

# Looking into the Galileo Signal Authentication Service: Early demonstration of the service and experimentation

Miguel A. Ramírez, Simón Cancela, David Calle, *GMV*  
Ignacio Fernandez-Hernandez, Tom Willems, Jon Winkel, *European Commission*  
Rafael Terris-Gallego, Gonzalo Seco-Granados, *Univ Autonoma de Barcelona, CERES-IEEC*

## BIOGRAPHY

Miguel Alejandro Ramirez holds a BSc in Electronic Systems Engineering by the Escuela de Telecomunicaciones, Universidad de Málaga. He joined GMV in 2021 and has been working in projects related with the design and development of GNSS signal processing, authentication, and anti-spoofing algorithms, including anti-replay, SAS, and enhanced PVT resilient platforms.

Simón Cancela holds an MSc in Advanced Mathematics by the Universidad Complutense de Madrid. He joined GMV in 2015 and he has been working in projects related with the design and development of GNSS authentication and anti-spoofing algorithms, including the Galileo Commercial Service Demonstrator and Commercial Service enhanced PVT resilient platform.

David Calle holds a MSc. in Computer Engineering from the University of Salamanca. He joined GMV in 2008 and he has been working in the GNSS business unit involved in the design and development of GNSS algorithms, applications and systems. He is currently Head of GNSS Services Section coordinating the activities related to the Galileo Commercial Service, Open Service Authentication and High Accuracy provision services.

Ignacio Fernandez-Hernandez has led the design and development of Galileo high accuracy and authentication services over the last years at the European Commission. He also chairs the Galileo Commercial Service and the EU-US Resilience Working Groups. He is an ICAI Engineer and has a PhD degree in Electronic Systems from Aalborg University.

Tom Willems obtained a PhD degree from Ghent University in 2006. From 2006 to 2021, he worked as embedded software engineer in GNSS signal processing and as system engineer at Septentrio and Antwerp Space. At both companies, he was deeply involved in the Galileo Test User Receiver projects for ESA. Next, he started working as an independent consultant. Since 2024, he is employed as Senior Consultant at CGI where his current assignment is to provide advisory services to the EC.

Jón Winkel received his Diploma in Physics from the University in Hamburg and his Ph.D. degree from the university FAF Munich. He has over 25 years' experience in GNSS, with more than 80 publications in journals and conferences. After 17 years as head of the receiver department at IFEN, he joined the Vehicle Motion and Positioning Sensor (VMPS) team in the Chassis Systems Control department at Bosch GmbH in 2018 as an expert on GNSS. In 2019 he was on the payload team developing the G2G Galileo satellites at Airbus. Since 2022 he is an advisor to the EC on GNSS, focusing on authentication services. He is currently an independent consultant.

Rafael Terris-Gallego received the M.Sc. degrees in Telecommunication Engineering from UPC, Barcelona, Spain, and Digital Communications Systems from Telecom Bretagne/IMT Atlantique, France, in 2001. He spent over 13 years in industry, primarily as a satellite-communications engineer. He is currently a GNSS researcher at the Institute of Space Studies of Catalonia (IEEC) and teaches at the Autonomous University of Barcelona (UAB), Spain. In 2024, he was awarded the Ph.D. in GNSS authentication.

Gonzalo Seco-Granados received the Ph.D. degree in telecommunications engineering from the UPC in 2000, and the MBA degree from the IESE Business School, Spain, in 2002. From 2002 to 2005, he was member of the European Space Agency. He is currently Professor at Signal Processing for Communications and Navigation (SPCOMNAV) research group of the Universitat Autònoma de Barcelona. He is also affiliated with the Institute of Space Studies of Catalonia.

## ABSTRACT

The Galileo Signal Authentication Service (SAS) is the next new feature to be offered by Galileo, the European GNSS. Its initial signal-in-space capability is planned for 2025, starting with the L3 (launch 3) satellites in elliptical orbits. SAS relies on encrypted spreading code sequences of the E6-C component, which are “re-encrypted” with cryptographic material provided by the Galileo Open Service Navigation Message Authentication (OSNMA). These Re-Encrypted spreading Code Sequences (RECS) are distributed to users following the semi-assisted authentication concept: future E6-C codes are re-encrypted with OSNMA key material and published by a server for user download. The European Commission launched an R&D project to develop a SAS receiver, an assistance server, and a test platform. The project, named *Message and Measurement Authentication Receiver for Initial Operations* (MMARIO), began in April 2024 and is now approaching its experimentation phase. The prototype receiver is capable of processing encrypted E6-C signals and generating authenticated position, velocity, and time (PVT) solutions, implementing additional anti-spoofing features such as anti-replay and vestigial signal detection. This paper reports on the first experimentation campaign carried out with real encrypted signals transmitted by Galileo L3 elliptical satellite E14 in June 2025. The use of the Test Platform is foreseen in the upcoming validation phase to simulate encrypted signals and spoofing attacks under controlled conditions.

## INTRODUCTION

The increasing reliance on Global Navigation Satellite Systems (GNSS) for various applications, from everyday activities to critical sectors such as navigation, banking, aviation and automotive, has made GNSS a prime target for spoofing attacks (SKAI Data Services, s.f.). Spoofing (Mukhtar, et al., 2019) involves the transmission of counterfeit GNSS signals to receivers, which can result in incorrect positioning and timing information. This threat underscores the need for robust authentication mechanisms to ensure the integrity and authenticity of GNSS signals.

Authentication in GNSS has been recognized for more than two decades as a key enabler for resilient Positioning, Navigation, and Timing (PNT) (Scott, 2003). Traditional GNSS open service signals are unprotected at the physical layer, which makes them vulnerable to meaconing, spoofing, and replay. Early mitigation efforts have relied on external monitoring networks or cross-checking with other sensors, but these approaches do not provide cryptographic guarantees.

Within the European Galileo program, two complementary authentication services are being developed: the Open Service Navigation Message Authentication (OSNMA) (European Union, Jan. 2024) and the Signal Authentication Service (SAS) (Fernandez-Hernandez I. , et al., 2024). The OSNMA, already operational and officially declared (InsideGNSS, 2025), protects the integrity of the navigation message, allowing the receiver to verify that broadcasted ephemeris and clock data are authentic. However, counterfeit signals can still replicate or manipulate the spreading codes while relaying valid signed messages.

SAS addresses this limitation by adding authentication to the physical layer. The concept is based on encrypted spreading codes, where the E6-C pilot sequences are not openly known but generated from cryptographic material. To make this compatible with an open service, SAS introduces the semi-assisted authentication approach (Fernandez-Hernandez I. , et al., 2023): the encrypted codes are “re-encrypted” with future OSNMA key material, generating Re-encrypted Code Sequences (RECS). These RECS are distributed through an assistance server, which users can access over the internet. The cryptographic framework ensures that only some sequences can correctly de-spread the signal, preventing counterfeit signals from correlating with the authentic one. Moreover, additional parameters such as the Key Delay Index (KDI) and randomization flags are used to increase the unpredictability of the sequences and mitigate pre-computation attacks.

Galileo SAS represents the first large-scale operational initiative to provide a free and open physical-layer authentication service. The MMARIO project, awarded to a consortium led by GMV, including Airbus, Universidad Autónoma de Barcelona (UAB), and Qascom, contributes to this framework by implementing the full SAS chain, from the generation of RECS and Broadcast Group Delay (BGD) files at the assistance server to the receiver processing and authenticated PVT computation. This end-to-end approach provides a unique opportunity to evaluate SAS performance under real signal conditions, ahead of its operational deployment.

## SERVICE ARCHITECTURE

Prior to the activation of encrypted transmissions, the server already holds the cryptographic material derived from OSNMA keys together with the Encrypted Code Sequence (ECS) keys. Using these inputs, it generates the RECS corresponding to future E6-C encrypted spreading codes. The RECS files together with BGD files are then made available to users through secure HTTPS

query requests. At the user side, once the OSNMA key is received and verified, the receiver generates a decryption key by applying a SHA-256 hash to the OSNMA key. This derived key is then used to decrypt the RECS using AES-256 in CBC mode (Daemen & Rijmen, 2020), with a time-dependent initialization vector (IV), as follows:

$$\begin{aligned}
 \text{RECS decryption Key} &\rightarrow K'_{j+D_K} = \text{SHA256}(K_{j+D_K}) \\
 \text{RECS decryption function} &\rightarrow \text{ECS}_{j,i} = \text{AES256}_{\text{CBC}}^{-1}(K'_{j+D_K}, \text{RECS}_{j,i}, \text{IV}) \\
 \text{IV} &= \text{trunc}(128, \text{SHA256}(P_j)) \\
 P_j &= (\text{GST}_{\text{SF},j+D_K} || \text{RAND} || p1)
 \end{aligned} \tag{1}$$

Where  $\text{RECS}_{j,i}$  is RECS  $i$  of subframe  $j$ ,  $D_K$  is the Key Delay Index (KDI), SHA256 is the hash function (NIST, 2012), *trunc* is the truncation function, GST is the Galileo System Time, and RAND is the randomization flag. The KDI defines how many I/NAV subframes separate the OSNMA key from the RECS it decrypts (where all KDI values also incorporate the so-called *key broadcast margin offset*, with a value of a few seconds currently to be fixed by design). Further details and justification can be found in (Fernandez-Hernandez I. , et al., 2024) and (European Commission, 2020).

- KDI = 0: the key and RECS are provided in the same I/NAV subframe,
- KDI = 1: the RECS can only be decrypted after a delay of 30 seconds.
- KDI = 2: the delay extends to 11 subframes, equivalent to 330 seconds.

This mechanism ensures that RECS remains unencryptable until the corresponding OSNMA key has been broadcast, thereby mitigating pre-computation attacks and reinforcing the unpredictability of the system. In addition, a randomization flag (RAND in (1)) may be applied to further obfuscate the temporal alignment of RECS within each service period. This increases the entropy of the authentication process and adds another layer of complexity for potential spoofing adversaries.

### SAS Server

The SAS Server is the central element enabling semi-assisted authentication. Its primary role is to generate and distribute the RECS and BGD files required for Galileo SAS operation. These files are precomputed using cryptographic material derived from OSNMA keys and E6-C encryption keys, which are securely loaded into the server prior to the encryption period. The implementation has been deployed on an enterprise-grade HP server platform, ensuring high availability, robustness, and sufficient processing resources for both real-time and batch generation of authentication data. By precomputing RECS and BGD for future time windows, the server allows receivers to operate in autonomous conditions without requiring continuous connectivity during the service period.

Before each service interval, the server loads satellite clock bias information and the relevant cryptographic material, including derived TESLA keys. It then generates the corresponding RECS and BGD files and makes them available to users through a secure HTTPS interface. Figure 1 shows the high-level design of the SAS server prototype.

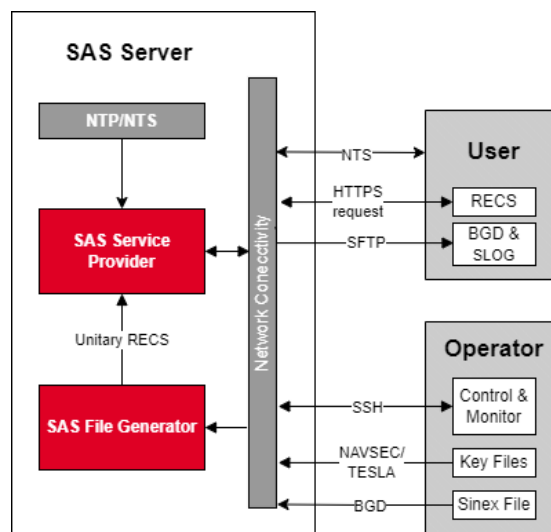


Figure 1 - SAS Server High Level Architecture

The server also supports Network Time Security (NTS), enabling authenticated and secure time synchronization between clients and the server. This capability ensures that receivers maintain accurate timing, a critical requirement for correlation with encrypted spreading codes.

Users can either download standard pre-generated files or query the server for customized RECS configurations. Parameters such as satellite, RECS period, KDI and randomization settings can be requested to tailor the data to specific operational scenarios.

### SAS Receiver

The MMARIO SAS receiver architecture (Figure 2), hereinafter referred to generically as *SAS Receiver*, has been designed to provide full support for the Galileo SAS Service, integrating both hardware and software elements to achieve position authentication.

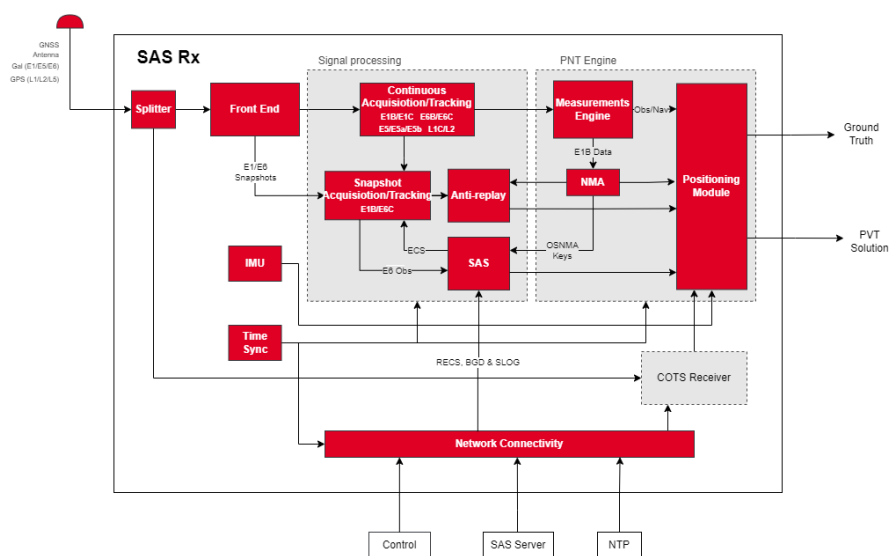


Figure 2 - SAS Receiver High Level Architecture

At the hardware level, the system incorporates a multi-band GNSS front-end capable of processing Galileo E1 and E6 signals. The receiver supports OSNMA authentication of navigation messages and includes a dedicated front-end for recording snapshots of the E6 and E1 signals. For performance validation and accuracy assessment, the experimental setup includes a Septentrio MOSAIC receiver providing reference solutions, an Inertial Measurement Unit (IMU) to capture motion dynamics, and a high-stability Real-Time Clock (RTC) ensuring precise time synchronization during periods without access to NTS. The hardware elements contained inside the MARIO receiver are described in Figure 3. Further details about the commercial equipment used can be found in (Fernandez-Hernandez I. , et al., 2025).

1. GNSS Antenna
2. GNSS Splitter
3. BROS Rx
4. MOSAIC Rx
5. IMU
6. RTC
7. Raspberry Pi
8. Processing HW
9. Switch

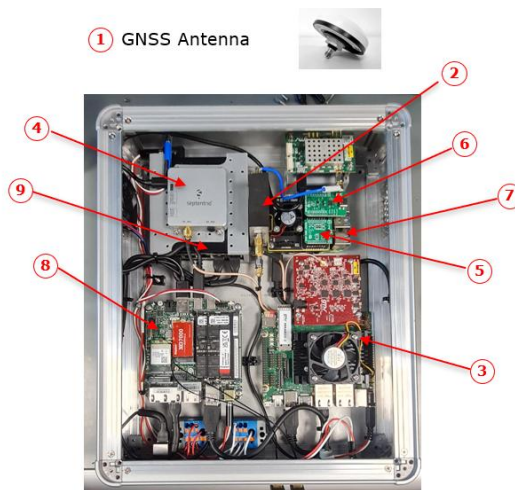


Figure 3 - MMARIO SAS Receiver

The receiver software integrates additional security monitoring capabilities, including anti-replay checks, vestigial signal detection (Winkel, et al., 2024), and consistency verification between E6 and E1 observables. This layered approach enhances resilience against advanced spoofing and replays attacks, complementing SAS.

## SAS SIGNAL PROCESSING

The SAS authentication process relies on correlating encrypted E6-C signal snapshots with decrypted RECS sequences. Here, the SAS Receiver uses a circular convolution FFT (Fast Fourier Transform)-based method, similar to, for example, that described in (Kaplan & Hegarty, 2006). This technique allows simultaneous search over time and frequency domains, where, for each frequency bin, the signal and ECS are separately FFT'ed, convoluted, and the inverse FFT computed. The result of this correlation is shown in Figure 4, where the plot on the left shows the correlation peak in the sample corresponding to the match between the replica generated with the ECS of E14 and the recorded signal snapshot of E6, and the plot on the right shows the value of this peak evaluated for each Doppler value configured in the search. To further optimize this process, the receiver can use measurements from the E1-B, E1-C or E6-B signal components to dramatically reduce the search space for the time and frequency parameters of the E6-C signal. This handover strategy significantly reduces the acquisition search space.

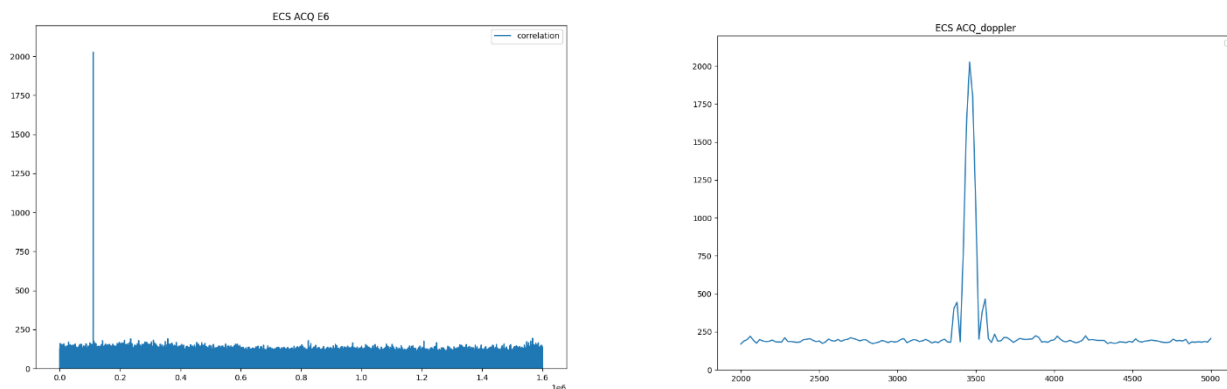


Figure 4 - Circular convolution between the ECS and the encrypted E6C signal transmitted by satellite E14

### E1 and E6 Handover

The handover from E1-B/C signals to E6-C enables efficient estimation of both time and frequency parameters for SAS processing. First, in the time domain, code phase offset from E1-B provides a reference for locating the RECS in E6-C snapshots, applying offsets due to BGD, ionospheric effects, and receiver hardware biases. Second, in the frequency domain, Doppler measurements from E1-B are scaled according to the carrier frequency ratio between E1 and E6-C, yielding initial Doppler estimates that reduce the frequency search space. The E1 handover process is described in (Fernandez-Hernandez I. , et al., 2023).

Using E6-B as an auxiliary signal provides an even further refinement of both time and frequency estimates for E6-C acquisition. By avoiding inter-frequency biases, particularly those introduced by ionospheric effects, the E6-B handover improves the precision of code phase and Doppler measurements compared to relying solely on E1-B/C. Further details are provided in (Terris-Gallego, et al., 2025).

These strategies collectively reduce the number of search cells required during E6-C acquisition. This optimization minimizes the computational load for snapshot correlation and allows the snapshot duration to be shortened, while maintaining high measurement accuracy and ensuring robust signal authentication.

## SAS AUTHENTICATION PROCESS

The SAS Receiver implements a comprehensive, multi-layered authentication strategy designed to provide resilience and reliability across a wide range of signal conditions and potential threat scenarios.

### Signal-Level Authentication

The first layer, signal-level authentication, verifies the integrity of the received E6-C signal by detecting valid correlation peaks. Successful acquisition of the encrypted signal indicates that the satellite is authenticated at the signal level, ensuring that the received signal originates from a legitimate source. Eq (2) shows the test statistic against a threshold used  $\gamma_{sig}$ , as per standard signal detection theory, and under the assumption that if there is signal correlation, the signal from that satellite is authentic (note that the satellite index is omitted for simplicity). Further considerations, such as finding the earliest peak (Winkel, J., et al, 2023) to protect against meaconing, are for the moment left out of scope.

$$\frac{MAX\{FFT(n)\}}{RMS(FFT(n))} \geq \gamma_{sig} \rightarrow \xi_{sig} = 1 \text{ (satellite authenticated)} \quad (2)$$

### Pseudorange Authentication

The second layer, pseudorange authentication, evaluates the consistency of the range measurements between different carrier frequencies. Specifically, the pseudorange measured from the E6-C correlation peak from the RECS, and after removing E1-E6 biases ( $BGD$ ) and ionosphere ( $I$ ), is compared against the corresponding E1 pseudorange measurement, also ionosphere-corrected, as per Eqs (3), where  $\hat{\rho}_{Ei}$  is the corrected pseudorange for frequency  $i$ , and where satellite indices have been removed for simplicity.

$$\begin{aligned} \hat{\rho}_{E1} &= \rho_{E1} - I_{E1} \\ \hat{\rho}_{E6} &= \rho_{E6} - BGD_{sat,E1,E6} - I_{E6} \end{aligned} \quad (3)$$

The difference between these measurements is used as a pseudorange consistency metric, as per Eq. (4). If this metric remains below a defined threshold  $\gamma_\rho$ , the pseudorange for a given satellite, is considered authenticated.

$$|\hat{\rho}_{E6} - \hat{\rho}_{E1}| < \gamma_\rho \rightarrow \xi_\rho = 1 \text{ (measurement authenticated)} \quad (4)$$

### Position Authentication

At the final layer, position-level authentication is performed to validate the overall navigation solution. This can be achieved in two complementary ways. One approach verifies that all measurements contributing to the E1-based PVT solution are individually authenticated via E6-C, ensuring the integrity of the position computation. Alternatively, a separate PVT solution can be calculated using only E6-C-authenticated measurements and associated navigation data, which is then compared to the E1-based solution, as per Eq. (5).

$$|\vec{x}_{E1} - \vec{x}_{E6}| = \Delta\vec{x}_{E1,E6} < \gamma_x \rightarrow \xi_x = 1 \text{ (E1 position authenticated)} \quad (5)$$

In both cases, the differences between the solutions are evaluated against a predefined threshold to determine the authentication status. This multi-level approach helps the SAS receiver to provides end-to-end signal and position verification, combining measurement integrity with position validation.

## E6-C ENCRYPTION ACTIVATION TEST ON GALILEO E14

On June 4th, 2025, a controlled activation of the Galileo Signal Encryption was performed on satellite E14. The encrypted E6-C signal was transmitted for a duration of 1 hour and 36 minutes. To validate the SAS chain under operational conditions, a fully integrated setup combining the SAS server and the SAS receiver was employed during the E6-C encryption activation on Galileo satellite E14. Both the OSNMA-derived keys and the E6-C encryption (formerly called CS, for ‘‘commercial service’’) traffic keys were made available in advance, allowing the generation of RECS and BGD files prior to the transmission of the encrypted E6-C signal. The SAS server was deployed in real time, providing the receiver with access to pre-generated authentication data, thereby replicating the intended operational mode in which users download RECS and BGD files ahead of signal reception. During the activation, the MMARIO receiver simultaneously recorded E6-C snapshots and received OSNMA keys from the E1-B signal in the Signal-in-Space (EU, 2023). Using the acquired keys, the receiver decrypted the RECS in real time, correlated the decrypted sequences with the recorded E6-C snapshots, and computed an authenticated PVT solution.

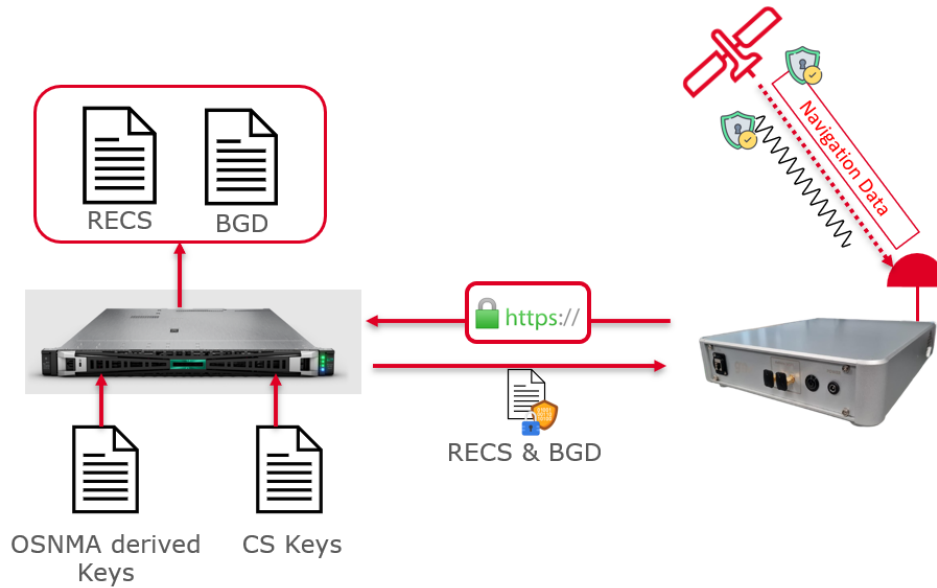


Figure 5 - Test Setup for the 4/6/2025 test, including SAS prototype server (left) and SAS receiver (right)

During this period, the reference receiver (Septentrio MOSAIC) lost tracking on the E6-C signal and automatically switched to tracking the E6-B component. This behavior confirmed the activation of encryption on E6-C. Meanwhile, the MMARIO SAS receiver continued operating and successfully processed snapshots of the encrypted E6-C signal every 30 seconds. These snapshots were correlated with RECS files generated by the SAS server, allowing the receiver to produce authenticated measurements.

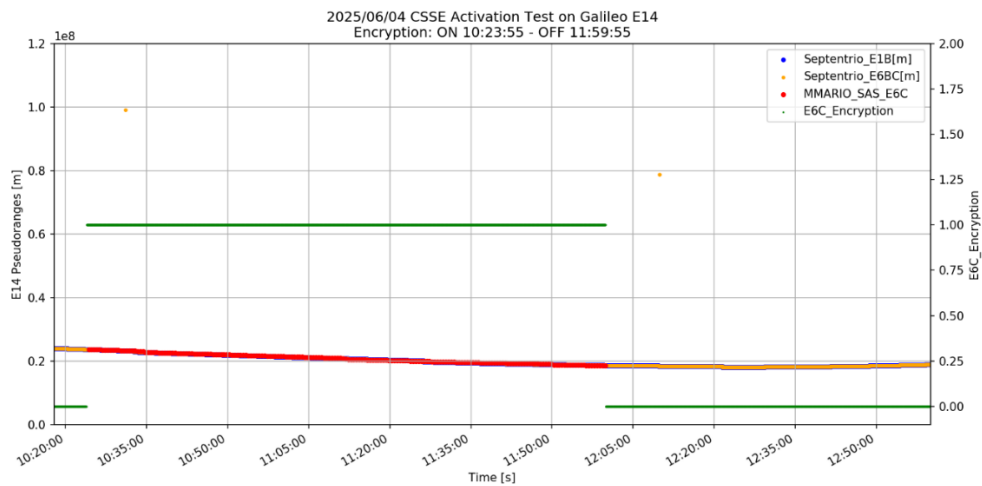


Figure 6 - E14 pseudoranges computed with Septentrio MOSAIC receiver and MMARIO SAS receiver

Figure 6 shows the results for the test. The red line indicates that, while the signal was encrypted, the SAS receiver was able to compute pseudoranges (note that, some time after the E6-C encryption/decryption transitions, the MOSAIC receiver generates punctual measurements with an offset, appearing as yellow dots in the figure). Figure 7 zooms into the first encrypted E6-C correlations. A bias was observed between the measurements from the MOSAIC and those from the MMARIO SAS receiver. This bias is attributed to clock differences, as the two receivers were not synchronized. However, despite the offset, the measurements from MMARIO were internally consistent, demonstrating the correct processing of encrypted signals and validating the SAS authentication chain.

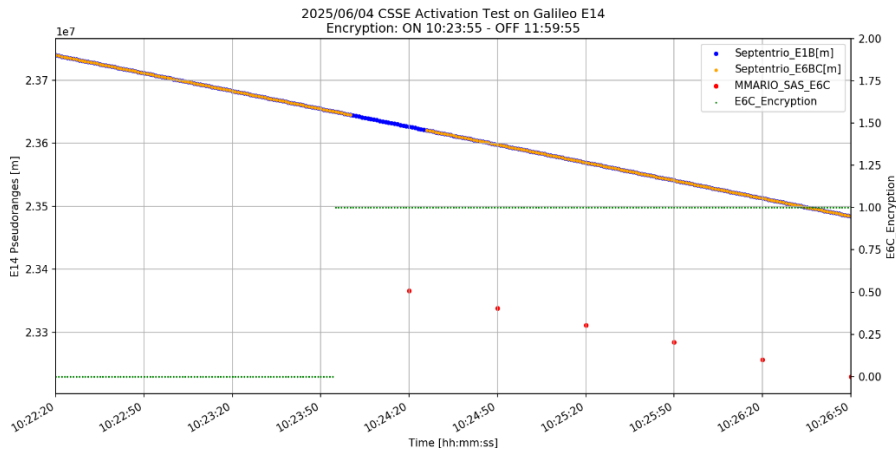


Figure 7 - E14 E6-C encryptions activation

Figure 8 shows the  $C/N_0$  values of all observed satellites during the scenario, including the E14 at the time of encryption (note that the  $C/N_0$  estimation method is different for E14 and the other satellites, which may explain the higher one for E14). The correlation was performed using a configuration of  $N_{chip}=4$ , corresponding to 16-ms sequences, with snapshots recorded every 30 seconds. The KDI was set to 1, meaning the OSNMA key used to decrypt the RECS corresponds to the next subframe after the RECS transmission.

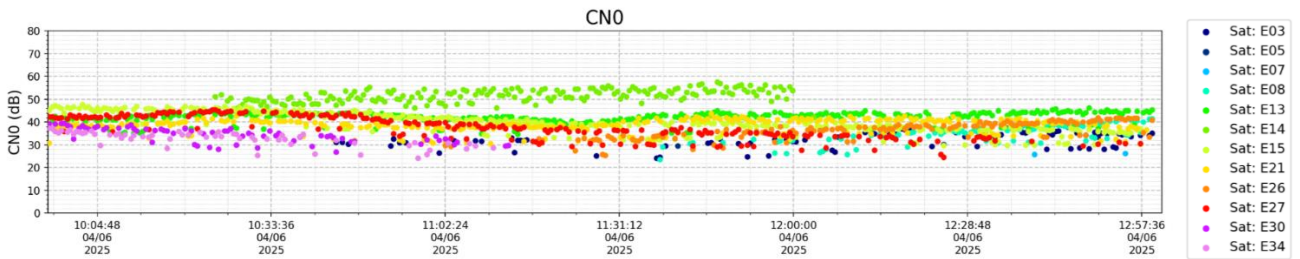


Figure 8 - E14  $C/N_0$  Values from MMARIO SAS Receiver

The results are consistent with nominal performance, validating both the cryptographic integrity of the RECS and the correct handling of key transitions during the encryption period.

### E1 SAS & OSNMA Authenticated Solution

The final authenticated solution obtained by the MMARIO receiver was evaluated in a static scenario, integrating both OSNMA and SAS capabilities. In this configuration, the receiver operated in Standard Point Positioning (SPP) mode, continuously tracking the Galileo E1 signal and processing navigation data authenticated via OSNMA. Measurement-level and position-level authentication were performed using SAS on the E6-C signal.

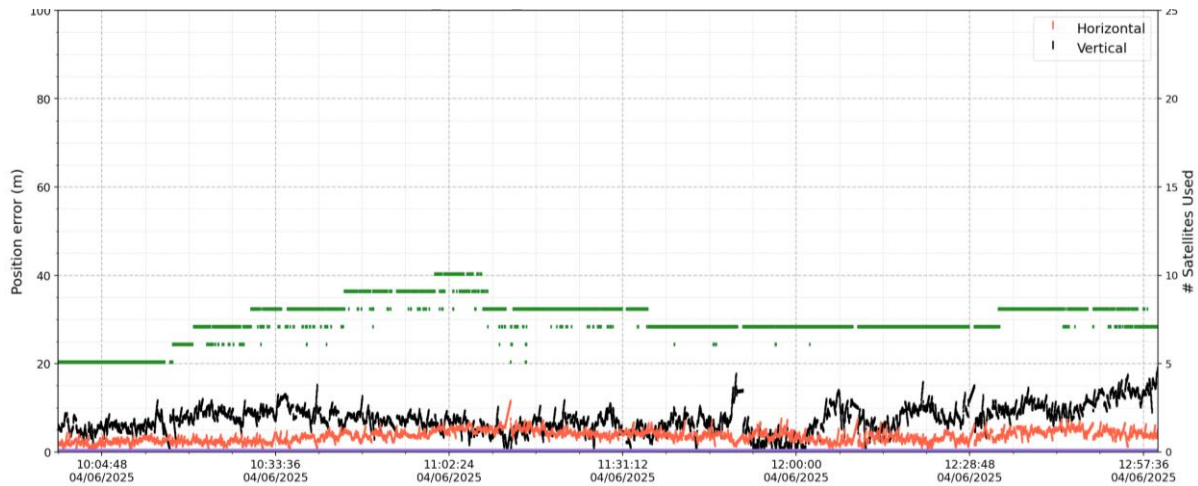


Figure 9 - E1 Authenticated Position Solution Error

The resulting PVT solution, computed from SAS-authenticated E6-C measurements recorded at 30-second intervals, included the encrypted satellite E14 alongside non-encrypted satellites. Despite the mixture of encrypted and open signals, the receiver produced a consistent and stable position throughout the scenario. While the combination of one authenticated pseudorange with non-authenticated pseudoranges into a single PVT cannot be considered as an authentic PVT, this test is representative of the performance to be obtained when all other E6-C signals are encrypted. Therefore, it demonstrates the successful integration of SAS within the receiver’s processing chain and validates the effectiveness of the authentication logic at both the measurement and position levels.

The results confirm that the receiver can reliably combine OSNMA and SAS data to generate an authenticated navigation solution under realistic operational conditions. Therefore, this test provided a valuable real-world confirmation that the RECS generated using pre-disclosed cryptographic material matched the encrypted signal transmitted by E14 and the OSNMA keys received via E1-B. These results are complemented by those performed in parallel under UAB lead and reported in (Terris-Gallego, et al., 2025).

## CONCLUSIONS AND FURTHER WORK

This work has presented the development and early validation of a complete software and hardware solution for real-time position authentication using Galileo SAS. Within the framework of the MMARIO project, we have successfully designed and implemented the end-to-end authentication chain, including the generation of RECS, secure distribution via the SAS assistance server, correlation with live E6-C encrypted signals, and multi-level authentication at both the measurement and position levels. The SAS-capable receiver was able to combine OSNMA-authenticated E1 navigation data with SAS-authenticated E6-C measurements, producing consistent and stable PVT solutions even when mixing encrypted and non-encrypted satellites. Experimental results using live encrypted signals therefore confirm the feasibility and robustness of the SAS approach in realistic operational conditions.

Future work will include testing different SAS configurations, such as varying RECS lengths and randomization settings. Validation campaigns using multiple encrypted satellites will allow assessment of full multi-satellite PVT accuracy. Additionally, resilience to spoofing attacks will be evaluated under controlled and realistic conditions, and further environmental testing will explore performance in kinematic scenarios and under degraded or challenging conditions.

## ACKNOWLEDGEMENTS

The authors would like to acknowledge the rest of the MMARIO team members, and ESA/EUSPA/GSOP teams involved in the E14 encryption testing.

## REFERENCES

- Daemen, J., & Rijmen, V. (2020). *The design of Rijndael (2nd ed)*. Springer.
- European Commission. (2020). *Galileo Assisted Commercial Authentication Service (ACAS) - Specification Proposal - DRAFT - V0.1 - defis.dg.c.2(2020)7166782*.
- European Union. (Jan. 2024). *Galileo OSNMA (Open Service Navigation Message Authentication) IDD ICD v1.1*.
- Fernandez-Hernandez, I., Winkel, J., O'Driscoll, C., Cancela, S., Terris-Gallego, R., López-Salcedo, J., . . . Blas, J. (2023). Semiassisted Signal Authentication for Galileo: Proof of Concept and Results. *IEEE Transactions on Aerospace and Electronic Systems*, 59(4), 4393-4404.
- Fernandez-Hernandez, I., Winkel, J., O'Driscoll, C., Caparra, G., Terris-Gallego, R., López-Salcedo, J., . . . de Blas, J. (2024). Galileo Signal Authentication Service (SAS). In *Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation* (pp. 3292-3307). Baltimore: ION GNSS+.
- Fernandez-Hernandez, I., Winkel, J., O'Driscoll, C., Willems, T., Cancela, S., Ramirez, M. A., . . . Simon, J. (2025). Prototyping Galileo Signal Authentication Service: Current Status and Plans. *ENC2025 - European Navigation Conference 2025, Engineering Proceedings*. Wrocław, PO.
- Galileo Open Service Navigation Message Authentication ICD*. (2025).
- InsideGNSS. (2025). *Galileo Leads the Way in GNSS Spoofing Protection with OSNMA*. Retrieved from <https://insidegnss.com/galileo-leads-the-way-in-gnss-spoofing-protection-with-osnma/>
- Kaplan, E., & Hegarty, C. (2006). *Understanding GPS Principles and Applications*. Artech House Inc.
- Mukhtar, A., Muhammad, A., Sheeraz, A., & Khalid, S. (2019). Impact and Detection of GPS Spoofing and Countermeasures against Spoofing. *IEEE Xplore*, 1-8.
- NIST. (2012). *FIPS PUB 180-4: Secure Hash Standard (SHS)*.
- Scott, L. (2003). Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems. *ION GPS*.
- SKAI Data Services. (n.d.). *GPSwise*. Retrieved 2025, from <https://gpswise.aero/>
- Terris-Gallego, R., Fernandez-Hernandez, I., López-Salcedo, J., & Seco-Granados, G. (2025). Efficient Detection of Galileo SAS Sequences Using E6-B Aiding. *Engineering Proceedings*, 46. doi:engproc2025088046
- Terris-Gallego, R., Lopez-Salcedo, J., Seco-Granados, G., Galan-Figueras, A., & Fernandez-Hernandez, I. (2025). Testing Galileo SAS with Encrypted Signal In Space. *Proceedings of IONGNSS+ 2025*. Baltimore, MA.
- Winkel, J., Fernandez-Hernandez, I., & O'Driscoll, C. (2024). Combining Galileo's Assisted Commercial Authentication Service (ACAS) with Vestigial Signal Search for Good Protection. In *Proceedings of the 2024 International Technical Meeting of The Institute of Navigation* (pp. 1225-1234). Long Beach, California: ION.
- Winkel, J., Fernandez-Hernandez, I., & O'Driscoll, C. (2023). Implementation Considerations for ACAS and Simulation Results. *IEEE Transactions on Aerospace and Electronic Systems*(DOI 10.1109/TAES.2024.3402196).