Strengthening GNSS Receivers via Authentication and High-Accuracy Overlays

Emmanouil Papadakis, Ivan Rey García, Iulian Diaconescu, Rafael Terris-Gallego, Gonzalo Seco-Granados, José A. López Salcedo
Universitat Autònoma de Barcelona, IEEC, CERES
Bellaterra, Spain

Víctor Gracia, Arnau Pena, Sílvia Navarta, Marc Solé
Satellite Navigation Department
Indra Space
Barcelona, Spain

2026 IEEE 13th International Workshop on Metrology for AeroSpace (MetroAeroSpace) | 979-8-3315-5125-4/26/$31.00 ©2026 IEEE | DOI: 10.1109/METROAEROSPACE69299.2026.11646685

***Abstract*— The increasing reliance on Global Navigation Satellite Systems (GNSS) in safety- and liability-critical applications exposes users to growing threats from spoofing, meaconing, and interference. While authentication services such as Galileo OSNMA improve signal trust, and high-accuracy overlays enhance positioning performance, these capabilities are often treated independently and not available to most of the existing receivers. This paper focuses on the in-house development of a GNSS analysis performance system (GAPS), a software overlay capable of processing raw measurements from a conventional Galileo receiver, and leveraging on the use of the Galileo OSNMA and Galileo HAS services to achieve authenticated and accurate positioning. Experimental results show that combining authentication with accuracy-enhancing services enables both improved positioning precision and increased protection against malicious signal manipulation. The proposed approach highlights the combination of existing hardware and with an additional software overlay, resulting in more trustworthy and high-performance GNSS receivers suitable for emerging aviation and aerospace applications.**

Keywords—GNSS, Galileo, authentication, high-accuracy, OSNMA, ACAS, SAS, HAS.

I. Introduction

Global Navigation Satellite Systems (GNSS) are critical for a myriad of applications, including transportation, asset tracking, emergency response, critical infrastructures and timing synchronization, among many other. However, most of the existing GNSS signals remain vulnerable to spoofing attacks and often lack the precision required for autonomous applications. To address these limitations, the European Galileo system has introduced two key features: the Open Service Navigation Message Authentication (OSNMA) to cryptographically verify authenticity of the received data, and the High Accuracy Service (HAS) to provide decimeter-level Precise Point Positioning (PPP) globally. Additionally, the Signal Authentication Service (SAS) has started to be broadcast in testing mode, and in the near future will provide an additional layer of security through signal and spreading code encryption.

In this context, the present work focuses on the implementation of the two currently operational Galileo added-value services, namely OSNMA and HAS. While these services are gradually being natively integrated into new generations of Galileo receivers, a vast population of already deployed receivers remains vulnerable to an increasing range of threats. Enhancing the robustness of such receivers, while simultaneously providing improved positioning accuracy, can be achieved through the addition of a dedicated software overlay. In particular, by processing the raw output measurements provided by many of the existing receivers and adding a dedicated software layer for combining these measurements with the information broadcast by the OSNMA and HAS services. In this way, it is possible to deliver the levels of security and accuracy required by many applications, especially those that are safety- or liability-critical.

To this end, the present work describes the development of an in-house GNSS analysis performance system (GAPS) capable of providing secure and accurate positioning as a software overlay to an existing GNSS receiver. The development is able to process the raw data provided by a conventional Galileo receiver through the smooth integration of three software modules implementing OSNMA functionalities for data authentication, HAS functionalities for accurate positioning, and positioning functionalities combining raw GNSS measurements with the information provided from OSNMA and HAS. The combination of these three software modules is able to bridge the gap between existing Galileo receivers and the stringent demands in terms of spoofing prevention and position accuracy.

The paper is structured as follows. First, a review of the Galileo services will be provided in Section II, in order to provide a brief overview of their motivation and operation. Section III will follow with the high-level description of the GAPS developed herein. The performance assessment will be carried out in Section IV, and finally conclusions will be drawn in Section V.

II. Overview of Galileo Services

A. Open Service Navigation Message Authentication

The Open Service Navigation Message Authentication (OSNMA) capability that is broadcast on Galileo's E1-B I/NAV signal adds a cryptographic "signature" to the navigation message so that a receiver can confirm two things. First, that the data really originated from an authentic Galileo satellite; and second, that it was not modified in transit. Authentication focuses on data-level integrity rather than signal-level encryption, so it can be delivered free-to-air and without extra receiver hardware. The authentication bits are inserted into previously reserved fields, meaning that the OS performance (data rate, legacy compatibility, etc.) is not affected.

From a protocol standpoint OSNMA adapts the TESLA (Time-Efficient Stream Loss-tolerant Authentication) scheme to GNSS. A Merkle-tree-protected public key is periodically signed on the ground with ECDSA-256; from that key, a one-way "root key" chain is generated, and short Message Authentication Codes (MACs) are produced for every I/NAV page. The corresponding symmetric key is disclosed by the satellite 30 seconds later, allowing the receiver to verify the MAC after a short delay but before it could be replayed by a spoofer. Public-domain test vectors [1], ICDs [2], [3], and receiver guidelines [4] are already available, so manufacturers and practitioners implement and test this feature today.

For users with accurate positioning requirements, authenticated data bring two direct benefits:

- Resilience to spoofing-assisted integer ambiguities. By letting the receiver detect and discard falsified ephemeris or clock data early, OSNMA prevents the positioning engine from fixing ambiguities on corrupted measurements, thus avoiding incorrect fixes and the long recovery procedures that follow.

- Trustworthy multi-GNSS weighting. Authenticated Galileo measurements can be given higher weight than unauthenticated signals from other constellations, yielding more robust Position Velocity Time (PVT) solutions.

B. High-Accuracy Service

The High Accuracy Service (HAS) is a free and open service provided by Galileo that is aimed at delivering centimeter-level positioning accuracy to users worldwide. Unlike standard GNSS positioning, which typically offer accuracy on the order of a few meters, HAS enhances it significantly, by broadcasting corrections on the satellite orbit, clock, and bias information directly through the Galileo E6-B signal. These corrections enable users to apply PPP techniques already with the data delivered by the signal-in-space, or alternatively, retrieved from the Internet thanks to the Galileo HAS Internet Data Distribution.

The service nominally broadcasts the high-precision corrections as part of the Galileo E6-B signal, centered at 1278.75 MHz. Users can receive this information with a dual-frequency Galileo receiver that supports the Galileo E6 signal, as the secondary signal, and implements a PPP algorithm on either the Galileo E1 or Galileo E5 signals. The initial time to convergence (i.e., the time needed for the positioning solution to reach full accuracy) can still range from a few minutes to tens of minutes, depending on receiver quality, signal environment, and data handling. As of its initial operational capability, HAS aims to provide horizontal positioning accuracy better than 20 cm, and vertical accuracy under 40 cm (95%), with ongoing improvements expected as the service matures [5]. The European Union plans to expand the capabilities of HAS in the future, including multi-frequency, multi-constellation support and possibly the inclusion of integrity information.

In summary, Galileo HAS represents a significant step in democratizing high-precision GNSS services, offering an open-access alternative to traditionally subscription-based correction services. Its integration into low-cost and embedded GNSS receivers opens new possibilities for mass-market applications requiring highly accurate positioning, such as precision farming, drone navigation, autonomous vehicles, and surveying, while ensuring European strategic autonomy in critical positioning infrastructure.

C. Signal Authentication Service

The Signal Authentication Service (SAS) is an upcoming Galileo service intended to protect users against GNSS spoofing at the signal level. It complements OSNMA, which authenticates navigation data on the E1-B signal, with ranging authentication on E6-C signal, by leveraging on pilot signal and spreading-code encryption (SCE) [6].

SAS avoids requiring receivers to store secret keys by relying on the cryptographic keys disclosed by OSNMA in the Galileo E1-B signal. The trade-off is a delay in PVT authentication, since TESLA keys are disclosed only after a defined latency. These keys are used to re-encrypt selected fragments of the already encrypted E6-C signal, generating RECS (Re-Encrypted Code Sequences). A SAS receiver may download the RECS ahead of the Signal-in-Space (SIS) broadcast, thus enabling autonomous operation over the intended time window, but until the associated keys are disclosed, no party, including a spoofer, can decrypt these sequences in advance.

After the E6-C signal is broadcast, the receiver captures a snapshot of samples at the predicted RECS time and waits for the associated key to be disclosed in E1-B. Once the key becomes available, the receiver decrypts the pre-downloaded RECS to reconstruct the corresponding E6-C code fragment and correlates it against the stored E6-C snapshot. If a correlation peak is observed and the relevant decision criteria are fulfilled, PVT authentication is achieved [7].

Following several years of definition and development [8], Galileo has recently started initial SAS testing using encrypted SIS transmissions [9]. SAS is expected to become fully operational in the near future.

III. GAPS Software Overlay

A. High-level Architecture

The GAPS is designed as a modular architecture that takes as input the raw measurements provided by a E1/E6 GNSS receiver, which is configured to produce a time-tagged data stream containing observables and navigation information, into a binary format file. As shown in Figure 1, the stream of data is split into three parallel streams, feeding a module implementing HAS functionalities, a module implementing OSNMA functionalities, and finally a positioning engine combining all the produced data, and providing high-accurate and authenticated position fixes.

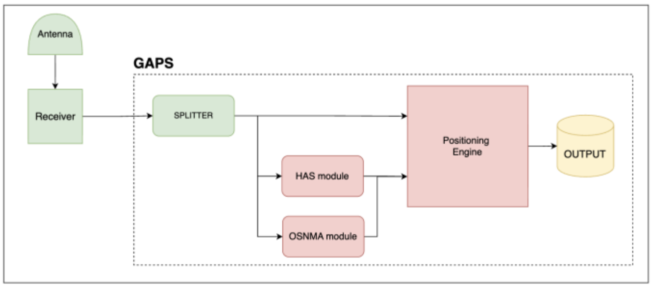

Figure 1. Block diagram of GAPS overall architecture

When HAS support is enabled in GAPS, the HAS decoding module consumes the data stream coming from the receiver, extracts the HAS information contained in the Galileo E6-B navigation pages, and outputs decoded corrections (e.g., in RTCM3 Radio Technical Commission for Maritime Services, format). The latter are provided to the positioning engine as an additional correction input. Similarly, when OSNMA support is enabled, the OSNMA module consumes the same input data stream coming from the receiver and provides authentication-related outputs. In this way, the positioning engine operates with a consistent two-input model: (i) rover observables/navigation data and (ii) optional external augmentation/authentication data, with the rover data path remaining unchanged across configurations.

B. OSNMA functionalities

The GAPS OSNMA module is organised as a three-layer real-time pipeline converting raw Galileo E1-B I/NAV pages into a per-satellite authentication verdict (AUTH / FAIL / PENDING) every second.

- Multi-format ingestion layer: accepts live or recorded I/NAV data. An input buffer re-orders pages and fills gaps by exploiting redundancy across satellites.
- Asynchronous cryptographic engine: runs as asynchronous coroutines with persistent caches to minimise latency.
  - ECDSA-256 signature check of DSM-PKR public-key messages.
  - TESLA chain reconstruction and authentication of DSM-KROOT root keys.
  - MAC/tag verification of MACK messages (ADKD 0, 4, 12) including FLX tags. These optimisations cut the Time-To-First-Authenticated-Fix (TTFAF) from ~100 s to as low as 44 s in hot-start conditions.
- Output & monitoring layer: Generates a real-time log that lists each satellite's authentication state and other key metrics (e.g., key-disclosure delay, lost pages), ready for further analysis or display.

C. HAS functionalities

The most representative key features provided by the GAPS HAS module are the following:

- Input Support: the HAS module can ingest raw Galileo E6-B data from various sources, including live streams via serial ports or TCP connections, as well as pre-recorded files. It supports different receiver data as well as the receiver-independent BINEX format.
- Decoding Capability: The module decodes the Reed–Solomon encoded Galileo E6 navigation data pages to extract HAS messages. These messages contain PPP corrections, including satellite orbit, clock, and bias information for both Galileo and GPS constellations.
- Output Formats: Decoded corrections can be converted into widely used formats such as RTCM3 State Space Representation (SSR) and International GNSS Service (IGS) SSR. This compatibility allows integration with existing GNSS receivers and PPP engines that do not natively support HAS formats.
- Data Distribution: Converted messages can be transmitted via a TCP server for real-time applications or saved locally in files. It also supports output compatible with the PPP-Wizard package, facilitating seamless processing.
- Modular Design: allows straightforward extension to support additional input and output formats, making it adaptable to various GNSS processing needs.

IV. Performance Assessment

The objective of this section is to provide some preliminary results obtained with the GAPS developed prototype. The focus is placed on integrating the combined OSNMA+HAS features, enabling authenticated and highly-accurate positioning to GAPS users.

A. Test setup and test plan

To ensure reproducibility, a pseudo-real-time operational mode was implemented in order to replay a previously recorded GNSS data binary file, if it was a real-time stream. For the undergone tests, this binary file contained raw Galileo E1 and E6 measurements collected for 6hours on 07/05/2026 from 21:07PM to 08/05/2026 at 03:07AM using a static Drotek DA910 multi-band GNSS antenna at the rooftop of UAB premises in Bellaterra, Barcelona (Spain).

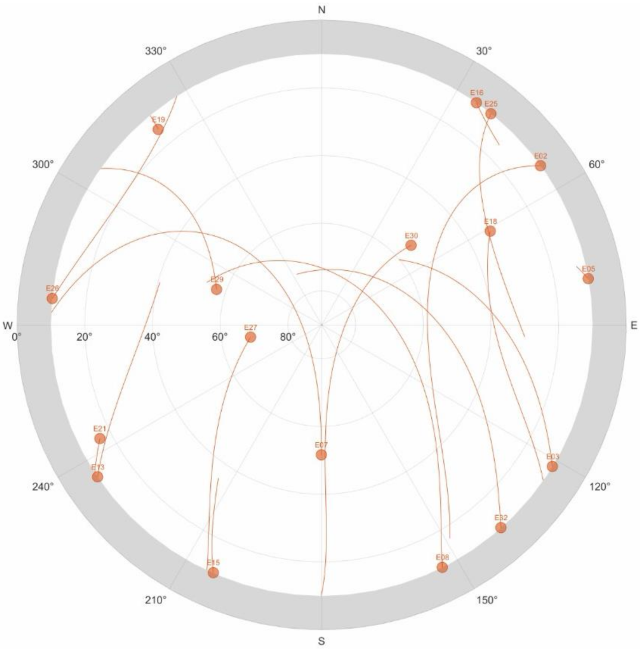

Figure 2. Skyplot of satellites during the test capture.

The test scenarios focus on Galileo-only positioning and are intended to simultaneously incorporate OSNMA and HAS functionalities. The overall processing chain is separated into two streams following standalone HAS and OSNMA, then the outputs are merged before being ingested in the Positioning Engine, where both HAS and OSNMA are truly combined. In addition, a HAS-only solution is simultaneously generated to be directly compared to the HAS+OSNMA combination result. The produced position solutions (HAS-only and combined HAS+OSNMA) are processed in the same way regarding parameters configured in positioning engine.

The mode used is PPP-static, with 10° elevation mask, forward filtering, dual-frequency ionosphere free combination and estimated Zenith Tropospheric Delay model (ZTD) for ionospheric and tropospheric delays respectively. The PPP filter estimates the receiver position, receiver clock offset and carrier-phase ambiguities while ambiguity resolution is disabled; therefore, the solution corresponds to float PPP. Regarding OSNMA a cold start configuration is used. Finally, two positioning solutions are compared the one enriched with HAS corrections only and the other both with HAS corrections and OSNMA filtered satellites.

B. Results for OSNMA+HAS test

HAS+OSNMA integration is realized by using PPP method with Galileo HAS corrections combined with OSNMA-based authentication. To declare the combination of those two features as a success, the results have to be evaluated both under strict HAS positioning thresholds and OSNMA authentication metrics.

Regarding positioning accuracy, the criteria to be met are 0.2m for Horizontal and 0.4m for Vertical by using HAS corrections for 95% of cases [5].

Except for positioning accuracy, the authentication filtering has to be validated by well-established metrics that reflect both the correctness and the continuity of the cryptographic authentication process. The main indicators are Time To First Authenticated Fix (TTFAF), Authenticated Data Availability at User level (ADA-U), and Authenticated Data Availability at Satellite level (ADA-S).[11].

Metrics	Results	Threshold
ADA-U (Time-Weighted)	100%	98%
Availability Ratio (HAS+OSNMA/HAS)	99.6%	95%
ADA-S	97.2%	95%
TTAF	90 seconds	120 seconds

Table 1. Metrics results for OSNMA filtering in 6hours scenario.

ADA-U quantifies how stable authentication remains after the initial warm-up, and is compared against service-level expectations (MPL ≥95%) while a stricter target (e.g., ≥98%) can be used in controlled tests to ensure robustness. For our test 100% is reached.

The position solution availability ratio is the percentage of outcome position fixes with and without OSNMA filtering. This ratio should be greater than 95%

ADA-S evaluates per-satellite authentication consistency over each stable tracking arc; although long-duration experimental campaigns often report values close to 100% for well-tracked satellites [11], using ADA-S ≥95% is appropriate for short-duration tests.

TTFAF measures the elapsed time from the start of processing until authentication becomes usable conservative acceptance threshold of TTFAF ≤ 120s is commonly adopted [12] [13] so this metric is easily reached.

Next, the positioning performance of HAS+OSNMA and HAS-only comparison are evaluated. Figures 3 and 4 show the horizontal and vertical positioning errors for the HAS+OSNMA and HAS-only configurations. Both solutions were generated from the same input data stream and processed simultaneously, allowing a direct comparison between the standard HAS processing chain and the combined HAS+OSNMA chain. The HAS-only solution provides its first position fix at 21:07:59, whereas the HAS+OSNMA solution starts at 21:09:34. The delay of approximately 95s is associated with the OSNMA authentication process. During the initial, non-converged phase, where the PPP filter is still stabilizing, and the solutions are more sensitive to measurement/model changes the two curves show small differences until their almost simultaneous convergence. Convergence is defined by a 300-second (5-minute) sliding window during which the Q95 horizontal and vertical errors remain below specified thresholds. HAS only converges at 21:36:47 (28m 48s after its start) and HAS+OSNMA at 21:36:26 (26m 52s after its start). In order to have a head-to-head comparison a common start should be considered as the start of HAS-only. So the absolute time they converge has a slight difference of 20 seconds which is considered negligible for the current experiment.

After convergence, both solutions are evaluated over a common interval of 19,847 epochs, corresponding to 5 h 30 min 47 s. The post-convergence horizontal performance is practically identical, with H95 = 0.138 m for both HAS+OSNMA and HAS-only, as reported in Table 2. This indicates that enabling OSNMA does not introduce a measurable degradation in the horizontal PPP accuracy under the conditions of this experiment. The vertical component also remains very close between the two configurations, with V95 = 0.217 m for HAS+OSNMA and V95 = 0.221 m for HAS-only. The small difference is consistent with the higher sensitivity of PPP height estimates and expected within the variability of the experiment, so it is not considered significant. Overall, the result indicates that the OSNMA-enabled processing chain preserves the vertical PPP performance of the HAS-only solution.

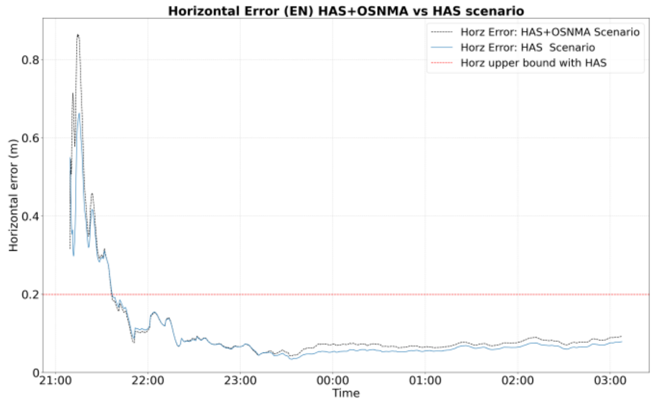

Figure 3. HAS+OSNMA vs HAS-only scenario in horizontal error.

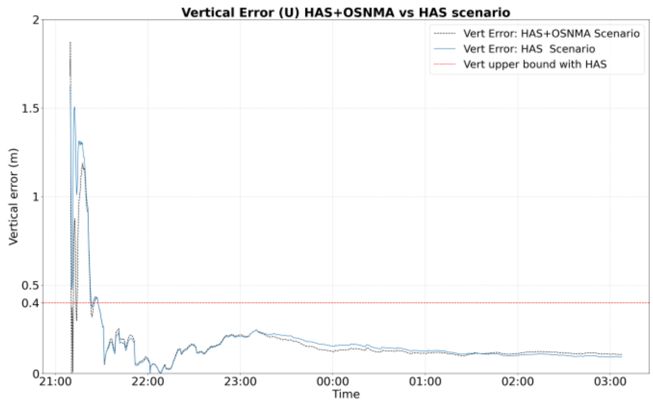

Figure 4. HAS+OSNMA vs HAS-only scenario in vertical error.

Scenario	Epochs	Hor. 95% (m)	Ver. 95% (m)
HAS+OSNMA	19847	0.138	0.217
HAS	19847	0.138	0.221

Table 2. HAS+OSNMA vs HAS-only horizontal and vertical accuracy.

At this point, it is important to remark that PPP convergence with Galileo HAS corrections has a well-known limitation in the current state of real-time PPP processing, and several studies report convergence times ranging from a few tens of minutes up to more than an hour, depending on the environment, receiver/antenna configuration, and processing engine. Similar results are reported in the literature: [14] achieved about 20.5 min convergence with a GPS/Galileo setup in an urban-like station; [10] reported 1 h 18 min convergence for a high-grade receiver in open-sky post-processed PPP with HAS; and studies using other engines also highlight that convergence may not be reached under single-constellation operation, while GPS+Galileo can still require long convergence (e.g., 67 min in [15]). Likewise, [16] shows that convergence below 300s is difficult to achieve, with typical static component-wise convergence on the order of tens of minutes. These outcomes are commonly attributed to practical and algorithmic factors, affecting filter stability during PPP [17], as well as to the sensitivity of the vertical component to modelling deficiencies such as missing antenna PCO/PCV corrections [16]. Therefore, the ~30–35 min convergence observed in this work should be considered a realistic result under current open-source PPP processing constraints rather than an anomaly.

C. *OSNMA scenario with EUSPA test vectors*

In an attempt to verify that OSNMA-enabled configuration works as expected, the official EUSPA Galileo OSNMA test vectors have been replayed using a Safran Skydel scenario. In this test, the signal evolution was defined in three phases: first, a nominal interval with clean signal conditions, second, a jammer transition used to force loss of lock on the authentic satellites while the spoofer was activated, third, a spoofing-only interval in which the spoofed signal remained aligned in time with the authentic but was transmitted with higher power. Under these conditions, the nominal receiver solution reacquired and tracked the spoofed signal after the jammer was removed.

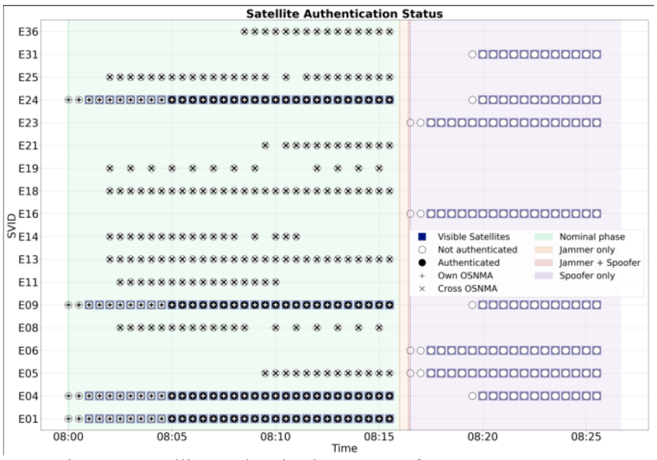

Figure 5. Satellite Authentication Status of EUSPA test vectors.

Figure 5 shows the Galileo satellite authentication status during the different phases of the spoofing scenario. In the initial nominal phase (i.e. green-shaded region), the receiver tracks those Galileo satellites that are indicated by the blue square background. The satellites in view for this phase include E01, E04, E09, and E24. Authenticated satellites are represented by filled black circles. The overlaid symbols distinguish the OSNMA authentication mechanism: the plus ("+") sign indicates own OSNMA authentication, while the cross ("x") indicates cross-authentication. During the nominal phase, satellites E01, E04, E09 and E24 are authenticated. Around 08:16 UTC, the jammer-only phase begins, followed by the combined jammer-spoofer phase. During these intervals, no valid satellite tracking/authentication is available. In the final spoofer-only phase (i.e. purple-shaded region), several satellites are again visible to the receiver; however, they are shown as hollow circles, meaning that they are not authenticated. This indicates that the OSNMA-enabled configuration does not accept the spoofed navigation data as authenticated. Consequently, the positioning engine does not use these unauthenticated measurements to produce a spoofed solution.

The 3D positioning error of the Nominal and OSNMA-enabled solutions during the spoofing scenario is compared in Figure 6. In both solutions, exactly the same positioning parameters are applied by using single point positioning mode with the difference to be that no authentication filtering is applied in Nominal case. During the initial nominal phase with no interference, the two solutions Nominal and OSNMA, overlap with position fixes to be scattered around 2–3 m accuracy. During the jamming-only and jammer-spoofer intervals, no valid position solution is produced from either mode. Once the spoofed signal becomes dominant, the nominal receiver resumes providing fixes but follows the forged solution, with the 3D error increasing to approximately 15 m. In contrast, the OSNMA-enabled solution does not follow the spoofed trajectory and stops providing valid fixes as shown in Figure 5. This behavior illustrates the degradation of the nominal solution under spoofing and the protective response of the OSNMA-enabled receiver, which favors solution unavailability over the use of unauthenticated navigation data.

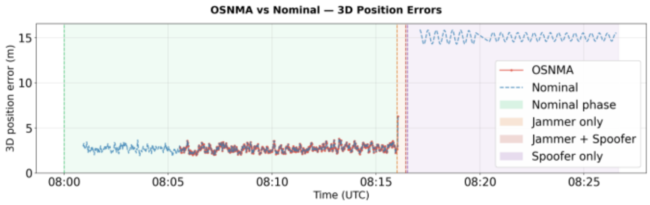

Figure 6. 3D Positioning errors for OSNMA vs nominal.

V. Conclusions

This work shows how Galileo authentication and high-accuracy services can effectively be combined as a software overlay on existing Galileo receivers, leading to a user terminal receiver with strengthened positioning performance and trustworthiness. In the tested scenario, the integrated HAS+OSNMA configuration produced a valid post-convergence solution and preserved HAS-level positioning performance on the common evaluated epochs. However, the experiment should be interpreted as a functional and scenario-based validation. Future testing would include additional tests with multiple receivers deployed at different locations, multi-day campaigns, in order to assess the long-term stability and availability of the solutions, as well as kinematic scenarios involving moving platforms, such as vehicles or UAVs.

References

[1] European GNSS Service Centre (GSC), "Annex B – OSNMA Test Vectors" (ZIP package, cryptographic material and sample data), Nov 2023

[2] European GNSS Service Centre (GSC), "Galileo OSNMA Signal-in-Space Interface Control Document, Issue 1.1", Oct 2023.

[3] European GNSS Service Centre (GSC), "Galileo OSNMA Internet Data Distribution Interface Control Document, Issue 1.1", Jan 2024.

[4] European GNSS Service Centre (GSC), "Galileo OSNMA Receiver Guidelines, Issue 1.3", Jan 2024.

[5] European GNSS Agency, “Galileo High Accuracy Service: service definition document (HAS SDD), issue 1.0, Jan. 2023, Publications Office of the European Union.

[6] I. Fernandez-Hernandez, S. Damy, M. Susi, I. Martini, J. O. Winkel, et al., “Galileo Authentication and High Accuracy: Getting to the Truth,” Inside GNSS, Feb. 2023.

[7] R. Terris-Gallego, J. A. López-Salcedo, G. Seco-Granados, and I. Fernández-Hernández, "Operating Modes and Performance Evaluation of Galileo Assisted Commercial Authentication Service," in Proc. ION GNSS+, Sept. 2022.

[8] R. Terris-Gallego, J. A. López-Salcedo, G. Seco-Granados, and I. Fernández-Hernández, "Preliminary Evaluation of Galileo ACAS using Existing E1-E6 Open Signals and a Low-Cost SDR Platform," in Proc. ION GNSS+, pp. 1388-1402, Sept 2023.

[9] R. Terris-Gallego, J. A. López-Salcedo, and G. Seco-Granados, "Testing Galileo SAS with Encrypted Signal-in-Space," in Proc. ION GNSS+, Sept. 2025.

[10] Cucchi, L., Damy, S., Gioia, C., Motella, B., & Paonni, M., “Galileo High Accuracy Service: Tests in Different Operational Conditions”, Journal of the Institute of Navigation, 71(4), 2024.

[11] C.Sarto, O. Pozzobon, S. Fantinato, S. Montagner, I., Fernández-Hernández, S. Cancela, D. Calle, P. Walker, D. Burkey, G. Seco-Granados, E. Gähler, “Implementation and Testing of OSNMA for Galileo,” in Proc. ION GNSS+, pp. 1508–1519, Sept. 2017.

[12] T. Hammarberg, J.M. García, J.N. Alanko, M.Z.H. Bhuiyan, “An Experimental Performance Assessment of Galileo OSNMA,” Sensors, 24(2), 2024.

[13] European GNSS Supervisory Authority. (2021). Galileo Open Service Navigation Message Authentication (OS-NMA): Info note. Publications Office.

[14] Prol, Fabricio S., et al. “Enabling the Galileo High Accuracy Service with Open-Source Software: Integration of HASlib and RTKLIB.” GPS Solutions, vol. 28, no. 2, Feb. 2024, p. 71. Springer Link, https://doi.org/10.1007/s10291-024-01617-7.

[15] A. Ramos, N. Lelarge, C. Gazzino, E. Bernadotte, V. Raviart, "Evaluation of the Galileo/GPS High Accuracy Service (HAS) Performance for Enhanced Navigation Precision," in Proc. ION GNSS+, pp. 1189-1218, Sept 2024.

[16] G. Marut, T. Hadas, K. Kazmierski, J. Bosy, “Affordable Real-Time PPP—Combining Low-Cost GNSS Receivers with Galileo HAS Corrections in Static, Pseudo-Kinematic, and UAV Experiments”. Remote Sensing. 16. 4008, 2024.

[17] Savchuk, S., Grzegorzewski, M., Gołda, P., & Kerker, V., “Positioning using the precision Galileo HAS service,” Annual of Navigation, 29, 60–68.