Validation of Galileo SAS Spreading Code Authentication with Snapshot Data and Pedestrian/Vehicular Field Tests

Toms Dorins[(1)], Mohamed Bochkati[(1)], Dominik Dötterböck[(1)],
Paulo Mendes[(2)] , Nikolas Dütsch[(1,2)], Thomas Pany[(1)],

[(1)] *Institute of Space Technology and Space Applications (ISTA), Space Systems Research Center (FZ SPACE)*
University of the Bundeswehr Munich (UniBw M)

[(2)] *IABG Industrieanlagen-Betriebsgesellschaft mbH*

BIOGRAPHY

Toms Dorins is a research associate at the Institute of Space technology and Space Applications ISTA) at the University of the Bundeswehr Munich (Unibw M). His reasearch foxuses on Navigation data and spreading code authentication and signal processing.

Dominik Dötterböck is a senior researcher at the University of the Bundeswehr Munich at the Institute of Space Technology and Space Applications. He received his diploma in Electrical Engineering and Information Technology from the Technical University Munich. His current research interests include signal design, signal-processing algorithms for GNSS receivers and LEO-PNT system analysis.

Mohamed Bochkati is a research associate at the Institute of Space Technology and Space Applications (ISTA) at the University of the Bundeswehr Munich (UniBw M). His research focuses on Deeply Coupled GNSS/INS integration and novel calibration techniques for MEMS-IMUs.

Paulo Mendes works at IABG since 2022 as a project manager and analyst. His main work focus on satellite navigation and space systems with one focus being the analysis of jamming and spoofing events. He has a background in Physics and developed his Ph.D work at the Max-Planck-Institut für extraterrestrische Physik obtaining a Ph.D. in Astronomy/Astrophysics at the Ludwig-Maximilians-University Munich.

Nikolas Dütsch works at IABG since 2016. His main work focus on satellite navigation and robust satellite navigation receiver design against jamming and spoofing. Since 2019 he is a research associate at University Bundeswehr München at the institute of Space Technology and Space Applications with the main focus on the detection and geo-location of GNSS interference sources from a LEO satellite. In 2015, he received a M.Sc Degree in Electrical Engineering from the Friedrich-Alexander-University in Erlangen-Nuremberg.

Prof. Thomas Pany is with the University of the Bundeswehr Munich (UniBw M) at Space Systems Research Center (FZ-Space) where he leads the satellite navigation unit LRT 9.2 of the Institute of Space Technology and Space Applications (ISTA). He teaches navigation focusing on GNSS, sensors fusion and aerospace applications.

ABSTRACT

This paper presents a validation and application-oriented evaluation of the signal authentication service (SAS) using snapshot-based processing. Building on our earlier availability analysis of open service navigation message authentication (OSNMA) and snapshot-based SAS authentication under scalar and vector tracking (Dorins et al., 2025), the present work advances the study toward encrypted signal validation and extended field-test scenarios.

The SAS authentication chain is first reproduced using an encrypted reference dataset provided through collaboration with the European Commission and the Universitat Autònoma de Barcelona (UAB). The dataset contains re-encrypted fragments of the encrypted E6-C spreading code, time-aligned OSNMA time efficient stream loss-tolerant authentication (TESLA) keys, and synchronised E1/E6 snapshots for satellite E14. By implementing the receiver cryptographic operations defined for SAS, the encrypted spreading sequences are reconstructed and correlated with recorded E6-C snapshots. Clear and consistent correlation

peaks are obtained for multiple key delay configurations, demonstrating successful Cryptographic spreading code authentication with encrypted data.

In addition, snapshot-based SAS authentication is evaluated using a representative pedestrian dataset, additionally, vehicular dataset is used to evaluate OSNMA authentication performance in an automotive driving scenario, extending the scope of previous railway-based analyses. The combined results provide a consolidated assessment of SAS authentication performance across encrypted reference data and realistic user scenarios, and establish a baseline for future evaluations with operational encrypted signals.

I. INTRODUCTION

Global navigation satellite system (GNSS) technologies, and in particular the European Galileo system, have become a key enabling component for a wide range of applications that depend on accurate and reliable positioning and timing. These include transportation systems, industrial automation, telecommunications, financial services, and emerging internet of things (IOT) applications. As the societal and economic dependence on GNSS increases, so does the impact of malicious signal manipulation. Open civil GNSS signals are inherently exposed to spoofing, replay, and other forms of interference, which can mislead receivers without obvious indication and pose serious risks to safety- and security-critical systems (Seco-Granados et al., 2021; Margaria et al., 2017). This has motivated the development of authentication mechanisms that allow users to verify the origin and integrity of received GNSS signals.

To address these challenges, Galileo provides two complementary authentication services. The OSNMA protects navigation data by enabling cryptographic verification of the transmitted messages using delayed key disclosure based on the TESLA protocol (European Union Agency for the Space Programme (EUSPA), 2023, 2025). While OSNMA ensures that the navigation message originates from the Galileo system and has not been modified, it does not directly authenticate the underlying ranging measurements. This limitation is addressed by the SAS, which extends authentication to the signal level by securing encrypted spreading codes on the E6-C signal. By enabling verification of pseudorange measurements, SAS provides an additional layer of protection against advanced spoofing and replay attacks (Fernandez-Hernandez et al., 2024, 2022; Winkel et al., 2023). When used together, OSNMA and SAS form a layered defence combining data-level and signal-level authentication.

The effectiveness of these authentication services in practice strongly depends on the availability of suitable signal observations. In real-world environments, especially those characterised by partial obstructions, strong multipath, or dynamic user motion, satellite signals may be intermittently attenuated or blocked. Typical examples include urban canyons, indoor-outdoor transitions, underpasses, and tunnel-like structures. Under such conditions, conventional scalar tracking (ST) receivers, which track each satellite independently, are prone to frequent loss of lock and repeated reacquisition. This behaviour can interrupt navigation message demodulation required for OSNMA and reduce the availability of signal snapshots needed for SAS, thereby limiting authentication continuity.

The proposed vector tracking (VT) acts as an advanced receiver architecture to improve robustness in degraded environments by jointly processing all tracked signals within a common navigation filter (Spilker Jr. et al., 1996). By exploiting the coupling between satellite measurements and shared state estimates (such as Doppler and code phase information), VT can bridge short signal outages and reduce the need for reacquisition. In our earlier work (Dorins et al., 2025), we investigated the impact of scalar and vector tracking on the availability of Galileo OSNMA and snapshot-based SAS authentication using an open-signal railway dataset collected during a Swiss Federal Railways campaign. That study showed that vector tracking can improve authentication continuity under challenging conditions; however, the SAS analysis was limited to replica-based correlation with unencrypted spreading codes.

The present paper extends this previous work in two important ways. First, we validate the SAS spreading code authentication concept using an encrypted reference dataset for which all required cryptographic material is available. The dataset, provided through collaboration with the European Commission and the Universitat Autònoma de Barcelona (UAB), contains re-encrypted fragments of the encrypted E6-C spreading code, time-aligned OSNMA TESLA keys, and synchronised E1 and E6 snapshots for satellite E14. By reproducing the Receiver Cryptographic Operations defined in the SAS specification (Fernandez-Hernandez et al., 2024), the encrypted spreading sequences are reconstructed and correlated with recorded E6-C snapshots, allowing a direct validation of SAS authentication for different key delay configurations.

Second, because operational re-encrypted code sequences are currently not publicly available-despite the continuous transmission of encrypted E6-C signals by satellites such as E14 and E18, we extend the snapshot-based evaluation methodology from our previous work to additional user scenarios using open-signal data. These include pedestrian field tests conducted in mixed environments, ranging from open-sky conditions to multipath-dominated urban areas, indoor passages through a library environment, and tunnel-like underpasses beneath buildings. In addition, a vehicular dataset from the VorTNAF automotive project is considered to evaluate OSNMA authentication performance in a dynamic driving scenario. By applying a consistent snapshot-based analysis framework to the pedestrian use case, and extending the OSNMA evaluation to an automotive driving

scenario, this study provides a comprehensive assessment of Galileo SAS authentication performance under realistic operational conditions and establishes a baseline for future evaluations once live encrypted datasets become available.

II. OSNMA AND SAS AUTHENTICATION SERVICES

The Galileo system provides two complementary authentication mechanisms to enhance robustness against spoofing and signal manipulation: the Open Service Navigation Message Authentication (OSNMA) and the Signal Authentication Service (SAS). A detailed description of both services, including their operational principles and availability aspects, is provided in our earlier work (Dorins et al., 2025) and is therefore only briefly summarised here.

OSNMA, specified in the OSNMA Service Definition Document (European Union Agency for the Space Programme (EUSPA), 2025), authenticates Galileo navigation messages using delayed key disclosure based on the TESLA protocol. Authentication tags are broadcast together with the navigation data, while the corresponding cryptographic keys are disclosed in later subframes. Successful verification ensures that the received navigation message originates from the Galileo system and has not been modified. OSNMA is bandwidth-efficient but requires continuous demodulation of the E1-B data symbols and does not directly authenticate the underlying ranging measurements.

The Signal Authentication Service (SAS) complements OSNMA by extending authentication to the signal level on the E6-C signal (Fernandez-Hernandez et al., 2024). SAS enables verification of pseudorange measurements by correlating recorded E6-C signal snapshots with reconstructed encrypted spreading code sequences derived from re-encrypted code fragments and OSNMA-disclosed keys. This approach provides protection against signal-level attacks, but introduces additional latency due to delayed key disclosure and requires storage of auxiliary authentication data (Fernandez-Hernandez et al., 2022; Winkel et al., 2023).

Used together, OSNMA and SAS form a layered authentication framework that combines data-level and signal-level protection. The practical availability of both services, however, depends strongly on signal tracking robustness. In challenging propagation environments, interruptions in tracking can affect symbol demodulation for OSNMA and snapshot availability for SAS. This motivates the investigation of advanced tracking architectures, such as vector tracking (VT), to improve authentication continuity under degraded signal conditions, as explored further in this study.

III. VECTOR TRACKING CONCEPT AND SAS INTEGRATION

Vector tracking is a well-established GNSS receiver architecture in which all tracked satellite signals are processed jointly within a common navigation filter, in contrast to conventional scalar tracking where each signal is tracked independently. A detailed discussion of vector tracking principles, architectures, and their impact on Galileo authentication availability is provided in our earlier work (Dorins et al., 2025) and is therefore not repeated here.

In the context of authentication, the main advantage of VT is its improved robustness under degraded signal conditions. By exploiting shared state information (such as Doppler and code phase estimates), VT can bridge short signal outages and reduce the need for reacquisition, which is critical for maintaining continuous navigation message demodulation for OSNMA and stable snapshot availability for the SAS. This property is particularly relevant in obstructed and multipath-dominated environments, where scalar tracking is prone to frequent loss of lock.

In this study, VT is implemented using the MuSNAT software receiver in a federated configuration, as described in (Dorins et al., 2025). Galileo E1B/E1BC signals serve as the primary input to the vector tracking loops, providing the basis for positioning and OSNMA processing. For SAS evaluation, the E6C channel is operated in slave mode with respect to the E1BC tracking loop. As a result, E6C snapshots used for SAS authentication are recorded only when the corresponding E1BC channel remains successfully tracked. This design directly links the availability of SAS snapshots to the robustness of E1BC tracking under VT.

While VT improves the continuity of E1B symbol availability under challenging conditions, the absence of carrier phase lock in the vector frequency-locked loop requires an alternative symbol detection approach for OSNMA, as discussed in (Dorins et al., 2025). For SAS, this limitation does not apply, since authentication is based on snapshot correlation rather than symbol demodulation. Consequently, SAS particularly benefits from the increased tracking stability provided by VT.

The specific SAS processing flow under vector tracking, including the interaction between the MuSNAT receiver and the snapshot-based authentication stage, is illustrated in Figure 1.

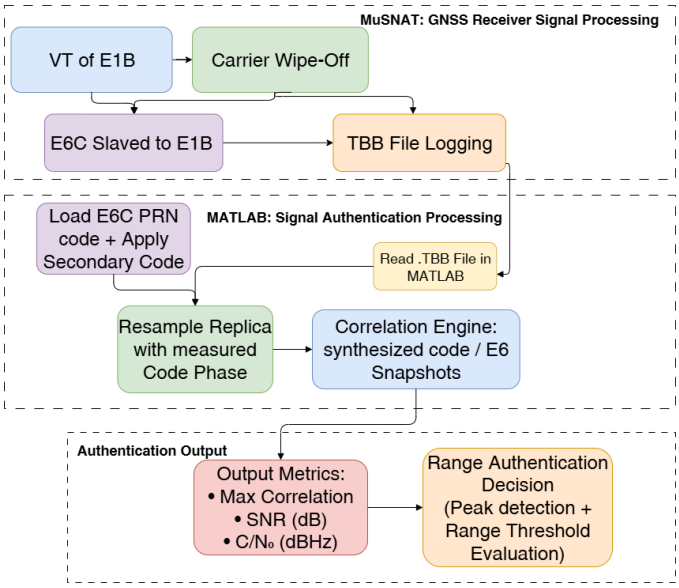


Figure 1: SAS processing architecture under vector tracking.

SAS Vector Tracking Architecture

Figure 1 illustrates the SAS processing flow under vector tracking, which is structured into three main stages. First, the MuSNAT receiver performs vector tracking on the E1BC signal and records time-aligned snapshots of the E6C signal together with the corresponding code phase information. Second, the recorded snapshots are processed in MATLAB, where local replicas of the E6C spreading code, including the secondary code, are generated and aligned according to the measured code phase. Finally, the correlation results are evaluated to derive authentication-relevant metrics, including the correlation peak magnitude, the signal-to-noise ratio (SNR in dB), and the carrier-to-noise density (C/N_0 in dB-Hz). These metrics form the basis for SAS range authentication, where authenticity is determined using peak detection and threshold-based decision criteria.

IV. EXPERIMENTAL SETUP

To process the recorded GNSS signals and extract authentication metrics, two specialised software tools were employed:

- **OSNMA Authentication and Encrypted SAS Processing:** The SiSiTau Tool v2.2 was used for decoding and verifying Galileo OSNMA messages. For the encrypted snapshot dataset, an extended cryptographic module of the SiSiTau Tool was employed to handle TESLA key verification and cryptographic processing required for SAS. The tool supports TESLA chain management, navigation data validation, and root key handling, and provides the verified cryptographic material used in subsequent SAS processing.
- **SAS Snapshot Correlation:** For spreading code authentication based on snapshot correlation, a MATLAB-based True Baseband (TBB) file reader was used. This tool enables correlation of recorded E6-C signal snapshots with locally generated spreading code replicas. The E6-C snapshots are captured in slave mode based on the successful tracking of the corresponding E1B channels.

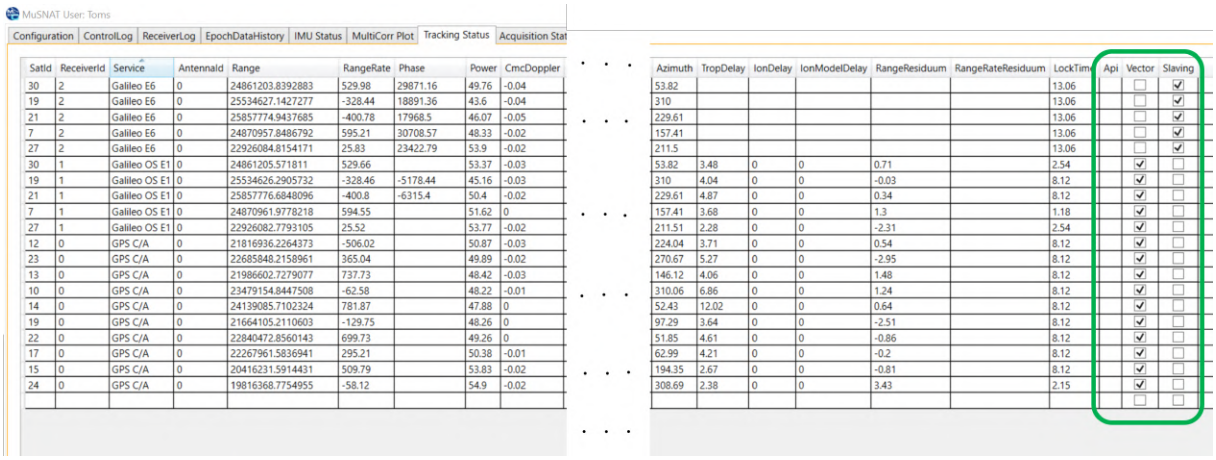


Figure 2: MuSNAT processing interface showing satellite channel status and tracking modes (scalar, vector, or slave)

The multi sensor navigation analysis tool (MuSNAT) graphical interface (Figure 2) displays the status of each satellite channel, shown inside a green rounded box, and indicates whether it is running in ST mode, in slave mode, or in VT mode. MuSNAT generates dumplog files, observables, navigation data files, and TBB recordings, providing all the inputs required for subsequent processing with the SiSiTau Tool v2.2 and the TBB file reader. To ensure interoperable data exchange and reproducible post-processing, all SDR files and associated metadata conform to the ION GNSS SDR Metadata Standard (Gunawardena et al., 2021).

Symbol Demodulator Implementation for Vector Tracking

In conventional scalar tracking systems, the E1B navigation message symbols are typically demodulated using a phase-locked loop (PLL), which ensures reliable carrier phase estimation and coherent bit decision. However, in the vector tracking configuration applied in this study, the MuSNAT receiver operates with a vector frequency-locked loop (VFLL) only. Since no carrier phase information is available under VFLL, a standard PLL-based demodulator cannot be employed.

To enable OSNMA operation under vector tracking, we implemented a new symbol detector. The detector estimates the E1B navigation symbol sign by exploiting the E1C pilot channel: the prompt data correlator output is compared against the prompt pilot replica, allowing recovery of the bit polarity even without carrier phase lock. This design effectively bridges one of the main limitations of VFLL-based VT, ensuring that symbol demodulation remains available when scalar tracking would typically lose lock.

The detector is mathematically defined as follows. First, the prompt pilot and prompt data correlators are formed, where P^{rep} and P^{imp} denote the real and imaginary parts of the prompt pilot correlator output, respectively, and P^{red} and P^{imd} denote the real and imaginary parts of the prompt data correlator output:

$$P_{\text{pl}} = (P_1^{\text{rep}} + P_2^{\text{rep}}) + j\left(P_1^{\text{imp}} + P_2^{\text{imp}}\right) \tag{1}$$

$$P_{\text{data}} = \left(P_1^{\text{red}} + P_2^{\text{red}}\right) + j\left(P_1^{\text{imd}} + P_2^{\text{imd}}\right) \tag{2}$$

A decision variable is then computed by correlating the prompt data with the conjugated pilot:

$$signal = \Re\left\{P_{\text{data}} \cdot \overline{P_{\text{pl}}}\right\} \tag{3}$$

Finally, the estimated bit sign is obtained as:

$$\hat{b} = \text{sign}(signal) \tag{4}$$

Table 1: Definition of symbol detector variables

Variable	Description
P_{pl}	Prompt Pilot (replica prompt, complex I/Q)
P_{data}	Prompt Data (received prompt, complex I/Q)
$\overline{P_{\mathrm{pl}}}$	Complex conjugate of Prompt Pilot
$signal$	Real part of correlation metric
$\hat{b}$	Estimated navigation bit (sign of $signal$)

All variables and their corresponding descriptions used in the detector formulation are summarized in Table 1. This detector introduces a theoretical sensitivity loss of approximately 3 dB compared to a coherent PLL-based demodulator, since the symbol decision is made without carrier phase alignment. However, the practical effect in dynamic and challenging conditions is the opposite: more symbols remain available because vector tracking maintains frequency lock through short dropouts where ST would lose phase lock entirely. As a result, OSNMA authentication continuity improves significantly.

For SAS, this limitation does not apply, since the E6C snapshots are triggered by E1BC tracking and do not rely on symbol demodulation. Consequently, SAS authentication also benefits indirectly from VT, as the more stable tracking increases snapshot availability and continuity.

V. RESULTS AND ANALYSIS

1. Measurement Campaign

The experimental evaluation in this study is based on two measurement datasets representing pedestrian and vehicular user scenarios. Both datasets were collected in the Munich area and were selected to capture a wide range of propagation conditions, from open-sky environments to strongly obstructed and multipath-dominated situations, which are particularly challenging for GNSS signal reception.

The pedestrian dataset was recorded on the campus of the University of the Bundeswehr Munich (UniBw M). The measurement route includes open-sky sections as well as challenging environments such as narrow passages between buildings, indoor and semi-indoor transitions through the university library, and an under-building passage resembling a tunnel-like structure. These conditions result in frequent variations in satellite visibility and signal quality, providing a demanding test case for authentication availability.

The vehicular dataset was collected within the framework of the VorTNAF automotive project during a drive through Ottobrunn in the Munich metropolitan area. GNSS signals were recorded using the Fraunhofer MGSE/GTEC Multi-GNSS Simulation & Test Environment with a modular radio-frequency front end (RFFE). The route includes a mixture of open-sky road segments, built-up areas, and infrastructure-related obstructions representative of real-world automotive use cases.

Figure 3 shows the pedestrian measurement route, while Figure 4 presents the automotive measurement route used in the VorTNAF project.



Figure 3: Pedestrian measurement campaign conducted on the UniBw M campus in Munich, including open-sky, multipath-dominated, and indoor or tunnel-like sections.



Figure 4: Automotive measurement campaign of the VorTNAF project along a route through Ottobrunn in the Munich metropolitan area.

The experimental results are divided into two parts: OSNMA navigation data authentication and SAS range authentication. OSNMA results are evaluated for both the pedestrian and vehicular datasets, whereas SAS results are reported for the pedestrian dataset.

2. Validation with Encrypted E6-C Snapshot Data

In addition to the replica-based SAS evaluation, a validation using encrypted snapshot data was performed to demonstrate the complete Galileo Signal Authentication Service (SAS) processing chain with real cryptographic material. This experiment provides an experimental validation of SAS spreading-code authentication using encrypted E6-C snapshot data.

The encrypted dataset was provided through collaboration with the European Commission and the Universitat Autònoma de Barcelona (UAB). It contains re-encrypted code sequences (RECS) for satellite E14, the corresponding OSNMA TESLA keys, and synchronised E1 and E6 snapshot recordings for the same Galileo system time (GST) epochs. The available data covers Key Delay Index (KDI) configurations 0 and 1, enabling validation of SAS authentication under different key-delay conditions.

The processing follows the receiver cryptographic operations defined for SAS (Fernandez-Hernandez et al., 2024). After verification of the TESLA keys using OSNMA, the RECS files are decrypted to reconstruct the encrypted E6-C spreading sequences (ECS). These reconstructed sequences are then correlated with the recorded E6 snapshots using a coherent integration time of 20 ms. Successful SAS authentication is indicated by the presence of a distinct and unambiguous correlation peak near the expected code phase.

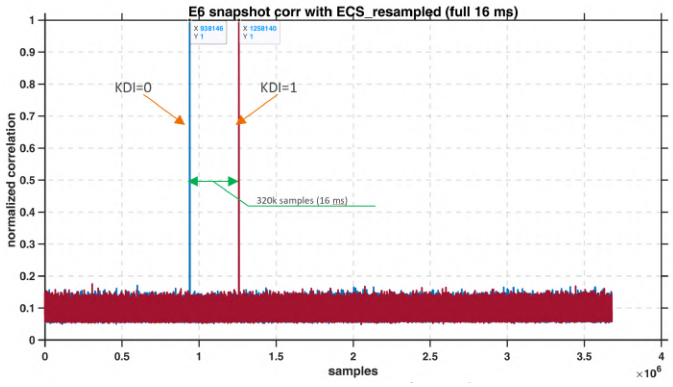


Figure 5: Correlation results obtained using reconstructed E6-C encrypted spreading codes for KDI = 0 and KDI = 1 (satellite E14). Two distinct correlation peaks are observed, with a separation consistent with the RECS unit timing and the applied sampling rate.

Figure 5 shows the correlation results obtained for KDI = 0 and KDI = 1. Two clear correlation peaks are visible, separated by a delay consistent with the unitary RECS duration and the 20 MHz sampling rate. This behaviour confirms correct TESLA key alignment and successful reconstruction of the encrypted E6-C spreading codes for both key-delay configurations.

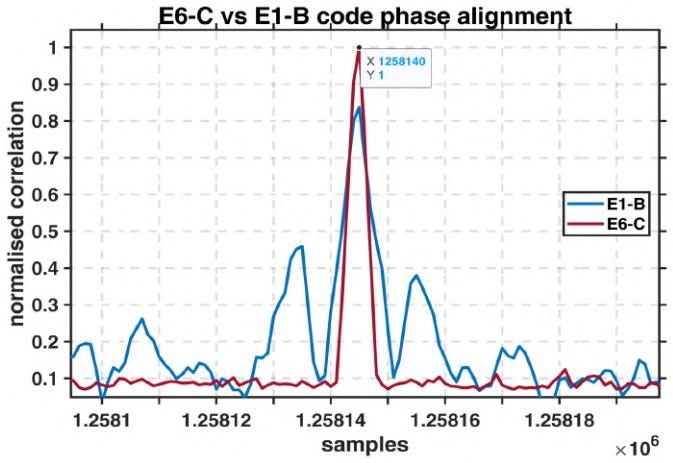


Figure 6: Zoomed view of the code-phase alignment between E1-B and E6-C, showing the normalised correlation peaks for both signals.

A zoomed view of the code-phase delay for E1-B and E6-C is shown in Figure 6. The normalised correlation peaks of the two signals are well aligned, indicating consistent code-phase estimation between E1-B and E6-C. The E6-C encrypted spreading

sequence aligns accurately with the recorded snapshot, with the detected peak lying well within the ± 1 chip tolerance used for SAS range authentication. This confirms successful spreading-code verification and demonstrates that the encrypted E6-C signal can be authenticated using snapshot-based processing.

With a 10-sample delay resolution, the plotted peak occurs at approximately 1 258 140 samples, while sub-sample interpolation yields a refined estimate of 1 258 144.76 samples. The close agreement between the E1-B and E6-C peak locations confirms proper inter-signal code-phase alignment, which is required for consistent SAS range authentication.

Range Error Calculation

Beyond the qualitative verification of encrypted spreading-code authentication, the correlation results can also be used to derive a quantitative range-consistency observable between the Galileo E1-B and E6-C signals. This observable is based on the relative code phase delay estimates obtained from the correlation peaks and follows the approach presented in (Terris-Gallego et al., 2025).

For each signal, the prompt correlator output is interpolated in the vicinity of the correlation peak in order to achieve sub-sample resolution of the estimated code phase delay. Let $\hat{\tau}_{0,1}$ and $\hat{\tau}_{0,6}$ denote the interpolated prompt code phase delay estimates, expressed in samples, for the E1-B and E6-C signals, respectively. The range error (RE) is defined as

$$\mathrm{RE} = \frac{c}{F_s}\left[(\hat{\tau}_{0,1} \bmod N_{\mathrm{scode}}) - \hat{\tau}_{0,6}\right], \tag{5}$$

where c denotes the speed of light, F_s is the receiver sampling frequency, and N_{scode} is the number of samples in one code period of the E1-B signal. The modulo operation accounts for the periodicity of the spreading code when forming the code phase difference.

In this work, the sampling frequency is fixed to $F_s = 20\,\mathrm{MHz}$, yielding the conversion factor

$$\frac{c}{F_s} = \frac{3 \times 10^8}{20 \times 10^6} = 15\ \mathrm{m/sample}. \tag{6}$$

For the analysed epoch, interpolation of the correlation peaks results in the following prompt code phase delay estimates:

$$\hat{\tau}_{0,6} = 1\,258\,144.763815 \quad \text{(E6-C)}, \tag{7}$$
$$\hat{\tau}_{0,1} = 1\,258\,144.705273 \quad \text{(E1-B)}. \tag{8}$$

The corresponding range error is obtained as

$$\mathrm{RE} = \Delta\tau \cdot \frac{c}{F_s} = 0.058542 \times 15 = 0.878\ \mathrm{m}. \tag{9}$$

Overall, these results validate the end-to-end SAS processing chain with encrypted snapshot data, including TESLA key handling, RECS decryption, and correlation-based verification. The encrypted snapshot validation constitutes an important step toward future real-time evaluations of Galileo SAS using live encrypted E6-C signals once operational datasets become available.

3. OSNMA Authentication Results

Since verified TESLA keys are a prerequisite for Signal Authentication Service (SAS) processing, OSNMA authentication is included in this study for completeness. OSNMA establishes the cryptographic trust anchor required for subsequent SAS spreading-code authentication by enabling verification of the TESLA root key and the associated key chain.

OSNMA authentication results were obtained using the SiSiTau Tool v2.2, which processes demodulated E1-B navigation symbols and provides diagnostics on navigation message availability, TESLA key verification, and authenticated data. In this work, the analysis is intentionally restricted to the ADKD 0 authentication mode. ADKD 0 represents the most stringent and operationally relevant configuration, verifying navigation data using TESLA keys disclosed in the immediately following I/NAV subframe (30 s delay), and requires receiver synchronisation to GST within the same tolerance.

Accordingly, OSNMA performance is evaluated using the following three observables:

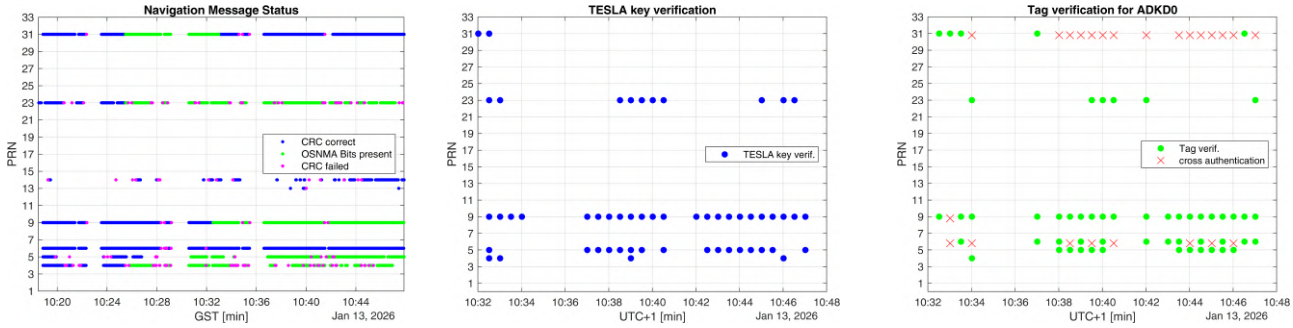
- **Navigation Message Status**: Indicates reception of valid OSNMA-capable navigation messages and successful Cyclic Redundancy Check (CRC) verification.
- **TESLA Key Verification**: Indicates successful verification of the TESLA root key and subsequent chain keys.
- **ADKD 0 Tag Authentication**: Indicates successful authentication of navigation data using TESLA keys with one-subframe delay.

Three receiver configurations are analysed:

1. Scalar Tracking (ST) with conventional symbol demodulation,
2. Scalar Tracking with pilot-assisted symbol detector,
3. Vector Tracking (VT), which inherently employs the pilot-assisted symbol detector.

All results are shown for the pedestrian dataset described in Section V.1.

Scalar Tracking (ST)

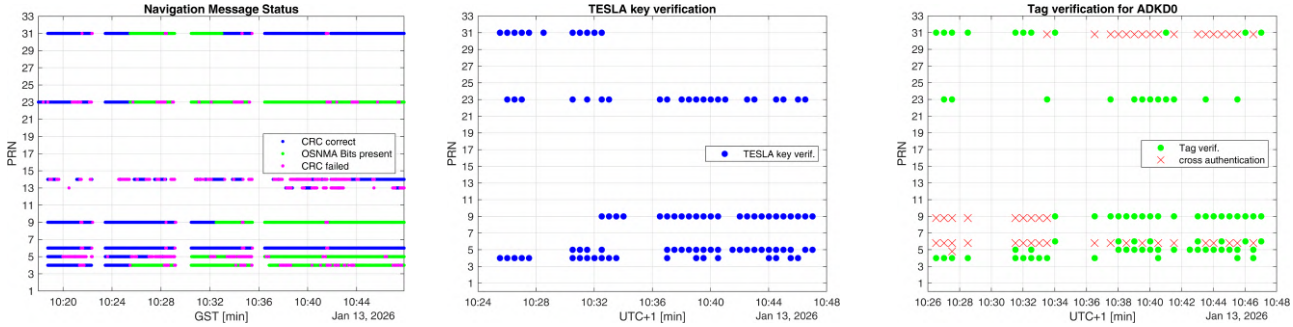


(a) Navigation Message Status **(b)** TESLA Key Verification **(c)** ADKD 0 Authentication

Figure 7: OSNMA authentication results under scalar tracking (ST).

Under conventional scalar tracking, OSNMA authentication is frequently interrupted. As shown in Figure 7, navigation message availability is degraded in challenging propagation conditions, which directly affects TESLA key verification. As a consequence, ADKD 0 tag authentication exhibits multiple gaps, particularly during indoor passages and strongly obstructed segments of the pedestrian trajectory. These results illustrate the sensitivity of OSNMA authentication to symbol losses under scalar tracking.

Scalar Tracking with Pilot-Assisted Symbol Detector

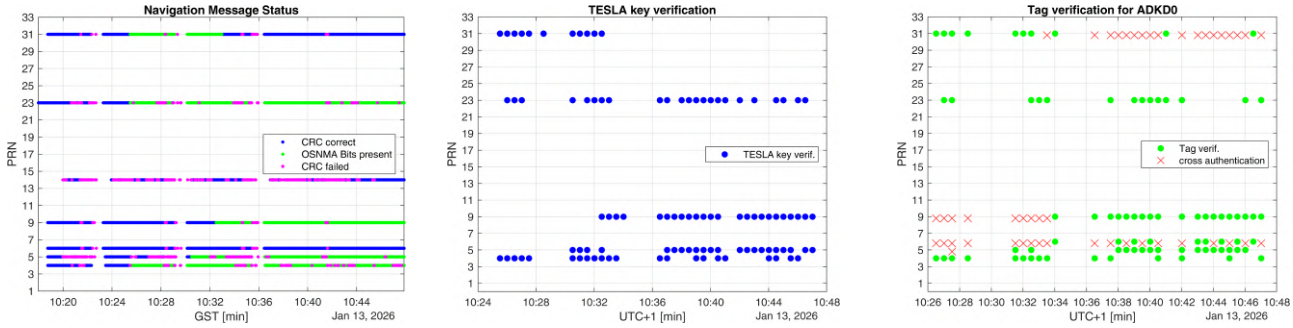


(a) Navigation Message Status **(b)** TESLA Key Verification **(c)** ADKD 0 Authentication

Figure 8: OSNMA authentication results under scalar tracking with pilot-assisted symbol detector.

Applying the pilot-assisted symbol detector significantly improves OSNMA authentication continuity. As shown in Figure 8, navigation message availability becomes more stable, enabling more reliable TESLA key verification. Consequently, ADKD 0 tag authentication exhibits fewer interruptions compared to conventional scalar tracking. This confirms that improved symbol detection robustness directly translates into increased OSNMA authentication availability.

Vector Tracking (VT)



(a) Navigation Message Status **(b)** TESLA Key Verification **(c)** ADKD 0 Authentication

Figure 9: OSNMA authentication results under vector tracking (VT).

Under vector tracking, OSNMA authentication continuity reaches its highest level. As shown in Figure 9, navigation message availability and TESLA key verification are significantly more stable than in the scalar tracking configurations. This directly results in more-continuous ADKD 0 authentication across the trajectory. The improved robustness stems from the ability of vector tracking to bridge short signal degradations and to maintain symbol availability through the pilot-assisted symbol detector. Overall, vector tracking provides the most favourable conditions for OSNMA authentication and establishes a robust basis for subsequent SAS processing.

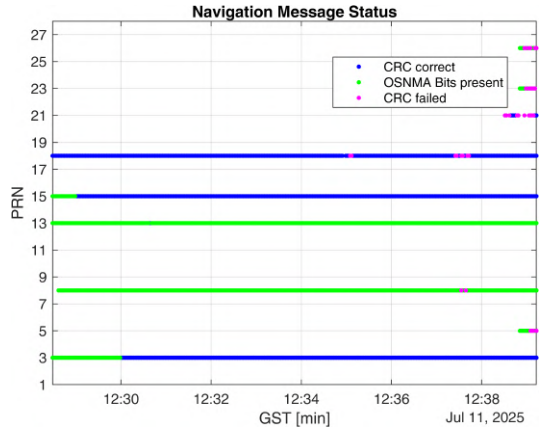
4. OSNMA Authentication Results for Automotive Dataset

The OSNMA analysis is extended to the automotive dataset from the VorTNAF project using the same processing chain as for the pedestrian case described in Section V.3. The same conditions, ADKD 0 configuration, and pilot-assisted symbol detector are used for all receiver configurations.

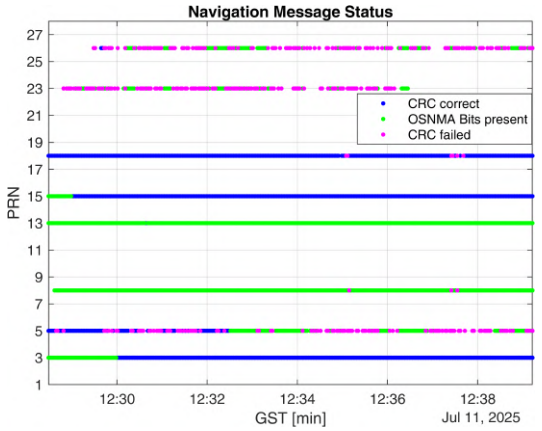
The automotive dataset represents a road-driving scenario in a light urban environment. In contrast to the pedestrian measurements, no strong indoor passages or tunnel-like obstructions are present. Signal conditions are therefore generally more stable, with only moderate variations caused by surrounding buildings or roadside infrastructure. Under such conditions, large differences between scalar tracking (ST) and vector tracking (VT) are not necessarily expected.

The results are presented for warm-start and hot-start conditions. For each start condition, ST and VT are compared. Since both configurations use the same pilot-assisted symbol detector, the comparison mainly reflects differences related to the tracking architecture rather than to symbol processing.

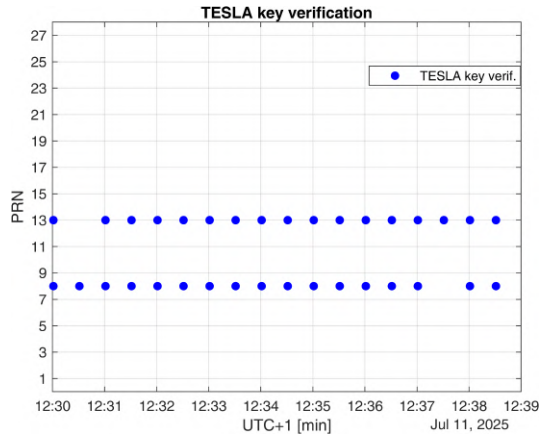
Warm Start: ST vs. VT (E1-C Symbol Detector)



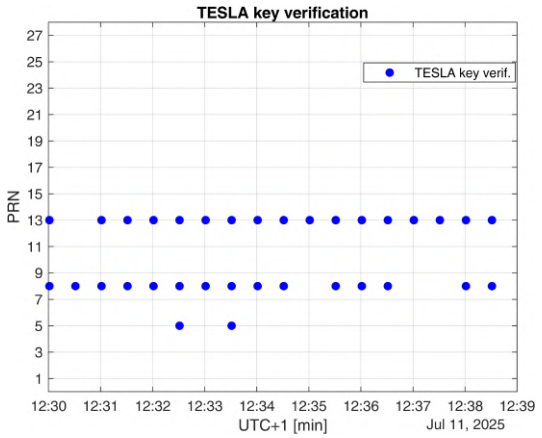
(a) ST: Navigation Message Status



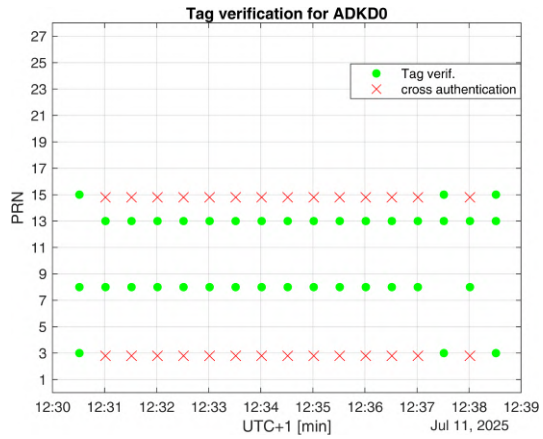
(b) VT: Navigation Message Status



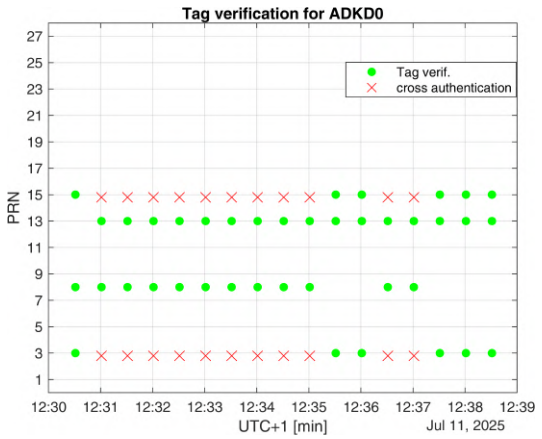
(c) ST: TESLA Key Verification



(d) VT: TESLA Key Verification



(e) ST: ADKD 0 Authentication



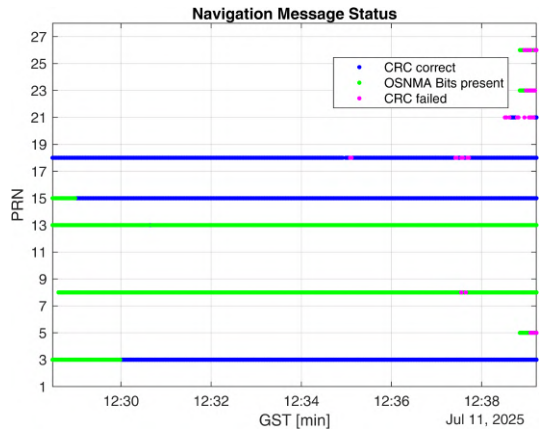
(f) VT: ADKD 0 Authentication

Figure 10: Automotive OSNMA results with warm start: comparison of ST and VT (both using pilot-assisted symbol detector).

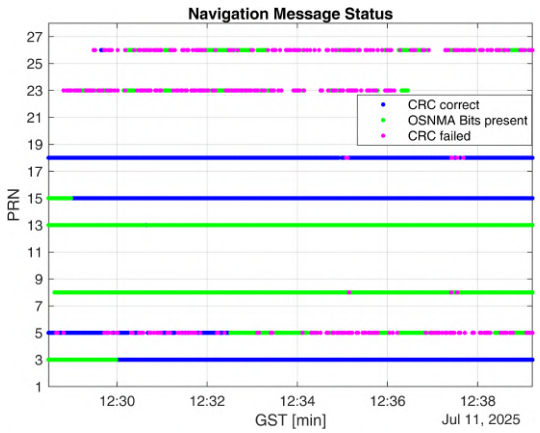
Figure 10 shows the OSNMA authentication results for the automotive dataset under warm-start conditions. In this case, authentication becomes available only after the required OSNMA root information has been received. Due to the generally stable signal conditions along the route, OSNMA authentication is possible for most of the trajectory for both ST and VT.

From the figures, no clear overall advantage of VT over ST can be identified. For some satellites, VT provides more authenticated navigation data, while for others ST performs slightly better. A more detailed inspection indicates that VT tends to produce a higher number of self-authenticated tags and more verified TESLA keys, whereas ST results in a higher number of cross-authenticated tags. This mixed behaviour reflects the stable reception conditions and applies to the warm-start case.

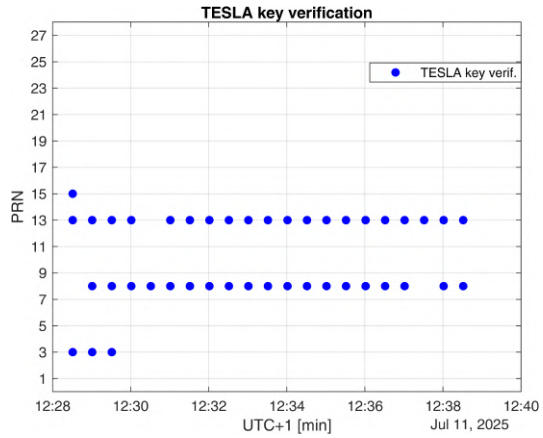
Hot Start: ST vs. VT (E1-C Symbol Detector)



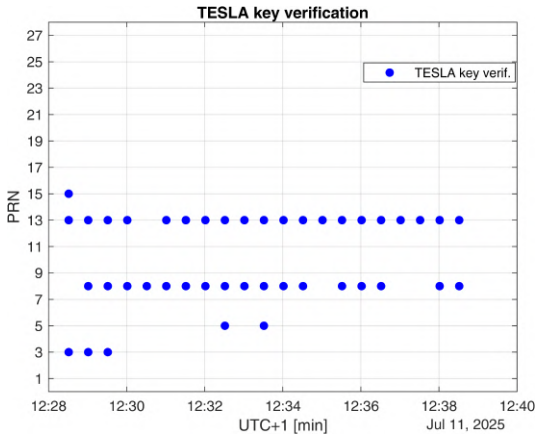
(a) ST: Navigation Message Status



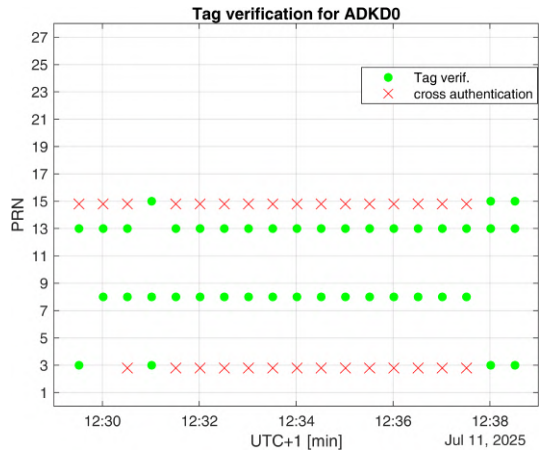
(b) VT: Navigation Message Status



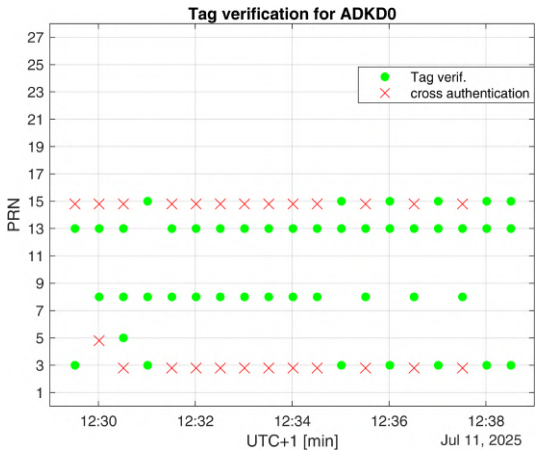
(c) ST: TESLA Key Verification



(d) VT: TESLA Key Verification



(e) ST: ADKD 0 Authentication



(f) VT: ADKD 0 Authentication

Figure 11: Automotive OSNMA results with hot start: comparison of ST and VT (both using pilot-assisted symbol detector).

Figure 11 shows the automotive OSNMA results under hot-start conditions. As expected, authentication starts earlier and is more continuous than in the warm-start case, due to the immediate availability of the TESLA root key information. However, similar to the warm-start results, the difference between ST and VT remains small.

Again, VT shows slightly more self-authenticated navigation data and TESLA key verifications, while ST exhibits a higher number of cross-authenticated tags for some satellites. This behaviour is consistent across both warm and hot starts and indicates that, in light urban driving scenarios with generally stable signal reception, the impact of the tracking architecture on OSNMA authentication availability is limited.

Overall, the automotive OSNMA results suggest that both scalar and vector tracking can provide reliable ADKD 0 authentication in typical vehicular environments. A more detailed evaluation using additional datasets and longer driving scenarios is required to fully assess the relative benefits of ST and VT for OSNMA in automotive applications.

5. SAS Range Authentication

The Galileo Signal Authentication Service (SAS) is designed to provide cryptographic protection of ranging measurements using the E6-C signal. In this study, the pedestrian dataset is evaluated using a replica-based SAS approach, where locally generated E6-C spreading code replicas are used instead of encrypted code sequences. This allows the assessment of snapshot-based correlation performance and authentication availability independently of cryptographic key disclosure.

Authentication is performed by correlating True Baseband snapshots of the E6-C signal with locally generated replicas (Figure 12). In the pedestrian experiment, snapshots are recorded at regular intervals when the receiver maintains the required tracking condition, and they are synchronised via the E1B tracking loop. The correlation function is evaluated in its real, imaginary, and absolute components, with the absolute value used to identify the presence of a valid correlation peak.

For the present analysis, a coherent integration time of 20 ms is applied. A snapshot is considered *authenticated* if two conditions are satisfied:

1. the carrier-to-noise density ratio C/N_0 exceeds 33 dB-Hz, and
2. the correlation peak lies within ± 1 chip of the expected code phase.

In the graphical representation, the correlation function is plotted as a function of code-phase offset relative to the expected E6-C replica. The E1BC pseudorange is represented by an arrow extending from the origin to the location of the correlation maximum, while the highlighted region around the detected peak corresponds to the SAS-authenticated E6-C range. This representation illustrates the principle of SAS range authentication, where a conventional E1BC pseudorange is supported by additional correlation evidence from the E6-C signal.

The same correlation-based principle applies to encrypted SAS operation once encrypted E6-C signals and the corresponding decrypted RECS are available. In that case, the locally generated replica are replaced by the decrypted Re-encrypted code spreading sequences, while the correlation and decision logic remain unchanged.

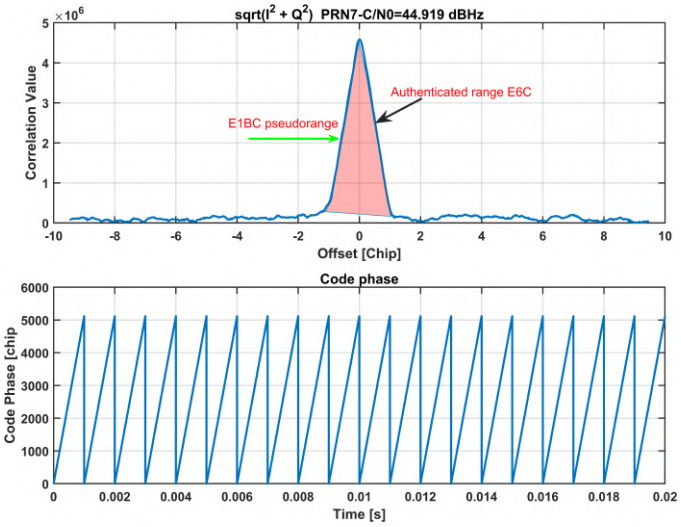


Figure 12: Galileo SAS range authentication: the E1BC pseudorange (arrow) and the authenticated E6C range (highlighted correlation peak).

6. SAS Results

This subsection presents the results of snapshot-based spreading code authentication using replica correlation on open E6-C data. The aim of this analysis is to study the influence of the tracking architecture on snapshot availability and on the continuity of SAS authentication in a pedestrian scenario. In contrast to the encrypted SAS validation presented in Section V.2, the results shown here are based on replica-generated E6-C signals and do not include the operational latency related to delayed TESLA key disclosure.

E6-C snapshots are generated in TBB format when the receiver maintains the required master tracking condition. In practice, this leads to snapshots being recorded approximately once per second during periods of stable tracking. This snapshot interval is a consequence of the logging configuration and should not be interpreted as an inherent SAS authentication rate.

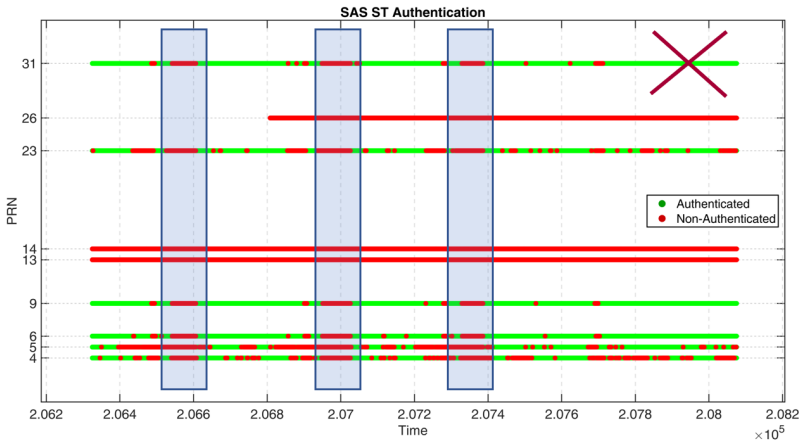


Figure 13: Replica-based SAS snapshot authentication results under scalar tracking (ST) for the pedestrian dataset. The three transparent boxes indicate the approximate time intervals corresponding to the three indoor crossings of the university library.

Figure 13 shows the SAS snapshot authentication results for scalar tracking. During open-sky parts of the pedestrian route, authentication is mostly continuous for several satellites. Inside the three highlighted intervals, corresponding to the library crossings, authentication becomes intermittent or unavailable. These interruptions are caused by strong signal attenuation and multipath, which reduce correlation peak strength and may also lead to missing snapshots when tracking is lost.

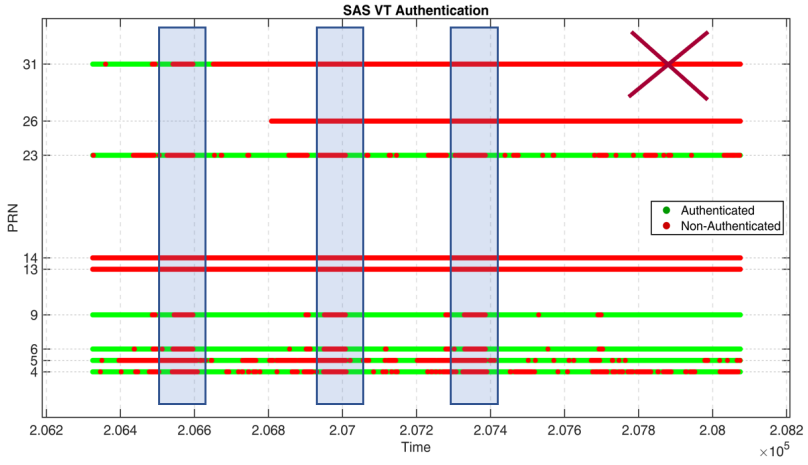


Figure 14: Replica-based SAS snapshot authentication results under vector tracking (VT) for the pedestrian dataset. The three transparent boxes indicate the same library crossings as in Figure 13.

The corresponding results for vector tracking are shown in Figure 14. Compared to scalar tracking, vector tracking provides more continuous authenticated snapshot sequences, including during the highlighted indoor segments. Although authentication

gaps still occur inside the library, vector tracking usually maintains authentication for a longer time and recovers faster after leaving the obstructed area. This behaviour is consistent with the ability of vector tracking to bridge short signal degradations by using joint processing of multiple satellites.

A quantitative comparison of the replica-based SAS authentication availability is shown in Table 2. The availability represents the fraction of recorded snapshots that satisfy the correlation-based authentication criteria. Overall, vector tracking shows a slightly higher availability than scalar tracking. However, one satellite (PRN 31) exhibits reduced availability in the vector tracking case. This issue is analysed in more detail in Section V.7.

Table 2: Comparison of replica-based SAS snapshot authentication availability for scalar tracking (ST) and vector tracking (VT) in the pedestrian experiment.

PRN	**4**	**5**	**6**	**9**	**23**	**All**
Auth score ST (%)	70.817	61.850	85.837	86.693	72.930	75.625
Auth score VT (%)	73.044	62.707	87.436	88.407	74.571	77.233

To further illustrate the difference between tracking modes, Figure 15 shows a zoomed view of the SAS authentication results for PRN 9 during one of the library crossings. Under scalar tracking, authenticated snapshots are sporadic, while vector tracking maintains more continuous authentication over the same time interval.

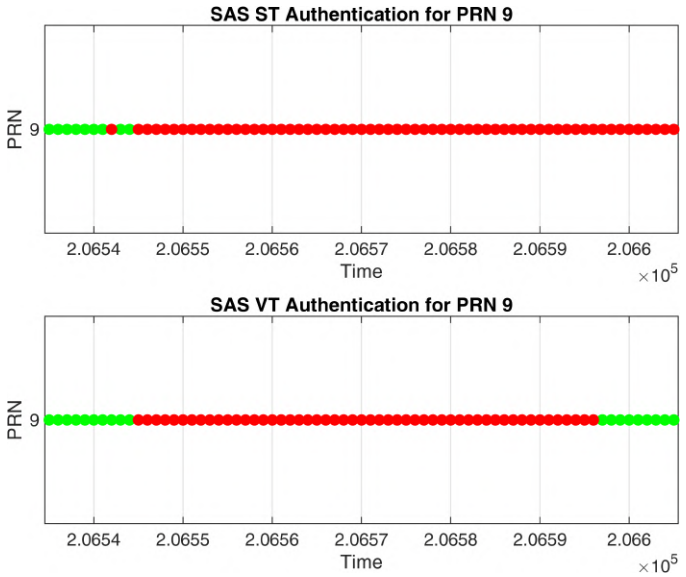


Figure 15: Zoomed replica-based SAS snapshot authentication results for PRN 9 during an indoor library crossing.

In summary, the replica-based SAS results show that snapshot-based correlation provides dense authentication evidence along the pedestrian trajectory, with a time resolution determined by the snapshot logging process. The results indicate that vector tracking can slightly improve the continuity of SAS authentication in challenging environments by helping to maintain snapshot availability and correlation peak detectability. These observations are consistent with the OSNMA findings and suggest that robust tracking architectures can support SAS processing under degraded signal conditions.

7. Closer Look at the PRN 31 Master-Slave Channel Issue

This subsection provides a closer look into the master-slave channel issue observed for PRN 31 in the VT processing chain. As described in Section V.6, the E6-C snapshot recording is triggered in slave mode and depends on the E1 tracking state (master). Therefore, for a correct master-slave behaviour, the E6 range-rate control should follow the E1 range-rate control.

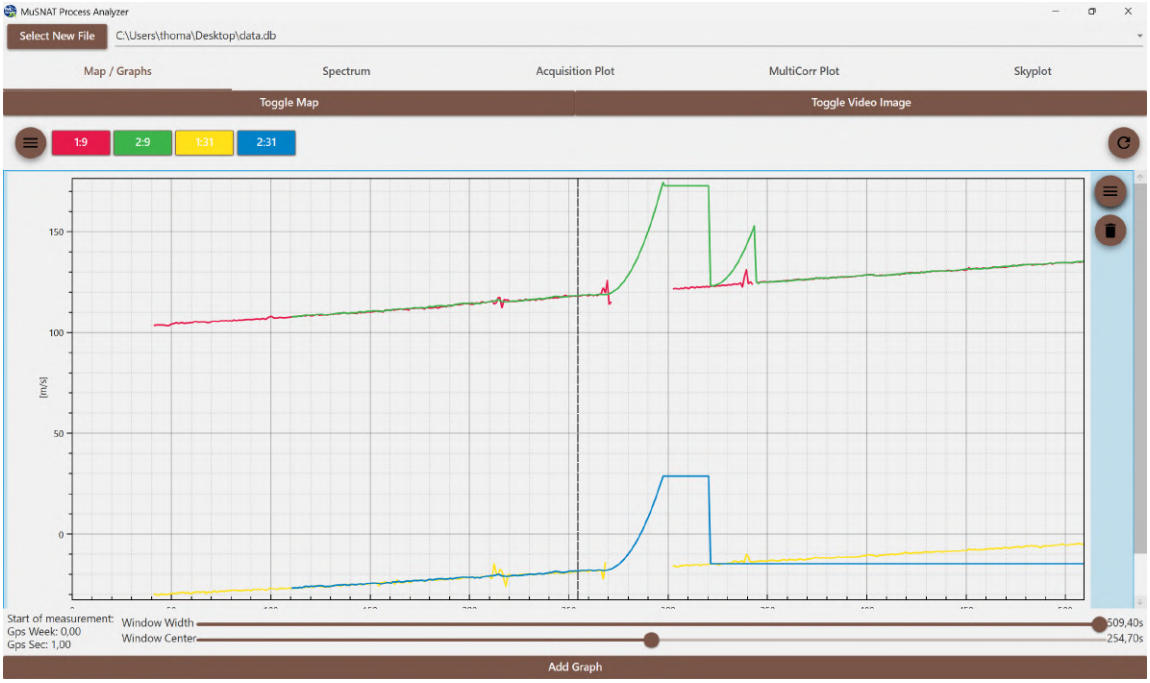


Figure 16: MuSNAT Process Analyzer view of range-rate behaviour for E1 and E6 channels for two satellites. Top: PRN 9 (green/red). Bottom: PRN 31 (blue/yellow).

Figure 16 shows the range-rate NCO behaviour for the E1 and E6 channels for two satellites within a single figure. The upper part of the figure corresponds to PRN 9 and shows two curves (green and red) representing the E1 and E6 range-rate estimates. In this case, the E6 range rate closely follows the E1 range rate, as expected in a correct master-slave configuration. This indicates that the E6 channel is properly updated based on the E1 tracking information.

The lower part of the same figure corresponds to PRN 31 and shows two curves (blue and yellow) for the E1 and E6 range-rate estimates. Here, a different behaviour can be observed. After some time, the E6-C range rate becomes nearly constant and no longer follows the E1 range rate. This indicates that the master-slave mechanism does not operate correctly for PRN 31, and the E6 channel is not properly updated from the E1 channel.

A possible reason is related to receiver implementation aspects. Signal tracking is done in different threads, and receiver mechanisms like vector tracking and master-slave operation require inter-thread communication with NCO buffering. Due to some mis-synchronisation, the slave channel was likely not able to find the correct NCO values of the master channel for PRN 31. This can explain why the E6 range rate stops following E1, and why PRN 31 shows reduced SAS availability in the VT case.

8. OSNMA Authentication Mapping on Google Earth

Figure 17–20 show the OSNMA authentication results mapped along the pedestrian trajectory using Google Earth. Each plot indicates the number of PRNs providing authenticated navigation data at the same time instant. The colour coding represents the number of simultaneously authenticated satellites, as indicated by the legend shown in the bottom-right corner of each figure.

The four maps correspond to scalar tracking (ST) and vector tracking (VT) under warm-start and hot-start conditions. This representation allows a direct comparison of authentication availability along the trajectory and highlights the influence of receiver start conditions and tracking architecture.



Figure 17: OSNMA authentication mapping for scalar tracking (ST) with warm start.

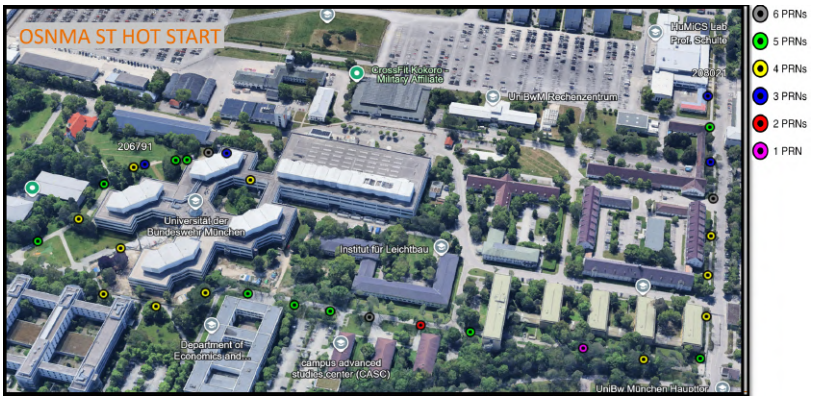


Figure 18: OSNMA authentication mapping for scalar tracking (ST) with hot start.

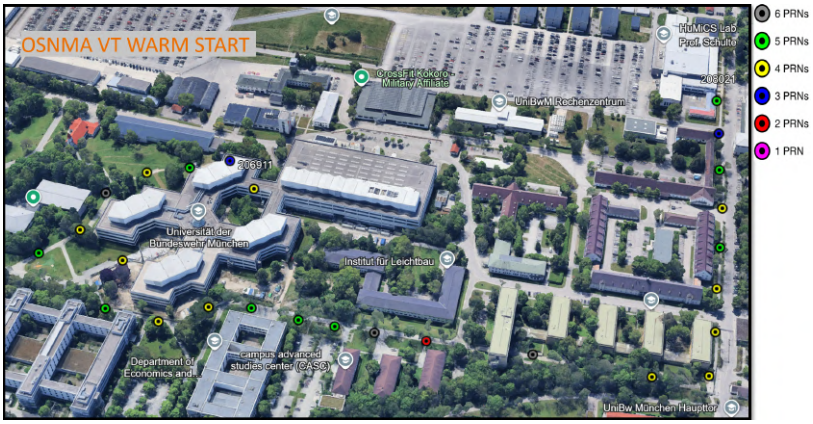


Figure 19: OSNMA authentication mapping for vector tracking (VT) with warm start.

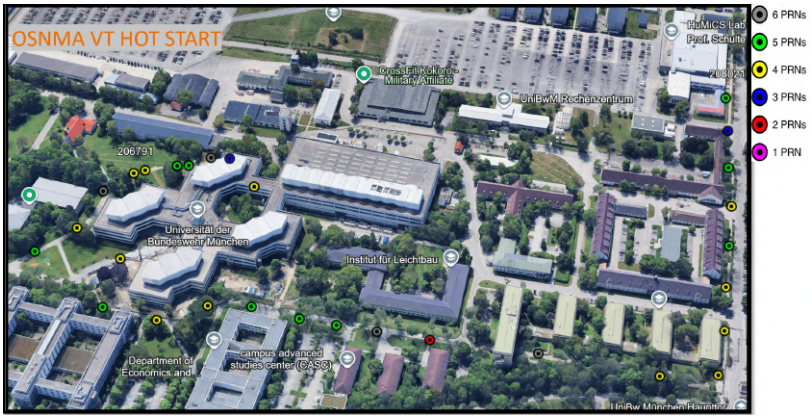


Figure 20: OSNMA authentication mapping for vector tracking (VT) with hot start.

The results show that hot-start operation provides better OSNMA authentication availability than warm start. In the hot-start cases, more PRNs are authenticated at the same time, and fewer gaps are visible along the trajectory.

Vector tracking further improves authentication continuity compared to scalar tracking. This improvement is especially visible in the hot-start case, where vector tracking achieves the best overall performance. In this configuration, several PRNs are authenticated simultaneously over most parts of the trajectory, and the system shows higher robustness against signal blockages and short signal interruptions.

9. SAS Authentication Mapping on Google Earth

Figure 21 and Figure 22 show the SAS authentication results mapped along the pedestrian trajectory using Google Earth. The two figures correspond to scalar tracking and vector tracking, respectively. The colours indicate the number of PRNs authenticated simultaneously at the same position, as shown by the legend in the bottom-right corner of each plot.

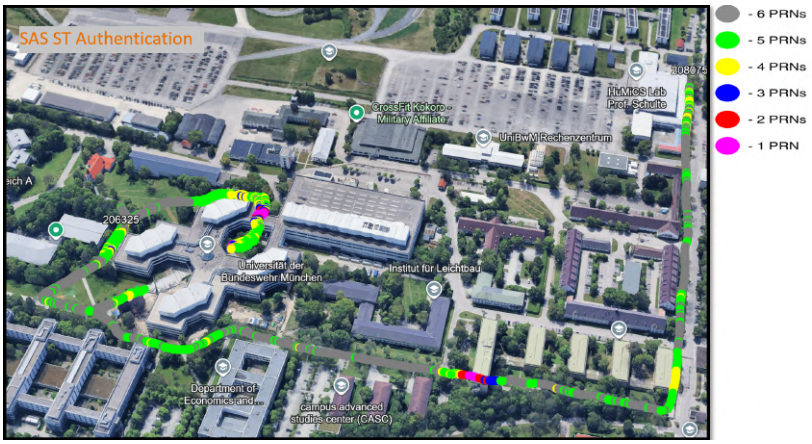


Figure 21: SAS authentication mapping for scalar tracking (ST).

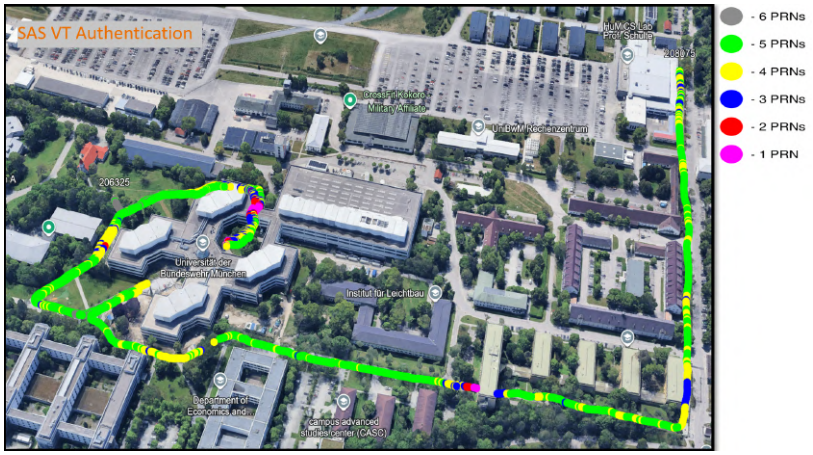


Figure 22: SAS authentication mapping for vector tracking (VT).

Compared to OSNMA authentication mapping, SAS shows significantly higher spatial continuity along the pedestrian trajectory. This is because SAS authentication is based on snapshot correlation, which provides frequent authentication evidence whenever valid E6-C snapshots are available. As a result, authentication gaps are shorter and less frequent, even in challenging environments.

When comparing scalar tracking and vector tracking, different aspects can be observed. With vector tracking, the SAS authentication availability is more continuous along the trajectory, especially after leaving obstructed areas such as the indoor library passages. This behaviour is consistent with the temporal SAS results and reflects the improved snapshot availability and correlation robustness provided by vector tracking.

However, when considering the number of PRNs authenticated at the same time, scalar tracking shows a slightly higher maximum availability. In the scalar tracking case, up to six PRNs are authenticated simultaneously over several parts of the trajectory, whereas vector tracking typically reaches a maximum of five PRNs. This difference is mainly caused by the reduced availability of PRN 31 in the vector tracking configuration. The underlying reason for this behaviour is analysed in detail in Section V.7.

Overall, the SAS authentication mapping confirms that vector tracking improves the continuity of SAS authentication, while scalar tracking may achieve a higher number of simultaneously authenticated PRNs in specific situations. These results highlight the importance of considering both authentication continuity and multi-satellite availability when evaluating SAS performance under different tracking architectures.

VI. CONCLUSION

This paper extends our previous study on Galileo authentication availability under scalar and vector tracking by validating the SAS processing chain with encrypted E6-C snapshot data and by analysing pedestrian and automotive field-test scenarios. The work combines OSNMA navigation message authentication based on Authentication Data and Key Distribution type 0 (ADKD 0) with snapshot-based SAS spreading-code authentication and evaluates their behaviour under different receiver configurations.

For OSNMA, the pedestrian results show that authentication continuity depends strongly on sustained navigation message availability and TESLA key verification. Introducing the pilot-assisted symbol detector improves symbol robustness compared to conventional PLL-based demodulation and increases the continuity of ADKD 0 authentication. Building on this improved symbol availability, vector tracking provides the most continuous OSNMA performance along the pedestrian trajectory, as evidenced by the temporal results and the Google Earth mapping.

For SAS, two complementary aspects were investigated. First, encrypted E6-C snapshot data were used to validate the complete SAS processing chain, including TESLA key handling, RECS decryption, and correlation-based spreading-code authentication for KDI = 0 and KDI = 1. Second, replica-based snapshot authentication was applied to the pedestrian dataset to quantify availability under realistic propagation conditions. With the applied decision criteria ($C/N_0 > 33$ dB-Hz and peak location within ± 1 chip), vector tracking yields a higher overall SAS snapshot authentication availability than scalar tracking (77.23% vs. 75.63% over PRNs 4, 5, 6, 9, and 23). For the individual PRNs, the VT gain ranges from about +0.86 to +2.23 percentage points.At the same time, scalar tracking can yield a higher number of simultaneously authenticated PRNs in specific intervals. This effect is mainly caused by a receiver implementation issue observed for PRN 31 in the vector tracking case, related to the master-slave interaction between the E1 and E6 channels, and not to a limitation of the SAS concept itself.

In addition to the pedestrian analysis, an automotive dataset was evaluated to assess OSNMA performance in a vehicular environment. Under the tested driving conditions, OSNMA authentication is generally stable for both scalar tracking and vectgor tracking, and the difference between warm-start and hot-start operation is comparatively small, reflecting the absence of severe indoor or tunnel-like obstructions in the route.

Overall, the results confirm that encrypted snapshot validation of SAS is feasible when the required cryptographic material is available, and robust tracking and symbol processing directly translate into improved authentication continuity. Future work will focus on real-time processing of live encrypted SAS signals and on extending SAS performance evaluations to automotive scenarios once suitable encrypted datasets and processing configurations become available.

ACKNOWLEDGEMENTS

The results presented in this work were developed within the project *GalileoFUSION-II*, funded by the German Federal Ministry for Economic Affairs and Climate Action (BMWK) and administered by the Project Management Agency for Aeronautics Research of the German Aerospace Agency (DLR) in Bonn, Germany (grant no. 50NA2301).

The encrypted SAS snapshot dataset used for validation was provided through collaboration with the European Commission and the Universitat Autònoma de Barcelona (UAB). The authors gratefully acknowledge their support and the provision of re-encrypted code sequences, TESLA keys, and synchronised snapshot data.

The vehicular GNSS dataset used in this study was collected within the framework of the VorTNAF project and was provided by Industrieanlagen-Betriebsgesellschaft mbH (IABG). The VorTNAF project is co-funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) through the German Aerospace Agency (DLR) under grant FKZ 50NA2307. The authors thank IABG for making the automotive measurement data available.

REFERENCES

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. *ION Proceeding*, page 23.

European Union Agency for the Space Programme (EUSPA) (2023). Galileo Open Service Signal-In-Space Interface Control Document (OS SIS ICD). Technical Report Issue 2.1, European Union Agency for the Space Programme (EUSPA), Prague, Czech Republic. November 2023.

European Union Agency for the Space Programme (EUSPA) (2025). OSNMA Service Definition Document (OSNMA-SDD), v1.0. Technical report, EUSPA. Version 1.0.

Fernandez-Hernandez, I., Cancela, S., Terris-Gallego, R., López-Salcedo, J. A., Seco-Granados, G., O'Driscoll, C., Winkel, J., Dalla Chiara, A., Sarto, C., Rijmen, V., Blonski, D., and de Blas, J. (2022). Semi-Assisted Signal Authentication Based on Galileo ACAS. *arXiv preprint arXiv:2204.14026*.

Fernandez-Hernandez, I., Winkel, J., O'Driscoll, C., Caparra, G., Terris-Gallego, R., López-Salcedo, J. A., Seco-Granados, G., Willems, T., 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.

Gunawardena, S., Pany, T., and Curran, J. (2021). ION GNSS software-defined radio metadata standard. *NAVIGATION: Journal of the Institute of Navigation*, 68(1):11–20.

Margaria, D., Motella, B., Anghileri, M., Floch, J.-J., Fernandez-Hernandez, I., and Paonni, M. (2017). Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives. *Proceedings of the IEEE*, 105(6):1167–1188.

Seco-Granados, G., Gómez-Casco, D., López-Salcedo, J. A., and Fernandez-Hernandez, I. (2021). Detection of Replay Attacks to GNSS Based on Partial Correlations and Authentication Data Unpredictability. *GPS Solutions*, 25(33).

Spilker Jr., J. J., Parkinson, S. U. J. S. B., and Parkinson, B. W. (1996). *Global Positioning System: Theory and Applications, Volume II*. AIAA.

Terris-Gallego, R., López-Salcedo, J. A., Seco-Granados, G., Galan-Figueras, A., and Fernandez-Hernandez, I. (2025). Testing Galileo SAS with Encrypted Signal-In-Space. In *Proceedings of the International Technical Meeting of the Institute of Navigation (ION GNSS+ 2025)*.

Winkel, J., Fernandez-Hernandez, I., and O'Driscoll, C. (2023). Implementation Considerations for ACAS and Simulation Results. *arXiv preprint arXiv:2307.12398*.