Article

Securing GNSS signals: a software solution for Galileo signal authentication

Miguel A. Ramírez *,‡, Adrián Chamorro †,‡,Simón Cancela ‡ and David Calle ‡

Algorithms, Products and Services department, GMV, Isaac Newton 11, 28760 Tres Cantos, Madrid, Spain; achamorro@gmv.com (A.C.);scancela@gmv.com (S.C.);jdcalle@gmv.com (D.C.)

* Correspondence: marn@gmv.com (M.R.)

† Presented at the European Navigation Conference 2023, Noordwijk, The Netherlands, 22-24 May 2024

‡ These authors contributed equally to this work.

Abstract: The Galileo program is adding a layer of security through the Galileo Assisted Commercial Authentication Service (ACAS). This service complements the Galileo Open Service Navigation Message Authentication (OSNMA) by introducing signal authentication through Commercial Service signals. In this framework, the ACAS employs a unique approach to protect pseudoranges by incorporating authentication features. These features are implemented at the spreading-code level, utilizing spreading code encryption on the signal to perform Spreading Code Authentication. The service is based on the re-encryption and publication of short-duration spreading sequences from an existing encrypted signal, such as the Galileo E6C signal. The re-encryption process enables the receiver to autonomously retrieve the required sequences without continuous communication with an external server. This paper details a commercial software solution implementing the ACAS service, designed for integration across a wide array of applications. A comprehensive solution description of the ACAS software solution, testing in nominal scenarios will be presented, leading to conclusions that assess the software solution's performance, capabilities in real scenarios, and suggestions for further improvements.

Keywords: Global Navigation Satellite System (GNSS);Galileo;Assisted Commercial Authentication Service (ACAS);Open Service Navigation Message Authentication (OSNMA);

Citation: Ramirez, M.A.; Chamorro, A.; Cancela, S.; Calle, D. Securing GNSS signals: a software solution for Galileo signal authentication.

1. Introduction

In our daily lives, GNSS have become a fundamental technology for the global infrastructure, supporting a wide range of applications in various sectors including transport, telecommunications and emergency services. In this area, the reliability and accuracy of GNSS signals are vital not only for navigation, but also for applications requiring temporal accuracy such as financial transactions and network management. As this technological dependence grows, so does the need to ensure the security and integrity of the signals. This aspect of GNSS technology is becoming increasingly important as potential vulnerabilities could lead to service disruptions that have economic repercussions or threaten public safety.

The objective of this paper is to address this need for securing GNSS signals by means of a robust software solution based specifically on the authentication of Galileo E1 and E6 signals that already have resources for this purpose. With this approach, the ACAS protocol has been analysed, a system that represents a significant advance in the security of GNSS signals by contributing to improve the security measures of GNSS systems by integrating authentication directly into the signal without altering the infrastructure or the signal plan.

The proposed software solution leverages the capabilities of the ACAS service to perform signal-level authentication, mitigating the risk of spoofing and jamming attacks. This solution includes advanced cryptographic techniques necessary for the use of the

service, real-time signal integrity monitoring and integration capability with existing GNSS infrastructure.

Through the following sections, this document will delve into the technical fundamentals of GNSS security, provide a detailed description of ACAS and discuss the development and integration of the software solution, ending with the results obtained in a controlled test scenario defined specifically for this purpose.

2. Overview of GNSS Security

It is crucial to understand that this global dependence also exposes GNSS systems to multiple security vulnerabilities. Threats range from deliberate jamming to more sophisticated manipulations of signals, each with the potential to cause significant disruptions. The main ones are:

- Jamming: This involves the intentional disruption of GNSS signals through interference, which can be executed even with low-power devices, leading to significant outages or loss of signal integrity.
- Meaconing: Type of interference attack on navigation systems. It involves maliciously re-radiating or repeating GNSS signals to deceive receivers, leading to incorrect position estimates or time estimation.
- Spoofing: Attacks that generate false signals to mislead GNSS receivers about their position or real time. These attacks can divert users from their route or manipulate systems that rely on precise timing. There are two main types of attacks:
  - Data-Level Spoofing: This type of attack involves the manipulation of the data transmitted by GNSS satellites. Attackers alter navigation data such as satellite positions or time, which can lead to errors in how GNSS receivers determine position or time.
  - Signal-level Spoofing: Unlike data spoofing, signal-level spoofing involves the creation and transmission of fake GNSS signals. This attack does not require the alteration of the actual data contained in the GNSS signal, but focuses on mimicking the signal transmitted by the satellites. Receivers receiving these fake signals can generate erroneous measurements that affect the position or timing of the device.

2.1. Signal and data authentication with OSNMA

The Galileo program already has a Navigation Message Authentication Service (OSNMA) [3]. This service offers a layer of security by providing authentication of navigation data broadcast by Galileo satellites. Through the use of cryptographic keys, OSNMA allows GNSS receivers to verify the integrity and origin of navigation data. However, OSNMA does not directly address signal-level spoofing, where the integrity of the signal itself is compromised. For this type of threat, additional detection and mitigation techniques are required to ensure the authenticity of the received signals. The implementation of the ACAS service complements the OSNMA by allowing the detection of attacks that directly interfere with the integrity of the signal, providing a more complete security to the Galileo system service.

3. Galileo Assisted Commercial Authentication Service (ACAS)

The ACAS is based on the total or partial spreading code authentication that is the most effective way to authenticate GNSS signals and measurements [1]. The satellite transmits an encrypted spreading code and NMA using the actual signal plan, satellite payload or key management. In this case, the scheme on which this service is based is semi-assisted authentication, i.e. the service provider, which for Galileo is the GSC, provides the encrypted code sequences, from now on called ECS, by re-encrypting these code sequences (RECS) using the Timed Efficient Stream Loss-tolerant Authentication (TESLA) key provided by the OSNMA protocol in the E1-B signal. The user records a snapshot of the E6C signal and once the OSNMA key is received by the I/NAV, RECS

are decrypted obtaining the ECS which correlates with the pre-recorded signal and if it is successful, it calculates the E6C pseudoranges together with the I/NAV authenticated data.

3.1. Service provider side

The keystream that is going to be transmitted by the satellites is generated by encrypting the spreading codes while maintaining the bandwidth of the data as established in the Galileo signal plan [2]. From this keystream, certain sequences are selected that are re-encrypted with the NMA keys $K_j, K_{j+1}, ...$, respectively. These will be transmitted via the OSNMA service such that the key used to encode each sequence is only obtained after the signal with the sequences encrypted with that key has been transmitted.

The RECS files are generated for each satellite for a specific operation time, for a certain number of chips in the sequence, denoted $N_{c,RECS}$, and a distance between sequences defined as the RECS period, denoted τ_{RECS}.

Additionally, the server provides the Bias Group Delay (BGD) files with the purpose of correcting the measurement in relation to the measurements obtained when processing the E1.

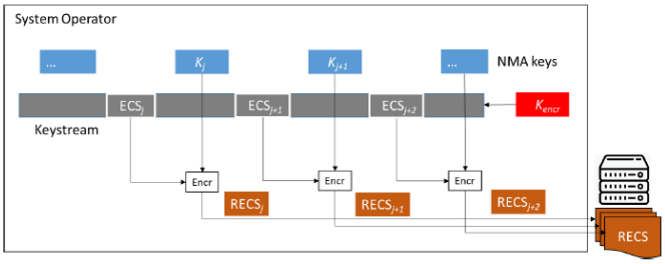

Figure 1. System Operator process [1]

3.2. User Side

To use the ACAS, the receiver must have the ability to record and store snapshots of the signal to perform the correlation which will be done after decrypting the RECS with the corresponding TESLA key. Normally, the RECS to be used during the operation time are pre-downloaded so that they are already available to the receiver. Once the receiver is synchronized with the satellite signal, snapshots are recorded and tagged with the corresponding epoch, and the RECS for that period are used. To perform the correlation, the RECS are first decrypted with the key corresponding to the subframe in which the signal was recorded, and with the ECS the signal is correlated, as shown in figure 2.

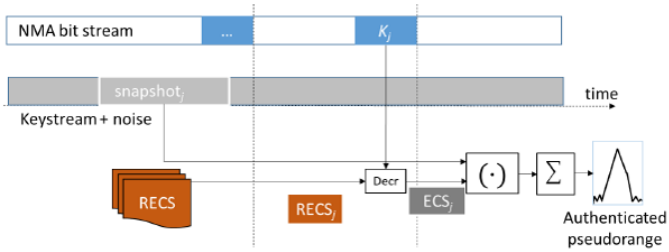

Figure 2. High level ACAS Receiver operation [1]

4. ACAS Solution Implementation

This section will focus on the implementation of the ACAS and the considerations that must be taken into account to obtain the metrics properly.

The high-level design of the software is depicted in figure 3, composed mainly of four modules. On one hand, the E1B and E1C measurements are commonly processed through acquisition and tracking processes. From this module, reference measurements of the E1C are generated, and authenticated navigation data is obtained using the OSNMA protocol, providing this key to the main execution line of the ACAS. The RECS are an input to the

Decryption module, obtained from the service provider, in this case, the European GNSS Service Center (GSC). The decryption process will be detailed in this section. Once the ECS is obtained, it is correlated with the recorded snapshot of the E6C, and along with the BGD also obtained from the GSC server, the authenticated solution is computed.

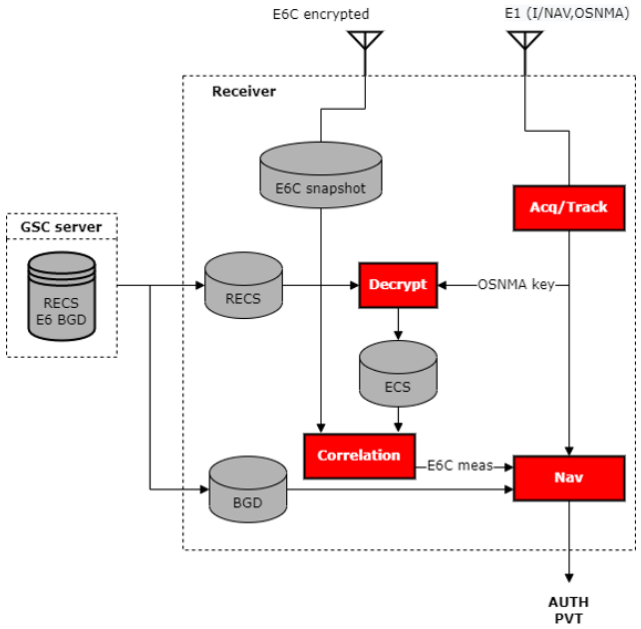

Figure 3. High level ACAS Module Design

4.1. RECS Decryption Process

The decryption key for the RECS is derived from the OSNMA key using the SHA-256 hash function. This ensures that the decryption key is only available once the corresponding OSNMA key is disclosed, maintaining security and integrity:

$$K'_j = \text{SHA256}(K_j) \tag{1}$$

where K_j represents the OSNMA key for block j.

The decryption of RECS is performed using AES in CBC mode, which requires an initialization vector (IV) and the RECS decryption key defined above:

$$\text{ECS}_{j,i} = \text{AES256}^{-1}_{\text{CBC}}(K'_{j+\text{SLRECS}}, \text{RECS}_{j,i}, \text{IV}) \tag{2}$$

This formula represents the decryption of the RECS into the original ECS, where IV is appropriately generated to ensure secure decryption.

4.1.1. RECS Time Randomization

To prevent predictable patterns in the placement of RECS within the signal, the start times of RECS are randomized within the bounds of $\Delta\tau_{\text{MAX}}$. This randomization is crucial for enhancing security against pattern analysis and replay attacks:

$$\Delta\tau_i^k = B_i^k \mod (\Delta\tau_{\text{MAX}} + 1) \tag{3}$$

where B_i^k is a byte derived from a cipher block generated by AES in OFB mode. The index k specifies the satellite within a RECS period, ensuring that each satellite's RECS timing is independently randomized.

4.2. Correlation process

Due to hardware limitations related to the capacity and bandwidth for snapshot recording, continuous recording would require more extensive memory management. To

optimize this process, various parameters are considered to determine the start and end times of the snapshot recording for subsequent correlation with the ECS generated by the process in the previous section. This section will detail how the acquisition of the encrypted signal is computed.

4.2.1. Snapshot definition

The synchronization and correlation of the ECS with the signal snapshot are critical for verifying the authenticity of the received signal. This process adjusts the start time of the snapshot based on prior synchronization with the E1 signal and incorporates the random delay introduced. This adjustment ensures that the snapshot includes the entire ECS, allowing the authentication.

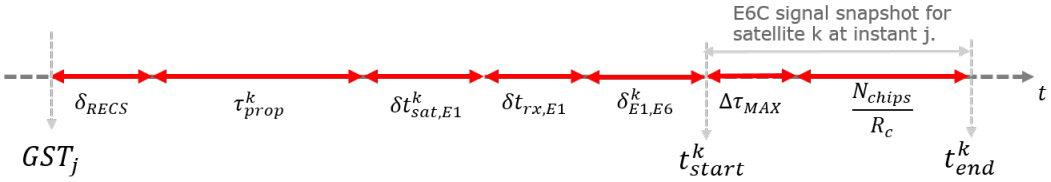

Figure 4. E6C Snapshot definition

$$t^k_{\text{start},j} = \text{GST}_j + \delta_{\text{RECS}} + \tau^k_{\text{prop}} - \delta t^k_{\text{sat},E1} + \delta t_{\text{rx},E1} + \delta^k_{E1,E6} \tag{4}$$

$$t^k_{\text{end},j} = t^k_{\text{start},j} + \Delta\tau_{MAX} + \frac{N_{chips}}{R_c} \tag{5}$$

GST_j refers to the Galileo System Time at epoch j, for which to authenticate. δ_{RECS} is the offset for the RECS within the signal, aligning the RECS timing with the receiver's internal clock. τ^k_{prop} represents the propagation delay for satellite k, accounting for the travel time of the signal from the satellite to the receiver. $\delta t^k_{\text{sat},E1}$ adjusts for any discrepancies in the satellite's clock for the E1 signal relative to satellite k. $\delta t_{\text{rx},E1}$ compensates for any drift or bias in the receiver's own clock. $\delta^k_{E1,E6}$ accounts for the differential delay between the E1 and E6 signals for satellite k.

$$\delta^k_{E1,E6} = BGD^k_{\text{sat},E1,E6} + \delta I_{E1,E6} + \widehat{HWB}_{\text{rx},E1,E6} \tag{6}$$

where $\delta I_{E1,E6}$ represents the differential ionospheric delay between these bands, and $HWB_{\text{rx},E1,E6}$ denotes the hardware bias at the receiver affecting the E1 and E6 signals.

$\Delta\tau^k_i$ introduces a random time offset for the i-th RECS of satellite k. $\Delta\tau_{\text{MAX}}$ sets the upper limit for the random time offset, ensuring the ECS remains within the snapshot window. N_{chips} determines the number of chips used for correlation, and R_c, the chip rate of the E6 signal.

4.2.2. Encrypted-E6C Signal Acquisition

The acquisition process in the is implemented through a circular FFT-based convolution between the recorded snapshot and a ECS obtainted form the RECS decryption. The primary objective of this process is to provide a coarse estimation of the code phase and the Doppler shift associated with the received signal.

To optimize the correlation process, the system utilizes Doppler measurements from the authenticated E1 signal.

The mathematical representation of the acquisition process is given by the following formula:

$$\hat{R}_{xd}(f_D, \tau) = \frac{1}{K}\sum_{k=0}^{K-1} x_{IN}[k]d[kT_s - \tau]e^{-2\pi j f_D k T_s} \tag{7}$$

where $x_{IN}[k]$ represents the complex vector containing the IQ samples, d is the ECS from teh decryption module, T_s is the sampling period, τ is the code phase, f_D is the Doppler shift, and K is the number of samples.

In this implementation, a resolution of 8IQ at 15MHz is used, which provides detailed insights into the signal characteristics. As a result of the acquisition process, both the Doppler shift and the code phase are determined.

4.3. Authentication metrics

Authentication metrics within ACAS are designed to validate various aspects of signal and data integrity. This section delves into the core methodologies applied in the ACAS software solution to authenticate the Line-of-Sight (LoS), the pseudorange measurements, and the position by cross-checking with the results obtained from processing the E1B measurements.

4.3.1. LoS Authentication

LoS authentication is based on the detection of the correlation peak which indicates the alignment of the code sequence obtained from decryption with the recorded signal. This metric is generated from the data obtained from the correlation, detecting the highest value in the set and comparing it with the base noise of the correlation following the equation:

$$\frac{\max\{\mathrm{FFT}(n)\}}{\mathrm{RMS}(\mathrm{FFT}(n))} \geq \gamma \rightarrow \xi_j^k = 1 \quad (\text{satellite authenticated}) \tag{8}$$

If the obtained factor is above the defined threshold, it is considered that the signal received on that line of sight is the one that was originally transmitted by the satellite.

4.3.2. Pseudorange Authentication

Once the LoS is authenticated, the authentication of measurements is verified by comparing the measured pseudorange with the estimated range, using a predefined error threshold γ_{auth}:

$$|\rho_{j,E1}^k - \hat{\rho}_{j,E6}^k| \leq \gamma_{\text{auth}} \Rightarrow \xi_j^k = 1 \quad (\text{measurement authenticated}) \tag{9}$$

This metric verifies that the code measurement obtained in the correlation process is similar to that obtained from the E1 signal, thereby confirming that the E1 measurement is reliable.

4.3.3. PVT Authentication

Finally, to obtain a global metric of the data set, the user's position is computed using the authenticated navigation data with the OSNMA protocol and the measurements authenticated by ACAS from the E6C, and this solution is compared with the one obtained using measurements from the E1;

$$|\vec{x}_{E1} - \vec{x}_{E6}| = \Delta\vec{x}_{E1,E6} \leq \gamma \rightarrow \xi_j = 1 \quad (\text{E1 position authenticated}) \tag{10}$$

Likewise, the E1 position is also authenticated if it is computed using only the measurements authenticated with the Pseudorange Authentication.

$$\prod_{k=1}^{k} \xi_j^k = 1 \rightarrow \text{E1 position authenticated} \tag{11}$$

5. Testing and Validation

As previously mentioned, the ACAS is a Galileo service that is not yet operational as of the date of the tests presented in this document. Therefore, for the proof of concept, a static artificial scenario has been generated following the considerations of section 4. For this

purpose, the scenario was recorded with a receiver that logs the raw data of the transmitted signals and the observations for each satellite.

Figure 5 shows how the scenario was set up to simulate the use of the ACAS.

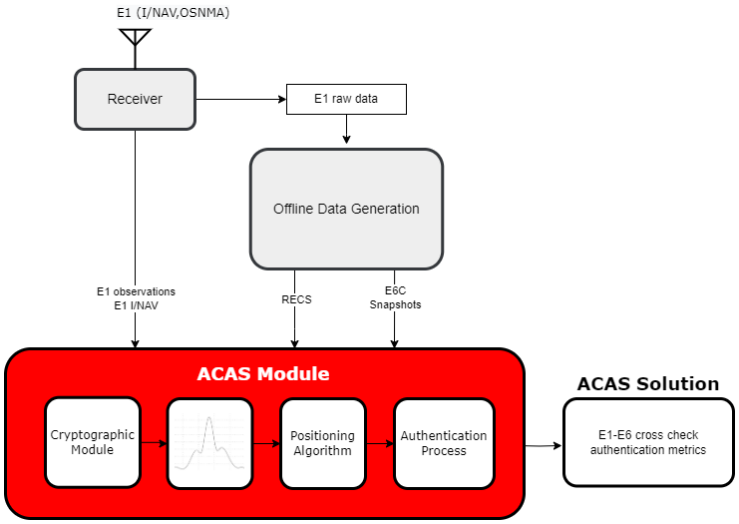

Figure 5. Outline of the ACAS software validation process

Firstly, the ECS were continuously generated for each satellite, and these code sequences, along with the navigation data, were used as input for an Signal Generator Tool that generated the necessary signal snapshots for the ACAS authentication process, with a resolution of 8IQ and at a rate of 15 MS/s.

From the raw data, the navigation data and the transmitted OSNMA keys were decoded. The ECS were re-encrypted with the OSNMA keys obtained from the scenario following the reverse process defined in equation 2, thus generating the RECS files that will be used.

After generating the necessary inputs offline, the ACAS module was launched and the authentication metrics studied were generated.

5.1. ACAS Solution Results

The correlation process generated the data for figure 6 where the magnitude of the acquisition metric is shown.

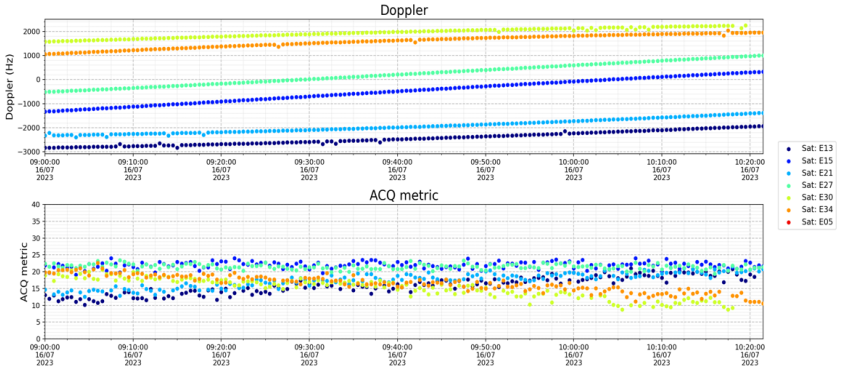

Figure 6. Doppler and Acquisition metric

Figure 7 displays the results obtained from the comparison of the pseudoranges of E1 generated by the receiver with the encrypted E6C pseudoranges calculated using the ACAS module.

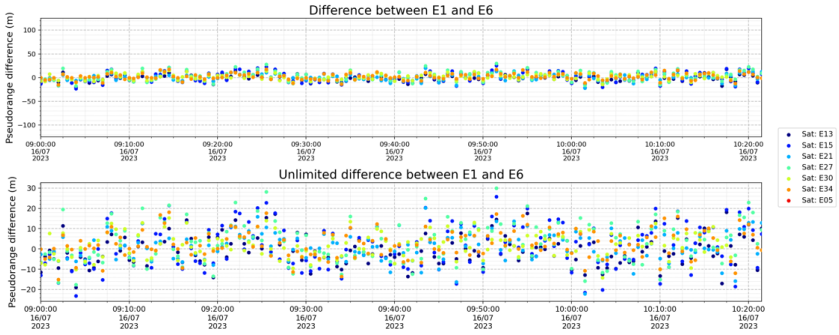

Figure 7. Pseudorange Authentication metrics

Finally, figure 8 shows the position differences using the observations from E1 compared to those calculated with observations from E6C. In both cases, only satellites with navigation authenticated by OSNMA were used.

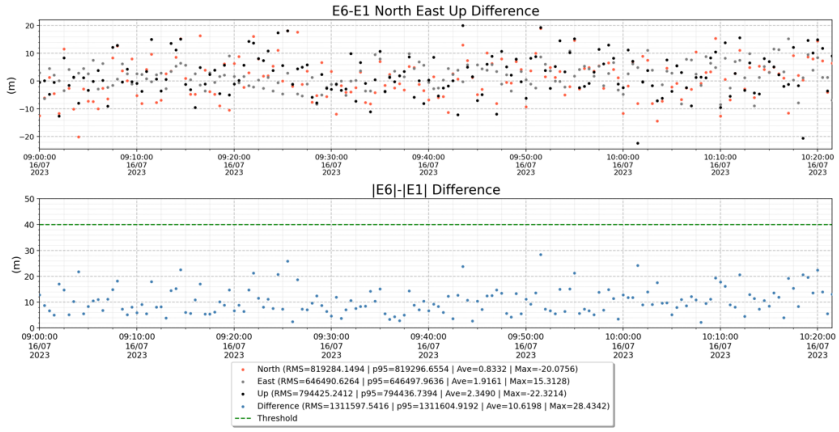

Figure 8. Position Authentication metrics

6. Conclusions

This paper has presented the development of software designed for real-time position authentication using the ACAS together with the OSNMA protocol. The software utilizes the capabilities of ACAS to ensure the integrity and authenticity of satellite navigation signals. Additionally, a defined procedure for utilizing the ACAS solution has been outlined, generating several metrics at differents levels which ensure the provision of an authentic and reliable solution for GNSS signal authentication.

While the current implementation of the software and procedures has proven effective, there are several avenues for further enhancement and validation. Future work will include experimentation with various configurations of ACAS to reveal insights into optimizing performance under different operational scenarios. Real encrypted signal validation will also be conducted to ensure the robustness and reliability of the software, pushing the boundaries of current testing environments. Additionally, extending tests to various environments will help in assessing the software's adaptability and performance in diverse conditions, providing a comprehensive evaluation of its capabilities. These efforts will enhance the understanding of ACAS's potential and pave the way for its broader adoption in critical GNSS applications.

Author Contributions: Conceptualization, S.C., A.C. and M.R.; methodology, A.C.; software, M.R. and A.C.; validation, M.R., and A.C.; formal analysis, M.R.; investigation, M.R., A.C. and S.C.; writing—original draft preparation, M.R.; writing—review and editing, A.C.; visualization, S.C.; supervision, S.C.; project administration, D.C.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available from the corresponding author on request. The data are not publicly available due to its data size and further explanations may be needed.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ACAS	Assisted Commercial Authentication Service
AES	Advanced Encryption Standard
BGD	Bias Group Delay
CBC	Cipher-block chaining
ECS	Encrypted Code Sequence
FFT	Fast Fourier Transform
GNSS	Global Navigation Satellite System
GSC	GNSS Service Center
GST	Galileo System Time
LoS	Line-of-Sight
NMA	Navigation Message Authentication
OSNMA	Open Service Navigation Message Authentication
RECS	Re-encrypted Code Sequence
RMS	Root Mean Square
SHA	Secure Hash Algorithms
TESLA	Timed Efficient Stream Loss-tolerant Authentication

References

1. Fernandez-Hernandez, I.; Cancela, S.; Terris Gallego, R.; Seco-Granados, G.; López-Salcedo, J.; O'Driscoll, C.; Winkel, J.; Chiara, A.; Sarto, C.; Rijmen, V.; Blonski, D.; Blas, J. Semi-Assisted Signal Authentication based on Galileo ACAS. In *Proceedings*; 2022.
2. European Union, "E6-B/C Signal-In-Space Technical Note", 2019.
3. European GNSS Agency. *Galileo Open Service Navigation Message Authentication (OSNMA) – Internet Data Distribution Interface Control Document (OSNMA IDD ICD) – Issue 1.0, July 2023.* Publications Office of the European Union, 2023. DOI: 10.2878/325903.