Received: 10 November 2021 | Revised: 7 October 2022 | Accepted: 11 December 2022

DOI: 10.33012/navi.572

ORIGINAL ARTICLE

Galileo Open Service Navigation Message Authentication: Preparation Phase and Drivers for Future Service Provision

Martin Götzelmann[1] | **Evelyn Köller**[1] | **Ignacio Viciano-Semper**[1] | **Dirk Oskam**[1] | **Elias Gkougkas**[1] | **Javier Simon**[2]

[1] Airbus Defence and Space GmbH
[2] European Union Agency for the Space Programme

Correspondence
Martin Götzelmann
Airbus Defence and Space GmbH
Robert-Koch-Str. 1, Bldg 5.1
82024 Taufkirchen, Germany
Email: martin.goetzelmann@airbus.com

Abstract

While Galileo approaches Full Operational Capability and is close to completion of the deployed satellite constellation, a portfolio of new Galileo service features is under development and validation. The Galileo Open Service (OS) is planned to be enhanced with the provision of Navigation Message Authentication (NMA). In November 2020, the Galileo satellites started broadcasting OSNMA test data for an internal preparation phase of seven months duration. The objective of this test period was to determine and select the OSNMA test signal configuration for a subsequent 'Public Observation phase.'

The paper presents the main outcomes of the preparation phase for a set of defined OSNMA performance parameters. Airbus is supporting the Galileo service provider, the European Union Agency for the Space Programme (EUSPA), both in Galileo service definition and in planning and execution of OSNMA test activities, which have been performed during this preparation phase.

Keywords

galileo, navigation message authentication, OSNMA, service performance characterization

1 | INTRODUCTION

"Reality or fake news?"—A question of our time, not only of crucial importance for the users of social media, but also increasingly relevant within the world of GNSS. Navigation users rely on GNSS as a ubiquitous utility and need to trust that received navigation message data is truly coming from the GNSS system. The standard GNSS receiver will often not be able to detect any attempt of insidious misguidance by falsified GNSS data from a fake GNSS signal.

In November 2020, Galileo became the first GNSS system to broadcast authentication data in an Open Service signal enabling the GNSS user to verify the authenticity of received navigation message data. This marked a first step towards the implementation of a new Galileo Open Service feature named Open Service Navigation Message Authentication (OSNMA), which is planned to be offered free-of-charge to all Galileo Open Service users world-wide. It will both protect the user receiver from malicious data spoofing attacks and prevent the user from

self-spoofing, as it enables any GNSS device to confirm that received navigation message data has been generated by the Galileo system.

A first system-internal test period has been performed, under the lead of EC, EUSPA, and ESA, between November 2020 and April 2021. In July 2021 the OSNMA data broadcast was resumed for an additional test period of three months duration.

Following this test and service preparation period, the Galileo OSNMA Test Signal-in-Space (SIS) Interface Control Document (ICD) and supporting Receiver Guidelines have been published for the subsequent 'Public Observation phase,' which started on 15 November 2021 (European Union, 2021a, 2021b). This ICD provides relevant simplifications of the previous specifications (as, e.g., addressed in Fernandez Hernandez et al., 2019), which were very flexible to mitigate possible risks of integration in the operational Galileo system. Receiver manufacturers, application developers, and research institutions are invited to participate in this Public Observation phase in order to test their user implementation of the OSNMA protocol and to provide feedback on this future Open Service feature.

This paper will shed some light on key aspects and performance parameters that drive the definition and implementation of the future OSNMA service. The current implementation of the OSNMA test signal will be further enhanced towards the service provision phase taking advantage of the lessons learned during the testing phase.

2 | OSNMA PROTOCOL

The key features of the OSNMA authentication scheme have been presented in various publications before (see, e.g., Fernandez Hernandez et al., 2014, 2016, 2019). The main elements and processing steps of the applied authentication mechanism are briefly recalled as follows.

The Galileo OSNMA authentication scheme is based on an adaptation of the TESLA protocol, which efficiently exploits the scarce GNSS bandwidth for data source authentication (Fernandez Hernandez et al., 2016; Perrig et al., 2002): The Galileo satellites provide the Galileo OS user with truncated Message Authentication Codes (MACs) that are generated as the output of a cryptographic hash function (Keyed-Hash Message Authentication Codes) which uses as input the Galileo navigation message data and a cryptographic key that is secret at the time of MAC generation.

The key that has been applied by the Galileo system to generate the MAC is disclosed to the user with some time delay after the MAC has already been broadcast and received by the OSNMA user.

All keys used for MAC computation belong to a pre-computed one-way chain of time tagged TESLA keys, where the key k_{n-1} is generated from key k_n as the output of an irreversible hash function, also known as a one-way hash function.

As the keys are applied and broadcast in reverse direction to their generation, the user is able to verify the received key by reproducing any other key of the chain that has already been received and verified earlier.

The key chain ends in a so-called "root key" k_0 which can be reproduced from any other key of the chain and serves to verify the authenticity of any other key of the chain. For this purpose, the root key k_0 of the TESLA key chain is provided to the user within the broadcast OSNMA data.

For authentication of the root key an asymmetric ECDSA mechanism is used. The Galileo system utilizes a Private Key to generate an ECDSA Digital Signature of the root key (and the broadcast NMA configuration data). The root key, the configuration data, and the Digital Signature are broadcast to the user and the user applies the corresponding ECDSA Public Key in order to verify the Digital Signature of the received root key and the received OSNMA configuration data.

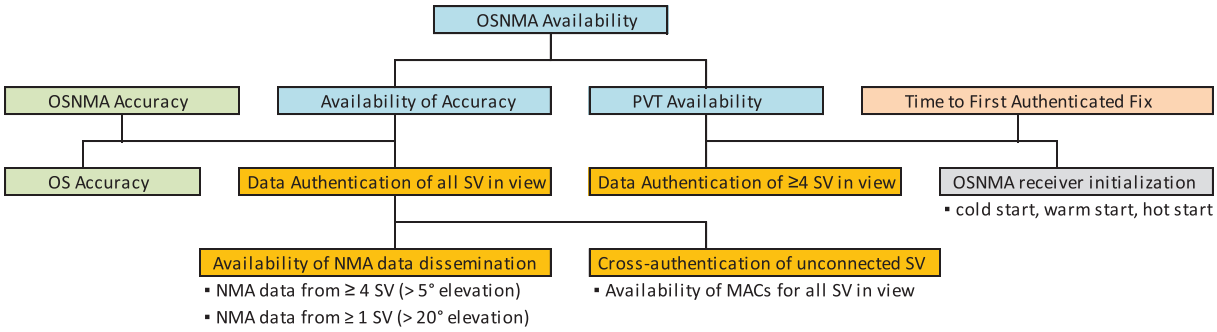

FIGURE 1 OSNMA user performance characterization

At this point, the user is able to verify the authenticity of the received navigation data by reproducing the received MAC from the received navigation data and the received and verified TESLA key. Depending on the MAC size and the required security level of the user, the user may be required to accumulate and verify two or more MACs for the same set of navigation data until a target equivalent accumulated MAC size is reached (Fernandez Hernandez et al., 2016).

The Public Key may be obtained by the OSNMA user in different ways. During the test and preparation phase, the Public Key is retrieved from a web server of the Galileo Service Centre. In addition, it is also foreseen for the service provision phase to transmit the Public Key in regular intervals within the OSNMA data in the Galileo SIS, to be verified by the user by means of a Merkle tree (Fernandez Hernandez et al., 2019). The applicable Public Key is expected to change only very infrequently.

3 | OSNMA SERVICE PERFORMANCE DRIVERS

The design of the future OSNMA service and the underlying authentication scheme needs both to satisfy the security needs required by OSNMA users (e.g., Smart Tachograph) and to maintain at the same time the high-class navigation service performance to which users of the standard Galileo Open Service are accustomed.

The cryptographic strength of the OSNMA scheme mainly depends on the selected MAC function and the configured size of the MACs, keys, and digital signature, which has been discussed in detail in Fernandez Hernandez et al. (2021).

The key performance parameters characterizing the navigation performance of the Galileo OSNMA user are the accuracy of the position solution of the OSNMA user, the availability of the OSNMA service, and the time to first authenticated fix (See Figure 1). In the following, we will discuss these performance parameters in more detail and provide in-field test results from the Galileo internal test period with live OSNMA signals.

3.1 | OSNMA Service Availability, OSNMA Data Availability, MAC Availability

With regard to the availability of the future OSNMA service, we distinguish between PVT availability, as the percentage of time that the Galileo OSNMA user is in view of at least four data authenticated satellites, and availability of OSNMA accuracy, as the percentage of time that the position solution of the Galileo OSNMA user is obtained with the required accuracy.

It is one guiding principle of the design of the future OSNMA service that the accuracy and availability of the OSNMA user are required to be the same or very similar to those observed by the standard Galileo Open Service user. While authentication of navigation messages from at least four satellites in view are sufficient for PVT availability and determine the time to first authenticated fix, the OSNMA service is to be designed to continuously provide the OSNMA user with the OSNMA data to authenticate I/NAV navigation message data from all satellites in view. If this objective is achieved, the accuracy and availability of the OSNMA user will be equivalent to that of the standard Open Service user and the position solution of the OSNMA user will usually be the same or very close to the OS position fix.

Whenever the broadcast navigation message of one satellite is updated, the OSNMA user is subject to a short delay, inherent to the OSNMA protocol, until the new set of navigation data has successfully been authenticated. During this time, the OSNMA user is usually still able to compute its Galileo position solution including this satellite and applying a previously authenticated (and still valid) navigation message without significant accuracy degradation with respect to the updated navigation message.

The OSNMA authentication data is generated on ground and uplinked to the Galileo satellites. For this reason, only those Galileo satellites that are presently in contact with a ground uplink antenna are disseminating OSNMA data at any point in time (Fernandez Hernandez et al., 2016).

Consequently, the availability of the future Galileo OSNMA service will depend on the 'OSNMA data availability' defined as the percentage of time in which at least n Galileo satellites broadcasting OSNMA data are in view of the Galileo OSNMA user. This is particularly relevant for users in urban environments that may be subject to increased elevation masks. OSNMA data availability is correlated with the number of operational uplink antennas that are available to serve the Galileo constellation with navigation messages and OSNMA data.

The Galileo system also needs to ensure continuous authentication of the navigation message data of those satellites presently not broadcasting OSNMA data. For this purpose, each satellite is not only broadcasting Message Authentication Codes that authenticate its own navigation message data, but is also sending OSNMA data for authentication of Galileo satellites that are not in contact with a ground uplink antenna. This concept is called cross-authentication.

The parameter that is ultimately relevant to measure the OSNMA user availability is the 'MAC availability,' which is defined as the percentage of time during which the Galileo system broadcasts a sufficient number of Message Authentication Codes that enable the OSNMA user to authenticate navigation message data for all (or a given number of) satellites in view.

Among other factors, observed MAC availability depends on the length of the defined cross-authentication sequence, which is the number of unconnected satellites that will be cross-authenticated by any connected satellite within any pair of two consecutive I/NAV subframes. The number of MACs broadcast in one I/NAV subframe depends on the size of the key that is broadcast in every subframe and the size of each MAC. Both parameters are configurable in order to adapt the OSNMA configuration to applicable security levels that may evolve over time.

Different from the position accuracy and service availability of the OSNMA user, the MAC availability, which characterizes the NMA data dissemination performance of the Galileo system, is independent of the user environment (residual ionospheric and tropospheric delay, multipath) and receiver noise. For this reason, this performance parameter is a suitable candidate to be specified as a Minimum Performance Level within the future Service Definition Document.

An adequate service commitment on MAC availability will implicitly guarantee that the service availability and position accuracy of the OSNMA user is similar to that of the standard OS user.

3.2 | Time to First Authenticated Fix

The OSNMA time to first authenticated fix (TTFAF) is a measure of the time interval required by an OSNMA receiver to acquire the satellite signals, to demodulate the navigation data, to authenticate the navigation message, and to calculate the first position solution using only the authenticated navigation parameters. It mainly depends on the receiver initialization condition (is a public key and a verified root key already available to the receiver?), the OSNMA data availability and MAC availability provided by the Galileo system, the required MAC accumulation target, and finally the delay between the broadcast of the MAC and the key.

4 | OSNMA CONFIGURATION FOR THE PUBLIC OBSERVATION PHASE

Each E1-B I/NAV sub-frame of 30-s duration consists of 15 different pages. Each I/NAV page contains 40 bits of OSNMA data within the odd part of the page. The 40-bit OSNMA field is further split into an 8-bit HKROOT message, which is used to broadcast the root key, the OSNMA configuration parameters, the digital signature required for the authentication of the root key, and a 32-bit MACK message, which contains the MACs and the TESLA chain keys for MAC verification (see Figure 2 and European Union (2021a)).

Three different types of MACs are supported during the Public Observation phase, which differ either regarding the type of navigation data being authenticated or regarding the delay between the broadcast of the MAC and the key, as per the ADKD (Authentication Data and Key Delay) field:

MACs of type ADKD 0 and ADKD 12 authenticate the complete set of I/NAV navigation data that is required for computation of a Galileo position fix: satellite ephemeris, satellite clock correction, Broadcast Group Delays, ionospheric

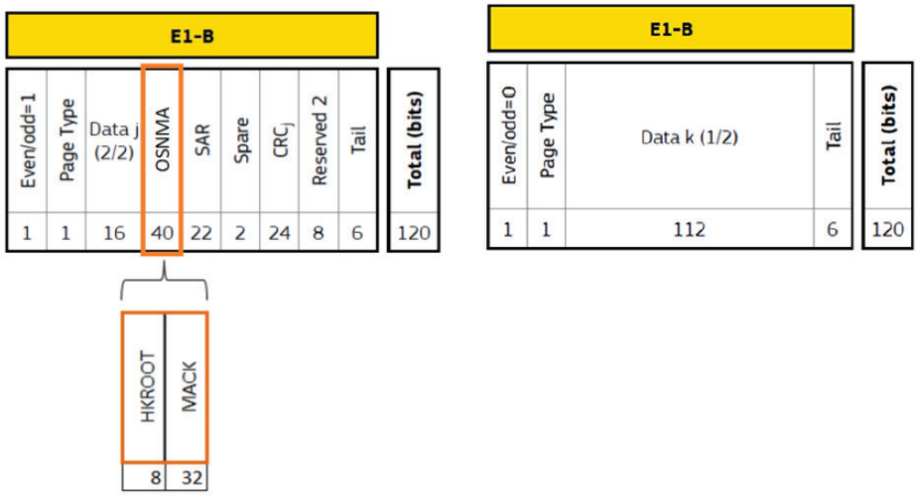

FIGURE 2 OSNMA field within an I/NAV page (odd and even part), as further detailed in European Union (2021a)

TABLE 1
MAC Types During Public Observation Phase

MAC type	Authentication Data (AD)	Key Delay (KD)
ADKD 0	I/NAV ephemeris, clock correction, ionospheric correction, BGD, health flags	1 I/NAV subframe
ADKD 12		1 + 10 I/NAV subframes (slow MAC)
ADKD 4	GST-UTC time conversion parameter, Galileo GPS Time Offset, TOW	1 I/NAV subframe

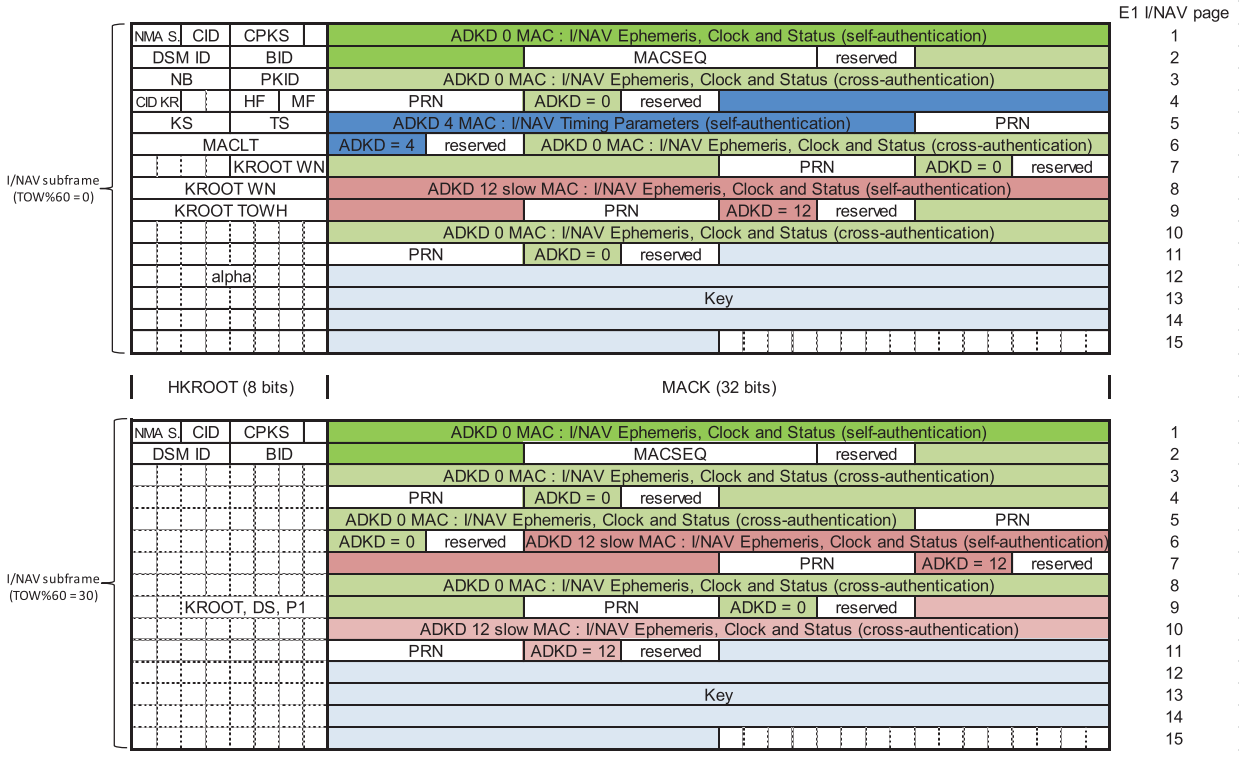

FIGURE 3 OSNMA configuration during Public Observation phase: sequence of MACs in two consecutive I/NAV subframes

correction parameters, and satellite health flags. MACs of type ADKD 4 may be used by timing users to authenticate GST to UTC time conversion parameters.

While the key that is required to verify ADKD 0 and ADKD 4 MACs is always broadcast in the subsequent I/NAV subframe, the keys of ADKD 12 'slow MACs' are transmitted with an additional delay of 300 s.

A key size of 128 bits and a MAC size of 40 bits have been configured for the Galileo OSNMA Public Observation phase, which implies that six MACs are broadcast in every E1-B I/NAV subframe of 30-s duration. The length of the Digital Signature is 512 bits. One key of the TESLA key chain is transmitted in every I/NAV subframe.

Figure 3 shows the distribution of the MAC types and the Tesla Key within the OSNMA data of an I/NAV subframe. Note that the sequence differs for two consecutive subframes. For completeness, the HKROOT section has been added as well. It contains the NMA and DSM header in the first two pages of an I/NAV subframe, followed by 13 HKROOT sections with DSM block content. Which DSM block is transmitted is to be read from the DSM header. As an example,

the distribution of a DSM block with ID 0 is displayed in the first subframe. In general, DSM blocks must be collected from several subframes in order to gather the complete information.

The OSNMA protocol requires the receiver to be synchronized in a secure way to Galileo System Time (which could be for example via an internal clock of adequate accuracy or secure network connection with time transfer capability). This is a requirement that the user segment needs to develop, implement, and verify during OSNMA data processing. The maximum time uncertainty of the time realization that is admissible for secure processing of the OSNMA data is on the order of several seconds and depends on the delay between the broadcast of the MAC and the key (Fernandez Hernandez et al. (2020)). ADKD 12 'slow MACs' are provided for users with less accurate time synchronization capability. European Union (2021b) provides further guidelines for users with known and unknown user receiver time uncertainty.

Each "connected" satellite will broadcast the same MAC sequence of 12 consecutive MACs, which repeats every two I/NAV subframes. Within these two consecutive subframes, two ADKD 0 MACs, two ADKD 12 MACs (for self-authentication of the I/NAV navigation message data of the broadcasting satellite), and six ADKD 0 MACs (for cross-authentication of six other Galileo satellites (prioritizing unconnected satellites)) will be transmitted. In addition, one ADKD 4 MAC and one cross-authenticating ADKD 12 MAC is sent in every second I/NAV subframe.

Current service design requires the OSNMA user to verify and accumulate two 40-bit MACs in order to consider a specific set of navigation message data as authenticated (considering an equivalent MAC size of 80 bits). The minimum equivalent MAC length may be modified in future and therefore this parameter should be configurable in the receiver.

5 | OSNMA USER PERFORMANCE MONITORING

During the Galileo internal test phase, OSNMA user performance has been measured by different entities operating different types of OSNMA-enabled test receivers at various locations in Europe. PVT accuracy and availability of the OSNMA user have been characterized for static and dynamic scenarios in open sky, rural, and urban environments.

In addition, Airbus developed a comprehensive software package, named N#MAtch, for OSNMA signal monitoring, which has been applied in order to monitor and characterize OSNMA user performance for a global grid of OSNMA user locations during the complete test phase. The software is capable of retrieving and processing OSNMA data from I/NAV navigation messages received by any type of standard GNSS receiver.

The whole set of received navigation message data from a system-external global network of fifteen ground monitoring stations has been made available to Airbus for OSNMA user performance analysis. These ground stations are maintained by ESA.

Processing both the continuous timeline of broadcast OSNMA data of each satellite and the orbit data of the Galileo satellite constellation, OSNMA data availability is evaluated on a global grid of 10242 user locations. Results are presented as global maps of OSNMA data availability over a measurement period of one month and by means of timelines of daily OSNMA data dissemination coverage for the Worst, Average, and Best User Location.

Monitoring the observed sequence of cross-authentication MACs (of type ADKD 0 and ADKD 12) from each broadcasting satellite, the percentage of time during which the OSNMA user is provided with

- ADKD 0 MACs to authenticate navigation data from all satellites in view
- ADKD 12 MACs to authenticate navigation data from at least four satellites in view
- ADKD 4 MACs to authenticate timing parameters from at least one satellite in view is evaluated over the measurement time period for each user location.

The MAC availability analysis needs to consider MAC accumulation up to an equivalent accumulated MAC size of 80 bits (within a given accumulation period), i.e., at least two different 40-bit MACs need to be received and processed by the user for authentication of a given set of navigation message data.

The complete and continuous set of received OSNMA data from each satellite is finally processed by the N#MAtch OSNMA signal monitoring tool applying the required cryptographic receiver operations in accordance with the OSNMA user algorithm specified in the Galileo OSNMA Test SIS ICD (European Union, 2021a). Considering a hypothetical OSNMA user that would be in view of the complete Galileo constellation and would both have access to any authentication data and any navigation message data broadcast by any Galileo satellite, it is monitored and confirmed that each broadcast MAC, each broadcast TESLA key, and each ECDSA digital signature can indeed be successfully verified by the OSNMA users. `

6 | OSNMA DATA AVAILABILITY

In the following, test results on monthly OSNMA data availability from August 2021 are presented and discussed. The following four maps display the percentage of time during this month that user locations were provided with OSNMA data

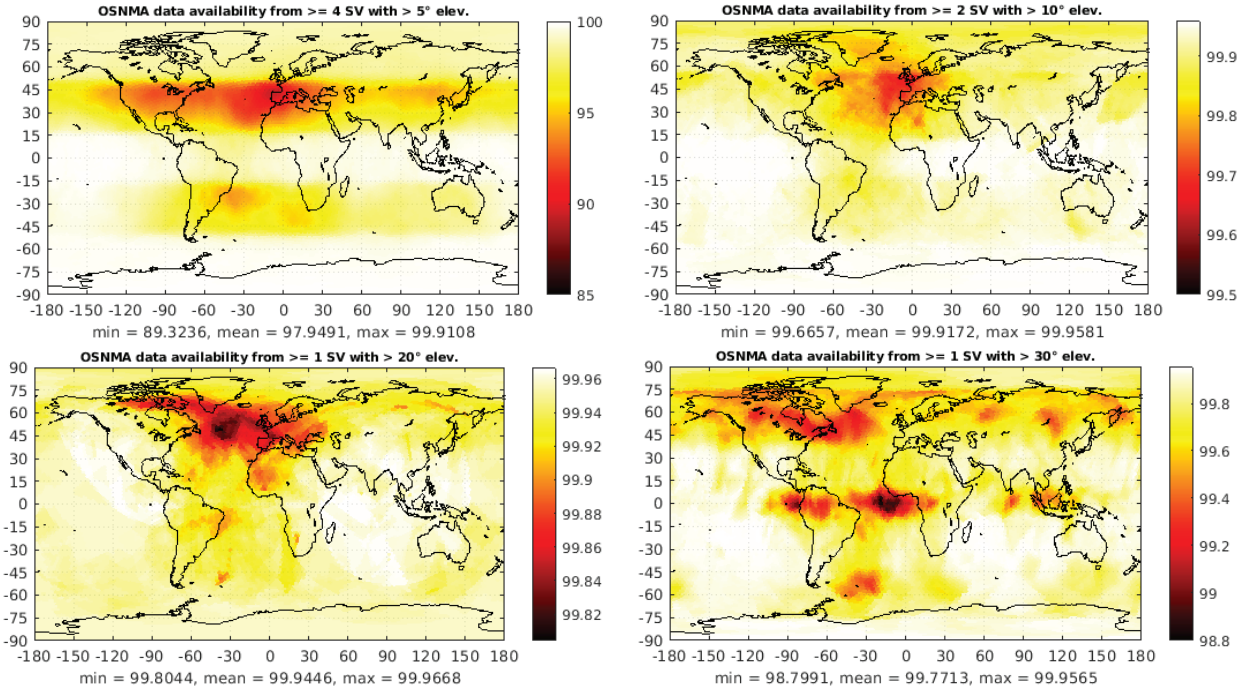

FIGURE 4 OSNMA data availability from at least 4 SV > 5° (upper left), from at least 2 SV > 10° (upper right), from at least 1 SV > 20° (bottom left), and from at least 1 SV > 30° (bottom right) in August 2021

- from at least four Galileo satellites above 5 deg elevation,
- from at least two Galileo satellites above 10 deg elevation,
- from at least one Galileo satellite above 20 deg elevation,
- from at least one Galileo satellite above 30 deg elevation.

While any user location was in view of at least two satellites broadcasting OSNMA data for more than 99.6% of the time during this month, any urban user with an increased elevation mask of 30 deg would still have had access to OSNMA data from at least one satellite for at least 98.8% of the time (see Figure 4). If OSNMA data availability is measured over an observation period of 24 hours, at least 98% daily data availability of OSNMA data provision from at least one satellite above 20 deg elevation is measured at any user location for any day in August 2021.

While these results fully meet the system design expectations, it is still to be highlighted that continuous OSNMA data broadcast is not guaranteed during the Public Observation phase. The user should expect that there may still be sporadic gaps in the OSNMA data broadcast in this phase (e.g., due to maintenance activities).

7 | MAC AVAILABILITY

The MAC availability analysis assesses for every user location, whether or not at least two 40-bit ADKD 0 MACs for authentication of Galileo I/NAV navigation message data from all satellites in view are broadcast within a 120-s period. The following map (Figure 5) demonstrates for the month of August 2021, that any user location is continuously provided with ADKD 0 MACs for data authentication of all satellites in view (above 5 deg elevation angle) with a minimum availability of 97%.

Even in time periods when ADKD 0 MACs have not been received at a specific user location for one or several Galileo satellites in view, the user receiver will often have valid navigation message data for those satellites in memory, which has already been authenticated previously. This implies that both the OS and the OSNMA user are using the same satellites for PVT computation during most of the measurement period.

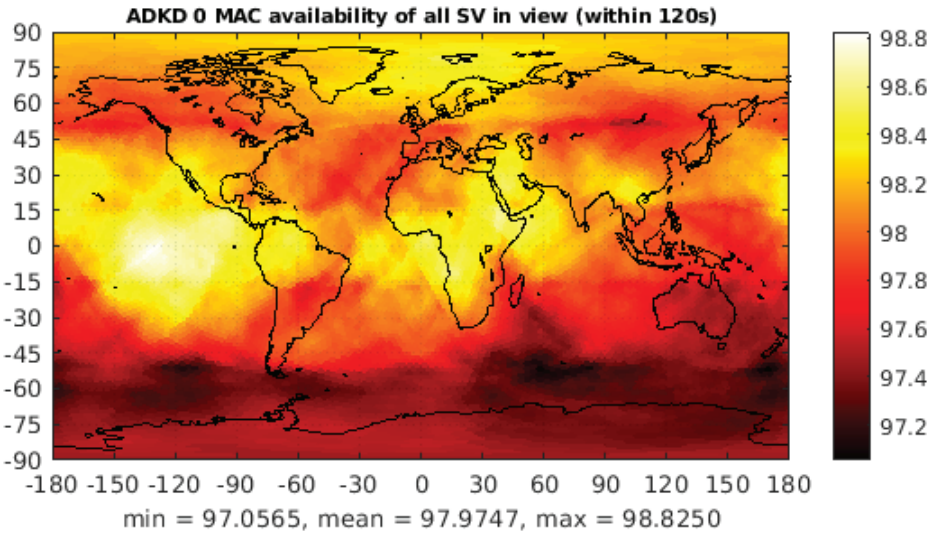

FIGURE 5 ADKD 0 MAC availability for all satellites in view (within 120 s) in August 2021

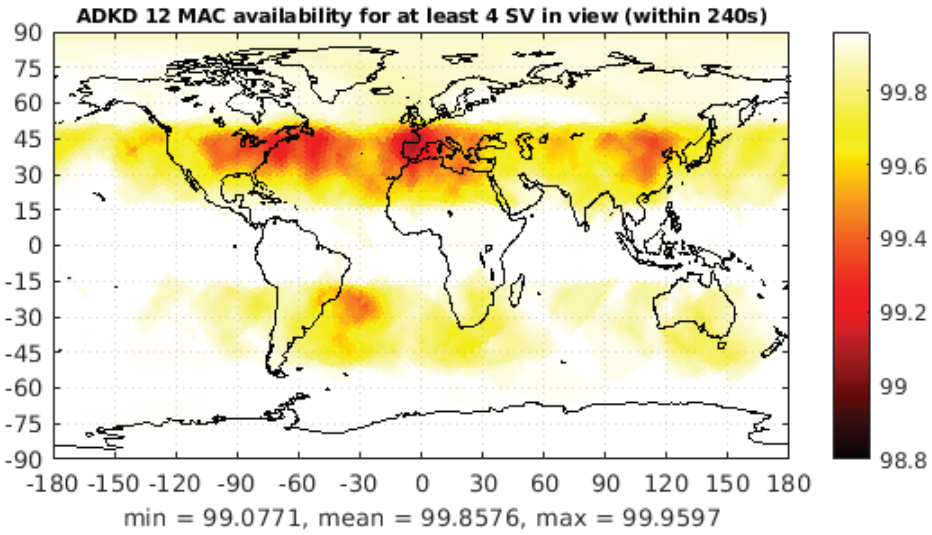

FIGURE 6 ADKD 12 MAC availability for at least four satellites in view (within 240s) in August 2021

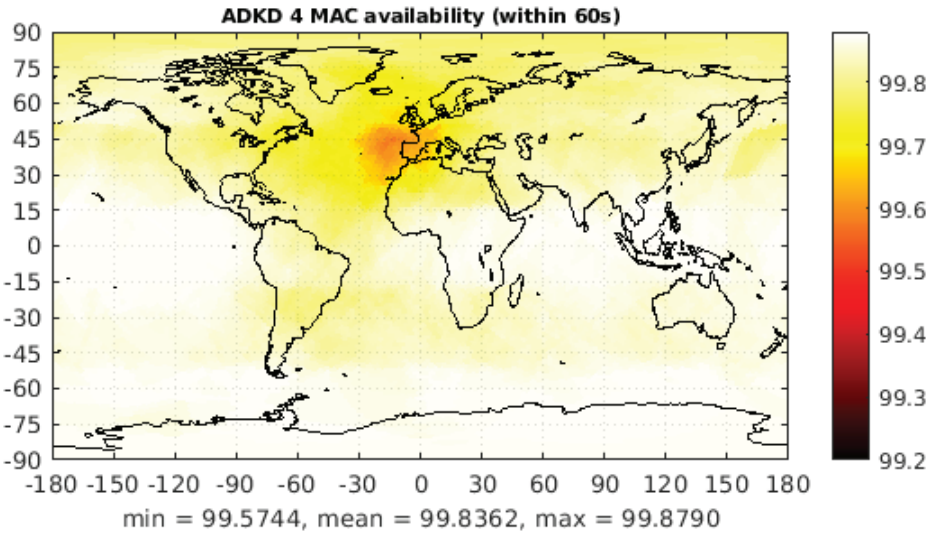

FIGURE 7 ADKD 4 MAC availability for at least one satellite in view (within 60 s) in August 2021

Note: Galileo satellites broadcasting dummy I/NAV messages (GSAT0104) and satellites not transmitting navigation signals (GSAT0204) are excluded from the analysis, as they are neither broadcasting OSNMA data, nor being cross-authenticated by other satellites.

Considering the limited number of ADKD 12 cross-authentication MACs in the proposed OSNMA configuration for the Public Observation phase (Figure 3), the objective is to guarantee ADKD 12 users PVT availability with authenticated data. For this reason, ADKD 12 MAC availability is measured as the percentage of time that any user location is provided with ADKD 12 authentication data for at least four satellites in view. Within a period of 240 s at least two 40-bit ADKD 12 MACs for authentication of at least four satellites in view are to be received at any user location.

The measured availability at the worst user location exceeds 99% in August 2021 (Figure 6). This implies that the 'slow MAC' ADKD 12 user will be capable of computing a Galileo position solution using only data-authenticated satellites with a

high availability. It is again noted that ADKD 12 users operating the user receiver over a continuous period of time, will successively authenticate navigation messages from all (or almost all) satellites in view.

The third MAC availability map illustrates that timing users were provided with ADKD 4 MACs for authentication of UTC time conversion parameters with an availability of more than 99.5% at any user location in August 2021 (Figure 7). It is sufficient to authenticate one set of timing parameters broadcast by any Galileo satellite, as all Galileo satellites usually transmit the same timing parameters.

8 | POSITION ACCURACY AND PVT AVAILABILITY

Position accuracy of the static OSNMA user has been evaluated in post-processing over the complete test period, making use of the aforementioned N#MAtch software toolset for OSNMA data processing and PVT computation. This set-up allows characterization of positioning performance for all different kinds of OSNMA user types. E1 Single Frequency, E1-E5b Dual Frequency, ADKD 0, and Slow MAC ADKD 12 users have all been processed in parallel and characterized both in rural and urban user scenarios.

8.1 | Static OSNMA User

Navigation data is collected with a Septentrio PolaRx5 GNSS receiver, connected to a fixed geodetic antenna at Airbus premises south of Munich. A snap-shot PVT solution is computed every second, considering the observation data and navigation messages logged by the receiver for the standard Open Service user, and processing only satellites that have been data authenticated by the N#MAtch software for the OSNMA user. An elevation mask is applied in post-processing to differentiate between rural (5 deg elevation) and urban static users (30 deg elevation). The PVT engine is configured for non-weighted least squares position solutions, applying a Hatch filter for carrier-smoothing of the code pseudorange observations, as specified for Galileo OS service validation. All analyses presented in the following consider a MAC accumulation target of 80 bits.

The timeline of positioning solutions is compared with the known coordinates of the antenna in order to obtain a timeline of horizontal and vertical positioning errors, from which further accuracy statistics have been derived.

All analyses performed during the test period demonstrate that the positioning performance of the static OSNMA user is very similar to that of the standard Galileo Open Service user. Figure 8 presents the horizontal position error distribution for different types of static users. The color code represents, in a logarithmic scale, the number of positioning solutions with a particular horizontal position error (denoted as 'nobs' in the figure). The plots present results for a time period of approximately 26 continuous days in July 2021, during which the OSNMA configuration was the same as that used in the Public Observation phase. The plots also present the 95-percentile of the horizontal positioning error during this period.

The 95% horizontal position accuracy is almost equal for all users during this time period. Coincidentally, the open sky ADKD 0 OSNMA user with 5 deg elevation mask (diagrams on the top) observes an even slightly better accuracy than the standard OS user during this particular test period. In general, the OSNMA position solutions tend to be very similar or equal to the standard OS one. OSNMA users are usually able to authenticate all satellites in view in a short time, but there

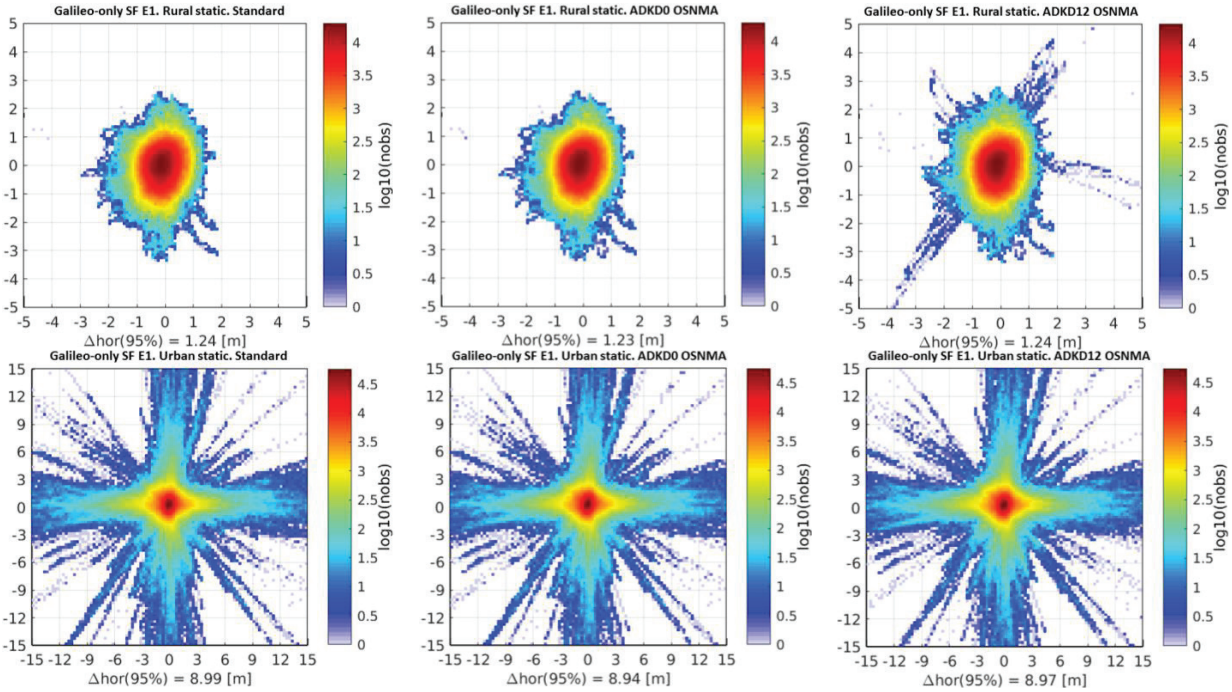

FIGURE 8 Horizontal position error distribution (North-East) for different static users: rural (top) and urban (bottom), standard Galileo E1 Single Frequency (SF) user (left), OSNMA ADKD 0 user (middle), and OSNMA ADKD 12 (right)

are short intervals in which the standard user may be able to use a new satellite rising above the horizon or to apply a newly refreshed navigation message from a satellite in view earlier than the OSNMA user. Adding an additional satellite or applying refreshed navigation message data for PVT computation does not necessarily imply a more accurate position solution, therefore the OSNMA users may sometimes even observe slightly better accuracy than the standard users. Due to the lower number of ADKD 12 cross-authentication MACs, the ADKD 12 user may not always be able to authenticate all satellites in view, but the observed position accuracy is still very close to the one observed by the ADKD 0 OSNMA user.

The position accuracy observed by static users in urban scenarios with 30 deg elevation mask, is again competitive with that of the standard OS user, while reduced PVT availability is obtained for this type of user.

Table 2 provides an overview of the positioning accuracy obtained by the OSNMA users during the test phase. Results are classified by seven different OSNMA configurations that have been applied during the test phase, each of them considering a different number of MAC and ADKD types and/or MAC and Key size. OSNMA Configuration 7 is applied during the Public Observation phase. Without discussing the different test configurations in detail, all tests confirm that the observed positioning accuracy of the ADKD 0 OSNMA user has been the same or very close to that of the standard OS user in any applied configuration scenario during the complete test phase.

Table 2 presents position accuracy results calculated over the complete test period in each test configuration (each of at least 10 days duration). Further studies have been performed to analyze the positioning accuracy and the divergence between the position solution of the OSNMA user and the standard OS user over shorter measurement intervals. Position accuracy has been analyzed for static users over sliding windows of 30-min duration. The horizontal and vertical position accuracy (95-percentile) is obtained for each time window for the standard OS user, the

TABLE 2
Summary of Positioning Accuracy Results for Rural Galileo-Only E1 Single Frequency (SF) Static User

OSNMA Configuration	Horizontal accuracy (95%) [m]			Vertical accuracy (95%) [m]		
	Standard	ADKD 0	ADKD 12	Standard	ADKD 0	ADKD 12
1	1.21	1.22	1.34	1.63	1.63	1.75
2	1.28	1.28	1.40	1.46	1.46	1.59
3	1.17	1.18	1.21	1.65	1.65	1.66
4	1.10	1.12	1.17	1.59	1.59	1.61
5	1.23	1.23	1.31	1.58	1.58	1.68
6	1.18	1.18	1.20	1.69	1.70	1.77
7	1.24	1.23	1.24	1.83	1.82	1.81

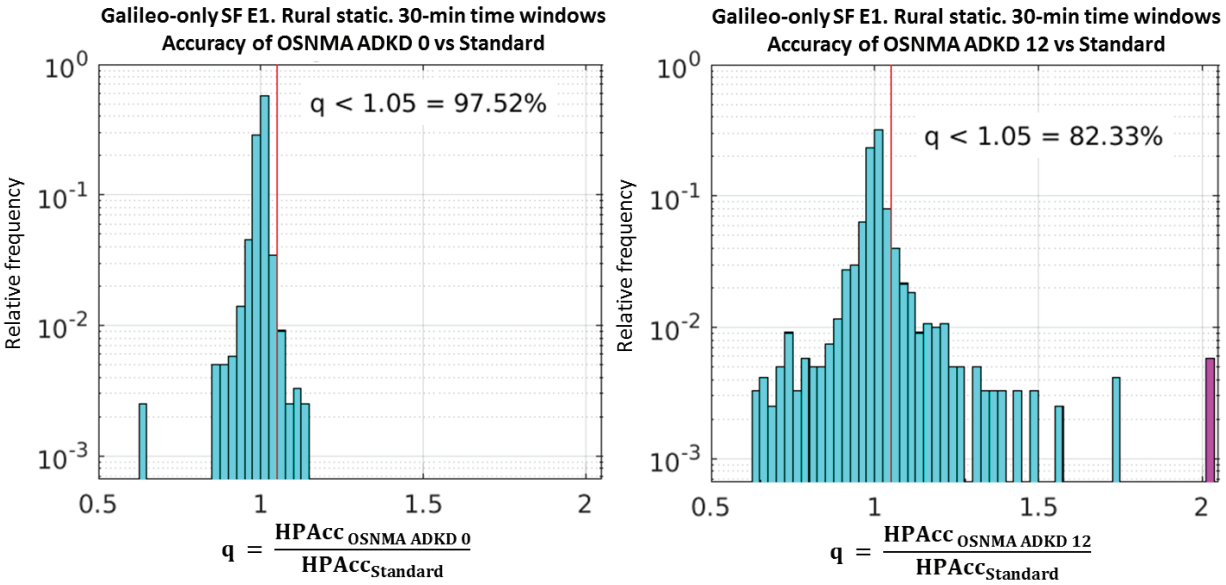

FIGURE 9 Comparison between the OSNMA and the standard horizontal position accuracy over short time windows. Note: purple bar in the right plot contains all time windows with q > 2

OSNMA ADKD 0 user, and the OSNMA ADKD 12 user. The quotient q between the position accuracy of the OSNMA user and the accuracy of the standard OS user assesses for each time interval if both user types observe the same accuracy (q=1), or if the accuracy of the OSNMA user is better (q<1) or worse (q>1) than that measured by the standard OS user.

Figure 9 presents the relative frequency of occurrence of the quotient q for the test period in July 2021 (around 624 samples derived from 30-min time windows over 26 days).

The diagram in the left displays the quotient between the OSNMA ADKD 0 horizontal accuracy and the standard OS user accuracy, while the diagram in the right refers to the accuracy of the OSNMA ADKD 12 user. As expected, the accuracy of the OS and the OSNMA user do not differ significantly in most time intervals: 97.5% of the time, the accuracy of the ADKD 0 OSNMA user is less than 5% worse than that of the standard OS user (or even better). The statistical dispersion of the ratio between the ADKD 12 position accuracy and the OS accuracy is larger than that for the ADKD 0 user. Still, more than 80% of the time the accuracy of the ADKD 12 OSNMA user is less than 5% worse than that of the OS user (or even better). It is recalled again that a simplified non-weighted least squares PVT

computation is applied for this analysis. When applying more sophisticated GNSS positioning engines an even higher degree of convergence between the standard and OSNMA position solutions would be expected.

8.2 | Dynamic OSNMA User

Further tests were performed in dynamic conditions, for different user types (pedestrian and vehicle) and user environments (rural and urban). Test campaigns for characterization of rural user performance were conducted in a rural area south of Munich, with good visibility conditions (but sporadic shadowing from trees or small houses). Tests of urban OSNMA user performance have been conducted in the city center of Munich. The same PVT and OSNMA engines as for the static user analysis have been applied. A Novatel SPAN system, which uses GNSS measurements and corrections, and inertial sensors, has been used to obtain a precise reference trajectory for each test.

Figure 10 presents an example of one mobile scenario (urban vehicle) in order to illustrate how standard and OSNMA ADKD 0 positioning solutions evolve over time. The diagram further demonstrates that both position solutions of the OSNMA and the OS user coincide during large parts of the test (orange dots representing the horizontal error of the OSNMA user coinciding with the blue circles representing the horizontal error of the standard OS user).

The two tables below summarize the results of the pedestrian and vehicle user tests in terms of positioning accuracy and PVT availability. The duration of each test was around 3 hr. As for the static scenario, the ADKD 0 OSNMA user results for positioning accuracy and PVT availability are in line with the standard Galileo Open Service user, in both rural and urban environments.

For the rural pedestrian scenario, the PVT availability is lower than 100% even for the standard user, as a short part of the trajectory passes below a bridge.

Similar performance has been observed for the ADKD 12 OSNMA user in rural scenarios, but not in urban settings. It should be noted that all mobile user testing was performed in OSNMA configurations without ADKD 12 cross-authentication, which is not representative of the OSNMA test configuration that will be in place during the Public Observation phase. It can be shown that one single ADKD 12 cross-authentication MAC within the MAC sequence, considerably improves the

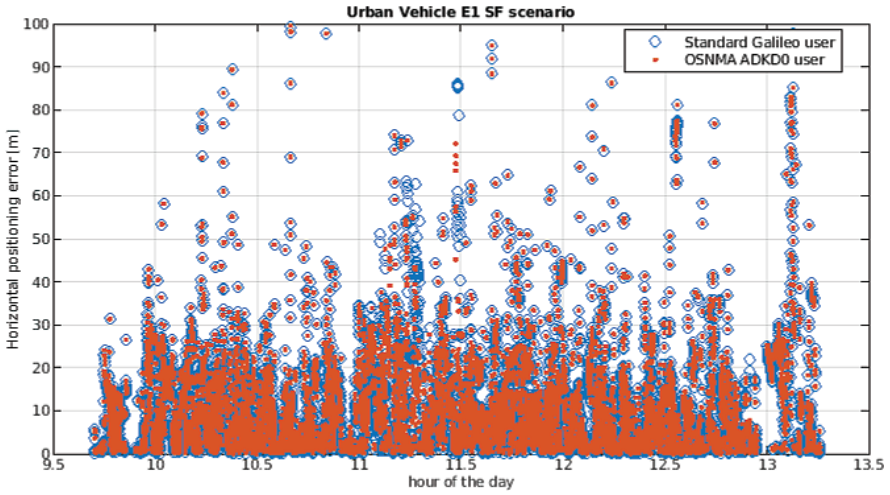

FIGURE 10 Timeline of horizontal position error for an urban vehicle scenario

TABLE 3
Summary of Positioning Accuracy Results for Galileo-Only E1 SF Mobile User

Scenario	Horizontal positioning accuracy [m] 95-percentile			Vertical positioning accuracy [m] 95-percentile		
	Standard	ADKD 0	ADKD 12	Standard	ADKD 0	ADKD 12
Rural Pedestrian	1.2	1.3	1.4	1.8	1.9	2.0
Urban Pedestrian	35.1	36.5	44.2	50.5	50.0	56.2
Rural Vehicle	2.0	1.9	1.6	3.1	3.0	2.2
Urban Vehicle	30.6	32.0	33.6	52.1	54.2	51.6

TABLE 4
Summary of PVT Availability Results for Galileo-Only E1 SF Mobile User

Scenario	PVT Availability [%]		
	Standard	ADKD 0	ADKD 12
Rural Pedestrian	98.9%	98.9%	98.9%
Urban Pedestrian	97.4%	97.1%	37.4%
Rural Vehicle	100.0%	100.0%	100.0%
Urban Vehicle	96.7%	96.7%	90.1%

percentage of time that navigation message data from at least four satellites in view are authenticated by means of ADKD 12 MACs. For this reason, the performance of the slow-MAC OSNMA users is expected to improve significantly with respect to results reported in Table 3 and Table 4.

9 | TIME TO FIRST AUTHENTICATED FIX

Different receiver initialization scenarios are defined for the OSNMA user:

- OSNMA Cold start: receiver neither possesses the Public Key nor the TESLA root key in force and needs to retrieve both from the Galileo Signal in Space
- OSNMA Warm start: the receiver possesses the Public Key and can retrieve and verify the TESLA root key and proceed with the MACK verifications
- OSNMA Hot start: the receiver already possesses a verified TESLA root key, so it can immediately start processing the MACK sections

The OSNMA Cold start was not tested during the preparation phase, as the regular provision of the Public Key via the Galileo Signal in Space will only be available for the OSNMA service phase, as mentioned earlier in this paper.

An OSNMA capable test receiver, connected to the fixed antenna at Airbus premises in Munich, has been used for the TTFAF tests. The receiver has been configured to Galileo-only E1 SF position determination, with an elevation mask of 5º. MAC accumulation up to 80 bits equivalent MAC size has been configured for OSNMA data processing. The test receiver is designed so that data fully transmitted before the MAC is used for MAC verification. For all tests, no ephemeris or almanac are available to the receiver at initialization.

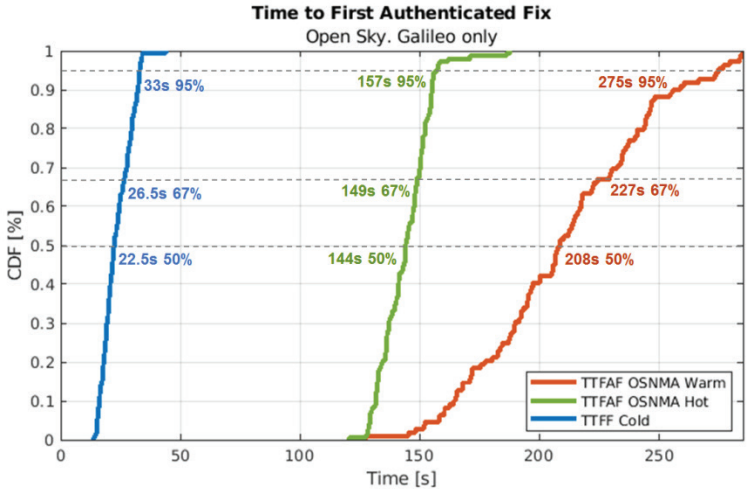

FIGURE 11 TTFAF results for OSNMA ADKD 0 user (green, red) and TTFF results for standard OS user (blue)

TABLE 5
TTFAF Results for ADKD 12 User OSNMA Hot Start

	50%	67%	95%
ADKD 12	446 s	454 s	570 s

Multiple restarts have been set-up in the laboratory and TTFAF statistics have been derived for the ADKD 0 user, as displayed in Figure 11. TTFAF is measured in an OSNMA Warm Start and in an OSNMA Hot Start and compared with the Time To First Fix of the standard OS user (not using the OSNMA data). It is noted that the TTFAF performance could be improved by further optimization of the NMA data processing by the test receiver.

Additional TTFAF tests have been performed for ADKD 12 users. The measured TTFAF is degraded with respect to that of the ADKD 0 user. The main reason is the additional delay of 5 min between the ADKD 12 MACs and the corresponding key, and also the reduced bandwidth allocated to this type of MAC.

10 | FURTHER ENHANCEMENTS FOR OSNMA SERVICE PROVISION

While all OSNMA user performance results, as observed during the test phase and as presented in this paper, are considered very encouraging and do fully confirm the system design expectations, some further enhancements have still been identified for implementation until the future OSNMA service phase.

The OSNMA user may face sporadic MAC verification failures during this period. The root cause is understood and corrective measures are under implementation. The "reserved" fields within the MACK section of the OSNMA data, as displayed in Figure 3, will be re-defined for the future OSNMA service phase in order to prevent such residual MAC verification failures and to provide the OSNMA user with an unambiguous link between MAC and navigation data to be used for MAC verification.

During the Public Observation phase, registered users are expected to retrieve the applicable Public Key from the OSNMA server of the Galileo Service Centre,

while in future the Public Key will also be broadcast in regular intervals within the OSNMA data in the Galileo SIS.

It is worth mentioning that the OSNMA protocol offers a high degree of flexibility to support future evolutions of the OSNMA service after the start of initial OSNMA service provision. MAC and key sizes are configurable to be adapted to evolving security needs. New MAC types for authentication of additional navigation message data may be defined and introduced after the start of the initial OSNMA service.

Authentication of Galileo F/NAV navigation message data and authentication of GPS L1 C/A navigation message data have already been successfully tested during the internal test phase, even though they will not be part of the initial OSNMA service.

11 | SUMMARY AND CONCLUSIONS

Completing the internal test and preparation phase, the Galileo Programme took important steps towards the implementation of the first-ever operational GNSS data authentication service provided within an Open Service signal. The Galileo OSNMA User ICD for the Test Phase has been published in order to make the protocol specification publicly available to receiver manufacturers, application developers, and research institutions ahead of the following Public Observation phase. The ICD is further complemented by Receiver Guidelines to support the secure implementation of the authentication scheme and to provide developers with test vectors and sample OSNMA data for verification.

The OSNMA test configuration for the Public Observation phase has been identified and validated. OSNMA user performance has been characterized for static and dynamic users in rural and urban user environments. Various test campaigns have been performed with different prototype OSNMA receivers by various participants of the OSNMA test phase at different test sites in Europe and complemented with additional analyses post-processing the I/NAV navigation message and OSNMA data received by standard Galileo OS receivers. All tests demonstrate that the position accuracy and PVT availability of the ADKD 0 OSNMA user are very close to that observed by the standard OS user, which confirms a fundamental objective of the Galileo OSNMA service design. ADKD 12 cross-authentication has been introduced for the Public Observation test signal in order to further improve the ADKD 12 OSNMA user performance in urban environments.

Time To First Authenticated Fix has been measured for ADKD 0 and ADKD 12 users in OSNMA Warm Start and Hot Start scenarios. Observed results can be improved by means of further receiver optimization regarding OSNMA data collection and processing by the test receiver.

The Airbus software package N#MAtch has been applied for OSNMA monitoring considering the global Galileo OSNMA service volume. Observed OSNMA data availability and measured MAC availability meet the expectations from system design. It is still to be decided which Minimum Performance Levels will be specified for a future Galileo OSNMA service declaration. MAC availability is considered a suitable performance parameter, as it is independent of the user environment, can be monitored and reported for any user location on a monthly basis, and correlates with the position accuracy and PVT availability of the OSNMA user.

By means of global OSNMA signal monitoring, it has further been verified that each digital signature, TESLA key, and MAC broadcast by any Galileo satellite may be successfully verified by the OSNMA user. Some sporadic failed MAC verifications have been observed during the testing. The root cause of these failed MAC verifications is known and corrective measures have been identified and will be

deployed for the service provision phase. Resilience of the operational infrastructure will be further enhanced towards operational service provision and further advancements of the authentication scheme will be implemented.

While not discussed in further detail in this paper, it is worth remarking that functional processes for Key Chain Renewal, Key Chain Revocation, Public Key Renewal, and Public Key Revocation that are required for operational OSNMA service provision have also been successfully tested in order to verify compliance with the User ICD and to ensure readiness of the infrastructure for entering into the Public Observation phase.

GNSS application developers, research institutions, and receiver manufacturers will have the opportunity to implement the Galileo OSNMA authentication mechanism specified in the OSNMA Test SIS ICD, to participate to the Public Observation phase, and to provide feedback on the OSNMA test signal.

ACKNOWLEDGMENTS

This work is funded by the European Union under the Galileo Programme budget and managed by the European Union Agency for the Space Programme (EUSPA).

The authors would like to acknowledge Antoine de Latour for his contribution to the definition and implementation of Galileo OSNMA and the work presented in this paper.

REFERENCES

European Union (2021a). Galileo open service navigation message authentication (OSNMA) - User ICD for the test phase, Issue 1.0. https://www.gsc-europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma.

European Union (2021b). Galileo open service navigation message authentication (OSNMA) – Receiver guidelines for the test phase, Issue 1.0. ISBN: 978-92-9206-056-5. https://www.gsc-europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma.

Fernández Hernández, I., Ashur, T, & Rijmen, V. (2021). Analysis and recommendations for MAC and key lengths in delayed disclosure GNSS authentication protocols. *IEEE Transactions on Aerospace and Electronic Systems, 57*(3), 1827–1839. https://doi.org/10.1109/TAES.2021.3053129.

Fernández Hernández, I., Ashur, T, Rijmen, V., Sarto, C., Cancela, S., & Calle, J. D. (2019). Toward an operational navigation message authentication service: Proposal and justification of additional OSNMA protocol features. *2019 European Navigation Conference (ENC),* 1–6. https://doi.org/10.1109/EURONAV.2019.8714151.

Fernández Hernández, I., Rijmen, V., Seco-Granados, G., Simón, J., Rodríguez, I., & Calle, J. D. (2014). Design drivers, solutions and robustness assessment of navigation message authentication for the Galileo open service. *Proc. of the 2014 International Technical Meeting of the Institute of Navigation (GNSS+ 2014).* 2810–2827.

Fernández Hernández, I., Rijmen, V., Seco-Granados, G., Simón, J., Rodríguez, I., & Calle, J. D. (2016). A navigation message authentication proposal for the Galileo Open Service. *NAVIGATION, 63*(1), 85–102. https://doi.org/10.1002/navi.125.

Fernández Hernández I., Walter T., Neish A., & O'Driscoll, C. (2020). Independent time synchronization for resilient GNSS receivers. *Proc. of the 2020 International Technical Meeting of the Institute of Navigation (ITM 2020)*, 964–978. https://doi.org/10.33012/2020.17190.

Perrig, A., Canetti, R., Tygar, J. D., & Song, D. (2002). The TESLA broadcast authentication protocol. *CryptoBytes, 5*(2), 2–13. https://doi.org/10.1007/978-1-4615-0229-6_3.

How to cite this article: Götzelmann, M., Köller, E., Viciano-Semper, I., Oskam, D., Gkougkas, E., Simon, J. (2023). Galileo open service navigation message authentication: Preparation phase and drivers for future service provision. *NAVIGATION, 70*(3). https://doi.org/10.33012/navi.572