Testing Galileo SAS with Encrypted Signal-in-Space

Rafael Terris-Gallego, José A. López-Salcedo,
Gonzalo Seco-Granados, *Univ Autonoma de Barcelona, CERES-IEEC, Spain*
Aleix Galan-Figueras, *KU Leuven, Belgium*
Ignacio Fernandez-Hernandez, *DG DEFIS, European Commission, Belgium*

BIOGRAPHY

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.

José A. López-Salcedo received the Ph.D. degree in Telecommunication Engineering from UPC in 2007. He is currently a Professor in the Dept. of Telecommunication and Systems Engineering at UAB. His research interests lie on the field of signal processing for GNSS receivers.

Gonzalo Seco-Granados received the Ph.D. degree in Telecommunications Engineering from UPC in 2000, and the MBA degree from the IESE Business School, Barcelona, Spain, in 2002. From 2002 to 2005, he was a member of the European Space Agency. He is currently a Professor in the Dept. of Telecommunication and Systems Engineering at UAB.

Aleix Galan-Figueras received the B.Sc. degrees in Computer Engineering and Telecommunication Systems Engineering from UAB in 2020, and the M.Sc. in Cybersecurity from UPC in 2022. He worked for two years in the industry at Septentrio NV on GNSS spoofing and developed an open-source library for Galileo OSNMA. Since 2023, he has been pursuing a Ph.D. in GNSS within the WaveCoRE Research Group at ESAT, KU Leuven, Belgium.

Ignacio Fernandez-Hernandez received the Electronic Engineering degree from ICAI, Madrid, Spain, in 2001, the MBA degree from LBS, London, UK, in 2011, and the Ph.D. degree in Electronic Systems from Aalborg University, Denmark, in 2015. He is in charge of Galileo high accuracy and authentication at the European Commission, DG DEFIS.

ABSTRACT

Galileo Signal Authentication Service (SAS) provides civil signal authentication by applying spreading code encryption on E6-C and TESLA keys disclosed via OSNMA on E1-B, thus avoiding any long-term secret storage in receivers. After years of development, Galileo has recently conducted encrypted E6-C signal-in-space trials, enabling end-to-end SAS testing. This paper reports the first results with encrypted signal-in-space using an SDR-based test-bed that implements the receiver-side SAS workflow: retrieval and parsing of Re-Encrypted Code Sequences (RECS), snapshot recording of E6-C and E1-B, and post-disclosure decryption and correlation. Campaign results confirm successful E6-C detections and validate key configuration parameters in the current specification, including RECS length and period, and the Key Delay Index (KDI). Acquisition is assisted by E1-B, consistent with the nominal SAS operating mode. These results represent a step toward operational SAS, validating the end-to-end transmission and reception chain.

https://doi.org/10.33012/2025.20223

I. INTRODUCTION

In recent years, Galileo has been actively developing new services to address the challenges users face in navigation and positioning. In addition to High Accuracy Service (HAS), which focuses on providing high-accuracy positioning, the European Global Navigation Satellite System (GNSS) has designed a twofold free-of-charge solution to combat the growing threat of spoofing. First, the recently launched Open Service Navigation Message Authentication (OSNMA) provides data-level authentication with minimal impact on receiver performance. Second, the still-in-development Signal Authentication Service (SAS) will offer range-level authentication by leveraging spreading code encryption. Together, these solutions will enhance security for civil users, similar to what Global Positioning System (GPS) aims to do with the Chips-Message Robust Authentication (CHIMERA) scheme (Anderson et al., 2017). Commercial services like Xona are also working on providing range authentication based on watermarks (Anderson, 2025).

Galileo SAS, formerly known as Assisted Commercial Authentication Service (ACAS), is designed to provide civil Spreading Code Authentication (SCA) using the existing first-generation Galileo infrastructure. It is based on the semi-assisted concept presented in (Fernandez-Hernandez et al., 2023), which enables authentication without requiring receivers to store any secret keys. The Galileo system re-encrypts predefined fragments of the already-encrypted E6-C signal—producing the so-called Re-Encrypted Code Sequences (RECSs)—with hashes of the Timed Efficient Stream Loss-tolerant Authentication (TESLA) keys used for OSNMA on E1-B, prior to their disclosure. This mechanism prevents spoofers from decrypting the RECSs and, consequently, from counterfeiting the signal.

This semi-assisted concept can be extended to other GNSS constellations that provide the necessary building blocks—namely, an encrypted signal and system-provided authentication keys. However, this approach has several implications: it introduces authentication latency due to the need to decrypt RECSs with the corresponding hashed TESLA keys, which may be unsuitable for certain applications, and it imposes connectivity and storage requirements on receivers because they must download and store RECS for the desired autonomy period. These limitations are expected to be addressed in Galileo Second Generation (G2G) (Fernandez-Hernandez et al., 2024).

In recent years, interest in Galileo SAS has grown significantly (Ardizzon et al., 2022b) (Dorins et al., 2025) (Schreiber et al., 2025). During this period, the authors have been actively involved in the definition and testing of Galileo SAS under the oversight of the European Commission (EC). Several operating modes have been analyzed (Terris-Gallego et al., 2022b), and an experimental platform has been implemented to validate the feasibility of SAS at the signal level (Terris-Gallego et al., 2023a). These initial tests were conducted using unencrypted Galileo E6-C signal. This required implementing specific workarounds so that the results would be representative of nominal operation (Terris-Gallego et al., 2023b).

In this paper, we present the first results of Galileo SAS using the encrypted E6-C signal-in-space with our test-bed, supported by the "Message and Measurement Authentication Receiver for Initial Operations (MMARIO)" project under the EC Defence Industry and Space Satellite Navigation (DEFIS) contract DEFIS/2023/OP/0011. To accomplish this, the initial experimental platform was updated to support end-to-end operation of Galileo SAS according to the latest published specification (European Commission – DG DEFIS, 2023), including RECS detection and range authentication. On the Signal-In-Space (SIS) side, Galileo used the GSAT0202/E14 satellite—currently declared as "NOT USABLE" for operations, together with the GSAT0201/E18 satellite—to run a trial with the encrypted E6-C signal on selected days in June and July 2025, enabling RECS processing and encrypted-signal correlation on the ground with our test-bed.

Our RECSs detection process consists of downloading the required RECS, recording E1 and E6 samples from the SIS at specific epochs, obtaining the corresponding TESLA keys from OSNMA, decrypting the RECS using hashes of those keys, and, finally, correlating the decrypted RECSs—known as Encrypted Code Sequences (ECSs)—with E6-C snapshots. While the individual tasks are not inherently complex, their synchronization requires special attention. Specifically, synchronous recording of E1 and E6 samples is crucial because code delay and Doppler estimates from E1 are used to accelerate RECS detection (Terris-Gallego et al., 2023b). Without these estimates, the search space in E6-C could become prohibitive (Terris-Gallego et al., 2022a) due to its non-repeating nature. To ensure alignment between E1 and E6 samples, the test-bed incorporates a fast Solid State Disk (SSD) hosted by the latest Raspberry Pi modules. This setup enables synchronous sample recording without overruns at the high sampling rates required for testing.

When the RECS detection process results in a successful correlation peak at the expected location in E6-C, the receiver can proceed with Position, Velocity and Timing (PVT) authentication. This process relies on the authentication mechanism described in (Ardizzon et al., 2022a), where one trusted ranging signal (E6-C) serves as an anchor for another unauthenticated ranging signal (E1-B) of the same satellite. Specifically, when the difference between the measurements of these signals falls below a certain threshold, the unauthenticated measurement can be considered

usable for PVT authentication. This involves modeling the contributions that may affect the measurements and, consequently, the confidence in the authenticated position.

The remainder of this paper is organized as follows. Section II provides a short overview of Galileo SAS, including its operating principles and key parameters—the interested reader can refer to (Fernandez-Hernandez et al., 2023) for more details. Section III describes the test-bed used for testing, including hardware and software components. Section IV presents the results obtained from the trials with the encrypted E6-C signal-in-space, including detection performance and validation of key parameters. Finally, Section V concludes the paper and outlines future work.

II. GALILEO SAS OVERVIEW

Galileo SAS is based on spreading code encryption and time-delayed disclosure. On the system side (see Fig. 1), some specific fragments of the encrypted E6-C signal are selected, named ECS. Then, these sequences are re-encrypted using the TESLA key to create the RECSs. Three main parameters are derived from this process: the length and period of the ECS/RECS, and the Key Delay Index (KDI).

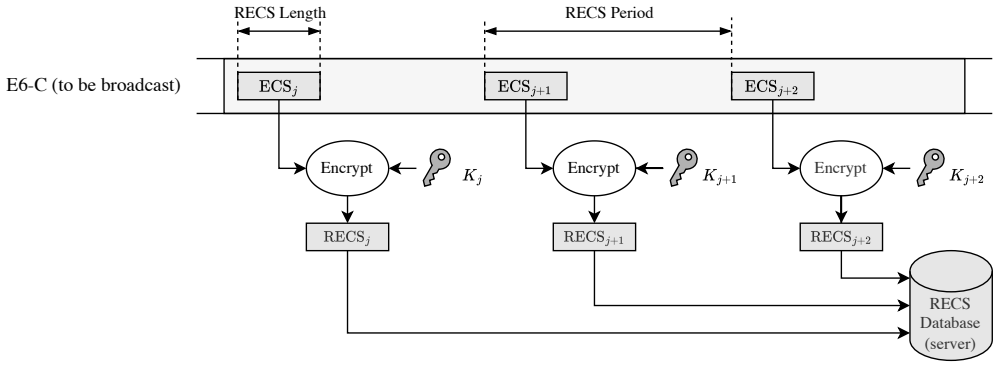

Figure 1: System-side schematics of Galileo SAS.

The length determines the duration of each sequence, while the period defines how often new RECSs are generated. These parameters impact detection performance, storage requirements, and how often the receiver can obtain an authenticated PVT, as discussed in (Terris-Gallego et al., 2022a). The KDI indicates the delay between the broadcasting of the RECSs and the TESLA key used to decrypt it. A KDI of 0 means that the TESLA key is disclosed in the same I/NAV subframe where the RECS is located. A KDI of 1 indicates that the TESLA key for OSNMA is from the next subframe—therefore implying a minimum authentication delay of 30 seconds. A KDI of 2 allows more relaxed timing—especially suitable for loosely synchronized receivers—where the TESLA key used is 11 subframes after the subframe of the ECS/RECS. Consequently, the choice of KDI affects the authentication latency.

On the receiver side (see Fig. 2), the operation of Galileo SAS can be summarized in the following steps:

1. Download the required RECSs from the GSC server and the associated metadata, including the expected broadcast times and the Broadcast Group Delay (BGD) between E1 and E6.
2. Wait for the E6-C signal to be broadcast and record snapshots aligned with the predicted ECS epochs, according to the RECS metadata. Store the snapshots until the corresponding TESLA keys are disclosed. The snapshot size depends on the uncertainty in the timing of the ECS epochs.
3. Retrieve the TESLA keys from E1-B when disclosed, according to the KDI configuration.
4. Decrypt the RECSs using the hashed TESLA keys to obtain the received ECS^R—to be used as local replicas.
5. Correlate the local ECSs against the stored E6-C snapshots to detect correlation peaks.
6. Cross-check timing and consistency with E1-B to perform PVT authentication.

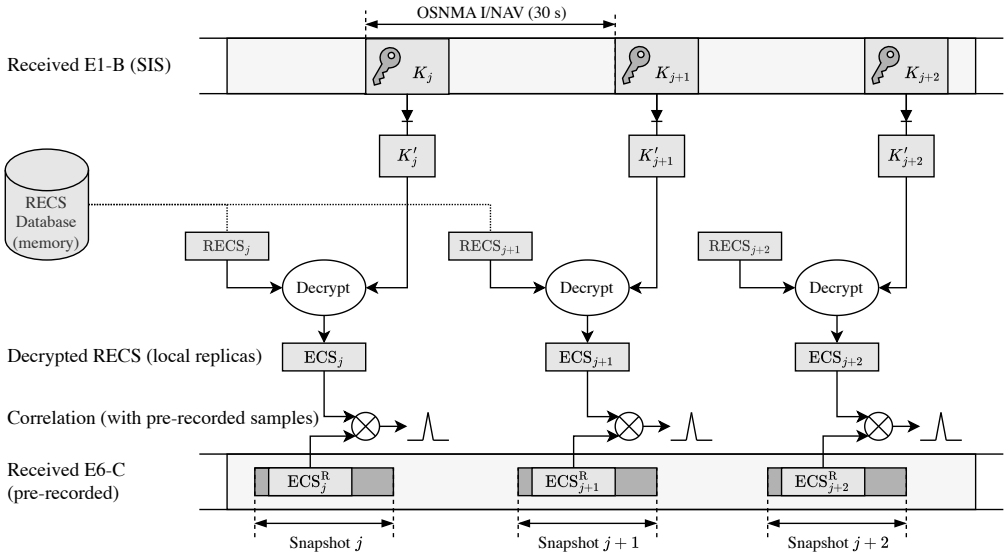

Figure 2: Receiver-side schematics of Galileo SAS. In this example, a KDI=0, so the TESLA hashed key K'_j used for decrypting the received ECS_j^{R} is the one disclosed in the same I/NAV subframe j. Also, in this example, the RECS Period is 30 seconds, as there is one ECS/RECS per I/NAV subframe. However, the specification foresees using shorter periods, using the same TESLA key for multiple ECSs/RECSs.

The latest Galileo SAS specification (European Commission – DG DEFIS, 2023) defines how RECSs are structured. Multiple 16-ms RECS are generated every 200 ms—the minimum RECS period—with randomization and different delays relative to the TESLA key disclosed by OSNMA, as shown in Fig. 3. Each 16-ms RECS is stored on the SAS server as a unitary RECS file. When a receiver queries the server for a specific time interval, it retrieves an aggregated RECS file that contains all unitary RECS files for that interval.

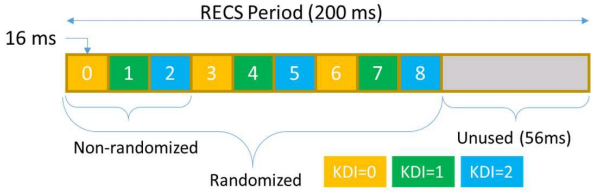

Figure 3: RECS structure definition according to the latest Galileo SAS specification (v1.2).

III. GALILEO SAS TEST-BED

An initial SDR-based evaluation platform was implemented (Terris-Gallego et al., 2023a) to validate Galileo SAS feasibility at the signal level. This platform enabled synchronized recording of E1 and E6 samples to verify the consistency of the estimated code delays and Dopplers, which demonstrated the convenience of assisted acquisition in E6-C using E1-B.

To perform an end-to-end test of Galileo SAS with the encrypted E6-C signal-in-space, a new test-bed has been implemented that updates the original platform to support the complete receiver-side workflow in accordance with the latest published specification (European Commission – DG DEFIS, 2023).

The test-bed is designed to be modular, allowing easy updates and improvements to individual components as needed. The software components are implemented in MATLAB, using the available toolboxes for efficient numerical processing, except for the Snapshot Recorder, which is implemented in Python using the bladeRF Software Defined Radios (SDRs) bindings provided by Nuand.

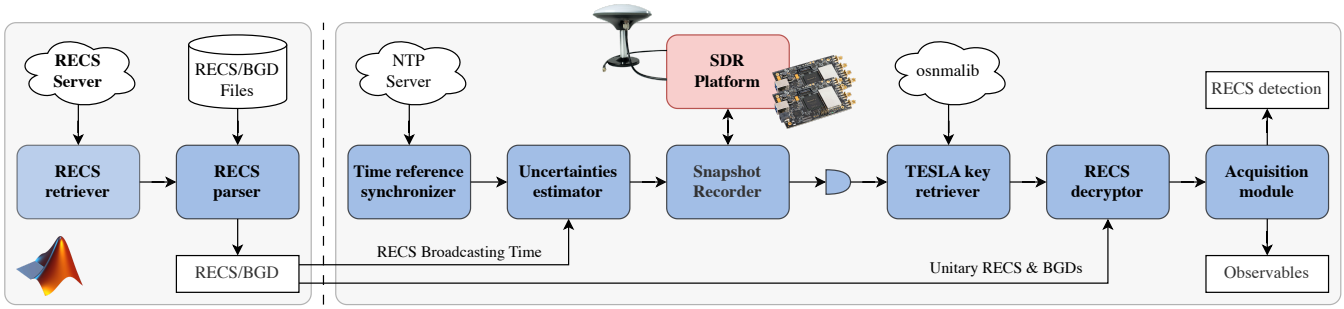

Figure 4: Schematics of evaluation test-bed for Galileo SAS with encrypted E6-C signal-in-space.

The test-bed, illustrated in Fig. 4, comprises the following main components:

- **RECS retriever:** downloads the required RECSs from the server, together with their metadata and BGDs, and stores them locally.
- **RECS parser:** processes the stored (aggregated) RECSs to obtain the corresponding individual RECSs.
- **Time reference synchronizer:** synchronizes the local clock with an NTP server. Depending on the stratum level of the server used, different timing accuracies can be achieved.
- **Uncertainty estimator:** estimates the timing uncertainty of the ECS epochs based on the local clock accuracy. This uncertainty determines the size of the acquisition window in E6-C and, consequently, the required snapshot size.
- **Snapshot recorder:** records E6 and E1 samples synchronously at the predicted ECS epochs, using the SDR platform—which employs hardware triggers to ensure alignment. The recorded snapshots are stored locally until the corresponding TESLA keys are disclosed.
- **TESLA key retriever:** retrieves the TESLA keys from E1-B when disclosed. In the current implementation, this component obtains the keys directly from the osnmalib.eu service (Galan-Figueras et al., 2025), which provides a public API.
- **RECS decryptor:** decrypts the stored RECSs using the hashed TESLA keys to obtain the local ECSs according to the KDI configuration.
- **Acquisition module:** performs correlation of the local ECSs against the stored E6-C snapshots to detect correlation peaks. The acquisition is assisted by E1-B, using the code delay and Doppler estimates to define a small search window in E6-C. The comparison of the code phase delays enables measurements to be flagged for authentication.

The acquisition module is based on using E1-B as an auxiliary signal, as described in (Terris-Gallego et al., 2023b). This assistance is crucial because it allows the receiver to narrow down the search space in E6-C, which would otherwise be prohibitive due to its non-repeating nature. The assistance is based on the fact that both signals are transmitted by the same satellite, allowing the Doppler shift observed in E1-B to be mapped to E6-C using the ratio of their carrier frequencies, and the fact that E1-B and E6-C are time-aligned within a known BGD. Therefore, the code delay and Doppler estimates obtained from E1-B can be used to define a small search window in E6-C around the expected location of the ECS.

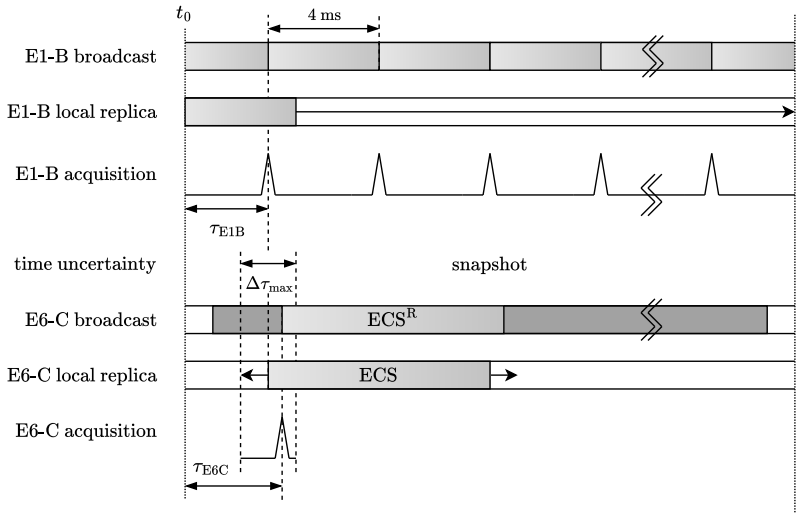

Figure 5: Proposed operating mode for Galileo SAS, where detection of RECS on E6-C signal is aided by the use of E1-B as auxiliary signal.

The SDR platform (see Fig. 6) is based on two bladeRF 2.0 micro SDRs with a shared clock, which allows synchronous sampling of E1 and E6 signals. The platform also includes hardware triggers to ensure alignment between the two SDRs. The use of a fast SSD hosted by the latest Raspberry Pi modules enables synchronous sample recording without overruns at the high sampling rates required for testing—typically 20 Msps at 12-bit resolution. Details about the synchronization mechanism and the performance of the SDR platform can be found in (Terris-Gallego et al., 2023a).

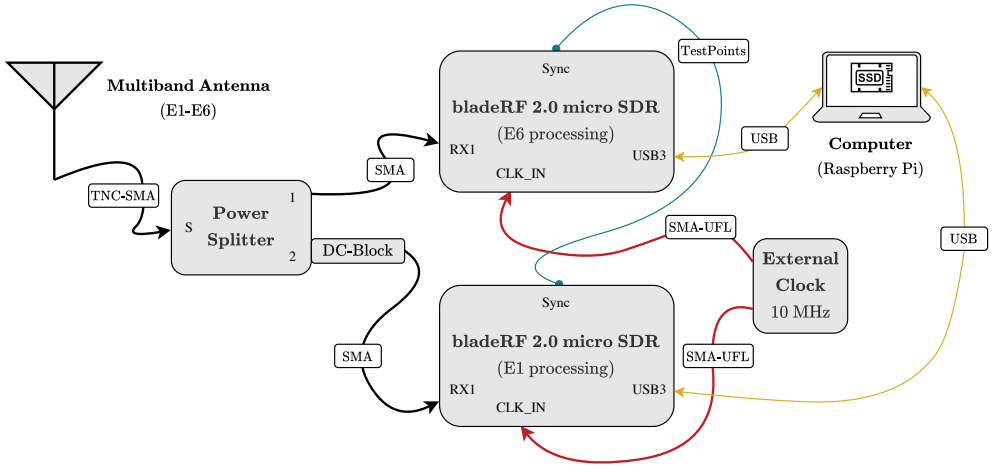

Figure 6: Schematics of the SDR platform.

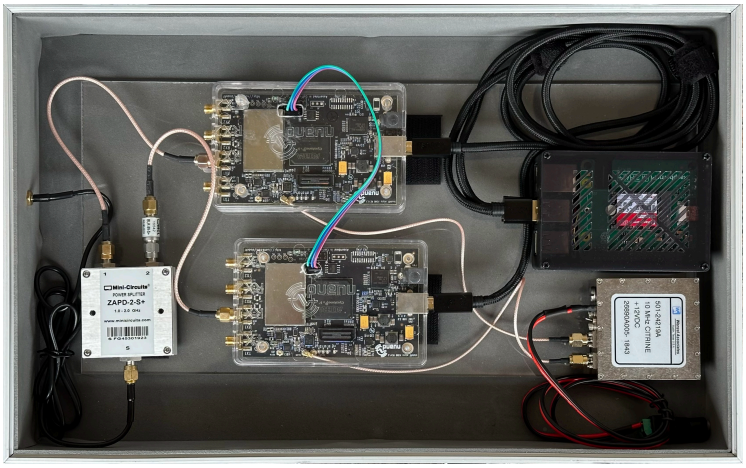

Figure 7: Prototype of the SDR platform.

IV. RESULTS WITH ENCRYPTED SIGNAL

The test-bed described in Section III was used to perform end-to-end tests of Galileo SAS with the encrypted E6-C signal-in-space. The results presented in this section correspond to the test campaign conducted on June 4, 2025. Tests were coordinated by EUSPA/European Commission (EC), which organized the transmission of the encrypted E6-C signal by the eccentric E14 satellite.

1. Test Configuration

The RECSs were generated a priori on the system side by GMV for all the configurations mentioned below and were made available for download on the internal MMARIO project server. The test-bed, located in the School of Engineering of the Autonomous University of Barcelona (UAB), Spain (41.5007° N, 2.1136° E), was configured to download the RECSs for the aforementioned satellite at the predicted ECS epochs. Different configurations were tested to validate key parameters in the current specification (European Commission – DG DEFIS, 2023), including the RECS length and period, as well as the KDI. The tested configurations were as follows:

- **RECS Length:** tests were conducted with lengths of 1 ms, 2 ms, 4 ms, 8 ms, and 16 ms.
- **RECS Period:** tests were performed with periods of 200 ms (the minimum) and 30 s (the maximum).
- **Key Delay Index:** tests were carried out with KDI values of 0 and 1.

The test-bed used a stratum-2 NTP server for time synchronization, providing approximately 50 ms of timing accuracy. This uncertainty was taken into account when setting the length of the E6 snapshots to be recorded. The test-bed also recorded synchronized E1 snapshots for assisted acquisition on E6-C. The sampling rate was 20 Msps.

2. Test Results

In Fig. 8, we present the acquisition results for E6-C and E1-B using a RECS length of 16 ms and a snapshot size of 50 ms. The results confirm successful detection of E6-C in the encrypted signal-in-space, with a clear correlation peak at the expected location. The E1-B acquisition also shows a strong correlation peak. The alignment of the E1-B and E6-C peaks confirms the correct operation of the synchronization mechanism of the SDR platform.

3. Parameter Validation

In Fig. 9, we present a comparison of the E6-C correlation peaks obtained with different RECS lengths, ranging from 16 ms (the maximum value according to the specification) to 1 ms (the minimum). The results confirm successful detection for all lengths, with longer lengths providing better detection performance due to the increased processing gain. However, longer lengths also require more storage and processing time, which may not be suitable for all

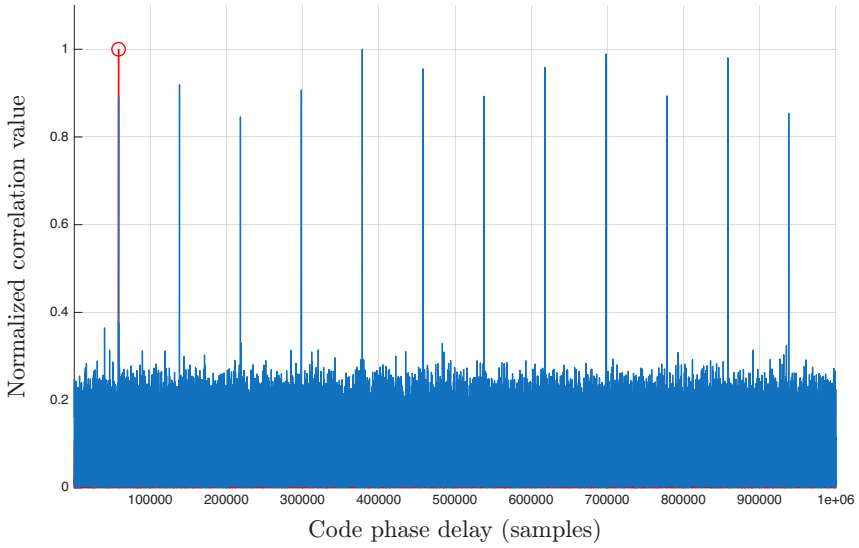

Figure 8: E6-C correlation peak (in red) using 16 ms RECS and a 50 ms snapshot (i.e. 1M samples at 20 Msps). Superposed (in blue) is the E1-B correlation peak(s) from the companion (synchronized) snapshot, which, as expected, is aligned with the E6-C peak at the expected location.

applications or receivers.

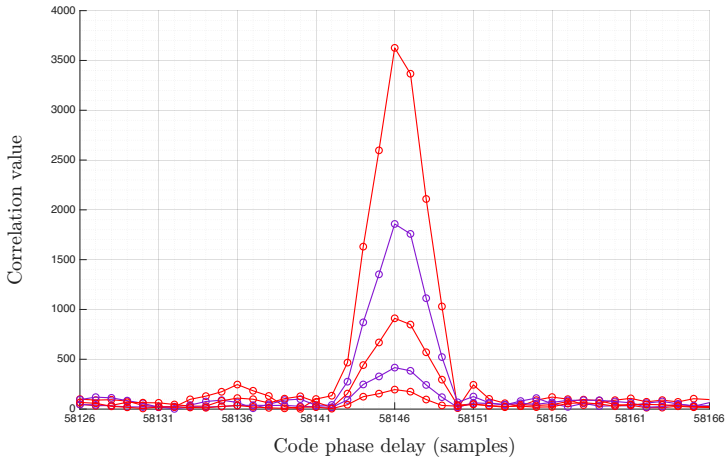

Figure 9: Comparison of the E6-C correlation peaks obtained with different RECS lengths, from 16 ms (top) to 1 ms (bottom).

Table 1 summarizes the Signal to Noise power Ratios (SNRs) measured at the output of the correlators for the different RECS lengths tested. The SNRs were computed as the ratio between the peak value and the standard deviation of the noise floor, estimated from the correlation values outside the main peak.

Table 1: Measured SNR at the output of the correlators for different RECS lengths.

RECS Length	16 ms	8 ms	4 ms	2 ms	1 ms
Output SNR	28.5 dB	25.3 dB	22.1 dB	18.7 dB	15.4 dB

In Fig. 10, we show the E6-C correlation peaks obtained for two consecutive RECS periods of 200 ms, with a RECS length of 16 ms. The results confirm successful detection in both periods at the expected locations. Shorter periods provide more frequent authentication opportunities, which may benefit certain applications. However, they also increase storage and processing demands, as the receiver must download and store more RECSs for the same autonomy period.

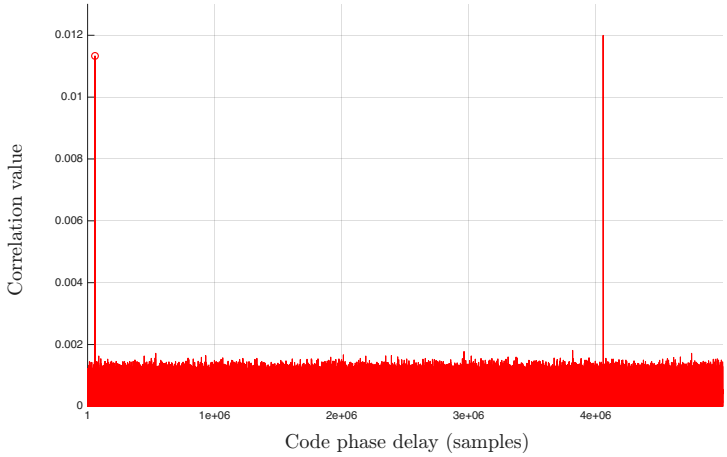

Figure 10: E6-C correlation peaks for two consecutive 200 ms RECS periods (i.e. 4M samples at 20 Msps.

In Fig. 11, we present the E6-C correlation peaks for KDI values 0 and 1, using a RECS length of 16 ms. The results confirm successful detection in both cases, with the expected 16-ms separation between peaks, as specified (see Fig. 3). The choice of KDI affects the authentication latency.

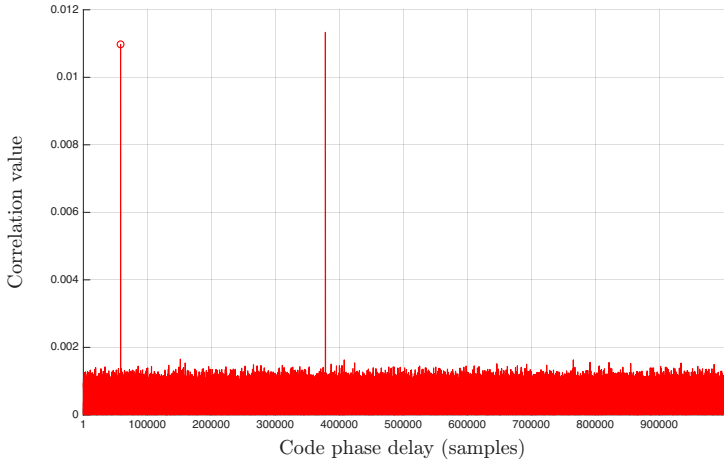

Figure 11: E6-C correlation peaks for KDI=0 and KDI=1, separated by 16 ms (i.e. 320k samples at 20 Msps.

4. Range authentication based on E6-C and E1-B alignment

Once the E6-C signal has been detected successfully, the receiver can proceed with range authentication. This process relies on the authentication mechanism described in (Ardizzon et al., 2022a), where one trusted ranging signal (E6-C) serves as an anchor for another unauthenticated ranging signal (E1-B) of the same satellite. Specifically, the measurement for the k-th satellite is authenticated only if the difference between the code phase delay observed on E6-C, denoted τ^k_{E6C}, and the code phase delay estimated for E6-C from E-1B—based on the code phase delay observed in E1-B after adjusting the ionospheric error and other biases—, denoted $\hat{\tau}^k_{E6C-E1B}$, is less than a predefined

threshold, denoted as γ_{auth}, as expressed in (1).

$$\left|\tau^k_{E6C} - \hat{\tau}^k_{E6C-E1B}\right| \leq \gamma_{\text{auth}} \tag{1}$$

This threshold is determined by modeling the contributions that may affect the measurements and, consequently, the confidence in the authenticated position. This includes the noise in the measurements, the multipath effects, and the estimation errors of the inter-frequency biases between the two signals. Finally, PVT could be authenticated by using the authenticated measurements required according to (1).

In Fig. 12, we present a zoomed view of Fig. 8 around the E6-C correlation peak, obtained with a RECS length of 16 ms. The peak of correlation E1-B is superimposed, which, as expected, aligns with the peak E6-C. The plot shows the normalized correlation values for both signals. This alignment confirms the correct operation of the SDR platform's synchronization mechanism and enables range authentication using the method described above.

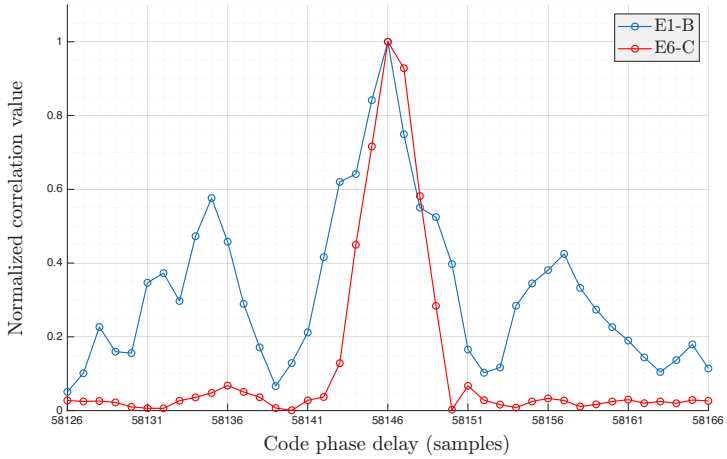

Figure 12: Alignment of E1-B and E6-C correlation peaks.

To obtain a more accurate estimate of the code phase delays, a quadratic polynomial interpolation of the correlation peaks is applied. In Fig. 13, we present the test-bed results for the acquisition of E6-C (main signal) and E1-B (auxiliary signal), with the interpolated values for both signals indicated. For the case analyzed, the difference between the code phase delays of E1-B and E6-C is approximately 0.41 samples. The Doppler frequency in E6-C is estimated from E1-B, with a residual difference of only 0.1 Hz.

SVID	SNRout	SNRoutAux	CN0	CN0Aux	PPSP	Doppler	DopplerAux	DopplerDelta	CodePhase	CodePhaseAux	CodePhaseDelta
14	28.3 dB	19.6 dB	47.3 dBHz	45.3 dBHz	7.01	4633 Hz	5708 Hz	0.1 Hz	58146.3 smp	58145.9 smp	0.41 smp

Figure 13: Acquisition metrics from the encrypted-signal test.

In terms of range error, this corresponds to approximately 6.15 meters. This range error is computed as follows:

$$\text{RE} = \frac{c}{F_s}\left[\left(\hat{\tau}_{0,1}\right)_{\bmod N_{\text{scode}}} - \hat{\tau}_{0,6}\right] \quad [\text{m}] \tag{2}$$

where c is the speed of light, F_s is the sampling rate, N_{scode} is the number of samples in a primary spreading code of E6-C (20,000 for the sample rate used in our tests), $\hat{\tau}_{0,1}$ is the estimated code phase delay (in samples) for the E1-B signal, and $\hat{\tau}_{0,6}$ is the estimated code phase delay (in samples) for the E6-C signal.

The obtained range error should be compared with the authentication threshold γ_{auth} defined in (1), as detailed in (Fernandez-Hernandez et al., 2023). A preliminary evaluation of this range error based on real signals across different C/N_0 scenarios was presented in (Terris-Gallego et al., 2023b). However, more accurate modeling of the

authentication thresholds—considering all relevant contributions—is still required and will be addressed in future work.

V. CONCLUSION

This work presented an SDR-based evaluation platform that exercises the complete Galileo SAS receiver workflow with encrypted E6-C signal-in-space. Using synchronized dual-SDR captures and a modular software pipeline, we verified end-to-end functionality: RECS retrieval and parsing, time-aligned E6/E1 snapshotting, TESLA key retrieval from OSNMA, decryption into ECSs, assisted acquisition, and correlation-driven detection, followed by measurement authentication using E6-C as the trusted anchor. E14 trials confirmed repeatable E6-C detections with encrypted signal-in-space at the predicted epochs and represent a step forward from previous open-signal tests.

Future work will focus on several directions. Test parameters will be extended to include configurations with KDI = 2 and intermediate RECS periods, and a broader range of operating conditions (e.g., weak-signal scenarios) will be exercised. Authentication thresholds will be modeled more accurately. Auxiliary mitigation and cross-check mechanisms—e.g., Vestigial Signal Search (VSS)—will be incorporated to strengthen the authentication process. The current snapshot-based post-processing chain will be transitioned to real-time operation. E6-B-aided positioning will be evaluated to reduce inter-frequency biases in the authentication chain. In addition, alternative auxiliary signals for assisting E6-C acquisition will be investigated, together with cross-checks using other Galileo components (e.g., E5 (Schreiber et al., 2025)).

Future work will focus on:

- Extending tests parameters (KDI = 2, intermediate RECS periods) and scenarios conditions (e.g. weak signal).
- Accurate modeling of authentication thresholds.
- Incorporating auxiliary mitigation and cross-checks—e.g., VSS—for improving authentication.
- Transition from snapshot post-processing to real-time operation.
- Evaluating E6-B-aided positioning to reduce inter-frequency biases in the authentication chain.
- Using alternative auxiliary signals to assist E6-C acquisition, and cross-checking authentication with other Galileo components—e.g., E5 (Schreiber et al., 2025).

ACKNOWLEDGEMENTS

We would like to thank all the participants of the MMARIO project (European Commission, 2023), which is in charge of implementing Galileo SAS. This work was supported in part by the European Commission Defence Industry and Space Satellite Navigation (DEFIS) contract DEFIS/2023/OP/0011, in part by the Spanish Agency of Research (AEI) under grant PID2023-152820OB-I00 funded by MICIU/AEI/10.13039/501100011033 and by ERDF/EU, and under grant PDC2023-145858-I00 funded by MICIU/AEI/10.13039/501100011033, in part by the Departament de Recerca i Universitats de la Generalitat de Catalunya under grant 2021 SGR 00737, and in part by the Catalan ICREA Academia Programme. The content of this article does not necessarily reflect the official position the authors' organizations. Responsibility for the information and views set out in this article lies entirely with the authors.

REFERENCES

Anderson, J. (2025). World's First Authenticated Satellite Pseudorange from Orbit. In *Proceedings of the 38th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2025)*, Baltimore, Maryland, US. [to be published].

Anderson, J. M., Carroll, K. L., DeVilbiss, N. P., Gillis, J. T., Hinks, J. C., O'Hanlon, B. W., Rushanan, J. J., Scott, L., and Yazdi, R. A. (2017). Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals. In *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)*, pages 2388–2416, Portland, Oregon.

Ardizzon, F., Caparra, G., Fernandez-Hernandez, I., and O'Driscoll, C. (2022a). A Blueprint for Multi-Frequency and Multi-Constellation PVT Assurance. In *NAVITEC*.

Ardizzon, F., Crosara, L., Laurenti, N., Tomasin, S., and Montini, N. (2022b). Authenticated Timing Protocol Based on Galileo ACAS. *Sensors*.

Dorins, T., Bochkati, M., Dötterböck, D., Pany, T., Baumann, S., Dütsch, N., Wenz, A., and Ehrler, R. (2025). An Analysis of Authentication Availability and Enhancements Through Vector Tracking for Galileo OSNMA Data and SAS Spreading Code Authentication. Baltimore, Maryland, US. [to be published].

European Commission (2023). Call for Tenders (DEFIS/2023/OP/0011) – Contribution to Radio-navigation Accuracy and Resilience.

European Commission – DG DEFIS (2023). Galileo Assisted Commercial Authentication Service (ACAS) – Specification Proposal v1.2. Technical report.

Fernandez-Hernandez, I., Winkel, J., O'Driscoll, C., Cancela, S., Terris-Gallego, R., Seco-Granados, G., López-Salcedo, J. A., Dalla Chiara, A., Sarto, C., Blonski, D., and de 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. A., Seco-Granados, G., Motella, B., Blonski, D., and 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 (ION GNSS+ 2024)*, pages 3292 – 3307, Baltimore, Maryland, USA.

Galan-Figueras, A., Iñiguez, C., Fernandez-Hernandez, I., Pollin, S., and Seco-Granados, G. (2025). Improving OSNMAlib: New Formats, Features, and Monitoring Capabilities. *IEEE Journal of Indoor and Seamless Positioning and Navigation*, 3:117–127.

Schreiber, B., Garzia Id, F., Parra, R., Gupta, H., Overbeck Id, M., and Rügamer, A. (2025). Range Authentication of Galileo E1 / E5 Signals Using Different Assisted Methods on a GNSS Hardware Receiver. In *Proceedings of the 38th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2025)*, Baltimore, Maryland, US. [to be published].

Terris-Gallego, R., Fernandez-Hernandez, I., López-Salcedo, J. A., and Seco-Granados, G. (2022a). Guidelines for Galileo Assisted Commercial Authentication Service Implementation. In *Proceedings of the International Conference on Localization and GNSS (ICL GNSS 2022)*, Tampere, Finland. IEEE.

Terris-Gallego, R., López-Salcedo, J. A., Seco-Granados, G., and Fernandez-Hernandez, I. (2022b). Operating Modes and Performance Evaluation of Galileo Assisted Commercial Authentication Service. In *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, Denver, Colorado, USA.

Terris-Gallego, R., López-Salcedo, J. A., Seco-Granados, G., and Fernandez-Hernandez, I. (2023a). E1-E6 SDR platform based on bladeRF for testing Galileo Assisted Commercial Authentication Service. In *Proceedings of the European Navigation Conference (ENC 2023)*, ESA ESTEC, Noordwijk, The Netherlands. MDPI.

Terris-Gallego, R., López-Salcedo, J. A., Seco-Granados, G., and Fernandez-Hernandez, I. (2023b). Preliminary Evaluation of Galileo ACAS using Existing E1-E6 Open Signals and a Low-Cost SDR Platform. In *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, pages 1388–1402, Denver, Colorado, USA.