Designing and Evaluating Next Generation of Resilience Receivers

S. Cancela, D. Calle, G. Arroyo; GMV; Spain
A. Dalla Chiara, G. Da Broi, O. Pozzobon, C. Sarto; Qascom, Italy
J. Winkle, I. Krol; Ifen, Germany
P. Webster; CGI, UK
I. Fernández; European Commission; Belgium
J. Simón; GSA, Czech Republic
G. Seco-Granados; UAB; Spain

BIOGRAPHIES

Simón Cancela holds a MSc in Advanced Mathematics by the Universidad Complutense de Madrid. He joined GMV in 2015 and he has been working in the Galileo Commercial Service Demonstrator validation and experimentation activities and he is currently working on the development of a Commercial Service enhanced PVT resilient platform.

J. David Calle has a Master of Science in Computer Engineering from the University of Salamanca. He joined GMV in 2008 and he is currently working in the GNSS business unit designing and developing GNSS algorithms, applications and systems. He has been involved in the development of the magicGNSS suite and the Galileo Time and Geodetic Validation Facility. He is currently the technical responsible for the development of the Galileo Commercial Service Demonstrator.

Guillermo Arroyo has Master’s degree in Telecommunication Engineering from the University of Deusto. He joined GMV in 2017 and is currently working in the development of a resilient platform for the Galileo Commercial Service.

Andrea Dalla Chiara is designer and project manager at Qascom, with focus on GNSS simulators and receivers and authentication techniques both at signal and data level. He is an electronic engineer, and has a PhD in Information Technologies by University of Padova.

Giacomo Da Broi is a designer and developer of GNSS and TT&C simulators at Qascom, specialized in authentication techniques both at signal and data level. He holds a MSc degree in Telecommunications Engineering from University of Padova.

Oscar Pozzobon is the founder and technical director of Qascom. He has a degree in information technology with a master in telecommunications engineering and a Ph.D. in Aeronautics and Satellite Applications. He has been pioneering GNSS authentication since 2001.

Carlo Sarto is the Software Manager at QASCOM. He graduated from Computer Science at the University of Padua. By joining Qascom in 2008, he participated in several projects concerning the design and development of algorithms and products for simulation, modelling and mitigation of GNSS threats.

Dr. Jón Ó. Winkel has been the head of receiver technology at IFEN GmbH since 2001. He studied physics at universities in Hamburg and Regensburg and received a Ph.D. (Dr.-Ing.) from the University FAF Munich, where his studies focused on GNSS modelling and simulations

Ilya Krol received his Diploma in Radioelectronic Systems from the Moscow Aviation Institute (MAI) in the year 2006. He is currently working for IFEN GmbH as a System FW Engineer.

Paul Webster is a Senior Software Engineer within CGI. He has worked on the Galileo Programme for over nine years; specialising in cryptographic architectures and security patterns.

Ignacio Fernández Hernández is the Galileo service definition coordinator at the European Commission, DG ENTR. He is an ICAI engineer, holds an MBA by LBS and a PhD in electronic systems by Aalborg University.

Javier Simon is Service Design Engineer within the European GNSS Agency, currently contributing to the definition and design of the Galileo OSNMA and CS services. He holds a MSc. degree in Telecommunications Engineering from the

Polytechnic University of Madrid, Spain. Before joining GSA he participated in several projects for the study and design of future GNSS algorithms and systems

Gonzalo Seco is professor with the Dept of Telecom. Eng. of Univ. Autonoma de Barcelona (UAB) and head of the Signal Processing for Navigation and Communications (SPCOMNAV) group. Previoulsy, he was staff member at the Radionavigation Section in ESTEC/ESA, and involved in the Galileo project and in the development of GNSS receivers and applications.

ABSTRACT

The Galileo program is in continuous evolution to develop and deploy all the necessary elements and functionalities for the provision of the Galileo services. In this regard, the European Commission (EC) has been working together with the European GNSS Agency (GSA) and industry for the definition, demonstration and performance assessment of the future capabilities of the Galileo Commercial Service (CS). With this purpose, the Navigation Authentication through Commercial Service-Enhanced Terminals (NACSET) project has been recently launched. The project has a twofold objective: to study and assess system evolutions for cryptographic key management, and to develop a resilient receiver combining receiver aids and sensors with the Galileo CS Authentication features to increase robustness against spoofing attacks.

NACSET comprises the design, implementation and experimentation phases of two key elements: a key management simulator (KMS) that will support the cryptographic key generation, transmission, storage, renewal and destruction, including signal-in-space and ground-assisted solutions; and a Commercial Service Resilient PVT Platform (CS-RPP), a navigation platform with improved anti-attack techniques based on different elements: two antennas, atomic clocks, dedicated signal processing techniques, inertial sensors, and remote assistance for navigation authentication and time synchronization through non-GNSS channels.

This paper presents the NACSET system, architecture, elements and operational modes. The assistance service and user terminal are described in detail, including the characteristics of all its elements: antennas and RF Front End (E1-E6 enabled), CSAC and TCXO clock features, signal processing techniques, IMU features, PVT algorithms (including integrity and authentication) and secured communication protocols. Special focus is put on the definition of the anti-spoofing measures to be implemented in the User Terminal, including Angle-of-arrival and Automatic Gain Control interference detection, clock drift monitoring, anti-replay signal processing techniques, etc., all integrated with the level of authentication obtained from code-encrypted Galileo CS signals.

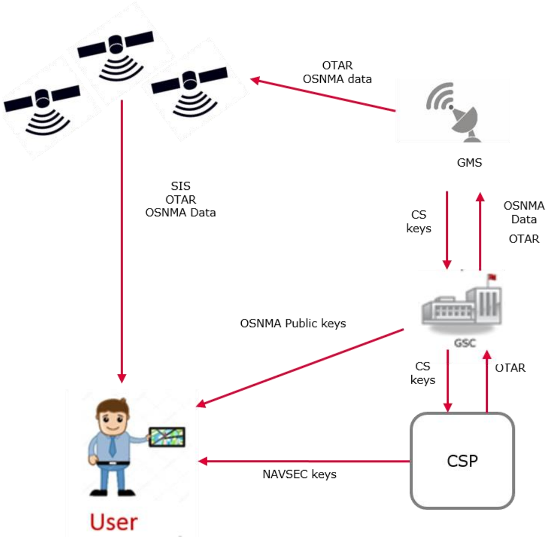
INTRODUCTION

The Galileo System will provide four basic satellite-only services to global GNSS users, Galileo Open Service (OS), Galileo Commercial Service (CS), Galileo Public Regulated Service (PRS) and Search and Rescue (SAR). The Commercial Service aims to provide added value services to the users, mainly authentication and high-accuracy. These services are planned to be deployed on top of the CS signals on the E6 band (1260–1300 MHz), which include a data component, the E6-B, and a pilot component, the E6-C. These signals are complemented with the future Open Service Navigation Message Authentication that is planned to be implemented in the “Reserved-1” fields in the Galileo I/NAV.

GNSS signals due to their low power nature can be easily jammed. In addition, the lack of authentication eases the possibility of being forged or “spoofed” utilizing the appropriate equipment. In this sense, protecting GNSS has become one of the major topics of interest for GNSS community.

GNSS information can be protected using two different protection layers: data-level protection also known as Navigation Message Authentication (NMA) and signal-level protection. For signal-level protection, a relevant feature of the CS E6 signal is that the primary spreading codes of both components can be either encrypted or disseminated in the clear. When encrypted, the spreading codes are replaced by an unpredictable chip-stream generated through a secret key, making the signal indistinguishable from noise for unauthorized receivers.

In parallel to other technical and regulatory measures, features in the GNSS signals allowing authentication are undoubtedly a key building block to improve the security of the navigation services. This feature allows authenticating not only the information encoded in the signal but also the



signal time of arrival, at least against certain threats and confidence levels. Both factors are compulsory for a trustworthy position and time estimation. On the other hand, some additional capabilities such as the key handling are required in the system to provide these new services.

Next sections present the design of a resilient GNSS receiver and assistance servers ready to be exploited and integrated inside the Galileo Commercial Service infrastructure.

NACSET PLATFORM

The European Commission has been working in the Commercial Service definition and demonstrator during the last years. The knowledge and experience gathered within recent projects motivated the challenge of developing a system to be integrated in the CS infrastructure and demonstrating different techniques focused on providing the maximum resilience and robustness.

NACSET platform comprises two main elements: a key management simulator (KMS) and a Commercial Service Resilient PVT Platform (CS-RPP). The CS-RPP is broken-down into two collaborative elements: a Synchronization and Authentication Server (SAS) and a User Terminal (UT). SAS and UT communicate to exchange information for several authentication solutions.

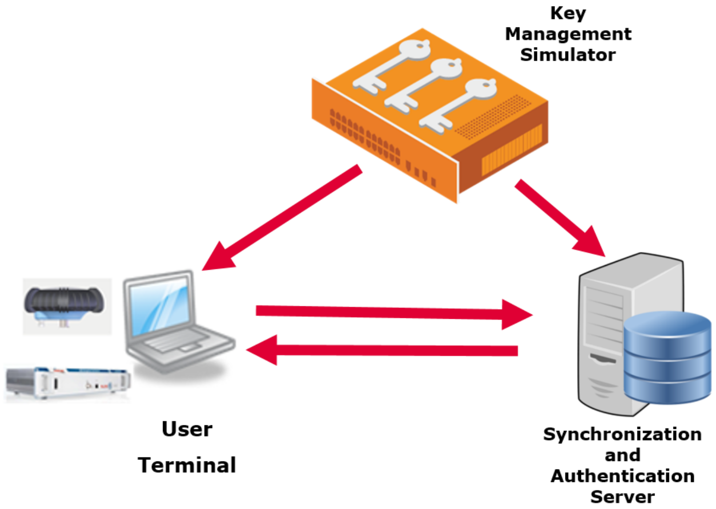


Figure 1: NACSET platform architecture

Key Management Simulator

The KMS activities cover the development of and end-to-end simulator to understand and evaluate the challenges and complexity inherent to secure key management and distribution. The KMS allows exploring and testing different key management distribution schemes suitable for the Galileo infrastructure. The outcomes of the development and experimentation will help to define the guidelines for the secure distribution of cryptographic keys, between the Commercial Service Providers (CSPs), Galileo Service Center (GSC) and final users, as well as for the Galileo OSNMA. This item is one of the cornerstones for the CS, since secure key-management procedures are required to allow signal and data authentication. In this sense, the threat analyses and experimentation activities foreseen will allow defining a reliable framework and techniques to guarantee the robustness to the cryptographic keys lifecycle and reduce the success of potential attacks.

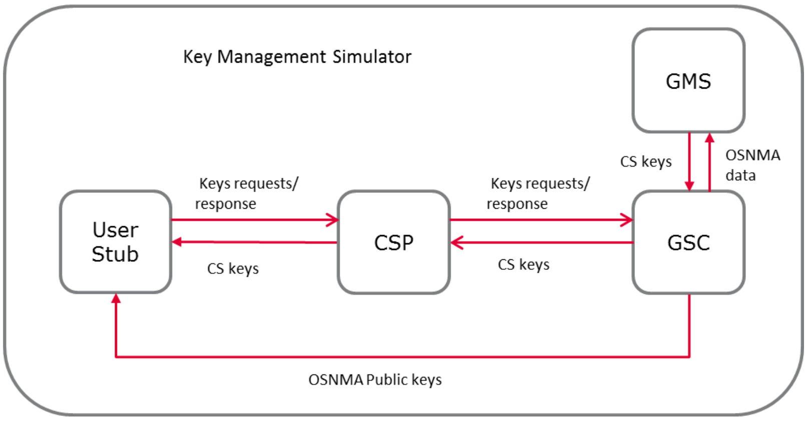


Figure 2: KMS standalone simulation

CS Resilient PVT Platform

The main objective of the CS-RPP is to demonstrate the viability of the provision of a future assisted service of accurate timing synchronization, authentic data provision and signal authentication combined with receiver-based signal protection techniques. As mentioned before, the CS-RPP includes two main components: the Synchronization and Assistance Server and the User Terminal.

The SAS is a remote system responsible of providing the assisted authentication capabilities as well as time synchronisation feature. It supports the provision of Chip Spreading Sequences (CSS), Encrypted Batches of CSS, authentic navigation and Remote Processing Authentication (RPA). The SAS makes use of secure TCP/IP connection towards the user terminals, to guarantee the secure and/or secret transfer of the authentication and time information.

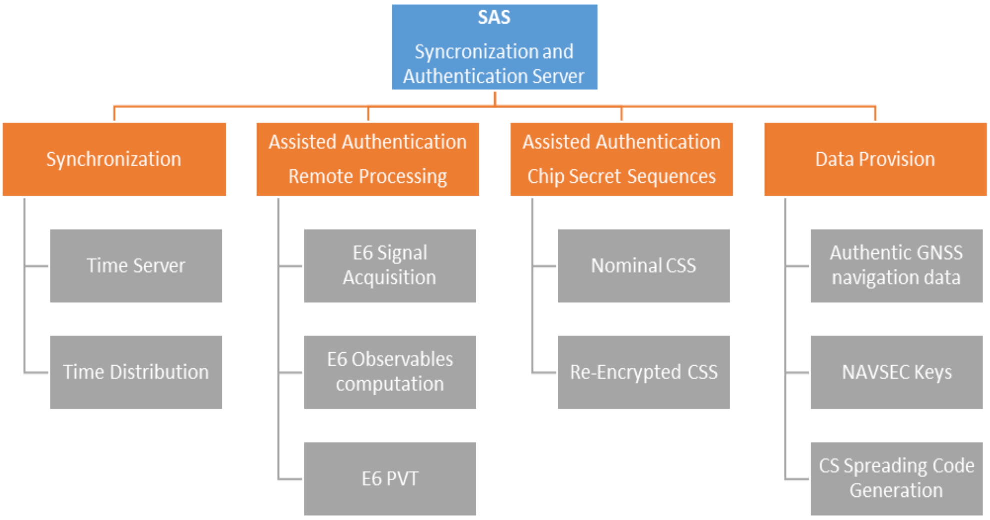

SAS
Syncronization and Authentication Server
Synchronization
Time Server
Time Distribution
Assisted Authentication Remote Processing
E6 Signal Acquisition
E6 Observables computation
E6 PVT
Assisted Authentication Chip Secret Sequences
Nominal CSS
Re-Encrypted CSS
Data Provision
Authentic GNSS navigation data
NAVSEC Keys
CS Spreading Code Generation

Figure 3: SAS provision overview scheme

User Terminal

The User Terminal (UT) is the element of the system in charge of receiving the signals, integrating the antispoofing protection techniques and generating the reliable PVT solution. The SIS interface is provided by a multi-GNSS and multi-antenna receiver, whereas the PVT resilience will be achieved by using the authentication properties of the Galileo SIS signals (SCE, NMA) together with other resilience features, such as angle-of-arrival detection using the dual-antenna, body-frame motion using an accurate IMU, assisted trusted time reference and secure real-time communication with the SAS to exploit the assisted authentication services. The architectural breakdown of the system shows three main functional modules:

- GNSS Receiver: a high-end GNSS receiver including high performance hardware (two antenna input, atomic clock, Inertial sensors, CS/OS-capabilities, and other built-in sensors).
- Authentication Engine: a software module in charge of implementing the designed protection techniques and the authentication solutions.
- PVT Engine: a software module in charge of computing the resilient PVT.

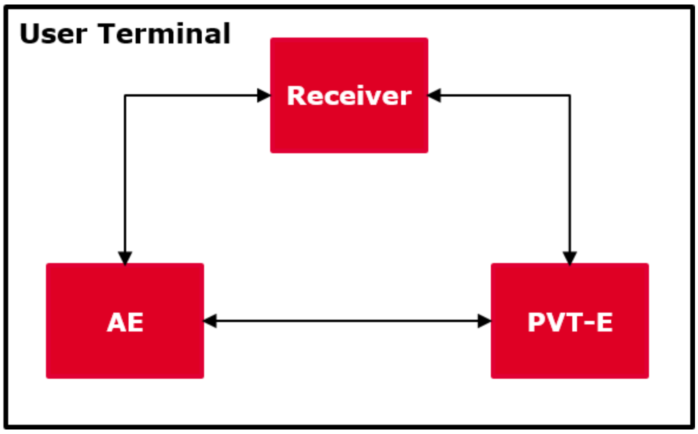


Figure 4: User Terminal architecture

RECEIVER SPECIFICATION

The Receiver acquires and tracks GNSS satellite signals, dumps the symbols, demodulates the data received and collects aiding information from the built-in sensors (e.g. IMU). The receiver supports the tracking of CS signals in the clear and encrypted, as well as handling the required crypto material when in encrypted mode. The Receiver consists of three main HW assets: an NTR GNSS receiver with GNSS antennas, a host PC and a separate USB IMU unit. The following subsections describe some of the main Receiver hardware components.

Antenna hardware

The Receiver shall be equipped with two GNSS antennas. The proposed antenna model is a Navtech navXperience 3G+C high-precision antenna. . Its installation is highly flexible thanks to the high LNA gain of 48 dB, which makes it usable with cable lengths of tenths of meters.

Table 1: Antenna specification

Specifications	3G+C reference
Galileo Signals	E1, E5a, E5b, E5a+b (AltBOC), E6
GPS Signals	L1, L2, L2C, L5
Resistance	50 Ohm
Passive Gain	3/5 dbic (min)
Polarisation	RHCP
LNA Power Gain	48 dB
LNA Noise factor	< 2 dB

Inertial Measurements Unit (IMU)

The IMU is in charge of providing accelerometer and gyroscope measurements in order to have an independent source of motion information to identify inconsistencies with respect to the GNSS, which may indicate a spoofing attack. A mid-cost IMU sensor MTi 10 series from the manufacturer XSENS (Xsens Technologies B.V., the Netherlands) has been selected. Next table contains the relevant specifications of the unit [1] :

Table 2: XSENS gyroscope/accelerometer performance specifications

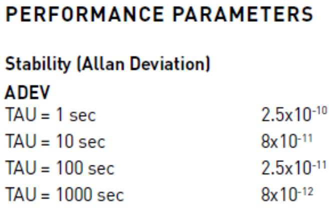
Gyroscope specification	MTi 10-series
Standard full range	450
Bias repeatability (1 yr)	0.2
In-run bias stability	18
Bandwidth (-3dB)	415
Noise density	0.03
g-sensitivity (calibrated)	0.006
Non-orthogonality	0.05
Non-linearity	0.03
A/D resolution	16

Accelerometers/magnetometers specification	MTi 10-series
Acceleration	
Standard full range	50
Bias repeatability (1 yr)	0.03
In-run bias stability	40
Bandwidth (-3dB)	375
Noise density	80
Non-orthogonality	0.05
Non-linearity	0.03
A/D resolution	16
Magnetic field	
Noise density	200
Non-linearity	0.1
A/D resolution	12

The characteristics herein presented show an IMU unit which might be used for coasting during several minutes. In the project, it will be used to perform instantaneous monitoring of the user dynamics versus the GNSS solution, objective for which the quality of the IMU is considered sufficient.

Chip Scale Atomic Clock (CSAC)

The chip-scale atomic clock is a clock frequency information source for the NTR, alternative to the usual TCXO. CSAC is intended to allow keeping track of the correct receiver time in case tracking restarts, to be able to detect spoofing that shift the computed PVT. The CSAC is integrated into the receiver hardware, the device model is the Quantum SA.45s CSAC, option 001 from Microsemi. The main specification relating to performance are shown on the right figure, but the reader is referred to [2] for a full specification of the device.



PERFORMANCE PARAMETERS

Stability (Allan Deviation)

ADEV	
TAU = 1 sec	$2.5\text{x}10^{-10}$
TAU = 10 sec	$8\text{x}10^{-11}$
TAU = 100 sec	$2.5\text{x}10^{-11}$
TAU = 1000 sec	$8\text{x}10^{-12}$

ASSISTED SIGNAL AUTHENTICATION

The CS-RPP platform includes a remote assistance server. One of its tasks is to provide signal authentication by means of an aiding channel. This signal authentication is given by two different techniques: Remote Signal Authentication and Chip Spreading Sequences. The great advantage of these techniques is that they do not require the user to possess the necessary decryption keys to be able to navigate using the encrypted signals.

Remote Signal Authentication (RPA)

RPA consists on a bidirectional communication between the UT and SAS where the user gathers E6 signal samples that are encrypted with SCE. This information is sent to the SAS together with the E1 observables and the user's PVT computation solution. Then, the SAS determines the authenticity of the E1 PVT data by computing a trusted position using the E6 signal samples. Its security is based on a very simple concept: the encrypted code never repeats, and, therefore, a code sequence in a certain position and time is unique. One limitation is that all the security is based on spreading code encryption: it could still work without encryption, but it would be vulnerable to spoofing the E6 CS signal. Another interesting feature is that RPA does not require any data, as it simply uses the code modulation of the E6B or E6C channel. For more details on the algorithm, see [12]

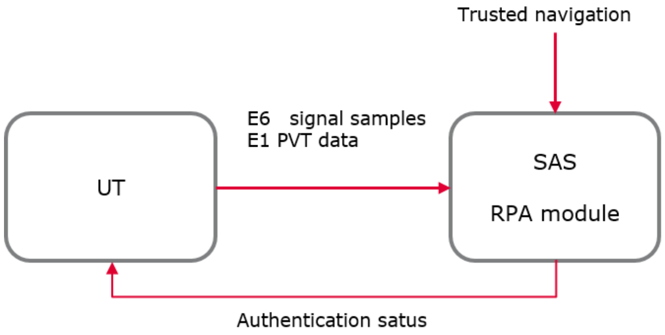


Figure 5: RPA process scheme

Chip Spreading Sequences (CSS)

This authentication concept is based on the fact that if the receiver is tracking an open signal, and in the same code offset and phase there should be a corresponding encrypted sequence, which is unknown to potential attackers. Hence, it is assumed that the receiver is able to track an open signal (e.g.: E6B) and an encrypted signal (e.g.: E6C).

In this technique, the SAS computes a small part of the sequence, called Chip Spreading Sequence (CSS) [12] , for a particular time and transmits it to a remote receiver. The receiver then attempts to correlate the CSS with the received signal; if the correlation peak is observed over a predetermined threshold, the signal can be considered authentic, otherwise it is considered spoofed and discarded.

It shall be noted that a standard application of SAS allows verifying the authenticity of the reference open signal against the encrypted one. Therefore, in a scenario where the open signal is Galileo E6B and the encrypted signal is Galileo E6C, the E6B signal can be authenticated. Due to the properties of spreading code encryption, the SAS authentication also verifies the authenticity of E6 pseudoranges. A consistency check between E1 and E6 pseudoranges therefore allows extending, with some tolerance, the authenticity claim to the E1 signals, which can be used for the calculation of the PVT.

NACSET platform implements two different provision schemes for the spreading sequences: in plain format where the CSS are sent to the UT with a minimum delay (ms-level) for the time of applicability; and in encrypted format where a batch of sequences might be delivered to the user in advance of their dissemination through the SIS. These batches are encrypted with secret keys that are later disclosed to the user. The encryption technique for the sequences is based on the delayed-key property of the proposal for the Galileo Open Service Navigation Message Authentication based on the TESLA protocol [11] The idea consists on generating the encryption/decryption symmetric key derived from the TESLA key sequence. Each encryption key is obtained applying a one-way hash function to the applicable TESLA key for a given transmission time. The derived keys are provided to the SAS, which is in charge of generating and encrypting the CSS sequences using the received keys. Then, the UT receives the encrypted CSS from the SAS through an internet connection and stores them. When it receives the correspondent TESLA key from the SIS, it is able to apply the same hash function and derive the correspondent CSS decryption key, enabling the CSS decryption and usage.

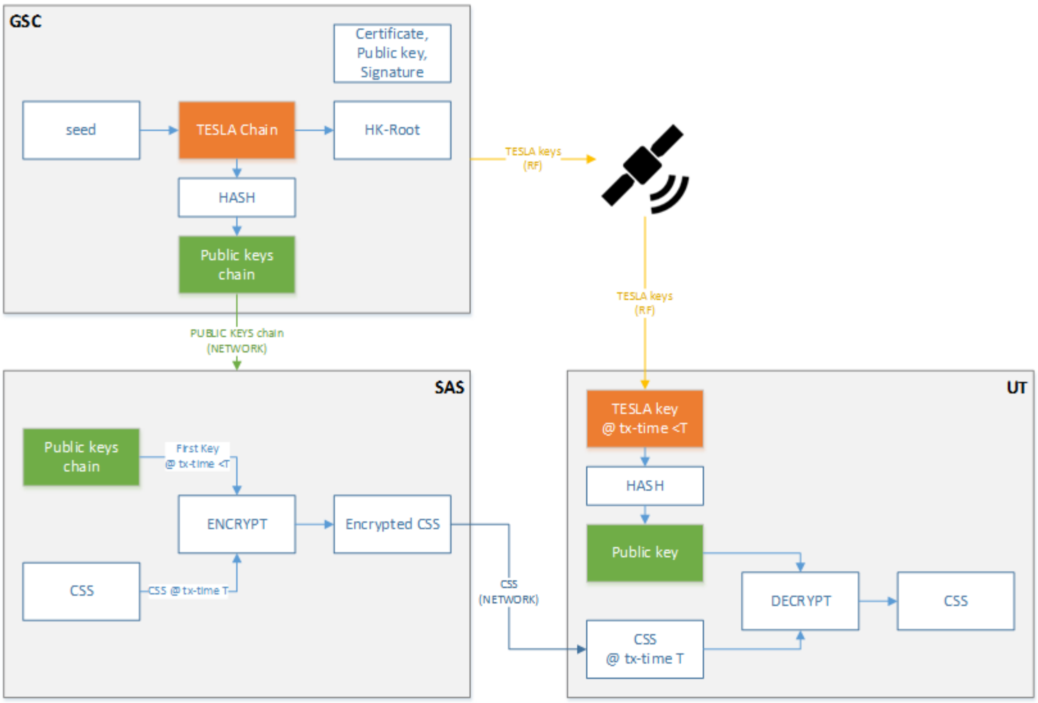


Figure 6: Encryption of CSS

ANTI-SPOOFING TECHNIQUES

The Authentication Engine (AE) is the software module in charge of monitoring the authenticity of the GNSS signal. The AE includes several subcomponents, each one devoted to a specific monitoring task:

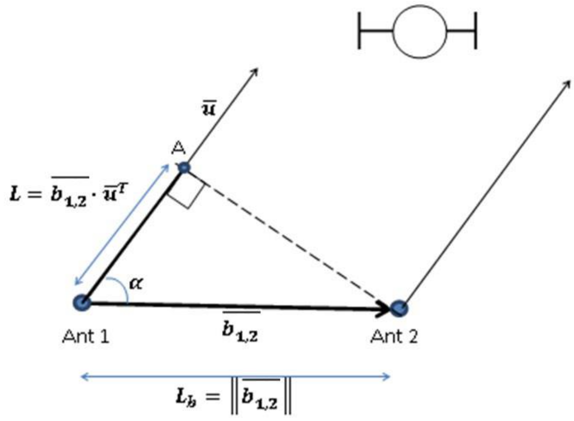
- Dual Antenna Spoofing Detector: autonomous module for spoofing detection based on multiple antennas data.
- IMU Spoofing Detector: autonomous module for spoofing detection based on integration with inertial measures.
- CSAC Spoofing Detector: autonomous module for spoofing detection based on the monitoring of coherency of time between the high precision clock (CSAC) and the time solution.
- AGC Spoofing detector module for spoofing detection based on the monitoring of the ACG values, also combining the C/N0 measurements.
- CSS authentication: module that exchanges data with the SAS, and the NavX-NTR. It loads CS encrypted chip sequences in the receiver, with their time of applicability. The returned correlation values are used for spoofing detection purposes.
- RPA authentication: module that exchanges data with the SAS, and the NavX-NTR. It delivers E6 signal samples to the remote server SAS: RPA processing provides the authentic PVT solution and spoofing flags.
- Anti-replay: module that monitors the received signal to prevent replay attacks

The AE manages the spoofing detection and authentication capabilities of the sub-modules, to provide the PVT-Engine (PVT-E) the data necessary to compute a secure navigation solution and integrity protection-levels.

Dual Antenna Spoofing Detector

The use of multiple antennas on the same receiver allows detecting the angle of arrival (AoA) of the received signals. This can be achieved using the carrier-phase differences between antennas as explained in [3] GNSS signals typically arrive to the receiver from different directions, but in case of being spoofed they would arrive with an angle different from the expected one, and in particular the signals for the spoofed satellites might have same direction of arrival.

In the particular solution explored in the project, the two antennas shall be located at a distance of λ/2 in order to get rid of the ambiguity term after simple or double differences are computed. Finally, the AoA


$\overline{u}$
A
$L = \overline{b_{1,2}} \cdot \overline{u}^T$
α
Ant 1
$\overline{b_{1,2}}$
Ant 2
$L_b = \left\| \overline{b_{1,2}} \right\|$

estimation is performed using the fractional part (λ-module) of the carrier phase differences.

$$\Delta\psi_{1,2} = \left\|\overline{b_{1,2}}\right\| cos(\alpha) + \Delta\tau_{1,2} + \epsilon_{1,2} \tag{1}$$

The main inconvenience of using single differences is that a-priori calibration of the hardware biases is needed. As typically a user does not have this information, the solution requires a final step to compute double differences by using a pivot satellite transmitting in the same wavelength.

$$\nabla\Delta\psi^{i,j}_{1,2} = \Delta\psi^{i}_{1,2} - \Delta\psi^{j}_{1,2} \tag{2}$$

$$\nabla\Delta\psi^{i,j}_{1,2} = \left\|\overline{b_{1,2}}\right\| \left(cos\left(\alpha^{i}\right) - \cos\left(\alpha^{j}\right)\right) + \epsilon^{i,j}_{1,2} \tag{3}$$

Figure 7 shows the results obtained when exercising the algorithm using real and spoofed signals.

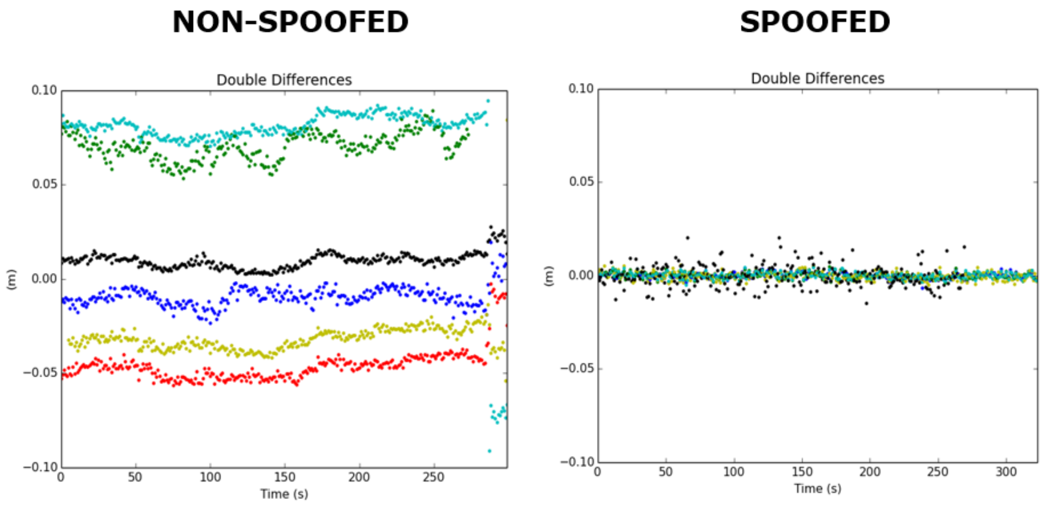


Figure 7: AoA results

IMU Spoofing Detector

The UT is able to process the GNSS and IMU information in a tightly-couple approach [10] . The particularity of the proposed implementation is that different weights can be applied to both data sources generating high measurements rejection when they are inconsistent. The spoofing detection algorithm will perform an instantaneous monitoring of the observed rejection and residuals of the measurements. The algorithm development will require the conduction of a set of pre-trials to fine-tune the weights for each type of measurement to maximize the spoofing detection probability without compromising the probability of false alarm.

CSAC Spoofing detector

A main concern of a spoofer will be to not be detected by the target receiver, so the common delay of the spoofing signals which will be absorbed by the receiver's clock-error estimate, must not deviate significantly from the receiver's authentic clock error. This means that the injected delay has to be as small as possible so that it cannot be separated from the typical random frequency (and thus time) fluctuations of the oscillator driving the receiver. In order to handle this issue, it is proposed to use the accurate time from the atomic clock to monitor any alterations on the time computed by the user.

A dedicated strategy to monitor the time evolution in the user terminal has been designed. The Receiver time (RxTime) is coarsely adjusted once (at the very first SV signal acquisition), incremented via NTR internal clock source (normally - TCXO) and transmitted to the PVT Engine as a timestamp with the pseudoranges in the observables. Using this coarse common receiver time and pseudoranges, the PVT Engine can deduce the exact signal transmission times, and knowing the satellite positions from the ephemeris, compute the receiver position. When using the CSAC as clock source, the RxTime will maintain a very exact shift with respect to the real system time (SysTime), computed in the PVT. With this approach, the algorithm shall monitor each new PVT computation (including after a signal tracking outage generated due to jamming or fading) that the computed SysTime maintains a continuous and consistent difference and evolution.

AGC Spoofing detector

The analog signal received by the antenna, comprised nominally of GNSS signals and white Gaussian thermal noise, is amplified, down-converted, filtered and then converted to a digital signal for processing to the acquisition and tracking blocks. The Analog to Digital Converter (ADC) performs signal sampling and quantization and is affected by quantization losses.

Before entering the ADC, the signal gain is typically (for receivers with more than 1 bit ADC) controlled by an Automatic Gain Amplifier (AGC) which acts over a variable gain amplifier, adjusting the power of the incoming signal to optimize the L/σ ratio, minimizing quantization losses. The automatic gain control concept and the overall dynamic range is a combination of analogue and digital technology. In the receiver, the analogue part consists of the first LNA and the programmable gain section in the last stage of the analogue front-end system. On the other hand, the AGC is controlled by the receiver software and has a dynamic range of 30.5 dB. The first LNA has a gain of 18 dB, resulting in an overall analogue dynamic range of 48 dB.

In case of spoofing attack, the AGC gain might drop in response to increased power. The gain drop would be dependent also on the sophistication of the attacker, whether it has the capability to generate signals that do not exceed the nominal noise floor level. In case of compliant power, the detection based on AGC is not effective. AGC monitoring is a powerful measure for detecting the presence of spoofing signals especially if their power level is considerably higher than that of the authentic ones. Furthermore these techniques are effective only if the receiver starts in a trusted mode (acquiring authentic signals). It would be desirable to have a very stable AGC measure under nominal conditions (performance varies also with temperature).
The proposed algorithm consists on a heuristic spoofing detection technique defined as follows:

- Input**:**
  - $G_{AGC}(t)$: value of AGC for E1 band. This is a value from 0 to 63 representing an attenuation from 0 to 31.5 dB
- Processing**:**
  - Filtering of $G_{AGC}(t)$ with a moving average filter (e.g. 10 s), obtaining $\overline{G_{AGC}}$
  - Check of the filtered value against a threshold Th_{AGC} to be computed using the probability density function of G_{AGC} values in a nominal scenario (calibration procedure). Th_{AGC} is determined on the base of the selected False Alarm probability (P_{fa})
  - The Detector is represented by the following equation where H_0 represent the non-spoofing case and H_1 represent the spoofing case.

$$\begin{cases} H_0: \overline{G_{AGC}} < Th_{AGC} \\ H_1: \overline{G_{AGC}} > Th_{AGC} \end{cases}$$

- **Output:** The output is a flag reporting the detector output. This has the same value for all the SVID in tracking

Anti-replay protection

One of the most dangerous threats an attacker may implement to manipulate the user's signal is the Security Code Estimation and Replay (SCER) attack. With this attack, the spoofer estimates the unpredictable bits, and it broadcasts them as soon as it has reliable estimates. Prior to broadcasting them, it can broadcast a random guess of these bits or its own poor best estimate. The selected technique focuses on dealing with zero-delay attacks, where the spoofer estimates and rebroadcasts the original signal with negligible delay to initially take control of the tracking loops and then starts gradually delaying the signal to spoof the pseudoranges and position. Psiaki and Humphreys [9] proposed to exploit the unpredictable bits protected with NMA to implement protection techniques against SCER.

The Open Service Authentication proposed for Galileo [11] provides data-level authentication with cryptographic information inserted in the navigation that may be considered unpredictable. Based on this characteristics, [6] defines a signal authentication solution aiming at exploiting this signal features for anti-replay purposes; it consists in using samples of NMA unpredictable bits to allow the user receiver discriminate between an authentic and a replayed signal. In order to detect if the signal is correct, the receiver shall store random samples of the chips of the spreading code for each of the unpredictable symbols over a given interval. Once the necessary symbols are received and authenticated, the receiver can generate a replica of the samples corresponding to the stored chips and correlate it with the signal samples. The correlation gain obtained by a receiver using the authentic signal can be approximated by the total number of chips correlated. Whether the receiver is tracking a spoofed signal subject to a zero-delay attack, the gain will be lower and will depend on the probability for the spoofer of successfully estimating the symbols with a reduced number of samples in each symbol.

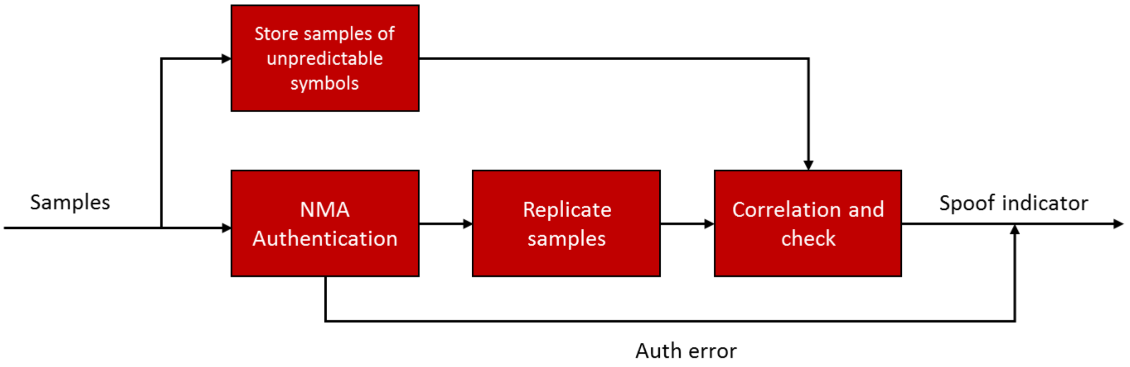


Figure 8: Anti-replay technique

WORKING MODES

NACSET platform has been designed to support two main working modes:

- Standalone: The full simulation of the Galileo CS infrastructure and CS providers
- Integrated: The integration of the platform in the real Galileo CS infrastructure and simulation only of required elements i.e. CS provider.

In the NACSET platform, all the key management related interfaces will be handled by the KMS, which can mimic both the CSPs and the Galileo system (i.e. the GSC and GMS). The GNSS signals will be simulated with a signal generator; also, the Synchronization and Authentication Server will be treated as a special CSP independent from the KMS that will interface directly with the GSC (both emulated by the KMS or the real instance). The CS-RPP UT and SAS will be able to interact with the KMS, or the GSC when the interface is available. The CS-RPP UT will be able to interact with the CSPs if available. Cryptography information aiming to exploit the Galileo OSNMA service, and to allow the receiver to track the CS signals when the Spreading Code Encryption (SCE) will be provided within the platform.

NACSET Standalone

The NACSET platform allows to fully simulating all the Galileo CS elements with respect to CS key and data management. The KMS simulates the GMS, GSC and potential CSPs (excluding the SAS) and interacts with both the UT and the SAS. When working with simulated scenarios, both UT and SAS are connected to the same signal generator to ensure that the scenario is consistent for both.

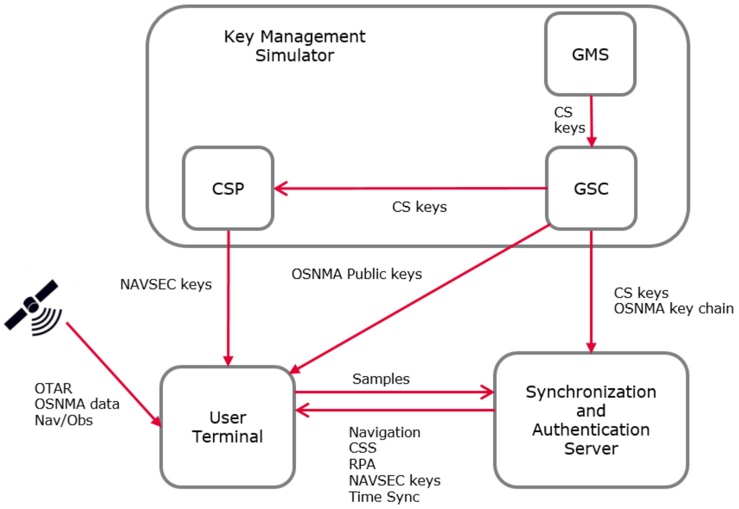


Figure 9: NACSET platform simulation

NACSET integrated mode

Full integration into the Galileo CS will be granted by the system. The KMS, simulating a CSP, and the SAS are able to interact with the real GSC for key related exchanges. This includes the provision the CS crypto information to the KMS for the simulation CSPs.

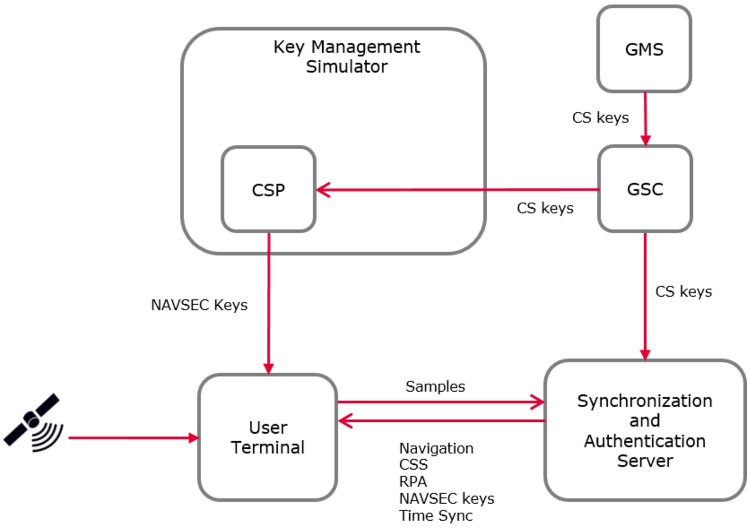


Figure 10: NACSET platform integration

CONCLUSIONS AND FUTURE WORK

NACSET platform represents an adequate framework to evaluate novel ideas not covered by previous activities, and the suitability of future services, which might be deployed within the Galileo services in the upcoming years. This framework will enable the conduction of a wide-range of analyses, tests and demonstrations to evaluate the designed solutions.

The expected objectives and outcomes are summarized below:

- Analyse potential threats at user-level and propose detection and/or mitigation actions.
- Design and evaluate standalone protection techniques implemented using the features available in the user-terminal.
- Assess assisted-based authentication and fine synchronization techniques
- Demonstrate the achievable performances at PVT-level taking advantage of the authentication and synchronization information provided by the implemented techniques.

- Define and carry out an experimentation campaign aiming to test the performances of the end-to-end system and the implemented techniques in standalone and combined modes. It shall consider simulated and real signals, and nominal and under-attack conditions.
- Evaluate key management schemes that could be used to provide the Galileo CS Authentication service

This paper has presented an outline of the main anti-spoofing mechanisms to be integrated in the NACSET platform, including a first characterization of its hardware (antennas, GNSS receiver, IMUs, CSAC), protection checks (antenna differential measurements, IMU and GNSS consistency, AGC) and signal processing techniques, both standalone and assisted. The next step after completing the design phase is to launch the implementation and validation activities of the system. Afterwards, a dedicated experimentation campaign to assess the implemented techniques for both key management and attack detection and protection will be carried out. During the tests phase, a first stage configuring the KMS and CS-RPP in autonomous mode will be conducted; afterwards the integrated mode to interact with the Galileo Commercial Service infrastructure will be exercised.

DISCLAIMER

The information appearing in this document has been prepared in the context of a R&D project, representing solely author's views. The solutions proposed will not necessarily be included in future Galileo operational services.

ACKNOWLEDGMENTS

We would like to thank all the people working in the NACSET team specially P. Thomas and G. Vecchione.

REFERENCES

[1] MTi User Manual, Document MT0605P, Revision J, 17 , 2017-08-14

[2] Quantum SA.45s CSAC data sheet. http://www.microsemi.com/products/timing-synchronization-systems/embedded-timing-solutions/components/sa-45s-chip-scale-atomic-clock

[3] E. Dominguez, J. M. Lopez-Almansa, G. Seco-Granados, J. A. Lopez-Salcedo, D. Egea-Roca, E. Aguado, D. Lowe, D. Naberezhnykh, F. Dovis, J. P. Boyero, "*Multi-Antenna Techniques for NLOS and Spoofing Detection Using Vehicular Real Signal Captures in Urban and Road Environments*", Proc. ION GNSS+, Sep 17 2015

[4] Akos, Dennis M., "*Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)*", NAVIGATION, Journal of The Institute of Navigation, Vol. 59, No. 4, Winter 2012, pp. 281-290.

[5] T. Krawinkel and S. Schön, "*Benefits of Chip Scale Atomic Clocks in GNSS Applications*" in Proceedings of ION GNSS+ 2015, the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation, Tampa, Florida, Sept. 14–18, 2015, pp. 2867–2874.

[6] I. Fernández-Hernández and G. Seco-Granados, "*Galileo NMA Signal Unpredictability and Anti-Replay Protection*" in ICL GNSS 2016.

[7] Todd E. Humphreys, "*Detection strategy for cryptographic gnss antispoofing*," Aerospace and Electronic Systems, IEEE Transactions on, vol. 49, no. 2, pp. 1073–1090, 2013.

[8] Christoph Günther, "*A survey of spoofing and counter-measures*," Navigation, vol. 61, no. 3, pp. 159–177, 2014.

[9] M. L. Psiaki and T. E. Humphreys, "*GNSS Spoofing and Detection,*" in Proceedings of the IEEE, vol. 104, no. 6, pp. 1258-1270, June 2016.

[10] C. Jekeli. "*Inertial navigation systems with geodetic applications*". De Gruyter, 2001

[11] Ignacio Fernández-Hernández, Vincent Rijmen, Gonzalo Seco-Granados, Javier Simon, Irma Rodríguez, and J David Calle, "*A navigation message authentication proposal for the galileo open service*," Navigation, vol. 63, no. 1, pp. 85–102, 2016.

[12] O. Pozzobon, C. Sarto, A. Dalla Chiara, A. Pozzobon, G. Gamba, QASCOM, Italy; M. Crisci, R.T. Ioannides, European Space Agency (ESA) "*Developing a GNSS Position and Timing Authentication Testbed GNSS Vulnerability and Mitigation Techniques*", InsideGNSS, January 2013.