FINAL REPORT

NACSET

Prepared by:	S. Cancela (GMV)
Approved by:	D. Calle (GMV)
Authorized by:	D. Calle (GMV)

Code:	NACSET-GMV-D1300
Version:	1.1
Date:	13/12/2019
Internal code:	GMV 24521/19 V2/19

DOCUMENT STATUS SHEET

Version	Date	Pages	Changes
1.0	25/11/2019	29	First version of the Final report prepared for the project closure milestone.
1.1	13/12/2019	29	Revision of the document implementing the RIDs raised at the FR: - NACSET-FR-RID-1: Phrase reworded on section 3. - NACSET-FR-RID-2. Typo corrected on section 3. - NACSET-FR-RID-3: Phrase reworded on section 4.1. - NACSET-FR-RID-11: Typo corrected in section 4.3.2. - NACSET-FR-RID-12: Added False alarms reference for the anti-replay in section 4.3.2. - NACSET-FR-RID-13,14 and 15: Added quantitative results to support the anti-spoofing techniques conclusions in section 4.3.2. - NACSET-FR-RID-16: Removed plot in section 4.3.2.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

1. INTRODUCTION

1.1. PURPOSE

The Final Report of the Navigation Authentication through Commercial Service Enhanced Terminals (hereinafter called NACSET) summarises the results of the work carried out by the NACSET consortium to develop, test end experiment a Commercial Service Resilient PVT Platform.

1.2. DEFINITIONS AND ACRONYMS

1.2.1. DEFINITIONS

Concepts and terms used in this document and needing a definition are included in the following table:

Table 1-1 Definitions

Concept / Term	Definition

1.2.2. ACRONYMS

Acronyms used in this document and needing a definition are included in the following table:

Table 1-2 Acronyms

Acronym	Definition
AALECS	Authentic and Accurate Location Experimentation with the Commercial Service
AC	Authentication Client
AGC	Automatic Gain Control
AT	Analysis Tool
CA	Certificate Authority
CCSIM	Control Centre Simulator
CCSIM-AS	Control Centre Simulator Authentication Server
CCSIM-KM	Control Centre Simulator Key Manager
COTS	Commercial Off The Shelf
CS	Commercial Service
CSAC	Chip Scale Atomic Clock
CSP	Commercial Service Provider
CSS	Chip Spreading Sequence
CS-RPP	CS Resilient PVT Platform
CSV	Comma-Separated values
DM	Data Manager
FTP	File Transfer Protocol
GMS	Ground Mission Segment
GNSS	Global Navigation Satellite System
GSC	GNSS Service Centre
GSS	Galileo Sensor Station
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
ICD	Interface Control Document
IF	Intermediate Frequency
IMU	Inertial Measurement Unit
IP	Internet Protocol
IRD	Interface Requirements Document
ITT	Invitation To Tender
JRC	Joint Research Centre

Acronym	Definition
KMS	Key Management System
KPI	Key Performance Indicator
MAC	Message Authentication Code
NAVSEC	Navigation Security
NMEA	National Marine Electronics Association
NTP	Network Time Protocol
OS	Open Service
OSNMA	OS Navigation Message Authentication
OTAR	Over The Air Rekeying
PFC	Pass-Fail Criteria
PKI	Public Key Infrastructure
PNG	Portable Network Graphics
PTB	CS Provider Test Bed
PVT	Position Velocity Time
PVTE	PVT Engine
RTCM	The Radio Technical Commission for Maritime Services
RxM	Receiver module
SAS	Synchronisation and Authentication Server
SCER	Security Code Estimation and Replay
SG	Signal Generator
SHA	Secure Hash Algorithm
SIS	Signal In Space
SRD	System Requirements Document
TBC	To Be Confirmed
TBD	To Be Defined
TESLA	Timed Efficient Stream Loss-tolerant Authentication
TS	Threat Simulator
TTFF	Time To First Fix
TTFAF	Time To First Authenticated Fix
UT	User Terminal
WSI	Web Server Interface

2. REFERENCES

2.1. APPLICABLE DOCUMENTS

The following documents, of the exact issue shown, form part of this document to the extent specified herein. Applicable documents are those referenced in the Contract or approved by the Approval Authority. They are referenced in this document in the form [AD.X]:

Table 2-1: Applicable Documents

Ref.	Title	Code	Version	Date
[ITT]	GALILEO COMMERCIAL SERVICE ENHANCEMENTS Invitation to Tender – Call for tenders No 555/PP/GRO/RCH/15/8382	555/PP/GRO/RCH/15/8382	-	24 May, 2016
[TS]	GALILEO COMMERCIAL SERVICE ENHANCEMENTS Tender Specifications	Call For Tender No 555/PP/GRO/RCH/15/8382	-	24 May, 2016
[CNTR]	SERVICE CONTRACT CONTRACT NUMBER – 555/PP/GRO/RCH/15/8382 for the provision of "Galileo Commercial Service Enhancements"	Contract number: 555/PP/GRO/RCH/15/8382	-	24 May, 2016

2.2. REFERENCE DOCUMENTS

The following documents, although not part of this document, amplify or clarify its contents. Reference documents are those not applicable and referenced within this document. They are referenced in this document in the form [RD.X]:

Table 2-2: Reference Documents

Ref.	Title	Code	Version	Date
[RD.1]	KMS Requirements Document	NACSET-CGI-D2100	2.1	20 Sep 2017
[RD.2]	KMS Test Plan	NACSET-CGI-D2300	1.1	27 Jul 2018
[RD.3]	KMS Experimentation Plan	NACSET-CGI-D2500	1.1	19 Dec 2018
[RD.4]	KMS Experimentation Report	NACSET-CGI-D2700	1.0	17 May 2019
[RD.5]	CS-RPP System Requirements Document	NACSET-GMV-D3310	1.5	31 Dec 2018
[RD.6]	CS-RPP Experimentation Plan	NACSET-QASCOM-D4110	1.1	2 Jul 2019
[RD.7]	CS-RPP Experimentation File	NACSET-QASCOM-D4120	1.0	25 Nov 2019
[RD.8]	I. Fernández-Hernández y G. Seco-Granados, «Galileo NMA Signal Unpredictability and Anti-Replay Protection,» *ICL-GNSS,* 2016	-	-	-
[RD.9]	G. Seco-Granados, D. Gomez-Casco y I. Fernández-Hernández, «Detection of Replay Attacks to GNSS based on Partial Correlations and Authentication Data Unpredictability,» in preparation for GPS Solutions.	-	-	-

3. EXECUTIVE SUMMARY

The Galileo infrastructure is in continuous evolution to develop and deploy all the necessary elements and functionalities for the provision of the planned Galileo services. The Navigation Authentication through Commercial Service-Enhanced Terminals (NACSET) project was launched aiming at evaluating and testing different techniques to improve the resilience and security of the overall system and in particular on the user segment.

The NACSET project is introduced in the CS development strategy pursuing the following objectives:

- Develop an end-to-end key management simulator and experiment to understand the challenges and complexity inherent to secure key management and distribution (KMS), including NavSec and OSNMA keys.
- Development of a resilient navigation platform (CS-RPP) with improved anti-attack techniques based on different assisted solutions i.e. assisted navigation message and signal authentication, time synchronization, external sensors. The CS-RPP includes a user terminal (UT) consisting on a resilient GNSS client able to perform attack detection, and calculate resilient PVT solutions making use of different data and signals sources.
- Support the provision of a prototype Synchronisation and Authentication Service (SAS) to external users based on the aforementioned platform.
- Carry out research on aspects related to the Galileo CS which have not been covered by previous activities, aiming to obtain valuable evidences and conclusions to contribute to the definition of future evolutions of the service.
- This section summarizes the main outcomes of the NACSET project related to the mentioned objectives:
- **Key Management**: the Key Management Simulator (KMS) implements secure key distribution algorithms both for CS and OSNMA. The platform is able to work in autonomous mode, simulating all the relevant parts of the Galileo infrastructure involved in the key management process, from the GMS and GSC elements to the user segment. In addition the KMS can be integrated with the Galileo elements, as it has implemented all the necessary interfaces (with the CSP-GSC, GSC-GMS, CSP- CS Users and GSC-OS Users) aligned with the official ones. The main features of the KMS are:
  - A binary group key distribution model was selected to simulate the CS key distribution. For the OSNMA, the ICD version 1.0 was implemented regarding both TESLA key and public key management. In addition, secure protocols have been used for the implementation of the interfaces between the key management platform and the users, this include SSH handshakes, Certificate Authorities, etc. For the details of these algorithms, please refer to [RD.1].
  - An experimentation campaign was performed using the KMS in autonomous mode simulating different kind of scenarios to evaluate the suitability of the selected key management solutions for the CS. Through the experimentation and assessments exercised, the selected key management engineering solution is concluded to be an effective solution meeting considering the security needs for the provision of the Galileo Commercial Service. The assessments have identified some possible configuration demands and codes of practice that could strengthen the architecture of the system. The detailed results of the experimentation campaign are included in the KMS Experimentation File [RD.4].
  - An experimentation campaign was performed using the KMS in autonomous mode simulating different kind of scenarios to test a range of configurations of OSNMA and the use of the OSNMA keys for the SAS related authentication techniques. It has outlined that the asymmetric OSNMA key model also meets expected security targets. However, the TESLA chain delivery approach, designated for the SAS essentially, may need some additional security considerations if / when it is extended for use in a real service environment. The detailed results of the experimentation campaign are included in the KMS Experimentation File [RD.4].
- **Anti-Spoofing/Authentication techniques:** 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 to implement several signal and data authentication solutions. In addition, the UT implements additional standalone anti-spoofing techniques.
- The UT element is the component part of the system aiming at providing the signal processing capabilities and exercising the defined standalone and assisted PVT protection techniques. The SIS interface is provided by a multiGNSS and multi-antenna receiver, whereas the PVT resilience will be achieved by using the authentication properties of the Galileo SIS signals (SCE, future NMA, unpredictable bits…) together with the innovative features as the angle-of-arrival detection thanks to multiple antennas, body-frame motion

using an accurate IMU, CSAC clock, AGC monitoring and secure real-time communication with the SAS which provides assisted authentication services. The following conclusions have been derived from the development and the experimentation results:

Table 3-1: Summary of the CS-RPP resilient techniques

Technique	Description	Advantages	Disadvantages
Remote Processing 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.	Trajectory spoofing is optimally detected. Not needed NAVSEC keys at UT to take advantage of the E6 encrypted signals.	Not autonomous, needs an external service. Bi-directional communication with users. Not able to detect timing spoofing
Cheap Spreading Sequences (CSS)	In this technique, the SAS computes a small part of the sequence, called Chip Spreading Sequence (CSS), for a particular time and transmits it to a remote receiver (the UT). 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 or not authentic.	Not needed NAVSEC keys at UT to take advantage of the E6 encrypted signals. Good performances detecting spoofing.	Latency on the reception of the CSS is critical for the system. Not practical to provide service for many users.
Re-encrypted CSS	This technique updates the traditional CSS scheme using encrypted batches of CSS sequences, protected using the keys derived by the TESLA chain. Specifically, the module retrieves an encrypted version of a given CSS (or a batch); and once the proper TESLA key is available in the SIS, the original CSS can be decrypted and loaded in the receiver to perform the CSS correlation.	Good performances detecting spoofing. Not needed NAVSEC keys at UT to take advantage of the E6 encrypted signals. Can store long batches of CSS without compromising the system. Compatible with OSNMA service.	Latency increased by the decoding of the TESLA keys from the SIS. Service availability depends on the Open Service (OSNMA).
CSAC monitoring	When using the CSAC as clock source, the receiver time will maintain a very exact shift with respect to the real system time computed in the PVT. The algorithm monitors each new PVT computation to check that the computed time maintains a continuous and consistent difference and evolution.	Very good performance to detect attacks when the receiver is tracking first the real signal. Autonomous technique, only needs the PVT computation.	Difficult to detect an attack in cold start conditions. CSAC are not available in standard receivers.
AGC monitoring	The AGC module monitors the Automatic Gain Control value to discriminate anomalous power jumps that indicate the possible intervention of a spoofing signal.	Fast at detecting different kind of attacks Simple to be implemented	Difficult to detect very complex attacks
Anti-replay detection	Anti-replay solution is mainly designed to address zero-delay SCER	It is able to detect optimally very complex	Depends on OSNMA performances, without

	(Security Code estimation and replay) attacks. This is a type of replay attack where an attacker estimates and rebroadcasts the original signal with a zero or almost negligible delay, taking control of the tracking loops and gradually modifying the signal. The NACSET terminal implements a method that takes advantage of the existence of unpredictable bits and symbols in the navigation thanks to NMA cryptographic information provided through the SIS. In order to conduct a zero-delay SCER attack on a signal containing NMA data, the attacker shall predict the unknown symbols with minimal or none information. The technique is based on the analysis of the signal correlation loss caused by the imperfect estimation of the signal chips corresponding to the mentioned unpredictable symbols.	attacks like the zero-delay attacks. Provide signal replay protection without encrypting the signal. Compatible with OSNMA service. Does not degrade significantly in degraded environments.	data authentication the scheme will not work. Need to be used with other techniques to detect simple attacks. Only focused on zero-delay attacks.
Dual antenna	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 double differences between antennas. 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.	Very powerful technique to detect all kind of attacks as the spoofer is probably using only one source for signal transmission GPS+GAL compatible.	Needs at least two antennas separated less than the wavelength. If several spoofers are used, the attack will not be detected
IMU hybridization	The UT is able to process the GNSS and IMU information in a tightly-couple approach. A PVT with IMU data is compared with a GNSS-only data to detect spoofing attacks that modify the user position.	Able to detect attacks even in cold start conditions. Autonomous technique.	The tightly couple approach may not be the most optimal to detect spoofing attacks. Attacks were the trajectory is modified progressively in small steps are difficult to detect.

4. MAIN OUTCOMES

4.1. COMMERCIAL SERVICE RESILIENT PVT PLATFORM (CS-RPP) DEVELOPMENT

The Galileo CS Resilient PVT Platform (CS-RPP) is a system focused on analysing and demonstrating different attack detection techniques. These techniques shall make use of the different equipment available in the system. The techniques work either in standalone mode or exploiting assisted services, which are suitable to be implemented in the near future by the GNSS system or by external service providers.

The following objective were identified for the CS-RPP platform:

- 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 as well as nominal and under-attack conditions.

The following figure describes the part of the NACSET platform inside the Galileo infrastructure:

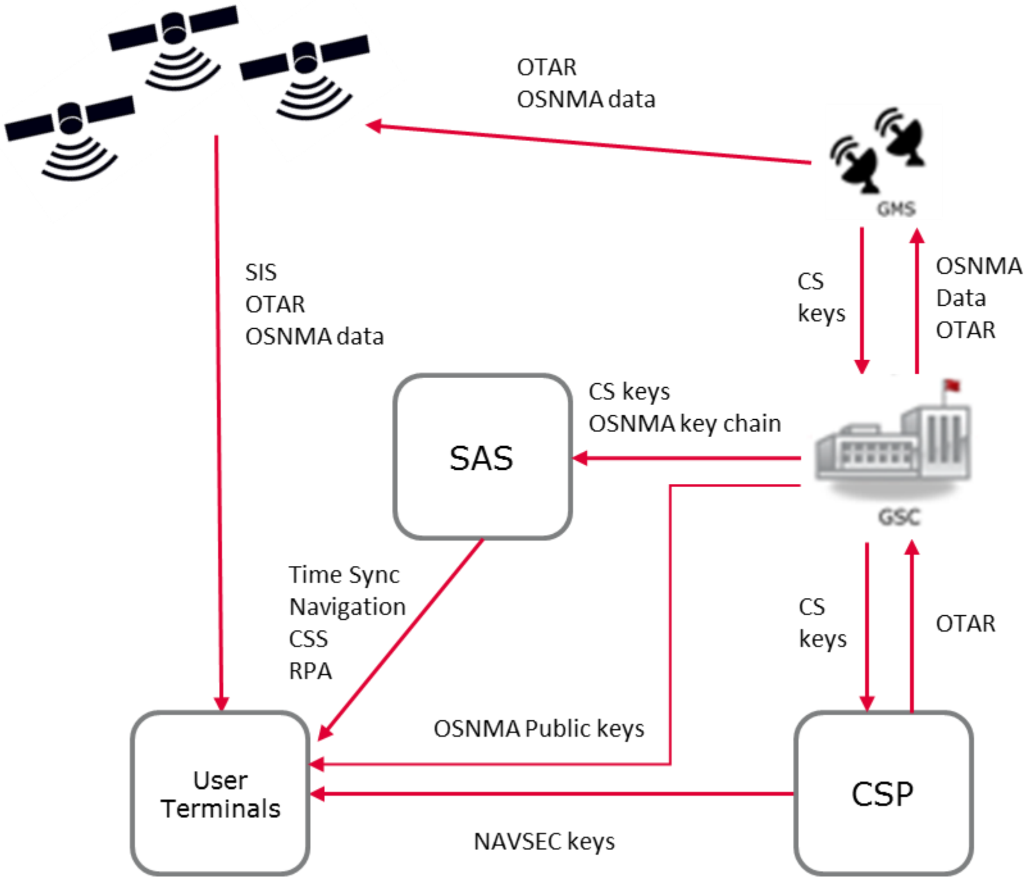


Figure 4-1: Real Galileo infrastructure

In the NACSET platform all the key management related interfaces are simulated by the KMS which can simulate both the CSPs and the Galileo system (i.e. the GSC and GMS).

The GNSS signals are simulated with the SG and AALECS PTB is used to generate GNSS data contained OSNMA data if needed.

Also, the NACSET platform includes a special CSP independent from the KMS that will act as a Synchronization and Authentication Server and may interface directly with the GSC (both simulated by the KMS or the real instance).

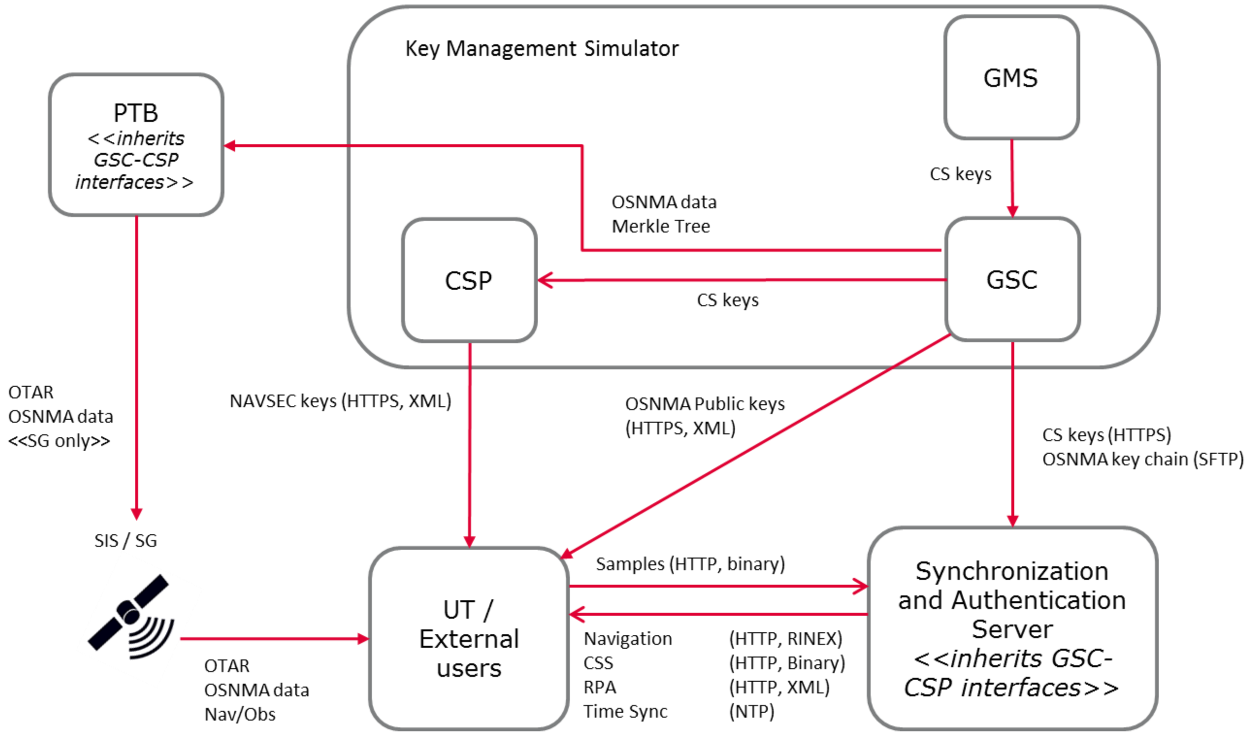


Figure 4-2: CS-RPP Architecture Overview

As described in Figure 4-2, the CS Enhancements platform is composed of the following elements:

- **Galileo CS Resilient PVT Platform (CS-RPP):** A GNSS-based navigation platform resilient to malicious attacks. Resilience will be achieved through the use of the Galileo SIS and its authentication features, and the inclusion of receiver-based sensors and real-time client-server authentication and synchronisation architectures. The CS-RPP is built upon the following elements:
  - **User Terminal (UT):** This element will incorporate a GNSS receiver, signal attack detectors and other technologies, including a real-time communication with a remote server providing authentication services (the SAS), to provide resilient PVT services. The UT is also configurable to obtain the PVT height from an external source.
  - **Synchronization and Authentication Server (SAS):** This element will allow the support of client-server PVT authentication protocols, including time synchronisation, remote data authentication, and remote signal authentication.
  - **Key Management Simulator (KMS):** An end-to-end key management simulator to understand and evaluate the challenges and complexity inherent to secure key management and distribution (NavSec and OS Authentication keys).
- **CS Signal Generator and Threat Simulator (SG):** A platform able to generate Galileo signals including E6 CS signals, and allowing the testing of a receiver under different user conditions and threats. The chosen signal generator must be able to simulate complex threats and must be compliant with cost efficiency and schedule requirements.

- **Performance Analysis Tools:** A set of performance analysis shall be part of the platform to extract the necessary information and metrics to evaluate the impact of the implemented techniques.

The CS-RPP UT and SAS are able to interact with the Key Management Simulator (KMS) developed in the project, or the GSC whether the interface is available. The CS-RPP UT also is able to interact with the CSPs if available. Both elements will provide cryptography information to exploit the Galileo OSNMA service, and to allow the receiver to track the CS signals when the Spreading Code Encryption (SCE) capability is enabled.

4.1.1. KEY MANAGEMENT SIMULATOR (KMS)

The Key Management Simulator, (KMS), is an aspect of the NACSET program (Navigation Authentication through Commercial Service Enhanced Terminals), targeted to provide and simulate a cryptographic security model solution deemed necessary to support the Galileo Commercial and Open Services. The KMS solution has been designed to propose an architecture pertaining to:

- **The distribution model for CS NAVSEC keys** amongst the Galileo Commercial Service users. A CS NAVSEC is a key that provides the spreading encryption used to protect the Galileo Commercial Service. Without knowledge of the current symmetric CS NAVSEC key used for broadcast, the user is not be able to decrypt the commercial service signals broadcast from the Galileo Satellite constellation. The CS NAVSEC key is uniformly used by all Galileo Satellites providing the commercial service and is used to address the entire user population under a singular encryption. The CS NAVSEC key is expected to be renewed for use upon the service on a frequent basis (approximately every week). User knowledge of the CS NAVSEC key shall ultimately dictate the users' access to the service and shall therefore be the GNSS's / CSPs' point of control for restricting service to users.
- The OSNMA signing and distribution management model for **OSNMA public keys** amongst the Galileo open service community users requiring navigation message authentication. An OSNMA public key is a public part of an asymmetric key pair used to authenticate navigation messages broadcast within the Galileo open service.

For full details of the NACSET key management architecture, please consult [RD.1].

In order to complement the proposed key management architecture design, the KMS solution consists of a supporting platform to simulate the proposed architecture and model all its exposed interfaces providing a platform that may be used as a test bed for the integration of end solutions satisfying each entity in the definitive key management architecture.

The NACSET KMS solution consists of multiple simulation components representing real world elements in the expected Galileo Commercial Service / Open Service key management model. The simulation is managed and modelled by a central KMS Simulation Management and Monitoring Tool.

The simulation components and sub-components provided as part of the KMS simulation platform comply with the cryptographic scoped interface protocols. This architecture allows both interaction between the simulation components and substitution integration of external component into the simulation realising some of the key management concepts.

4.1.2. SYNCHRONIZATION AND AUTHENTICATION SERVER (SAS)

The Synchronisation and Authentication Server (SAS) is intended to support the client-server PVT authentication protocols. The SAS will embed the following three main functionalities:

- **Time Synchronization:** it implements accurate and authenticated time synchronization protocols to provide timing service to the UT or other external users by means of a NTP server. The time synchronization feature was initially meant to provide a trusted and accurate (about 1 us or below) time source to the clients. In this configuration, the SAS acts as a server, and the PTP protocol was initially considered the solution to be implemented. The viability analysis later executed pointed out that several issues interfere with the possibility of implementing the service using PTP protocol:
  - Need of specific hardware both at server and receiver side;
  - No redundancy and consequent risk of continuity breaks in the synchronization service
  - Poor synchronization performance when used through the Internet.

  - For these major reasons, the NTP service was selected as alternative solution.

- **Remote Data Authentication:** this functionality provides trusted Navigation Message (independently from the SIS NMA) via an aiding channel. For this purpose, a COTS receiver is incorporated in the SAS that serves as trusted source of the navigation message.
- **Remote Signal Authentication** that supports two main assisted authentication modes:
  - The provision to the UT of chip synchronisation sequences containing cryptographic features to the UT (allowing to calculate an authentic PVT). Those sequences can also be encrypted using the TESLA OSNMA keys (or derived ones) that shall be retrieved from the KMS module.
  - The processing of signal samples received from the UT (Galileo E6B/C) and calculate a PVT with them, by using the navigation data extracted from an external – trusted – source.

Figure 4-3 shows the high-level components of the SAS:

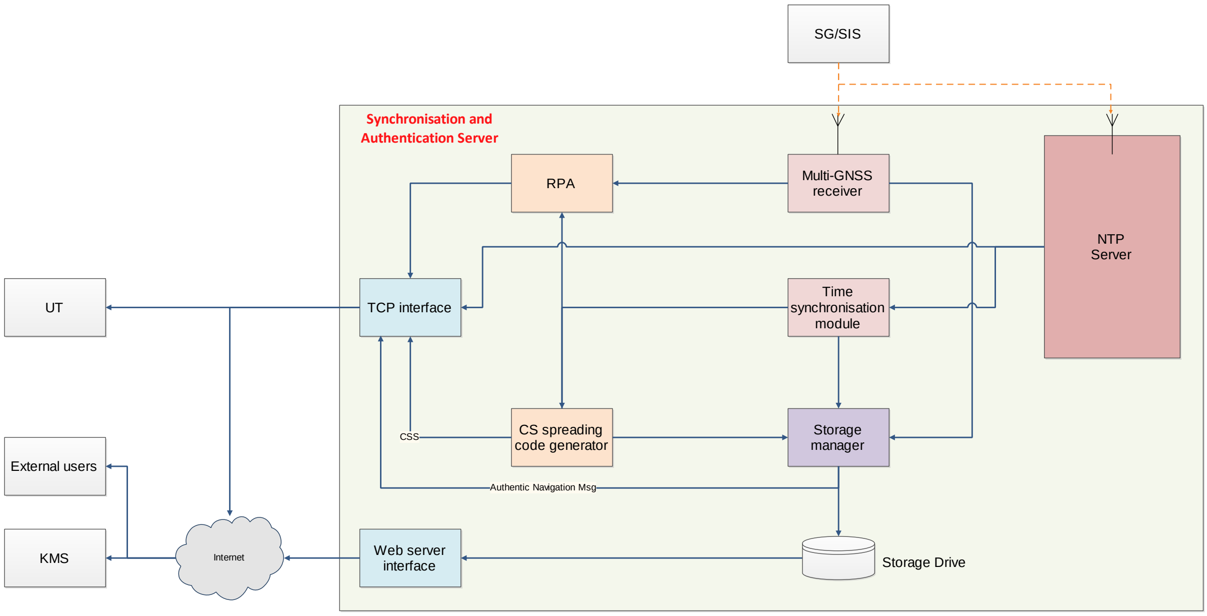


Figure 4-3: SAS high-level architecture with COTS time synchronisation server

- The architecture of the SAS is the following:
- The **SAS TCP interface (TCP-I)** is responsible for the data provision/acquisition to/from the other modules of the test-bed and external services. All the modules report to the external interface for making available all the information necessary for authentication;
- The **Multi-GNSS receiver** is in charge of decoding the navigation messages from the signal in space and providing time reference for time synchronisation in case of embedded time synchronisation server;
- The **Galileo E6 code generator (SCG)** is responsible of receiving the NAVSEC and generating the E6 Galileo CS spreading codes; it provides the spreading codes to the RPA and to the TCP-I for the UT;
- The **Remote Processing Authentication (RPA)** is responsible for the E6 PVT computation given the samples gathered at the receiver side; the modules need the authentic navigation messages either from the Multi-GNSS receiver or external source and the Galileo E6 spreading codes from the code generator;
- The **Time synchronisation (TS)** module is an NTP server itself;
- The **COTS time server** module is responsible for getting real time reference from the GNSS signal and provide it to the SAS machine;
- The **Storage manager (SM)** module is responsible for the storage on a local drive of the NAVSEC keys and the authentic navigation messages;
- The **Storage drive (SD)** contains all the information that are useful for the SAS operation and that have to be published;

- The **Web Server Interface (WSI)** is responsible for managing the requests of published data from external users.

4.1.3. USER TERMINAL (UT)

The NACSET User Terminal (UT) element is the component part of the system aiming at providing the signal processing capabilities and exercising the defined standalone and assisted authentication and PVT solutions.

The SIS interface is provided by a multiGNSS and multi-antenna receiver, whereas the PVT resilience is achieved by using the authentication properties of the Galileo SIS signals (SCE, future NMA, unpredictable bits…) together with the innovative features as the angle-of-arrival detection thanks to multiple antennas, body-frame motion using an accurate IMU, assisted trusted time reference and secure real-time communication with the SAS which provides assisted authentication services.

The UT consists of 3 main parts, as is shown on the

Figure 4-4: UT Overview

:

- Receiver Module (RxM)
- Authentication Engine (AE)
- PVT Engine (PVT-E)

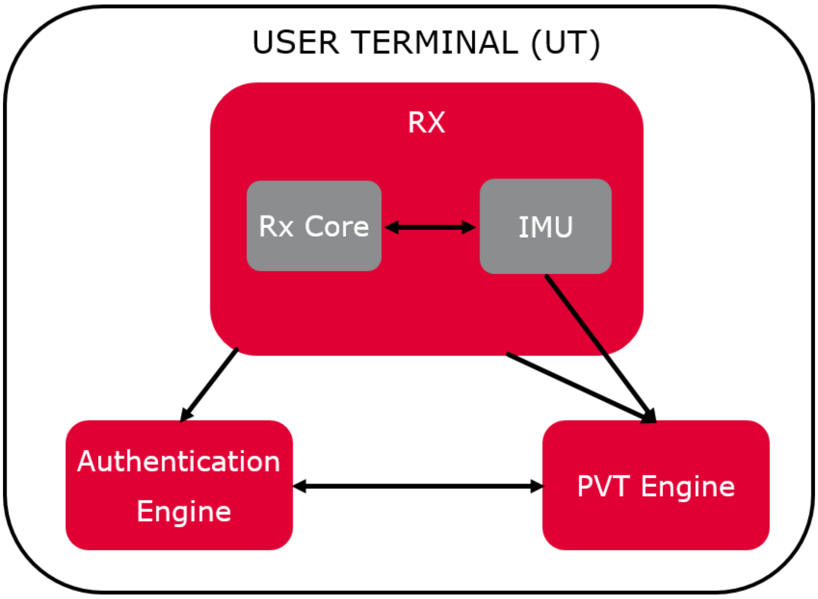


Figure 4-4: UT Overview

The RxM main objective is to provide GNSS satellite signal observations, navigation message data, IF signal samples, IMU data and other kinds of information. In order to do that, RxM acquires and tracks GNSS satellite signals, processes the data received from them, and collects some extra data from various sensors (e.g. IMU). The RxM shall be capable of receiving the signal authentication keys from the AE in order to be able to track the encrypted signal.

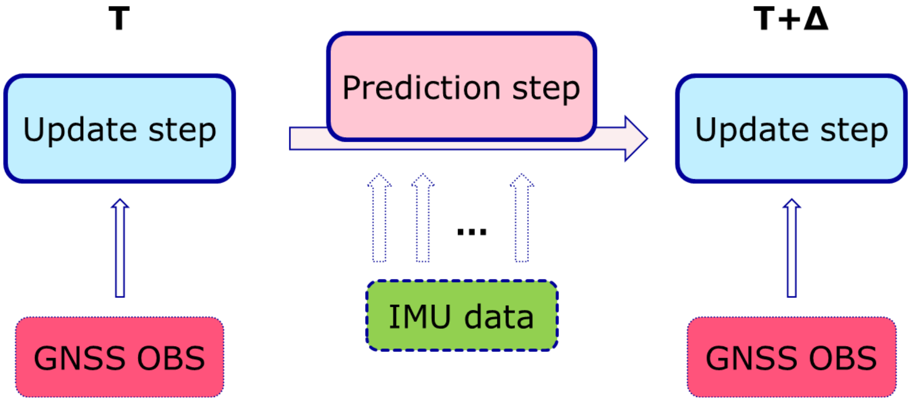
The AE main objective is to manage all the authentication aspects of the UT. It is responsible for the communication with Synchronisation and Authentication Server (SAS) for the remote authentication techniques. Moreover, it gathers the outputs of all the anti-spoofing techniques and metrics and supports the PVT-E with the authentication information available.

The PVT-E main objective is to compute a resilient PVT solution with different configurations and inputs. In order to achieve this goal, the PVT-E shall be able to receive GNSS measurements and navigation data from the GNSS receiver, and authentication information (authentication status and spoofing indicators) from the

Authentication Engine (AE). An Assistance Sever (SAS) shall also provide the possibility to retrieve trusted navigation information to be used in the PVT calculation.

The following techniques have neem implemented in the UT:

- **Dual Antenna Spoofing Detector:** autonomous module for spoofing detection based on carrier phase double differences. The use of multiple antennas on the same receiver allows to detect the Angle of Arrival (AoA) of the received signals by using the carrier phase (CP) differences between antennas. Taking into account that when the GNSS signals are being spoofed they will arrive to the receiver with an angle different from the expected one and that the signals spoofed by the same transmitter arrive to the receiver with the same angle, the carrier phase differences can be employed to detect if the receiver is under a spoofing attack. When a receiver is spoofed by one single source all the signals will arrive from the same direction and in such situation the carrier phase single differences for all the satellites will have similar values at baseline, so the presence of a spoofer can be detected by comparing the CP Single Differences (SD) between satellites, which is the same as making CP Double Differences (DD) between satellites. A satellite is selected as a pivot, and the CP DD are calculated between the pivot and the rest of satellites in view. Then, a different satellite is selected as a pivot and CP DD calculated again. This process is done on every epoch. If values of CP DD are below a threshold then both satellites are considered to arrive from the same direction. In order to evaluate if one satellite is being spoofed, the number of satellites coming from the same direction as the satellite under analysis is checked and if it is above certain percentage of the total satellites then it is considered to be potentially spoofed. If, after checking all the satellites, more than a certain percentage are marked as spoofed then the spoofing flag is raised at that epoch. Also, several consecutive epochs must satisfy this condition in order to avoid false positives. An epoch window can be defined with a certain size so a certain number of epochs in that interval must be spoofed before raising the spoofing alarm.
- **IMU Spoofing Detector:** The IMU processing is carried on by the implementation of a tightly coupled Kalman filter. It uses IMU data to complete the prediction step



Then, both a GNSS-only and the IMU-assisted solutions are compared and monitored to detect and attack.

- **CSAC Spoofing Detector:** When using the CSAC as clock source, the receiver time maintains a very exact shift with respect to the real system time computed in the PVT. The algorithm monitors each new PVT computation to check that the computed time maintains a continuous and consistent difference and evolution.
- **AGC Spoofing detector:** a module for spoofing detection based on the monitoring of the ACG values, also combining the CN0 measurements. The analogue 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. These losses depend on a number of factors including the ADC's maximum quantization threshold (L) the number of bits utilized and the acquired signal standard deviation (σ). 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. Since the power of the signal transmitted by the satellite is roughly constant with a

determined range (based on elevation), the primary role of the AGC is to adjust to different active antenna gain values. 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.

- **CSS authentication:** Two different versions has been implemented for the chip spreading sequences, one in plain format and another in encrypted format:
  - In this approach, it is assumed that the receiver can track an open signal (for example the E6B) and an encrypted signal (for example the E6C). The authentication concept is based on the fact that if the receiver is tracking an open signal, in the same code offset and phase there should be a corresponding encrypted sequence, which is unknown to potential attackers. According to this approach, the AS computes a small part of the sequence, called Chip Spreading Sequence (CSS), for a particular time and transmits it remotely to the receiver. The receiver then attempts to correlate the SAS with the received signal: if a correlation peak is observed over a predetermined threshold, the signal can be considered authentic, otherwise it is considered as spoofed. The CSS is generated by the SAS using the NAVSEC keys, therefore no keys are required on the receiver. The only way for an attacker to generate CSSs would be to obtain them from space. This would result in a meaconing attack, and the attacker would be forced to introduce a delay, that can be detected at receiver.
  - The module also implements this authentication scheme using the re-encrypted version of the CSS sequence, using keys derived by the TESLA chain. Specifically, the module retrieves an encrypted version of a given CSS; once the proper TESLA key is available in the SIS, the original CSS can be constructed and loaded in the receiver for performing the correlation at its applicability time. The decryption keys are delivered in the SIS, as a hashed version of an OSNMA key. Specifically, considering an encrypted CSS sequence with time of applicability T, the corresponding OSNMA key is the last one available before T. Once the OSNMA key is available, the module performs the hashing to obtain the decryption key and then reconstruct the CSS sequence; this approach prevents the diffusion of the TESLA chain in the SAS server.
- **RPA authentication:** In this technique, a small RF signal sample of the E6 encrypted signal is acquired by the RXP at a certain position and time and is transmitted to the AS, which attempts to verify the position and time obtained by E1 with the E6 signal received at that position and time. To do this, first a check is done on the acquisition correlation peak with respect to a correlation authentication threshold. The E6 computation is done by means of ephemeris safely received by the SAS. The coherency between the E1 PVT computed at the receiver and the E6 computed by the SAS is done. Hence, the UT does neither need to know the NAVSEC keys, nor to have a security module for their storage. It only requires an E6 front-end in addition to standard E1 positioning hardware and software processing. The 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. The algorithm uses as input the E1 position and time, and it generates the corresponding encrypted channels that should have been travelling at that time and location.
- **Anti-replay:** If a GNSS signal stream contains data that is authenticated, a spoofer can only alter the pseudorange measurements to spoof the receiver position. This attack falls under the category of signal replay attacks. In order to protect pseudoranges from replay attacks, the pseudoranges can include authentication features. Ideally, these authentication features can be implemented at spreading-code level. However, if the data modulated includes unpredictable symbols, this unpredictability can be also exploited against replay attacks. The UT anti-replay protection is based on the unpredictability bits of NMA data present on a GNSS signal. Some cryptographic information included in the GNSS data stream is unpredictable for a real-time attacker. For this reason, an attacker has to estimate this unpredictable data. The attack assessed by this technique is a zero-delay SCER attack that consists of estimating and reproducing the original signal with zero, or negligible, delay, to take control of the tracking loop so it needs to estimate the unpredictable symbols on the fly. The NMA solution taken as reference for this implementation is the Galileo Open Service NMA (OSNMA) protocol. This service is to be included in the navigation information transmitted on the Galileo E1-B signal (I/NAV). I/NAV data is structured in frames every 750 seconds, composed by 25 subframes of 30 seconds duration each. Every subframe is divided into fifteen 2-second pages, each of which contains one word and some other fields. All the data is convolutionally encoded and interleaved, to prevent data errors. The convolutional code has a ratio of 1/2, which means that it returns twice the input data. In each of the two subpages of a 2-second page, there are 120 data bits, and at the end of this conversion function we obtain 240 encoded symbols. After adding at the beginning the 10-symbol pattern needed for synchronization, the 250 symbols are transmitted through the SIS. Every satellite has his own spreading code of 4092 bits (or chips). Each symbol transmitted is modulated by one spreading code array, which means that the 4092 modulation chips are transmitted per

symbol. While standard receivers perform continuous signal correlation, the idea behind the technique is to perform partial correlations using different subsets of the signal chips on every symbol to be able to detect the imperfect estimation in case of an attack. The high-level concept behind this technique is to detect correlation losses in the parts of the symbols the spoofer is estimating incorrectly due to the lack of information. This partial correlations are done at software level using the signal samples collected by the receiver. Two different detection metrics have been implemented from [RD.9]:

- R3 method: consists on computing the average of the difference between the beginning and end partial correlation of the symbols.
- C/N0 method: is based on using a traditional Narrowband-Wideband Power Ratio (NWPR) estimator to estimate the C/N0 values at the beginning and at the end of each symbol.

4.2. KMS EXPERIMENTATION CAMPAIGN

The NACSET KMS Simulation Solution has been tested under the scenarios and procedures defined in the KMS Test Plan and Report [RD.3]. The focus of the KMS Test Plan has been to verify the KMS simulation components compliance to requirement. The focus of this experimentation campaign is to provide an enhanced assessment of the proposed NACSET Key Management solution architecture, to reflect on its fitness for purpose and try to identify possible enhancements or practices to complement the solution.

There are two primary objectives of the experiment assessments exercised in the KMS experimentation campaign:

- To assess whether the solution satisfies the security demands, by means of assessing the solution against possible posed security threat scenarios.
- To assess the solution scalability and adaptability to meet the expected services and market demands.

4.2.1. CS KEY MANAGEMENT

In the majority of cases the KMS CS crypto distribution model facilitates a high standard of authentication and integrity on the origin of received key material when an interface is exposed. All the proposed publically accessible interfaces are covered by security protocols in this model.

The KMS crypto model in general facilitates that key material would be rejected by recipients if they cannot authenticate the integrity of its origin for all perceived critical cases.

In principle the KMS crypto architecture is strong at preventing CS key exposure, assuming that the recommended measures, (defined in [RD.1]), are put in place with regards to crypto handling practices. The KMS CS crypto solution is well modelled to defend against, and recover from, a key compromise situation.

The proposed KMS CS crypto-model solution provides effective scalability for CS receiver handling and management. With the exception of CS NAVSEC key crypto periods, most of the crypto-periods and trust allocations fall to the discretion of the business models pursued by individual CSPs. The CSPs would need to be regulated on their crypto-period and trust allocation policies, in case a relaxed policy at one CSP causes jeopardised security on another CSPs service.

4.2.2. OSNMA KEY MANAGEMENT

The OSNMA asymmetric key model is perceived to be strong at preventing private OSNMA key exposure. There may still need to be some consideration with regards to exposure of TESLA hash material if / when a TESLA hash delivery interface is truly realised. The KMS OSNMA crypto solution is reasonably modelled to defend against a key compromise situation.

Based on the performed analysis carried out against OSNMA TESLA key sizes and derivation algorithms, the SHA3-224 or SHA3-256 algorithms are recommended over the older SHA-256 algorithm because they are more finely tuned for performance, and their performance is relatively consistent, (this should also be true of the derivation carried out on the receiver side of the interface).

The key bit length using in combination with the SHA3 algorithms performs better with a short bit length (but may be consider more secure, and integral, at a long bit length). Shorter TESLA keys also reduce overhead within the OSNMA signal in space service.

Due to the rapid frequency for key change within the TESLA model, most of the security concerns are mitigated, and performance could be perceived to take precedence. Therefore, under these circumstances, a shorter key length using a SHA3 algorithm is recommended for service.

4.3. CS-RPP EXPERIMENTATION CAMPAIGN

The objective of the experimentation campaign is to be able to test the anti-spoofing techniques implemented in the CS-RPP in a controlled manner making use of real data (recorded or SIS) and simulated signals.

The CS-RPP experimentation campaign includes:

- Testing the system in nominal conditions using real SIS or simulated data.
- Testing the system under attack conditions simulating the spoofing attacks with in-lab testing. The threats to be simulated under the NACSET experimentation campaign will be the following:
    - Data bits manipulation spoofing attacks
    - Observables modification spoofing attacks
    - Spreading sequences and carrier generation attacks: SCER attack performed at sample level
    - Meaconing attacks: Record & Replay and Real Time Replica

4.3.1. EXPERIMENTATION ENVIRONMENTS

The experimentation environment includes a Signal Generator (SG) and several threat generation techniques needed to test the system capabilities.

Spirent Signal Generator

The Signal Generator (SG) is a key element of the system infrastructure. In fact, part of the in-laboratory performance analyses proposed is supported by the simulator. This is especially relevant for the first tests without integration with the Galileo infrastructure. For this purpose, the Commission offers the possibility to use two Signal Generators and a Threat Simulator that cover most of the attacks scenarios proposed in [RD.6] (except IMU simulator, multiple-RF output and SCER attacks). These Signal Generators are located at the EC Joint Research Centre (JRC) facilities at Ispra (Italy). The specific models offered are based on Spirent's GSS9000 and Spectracom GSG-6.

SCER Simulator

In order to demonstrate the functionality of the anti-replay technique, a SCER attack simulator has been developed. For this purpose, a tool able to generate both trusted and spoofed signals to simulate the attack has been implemented. The tool consists of two elements: a software module and a software-defined radio (SDR) platform. The SDR is needed to convert to RF the GNSS baseband signal data streams generated and replay it with the antenna.

The software module is in charge of simulating the zero delay SCER attack. It has two main duties, generate the "genuine" Galileo E1B signals and generate the signals needed to simulate the SCER spoofer in a realistic way. The OSNMA data is generated by means of the Commercial Service Demonstrator PTB from AALECS. The simulator can only generate the E1B signal.

In order to simulate the SCER attack the developed tool generates two signals at the same time. The first signal reproduces the real signal coming from the satellites, while the second is the spoofed signal, coming from a transmitter that tries to accomplish the attack. The simulation of the attack can be divided in three phases:

- **Phase 1**: Only the signal without spoofing is generated. The receiver tracks only this real signal.
- **Phase 2**: The spoofing signal perfectly aligned with the real signal, simulating a theoretical perfect zero delay.
- **Phase 3**: After some time, when the receiver tracks the spoofing signal, the spoofing signal starts delaying the signal to spoof the receiver position

The imperfect estimation of the symbols is simulated by modifying the sample chips on the spoofed signals. It can be complemented with different levels of signal power in the spoofer.

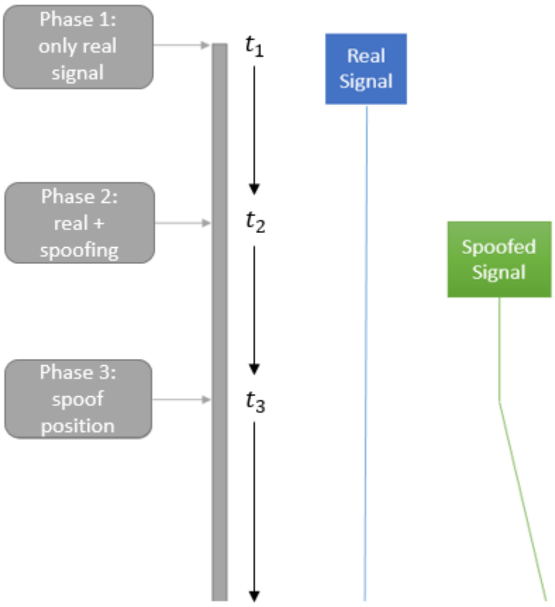


Figure 4-5: SCER attack phases

This tool can also simulate two kind of environment conditions: open sky and urban. The user and the spoofer could have different conditions in order to allow simulating three real situations:

- User in open sky and spoofer in open sky.
- User in urban and spoofer in urban. Spoofing attack accomplished in urban environment. As the signal received by the spoofer is also under urban conditions, the chip estimator of the spoofer is more prone to errors.
- User in urban and spoofer in open sky. The spoofer has better conditions than the user to get clean signal for its estimator.

4.3.2. EXPERIMENTATION RESULTS OVERVIEW

An extensive campaign has been carried out as part of the NACSET project, several results and conclusions have been obtained for every technique implemented in the platform. The techniques have been tested against spoofing attacks with the following characteristics:

- The spoofing attack starts when the receiver has already tracked the real signal.
- Once the attack starts both the spoofed and real signals present for the receiver.
- The power of the spoofed signal is greater than the real signal.

The following conclusions have been derived from each technique:

- **Dual Antenna Spoofing Detector:** In order to test the Dual-Antenna module, Signal-in-Space and a simulated signal from Signal-Generator are required. In Figure 4-6 the test setup is presented.

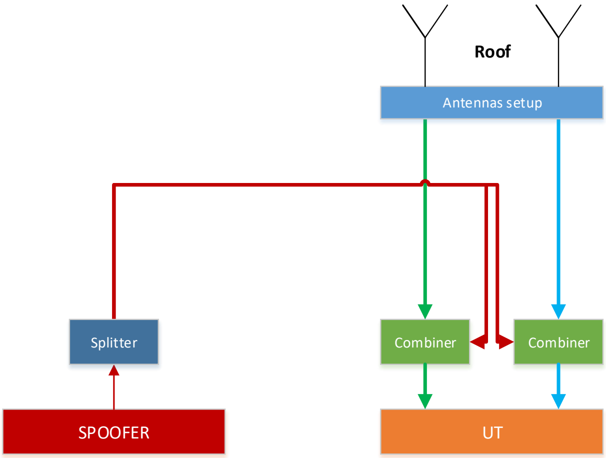


Figure 4-6 Dual Antenna Scheme

The spoofing signal is conducted and the phase difference between the two paths is the same for all the satellites, because they all come from the same source, with no geometrical diversity. Conversely, the signals coming from the SIS is naturally characterized by spatial difference. The spoofed signal has +6dB power advantage over the real signal. The probability of false alarm was 0% during all the tests and the attacks were detected always when the receiver was able to track all the required satellites. A 93.27% of spoofing detection probability has been measured over 10 test execution.

- **IMU Spoofing Detector:** Because the SG is not able to simulate the IMU data the following approach has been used to test the IMU: A previous recording is done a i to store the IMU data. Then the trajectory + the navigation data recorded during the trajectory is used in the SG to generate the scenario including the spoofing attack.

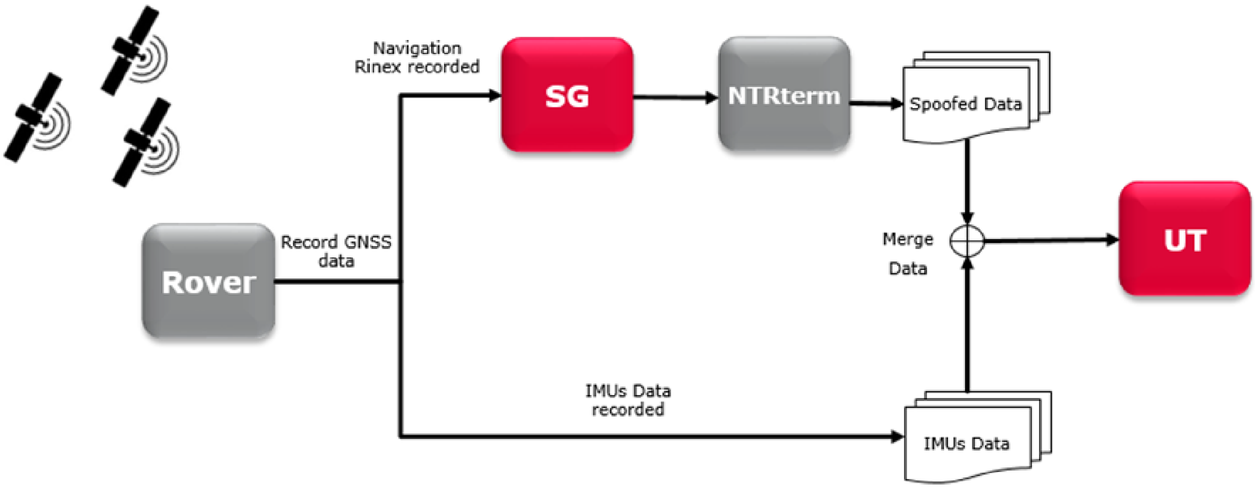


Figure 4-7 : NTRTerm Sync approach

The SG setup is the same as the nominal setup but the simulation of the IMU is done by the UT replay mechanism (NTRTerm) after generating the data to be replayed with the SG. The simulated attack consists on three phases. First, it simulates a static position with a power increasing rate of 0.4dB/s. Then, after achieving +6dB of advantage, it simulates a constant acceleration of (a_e; a_n; a_u) = (0.0; 1.8; 0.0) [m/s^2]. Finnaly, it remains in constant velocity of 9m/s. The attack was detected in the test but, as the attack simulated was just gradually modifying the position, the shift in the position is not detected at the beginning as it is masked by the position error noise. This can be seen in the values of spoofing detecting probability (56.62 %) and probability of false alarm (4.84 %). When the difference between the IMU and PVT position is big enough the technique is able to detect it. A tightly coupled approach was selected to fuse the IMU and GNSS measurements as it was not found any analysis in the literature testing this approach. Nevertheless, after seeing the results of the experimentation it may be more optimal for spoofing detection a loosely coupled approach or even just monitoring the accelerations of IMU and the ones calculated with GNSS data.

- **CSAC Spoofing Detector:** The CSAC detector is tested using the Spirent signal generator and the Threat simulator. The attack was defined to alter only the pseudoranges gradually. The spoofed signal was generated with +6dB advantage and a ramp offset on the pseudorange was simulated (af1=9e-9). This impacts the PVT solution, which allows the clock bias monitor to detect, a strange behaviour, almost instantaneously. The time to detect the attack was 2s on the tests performed, and the spoofing detection probability was very high at 99.65% having only 0.38% of false alarms. Note that this attack was performed after a period of time of tracking the real signal from the satellites, if the attack is performed from a cold start the detection will be much more difficult.
- **AGC Spoofing detector**: AGC module based its detection on gain variation of each satellites. It has been tested against spoofing attacks which increments the power progressively in small steps. The spoofed signal was generated with a power ramp of 0.4dB/s. It is one of the most reactive modules, having the capability of sensing rapidly the in-channel power. The time to detect the attack was 3s on the tests performed and the spoofing detection probability was 99.47% with no false alarms (0%). Considering the test ramp 0.4 dB per second, and a detection of 3 seconds, a power jump around 1-2 dB is detected.
- **CSS authentication**: the CSS authentication has been testing using its standard version and re-encrypted version, i.e. encrypting CSS batches with the OSNMA TESLA keys. The Spirent SG and the CSDemo PTB have been used to generate SIS with OSNMA data. The attack simulated consisted on three phases. First, it simulates a static position with a power increasing rate of 0.1dB/s. Then, after achieving +6dB of advantage, it simulates a constant acceleration of (a_e; a_n; a_u) = (0.0; 1.8; 0.0) [m/s^2]. Finnaly, it remains in constant velocity of 9m/s. The attack is detected with a time to alert of 13.12s in average of the 10 different tests executed. The attacks are detected as expected but two main observations related to the technique latency are highlighted:
  - In case of encrypted, the delay of broadcast of the corresponding TESLA key is the driver.
  - In case of unencrypted, the delay corresponds to the multicast delay (in a timely on-line configuration).

  This means that the latency and time to authenticate are essentially driven by system-side choices.

- **RPA authentication:** for the RPA experimentation the following setup has been used:

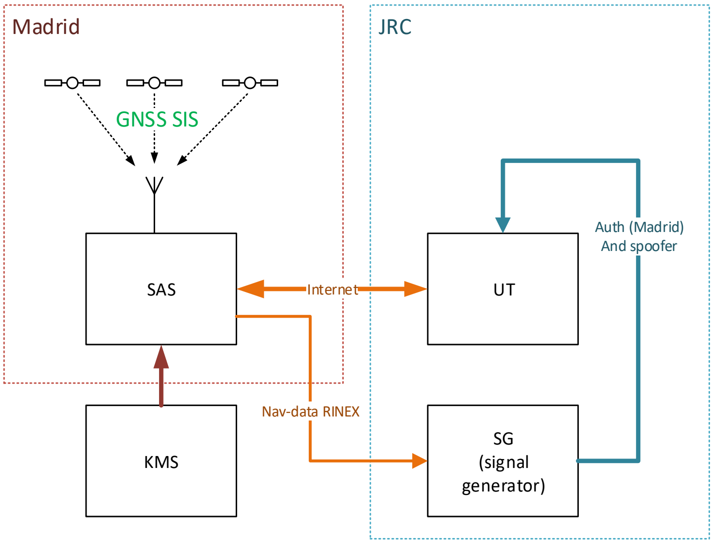


Figure 4-8: Final test connections

A spoofing threshold is defined so that if the spoofer alters the user position more than that distance, the attack is detected. During the experimentation several executions with the Threat simulator generating trajectory spoofing shows that the RPA technique is able to detect the attack every time. The attack simulated consisted on three phases. First, it simulates a static position with a power increasing rate of 0.1dB/s. Then, after achieving +6dB of advantage, it simulates a constant acceleration of (ae; an; au) = (0.25; 0.0; 0.0). Finally the velocity is maintained at 30m/s. The spoofing threshold was set to 20m at SAS side. This means that a spoofing attack was detected when a displacement greater than 20m (in the position) was generated by the attacker.

- **Anti-replay:** The anti-replay solution has been tested simulating different kind of environments both for the signal received by spoofer generating the attack and the user receiving the attack (Open sky and Urban). The technique is considered successful as the attacks are detected in every environment, even in environments where the estimation errors of the spoofer are low and may be masked by the errors of the channel (user in urban environment and spoofer in open sky). The impact of an imperfect estimation of the beginning of the unpredictable symbols by a spoofer can be observed and used for spoofing detection. Even with few unpredictable symbols (32 symbols per page, for a sliding window of 20 pages), the attack can be detected for all satellites. The partial correlations difference (R3 method) detector performs slightly better than C/N0 estimations but they are both promising. In all the environments the differences between both methods are similar, but the partial correlation results show higher jumps when the estimation errors are present, making the detection easier to be successful. Note that the implemented approach was done to detect jumps in the partial correlation differences because the focus was to detect the beginning of the attack. This was done because it is considered that once the spoofer gains the tracking loop of the user it can delay the signal and the estimation would be perfect. If the imperfect estimation is maintained during the whole duration of the attack, it could be detected establishing a static threshold which takes into account the expected difference of the partial correlation in case an attacker is present.

  Further improvements on the technique may include testing different statistics for the partial correlation analysis and also to accumulate different quantity of chips for the correlation computation. Tests accumulating different amounts of symbols and using other detectors shall be assessed as well.

4.4. PROJECT PUBLICATIONS

During the execution of the project several publications have been made with details of the project, technical analyses of the solutions, results and outcomes of different techniques developed throughout the project. The following table contains the articles published containing information about the project:

Table 4-1: NACSET project publications

Conference	Title	Abstract
ION GNSS+ 2017	Designing and evaluating next generation of resilience receivers	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 the industry on the projects 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 system 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.
ITSNT 2018	ITSNT2018 Testing receiver resilience against signal replay attacks	The Galileo program is implementing enhancements with respect to standard GNSS services. Some of these enhancements relate to complementing the Galileo Open Service with Navigation Message Authentication (NMA) and providing signal authentication through the Commercial Service. These new features will improve resilience of the GNSS applications and reduce the likelihood of successful attacks to GNSS users. However, these upcoming Galileo services still require a step to be completed on the user side: the definition and implementation of algorithms to successfully exploit them. In this context, the European Commission launched the Navigation Authentication through Commercial Service-Enhanced Terminals (NACSET) project aiming at investigating and implementing techniques to detect and mitigate spoofing attacks, improving user-level resilience. As part of the NACSET project, a resilient user terminal has been developed based on a high-end multi-GNSS receiver. This GNSS receiver is complemented with a software module that implements several protection techniques that exploit Galileo authentication. This module includes standalone techniques such as direction of arrival estimation, clock monitoring, IMU hybridization, AGC-C/N0 monitoring, a navigation message authentication (NMA) module and an anti-replay technique based on the use of NMA unpredictable symbols. This paper focuses on the proposed anti-replay technique. While plenty of literature is already available on GNSS spoofing and replay attacks, most of the research available is based theoretical models and simulations. The paper details a hardware and software implementation of anti-replay capabilities in a real high-end receiver in order to complement the existing work. The implementation is then tested in real time against a simulated attack implemented explicitly for the technique validation. Results and conclusions are derived and presented
ION GNSS+2019	Field Testing of GNSS Users Protection Technique	GNSS is a key element for a wide range of applications in our daily lives. Mass-market applications such as sports tracking or user guidance, liability-critical applications such as banking and telecommunication time synchronization, and safety critical services such as aviation and automotive-related solutions, all rely on GNSS. The huge growth experimented during the last decade puts GNSS in the target of attackers.

		The Galileo program is complementing the Galileo Open Service with Navigation Message Authentication (OSNMA) and providing signal authentication through the Commercial Service signals. These new services will be able to provide added protection to the current GNSS applications. Nevertheless, these features will require the users to implement new algorithms to exploit them. In this context, the European Commission launched the Navigation Authentication through Commercial Service-Enhanced Terminal (NACSET) project aiming at researching and implementing different techniques to detect and mitigate thus improving the resilience at user-level. In the frame of the NACSET project, a user terminal has been developed based on a high-end multi-GNSS receiver that is able to track E1/L1 and E6-B/C signals for data and signal protection. The terminal is equipped with a set of resilience techniques. Among these techniques, this paper focuses on an anti-replay technique protecting against zero-delay Secure Code Estimate-Replay (SCER) attacks based on the analysis of the unpredictable symbols from OSNMA cryptographic data. This paper firstly describes the NACSET project and its aim. Secondly, the theory of Anti-replay protection is explained from the point of view of a receiver, and anti-replay techniques based on OSNMA are introduced. Then, we describe the SCER simulator developed to assess the performances of the technique. To conclude, an attack is defined and performed with the SCER simulator over a real receiver. The results with and without OSNMA replay protection are presented and explained, and some conclusions of the experiment are derived.

5. CONCLUSIONS AND LESSONS LEARNT

The NACSET project has been focused on the definition, implementation, validation and experimentation with a set of techniques aiming at improving the resilience at user level. Both during the development of the system, integration and testing stages valuable conclusions and lessons learnt to be considered for future activities have been identified. Main conclusions are listed below:

- Regarding the **KMS experimentation** campaign, through the experiment assessments exercised within this project, it is considered that the proposed key management engineering solution implemented at the KMS, to be an effective option which fulfil security target required for the Galileo Commercial Service. The assessments have identified some possible configuration demands and codes of practice that could strengthen the architecture during its use in service.

  The KMS experimentation assessment has also outlined that the asymmetric OSNMA key model also meets expected security targets. However the TESLA chain delivery approach, may need some additional security considerations if / when it is extended for use in a real service environment. The experiment assessments have also demonstrated that the proposed key management engineering solution may be considered scalable and adaptable enough to meet market expectation for service needs with respect to user capacity within the service and flexibility for varying consumption demands.

- Regarding the **CS-RPP experimentation** results, all the techniques have been tested against real spoofing attacks with successful results. Nevertheless several considerations can be done which have been retrieved by the experience on working with the platform and analysing the results of all the tests performed with the system.

  - Regarding the **assisted signal authentication** techniques, the most promising one for a future service implementation is the re-encrypted CSS. This is because the RPA technique needs bi-directional communication between both users and the service provider which it is not very practical for implementation. And also, the RPA is focused only in trajectory spoofing which limits a bit its applicability. The plain CSS give the best results in terms of authentication but its implementation is not feasible as batches of CSS cannot be provided in plain format because it will compromise the security of the NAVSEC keys. The best solution then is the re-encrypted CSS which according to the results is able to detect the proposed attack in reasonable time (the latency depends on the TESLA key disclosure which, at the same time, depends on the OSNMA configuration).

  - The **anti-spoofing techniques** implemented at the UT have performed significantly well in the experimentation campaign.

    The **Dual antenna** technique is a very powerful method to detect standard spoofer (one signal source) that is considered the most probable threat to the typical GNSS user. The technique is able to detect the almost instantaneously as soon as it has enough satellites tracked to perform the carrier phase double differences. The considerable difference between spoofed and non-spoofed results makes very easy to define a static thresholds that works in all the cases.

    On the other hand the **CSAC monitoring** is considered to be a very useful technique to detect the start of a spoofing attack but it is recommended to be used with other spoofing techniques as it is very dependent on the PVT noise (even though the CSAC clock is very stable), thus depending on the environment.

    Another technique implemented is based on the **monitoring of the AGC and C/N0** values of the receiver, it is one of the most reactive modules, having the capability of sensing rapidly the in-channel power.

    At the beginning of the project, seeing that in the research literature a tightly coupled approach to hybridize the IMU data with the GNSS was not tested, this method was select to compute the IMU-assisted PVT for the **IMU detection** technique. After analysing the results of the project it is worth noticing that other algorithms like loose coupling or monitoring the acceleration could be more optimal for spoofing detection. However, even taking this into account, the technique implemented in NACSET UT is able to perfectly detect trajectory spoofing but there is room for improvement in the PFA and TTA performances.

    Finally, one of the main activities of the project was to research, develop and test an **anti-replay solution** which takes advantage of the unpredictable symbols contained on the Galileo OSNMA data transmitted on the E1B signal. The technique was implemented based on the research papers [RD.8] and [RD.9]. To summarize the publication and the experimentation campaign results, it can be concluded that a demonstration on anti-replay capabilities of OSNMA simulating different kind of environments has been achieved. The impact of an imperfect estimation can be observed analysing the unpredictable symbols, even with few unpredictable symbols the analysis is successful. Nevertheless, it is recommended to assess different number of chips to be accumulated together with different kinds of statistics to be used to analyse the correlation results.. As a summary of the anti-replay technique, it is considered to be a very promising technique and it will improve when implemented in a hardware receiver which allows more flexibility on the correlations computations.

END OF DOCUMENT