issued depending on the specific event to be communicated.

The information provided here, together with the list of active and archived NAGUs can be also found in the GSC web page[15] under "System Status".

C.1. LIST OF DEFINED NAGUS

Related to the NAGU categorization, the lists of NAGUs presented in the OS SDD [RD-04] and HAS SDD [RD-06] are complemented with specific NAGUs for the OSNMA as follows:

Table 6 - OSNMA NAGU types

Category	Event description	NAGU types	Definition
Planned	Public Key renewal	OSNMA PK_RENEWAL	An OSNMA Public Key renewal will take place.
	TESLA chain renewal	OSNMA TESLA_CHAIN_RENEWAL	An OSNMA TESLA Chain renewal will take place.
	Merkle Tree renewal	OSNMA MT_RENEWAL	An OSNMA Merkle Tree renewal will take place.
	Planned Outage	OSNMA PLN_OUTAGE	A planned operation affecting the OSNMA service provision will take place.
Unplanned	Public key revocation	OSNMA PK_REVOCATION	An OSNMA Public Key revocation took place.
	TESLA chain revocation	OSNMA TESLA_CHAIN_REVOCATION	An OSNMA TESLA Chain revocation took place.
	OSNMA Alert message	OSNMA ALERT_MESSAGE	OSNMA Alert Message was broadcast.
	Unplanned outage until further notice	OSNMA UNP_UNUFN	An unplanned outage affecting the OSNMA service provision took place.
	Unplanned Short Recovery	OSNMA UNP_SHTRCVR	An unplanned event, that caused an OSNMA outage, that has been already recovered before a dedicated NAGU could be published to notify its occurrence.

[15] https://www.gsc-europa.eu

Category	Event description	NAGU types	Definition
	Cancellation	OSNMA CANCEL	Cancellation of published OSNMA NAGU (e.g., due to the withdrawal of a planned outage).
	Reschedule	OSNMA RESCH	Provision of new start/end times for an already published PLANNED OSNMA NAGU.
	Extension	OSNMA EXTNS	Provision of a new end time for an already published PLANNED OSNMA NAGU.
Service Availability	OSNMA usable	OSNMA USABLE	The OSNMA service is restored after an Alert Message broadcast or a planned/unplanned outage.

It is to be noted that OSNMA related NAGUs will always concern the SIS interface of the OSNMA service. Relevant events concerning only the IDD interface will be directly notified to the registered OSNMA users via email.

C.2. NAGU FORMAT

The format of the OSNMA NAGUs issued to Galileo users through the European GNSS Service Centre web portal follow the following template:

NOTICE ADVISORY TO GALILEO USERS (NAGU)	YYYYNNN
DATE GENERATED (UTC):	YYYY-MM-DD hh:mm
NAGU TYPE:	AS PER NAGU DEFINITION
NAGU NUMBER:	YYYYNNN
NAGU SUBJECT:	AS PER NAGU TEMPLATE
NAGU REFERENCED TO:	YYYYRRR OR N/A
START DATE EVENT (UTC):	YYYY-MM-DD hh:mm
END DATE EVENT (UTC):	YYYY-MM-DD hh:mm OR N/A
SATELLITE AFFECTED:	ALL
EVENT DESCRIPTION:	AS PER NAGU TEMPLATE

The fields used within the NAGUs are defined here below:

1) HEADER: The first line of the text field refers to the title “NOTICE ADVISORY TO GALILEO USERS” (NAGU), followed by the NAGU number in the format YYYYNNN, where:
    a. YYYY: Gregorian year.
    b. NNN: sequential number of the NAGU, starting with 001 on the 1st of January every year and incrementing by 1 for each subsequent NAGU.
2) DATE GENERATED (UTC): The date when the NAGU is generated on the GSC web portal, in UTC time scale with format YYYY-MM-DD hh:mm, where:

a. YYYY: Gregorian year.

b. MM: number of the month from 1-12 in sequence starting with 1 being January and finishing with 12 being December.

c. DD: day within the Gregorian month

d. hh: hour in the 24-hour format

e. mm: minute

3) NAGU TYPE: The different NAGU types as defined in Table 6.

4) NAGU NUMBER: Reference to the NAGU number in the format YYYYNNN (as defined in the Header field).

5) NAGU SUBJECT: The subject of the NAGU summarizing the information provided in the "Event description". The text to be used in the subject is defined by the template of each NAGU.

6) NAGU REFERENCED TO: If the current NAGU refers to a previous NAGU, this field contains the referenced NAGU number in the format YYYYRRR, where:

a. YYYY: Gregorian year when the NAGU was issued.

b. RRR: issue number of the NAGU for that year.

Otherwise, the field contains N/A (not applicable) when there is no reference to a previous NAGU.

7) START DATE EVENT (UTC): The start date of the event notified by the NAGU, in UTC time scale with format YYYY-MM-DD hh:mm.

8) END DATE EVENT (UTC): The end date of the event notified by the NAGU, in UTC time scale with format YYYY-MM-DD hh:mm or defined as Not Applicable or defined as Until Further Notice.

9) SATELLITE AFFECTED: ALL.

10) EVENT DESCRIPTION: The event description following the templates defined for each NAGU.

ANNEX D - TIME TO FIRST FIX WITH AUTHENTICATED DATA

As stated in section 2.2, besides commitment performance (MPLs), this appendix provides additional performance characterisation for PVT when using OSNMA data.

The Time to First Fix with Authenticated Data (TTFF-AD) is defined as a measure of the elapsed time required for a receiver to acquire the satellite signals and navigation data, including authentication data, to authenticate the navigation message and calculate the first position solution using the authenticated navigation parameters.

This appendix presents the performance metrics associated to the achievement of TTFF-AD for different OSNMA start-up conditions: cold start, warm start, and hot start as defined in the OSNMA Receiver Guidelines [RD-03]. In summary:

- Cold start condition: a receiver in cold start does not have any of the cryptographic information required to authenticate navigation messages and that is broadcast by the Galileo satellites (i.e., excluding the Merkle Tree root that cannot be obtained from the satellites). The receiver must first obtain this cryptographic information through the Signal in Space before the first authentication can be performed. For example, this requires the receiver to retrieve the public key used in the OSNMA TESLA root key verification. The TTFF-AD in cold start includes the time taken to obtain the public key, the time to obtain and verify the TESLA root key and the time to authenticate the ephemerides for at least four satellites in view.
- Warm start condition: a receiver in warm start already has the OSNMA public key in force but does not have a previously verified TESLA key. The TTFF-AD in warm start includes the time to obtain and verify the TESLA key and the time to authenticate the ephemerides for at least four satellites in view.
- Hot start condition: a receiver in hot start is assumed to have both the public key in force and a previously verified TESLA root key. The TTFF-AD in hot start includes only the time taken to receive and authenticate the ephemerides from at least four satellites in view.

The results shown in Table 7 are the result of applying the following optimisations to the Receiver Setup:

- For all cold/hot/warm start:
    - The WT 1-4 data[16] can be retrieved in the same subframe of the MAC given that:
        - The WT 1-4 data is received at the same time or before the MAC.
        - There is at least 1 word from WT 1-4 received within the COP range with the same IOD.
    - WT5 has to be received within the COP range.
- For warm start, the following specific considerations are taken (see [RD-01] and [RD-03] for reference):
    - The receiver starts to gather MACK data and HKROOT data in parallel.
    - When a DSM BID 0 is received, the chain parameters are retrieved from the DSM-HKROOT and applied to decode the information in the MACK message.

[16] Note that in the current OSNMA configuration, for the case of SF users, only WT2 and WT4 are transmitted early enough in the subframe to be used under the described optimization.

- Due to the parallelization of the MACK and HKROOT data reception the warm start TTFF-AD is the longest time between:
  - Time to obtain and authenticate navigation data and MACs for at least 4 SV.
  - Time to obtain and authenticate a DSM.

The above are potential strategies of receiver optimisation. The user can apply different strategies for the receiver design optimisation as long as they are compliant to the OSNMA User Receiver Guidelines [RD-03].

Table 7 - TTFF-AD associated metrics

MAC type	Hot start 95%	Warm start 95%[17]	Cold start 95%[18]
ADKD0	130 seconds	300 seconds	≤ 6 hours
ADKD12	460 seconds	520 seconds	≤ 6 hours

[17] The warm start target is met for configurations with DSM size of 8 blocks.

[18] The result for this metric is driven by the provision of the DSM-PKR in the SIS, which is provided to allow the users to retrieve the PK and is scheduled to be broadcast every 6 hours at defined times.

END OF DOCUMENT

978-92-9206-080-0

EUSPA
European Union Agency for the Space Programme

LINKING SPACE TO USER NEEDS

www.euspa.europa.eu

@euspa.bsky.social

@EU4Space

EUSPA

@space4eu

EUSPA

#EUSpace