GALILEO COMMERCIAL SERVICE DEMONSTRATOR – SIGNAL IN SPACE PROOF-OF-CONCEPT

E. Carbonell(1), D. Calle(1), I. Rodríguez(1), G. Tobías(1), I. Fernández(2)

(1)GMV
C/ Isaac Newton 11, PTM Tres Cantos, Madrid (Spain)
Email: ecarbonell@gmv.com, jdcalle@gmv.com, irodriguez@gmv.com, gtobias@gmv.com

(2) European Commission
DG Enterprise and Industry – Av. Auderghem 45, Brussels (Belgium)
Email: Ignacio.FERNANDEZ-HERNANDEZ@ec.europa.eu

ABSTRACT

The Galileo Commercial Service (CS) has been conceived to provide an added value with respect to the Galileo Open Service (OS) and other GNSS signals. Since 2012, the European Commission has been working in conjunction with the European GNSS Agency and the European Space Agency on the strategy that will lead to an operational Commercial Service, and on its associated exploitation model.

At the end of 2013, a consortium led by GMV was awarded with a contract for the development and operational validation of the CS Demonstrator. The CS Demonstrator will be fully operative by late-2015, but a first analysis of the CS capabilities and services performance is already available. These preliminary results have been produced by the CS Early Proof-Of-Concept (EPOC), which is embedded in the CS Demonstrator and conceived as a simplified version of the complete system. The testing capabilities of the EPOC are limited to an off-line interface with the Galileo Core Infrastructure and to one single approach to the Authentication and High Accuracy services, which are intended to be provided by the operational Commercial Service.

The objective of this paper is to present the context of the Galileo CS Demonstrator, and focus on description of the architecture and operation of the CS Demonstrator Early Proof-Of-Concept. In addition, it is also the aim of the paper to describe in detail the Signal-In-Space (SIS) test strategy of the EPOC and present the results of the test campaign as for the Galileo Early Service Declaration initially foreseen in October 2014.

INTRODUCTION

The European GNSS system, Galileo, plans to provide five different services to the user community: Open Service (OS), Commercial Service (CS), Public Regulated Service (PRS), and Search and Rescue (SAR).

The Galileo CS [3] is aimed at market applications requiring higher performance and security than those offered by the Open Service. The main capabilities offered by the Galileo infrastructure to be exploited in the frame of the CS are:

- Dissemination of data with a rate of 448 bps through the E6B signal [1].
- Possibility of enabling Spreading Code Encryption (SCE) in the E6B and E6C signals.
- Broadcasting information through the External Regional Integrity Services (ERIS) bits part of the OS.

In January 2014 a project to develop a CS Demonstrator was launched, under the name of AALECS, “Authentic and Accurate Location Experimentation with the Commercial Service”. The project was awarded to a consortium led by GMV including CGI, Qascom, IFEN, Veripos and KU Leuven.

The final outcome of the project will be a platform able to connect to the European GNSS Service Centre (GSC) and transmit real time CS data through the Galileo satellites, with the aim of demonstrating the real performance of future High Accuracy (HA) and Authentication services of Galileo. As part of the first stages of the project, a test-bed named CS Early Proof-Of-Concept (EPOC) has been developed and exploited to perform an early demonstration, as well as an analysis of the CS system capabilities and achievable performances.

GALILEO COMMERCIAL SERVICES

As a result of the Commercial Service definition studies, High Accuracy and Authentication have been identified as the services to be implemented in the CS. Nevertheless, this decision does not cast aside the possibility of provision of other services to meet industry needs in the future.

High accuracy is understood as the ability of the system to provide a positioning accuracy in the order of a few centimeters. The selected technique for the provision of this service is Precise Point Positioning (PPP).
PPP relies on the use of precise orbit and clock estimations to calculate the user’s position. This approach allows a worldwide service, provided that a global communication channel is available. Different analyses have been conducted; showing that a 448 bps bandwidth per satellite permits the transmission of satellite orbits and clocks data at an adequate update rate to provide accuracy in the centimeter level.

Authentication is an area of high interest for research & development in GNSS [2]. It differs from information authentication, as in GNSS the objective is not only to authenticate the information encoded in the signal but also to authenticate the signal travelling time in order to perform a trusted position and time estimation. In this sense, GNSS signal authentication is going towards two possible directions:

- Data level authentication
- Spreading code level authentication

Data level authentication is more vulnerable to replay attacks. An attacker can observe the data travelling from space that contains authentication, forward it to a signal generator and change the pseudorange to the desired one.

Spreading code level authentication provides a more robust approach to signal authentication. If either the PRN code or parts of PRN sequences are unknown (encrypted), it is difficult for the attacker to replicate the signal as it is masqueraded by the receiver thermal noise.

EARLY PROOF-OF-CONCEPT IN THE AALECS PROJECT

The EPOC is the first outcome of the project AALECS project, which has proved the CS capabilities in an early stage. The initial objective of the EPOC was to demonstrate the main functionalities (transmission, encryption, tracking, authentication and positioning) of the Commercial Service for the Galileo Early Services milestone, which is foreseen for the end of 2014. This fact has led to a design philosophy in which the simplicity has been the dominant driver.

The EPOC development and validation activities were completed in June 2014 and the SIS-Tests campaign was officially launched immediately after. The first remarkable achievement took place on June 17th 2014 when the E6 data loop was closed. It was the first time that the Galileo satellites had disseminated data generated by a third party external to the Galileo core infrastructure through the E6 signals, and it was properly received. Another relevant achievement was the successful tracking of E6B signals with enabled Spreading Code Encryption (SCE). During July 2014 a 10-day test campaign was conducted showing successful tracking and data demodulation of the SCE signals from the available Galileo satellites.

The disseminated data contains Authentication and High Accuracy information. This allows the receiver to determine the authenticity of the data source and to calculate a precise positioning solution using authenticated products. Dissemination activities have been repeated in 6-hour periods on a weekly basis from mid-June to end of September.

System Description

In order to complete the EPOC objectives, the platform had to be able to close the loop of E6 data transmission from its generation to its reception. Fig. 1 depicts the communications links established between the EPOC and third parties.

First of all, the EPOC receives satellite orbit and clock predictions (Step #1) for the desired testing period. Only for tests with SCE enabled, the operator receives the NavSec from GMS (Galileo Ground Mission Segment), stores it in the EPOC archive and installs it on the receiver (Step #2). With this information the operator can generate CsData files and send them to GMS (Step #3). The GMS operator ingests the files in the system and the CsData uploading starts to the satellites connected to an Uplink Station (Step #4). Automatically, the Galileo satellites broadcast the received data through the E6-B signal and the receiver collects it (Step #5). Finally, the EPOC operator launches the analysis tool to obtain the transmission metrics, authentication solution and PVT solution.

![Fig. 1: EPOC test dataflows](image-url)
The system designed to accomplish this objective is composed of three independent hardware and software items: the EPOC-RXP, the RXP-Host and EPOC-Host. Note that RXP stands for CS Receiver Platform. With these elements the physical layout remains as in Fig. 2.

The EPOC-RXP is based on the CS Receiver developed in the frame of the AALECS project; concretely an early version of this element named NAVX-NTR and developed by IFEN. It is capable of performing E6 ranging (with and without SCE), and decoding data from the E6-B channel. Tracking of E1, E5, L1, L2 and L5 signals is required to retrieve observation data and calculate a PVT solution using authenticated products decoded from the E6.

The RXP-Host hosts the NTRTerm software in charge of commanding the NAVX-NTR receiver; and the RXP-Host SW. This software includes an Authentication Client (AC) and a PVT client to process the received CsData together with the observations gathered for Galileo and GPS.

The EPOC-Host hosts the Data Generator in charge of processing the High Accuracy data and generating the Authentication information. It also hosts the historical archive, where the generated and received data is stored; and the analysis tool. This tool is in charge of analyzing the received data, comparing it to generated data and producing a PDF report with the most relevant information.

Note that for the EPOC no real-time interface has been implemented between the different elements. Therefore the data generation, authentication and PVT algorithms are file-based. Fig. 3 depicts the interfaces between the different hardware elements within the EPOC.

**EPOC Datagen**

The EPOC Datagen (E6 Generator) comprises two elements: the High Accuracy (HA) datagen and the Authentication (Auth) datagen, as depicted in Fig. 4.
The High Accuracy datagen receives an SP3 file containing Galileo and GPS precise orbit and clock predictions generated by *magicGNSS*, which are suitable to compute a PPP solution. *magicGNSS* is a set of software tools that supports a wide variety of GNSS projects and objectives, including service volume simulations, core operational functions (such as orbit, clock, and ionosphere determination and prediction, PPP), receiver performance analysis, added-value services including integrity, local augmentation developments, and all related performance and accuracy analyses [7]. For the EPOC, input data used to feed *magicGNSS* for products generation is obtained from the IGS MGEX station network. Predictions are generated 2-3 days in advance of the planned SIS-Test; therefore the achievable performances are limited due to degradation of the predicted products. The HA datagen output is basically a set of 160-bit messages; each message containing the position and clock offset for a satellite at a given epoch. These HA messages are forwarded to the Authentication generator where the authentication information is produced. Finally, HA and Authentication messages are packed together to fit in the 448 bps available in the E6 pages.

The authentication solution used for the EPOC is an adaptation of the synchronous Timed Efficient Stream Loss-tolerant Authentication (TESLA) algorithm [5]. TESLA proposes to generate a single one-way chain of keys (K) used for data authentication. In the EPOC, this chain is generated from an initial random seed key (K₀) by performing a given number of hashes using the SHA-256 algorithm. As a result, the length of each key is of 256 bits, although future implementations to be tested in the AALECS will truncate the hash function output and use shorter keys to reduce bandwidth [6]. The chain is generated from K₀ to Kₙ but keys are disclosed to the user from K₀ to Kₙ, hence future keys cannot be inferred from disclosed ones. However, this approach gives the user the possibility of recovering an old key from a recently-disclosed one if there is a key loss. This concept is illustrated in Fig. 5.

![TESLA key chain generation](image)

Each TESLA key (Kᵢ) is associated to a set of HA data which is referred to as “key-slot”. HA data transmitted in a key-slot is HMAC-signed using the same key (Kᵢ) for all satellites. Each key-slot has duration of 5 seconds and includes HA data and related MACs during the first 4 seconds, while Kᵢ is disclosed in the last second (see Table 1).

<table>
<thead>
<tr>
<th>Second</th>
<th>Page Type</th>
<th>Page Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1ⱼ</td>
<td>HA</td>
<td>HMAC(HAᵢ</td>
</tr>
<tr>
<td>2ⱼ</td>
<td>HA</td>
<td>HMAC(HAᵢ</td>
</tr>
<tr>
<td>3ⱼ</td>
<td>HA</td>
<td>HMAC(HAᵢ</td>
</tr>
<tr>
<td>4ⱼ</td>
<td>HA</td>
<td>HMAC(HAᵢ</td>
</tr>
<tr>
<td>5ⱼ</td>
<td>Key</td>
<td>Bit Pattern</td>
</tr>
</tbody>
</table>

Hence, received HA data can be authenticated every 5 seconds. In the context of the EPOC this is known as “Short-Term Authentication”, as opposed to “Long-Term Authentication”, which is introduced in the next paragraphs. It is important to note that the use of a single key chain allows data cross-authentication [4], since data received from all satellites can be authenticated using the key received from any satellite.

HMACs included in HA pages at a given j-th key-slot are computed by the HMAC-SHA-256 algorithm using the associated Kᵢ. In order to enhance security, HA data is appended with the SVID (IOVᵢ) of the broadcasting satellite, avoiding identical HMACs being broadcast simultaneously (see Table 1). Resulting 256-bit HMACs are truncated to the 64 MSB, which is considered secure enough for real-time authentication purposes.

Key pages also include a 64-bit truncated HMAC which is computed upon the last HA packet in the key-slot (HAₙ) and the 32-bit Galileo System Time (GST) of the Key page using a key to be disclosed later in time (Kᵢₙ₋₁); see Table 1. This HMAC is used to detect a delayed attack during a receiver cold start, in which an old key is presented by the attacker as the current one. This is referred to as “Long-Term Authentication”.

Finally, the initial key in the chain K₀ is saved in a file. This key is the “TESLA Root Key” to be installed onto the Authentication Client in the RXP-Host. By means of K₀, the AC can verify the authenticity of any Kᵢ key by traversing the chain until the start point K₀ is reached. The number of hashes to reach K₀ is fully determined by the timetag (GST) disclosed at each Key page and the number of seconds between keys.
EPOC RXP- Clients

The EPOC contains two clients designed to process the received Authentication and HA information, namely the Authentication Client and the PVT Client. Once the CS Receiver has gathered the E6 data, it is processed by the AC, which generates an authentication log including relevant authentication events; and reconstructs two sets of satellite orbit and clock files. One of them comprises only authenticated products while the second one includes all data.

The PVT client is the component in charge of receiving the Galileo and GPS satellite orbits, clocks and the observables collected by the receiver; and generating a PVT solution. The PVT algorithm itself is not developed in the frame of the AALECS project; instead of that, the EPOC includes an instance of the magicPPP product licensed by GMV. Two PVT solutions are generated depending on the products used: standard and data-authenticated.

EPOC Analysis

The last relevant constituent of the EPOC is the “Analysis Tool”. It contains all the necessary functionalities to analyse the authentication solution and the received E6 data versus the generated data. Several metrics are generated, including pages loss rate, and Authentication Error Rate (AER) versus C/N0 amongst others.

Analysis results are presented in an automatically-generated PDF report to ease its study and handling.

EXPERIMENTATION ACTIVITIES

The Signal-In-Space test campaign has spanned from mid-July until the end of September. The aim of the EPOC experimentation activities has been twofold:

1. Test the system capabilities: Transmission of data in the E6-B band, encryption and decryption of the CS signal, robustness and performance of a timing and positioning authentication application with the real E6 signals based on SCE, and reception conditions of the E6 signal in realistic target user environments.

2. Evaluate the results obtained by the TESLA-based authentication algorithm, as well as the performance of a PVT solution using TESLA-authenticated HA data transmitted through the E6B.

Two main scenarios have been addressed:

- Static: The receiver antenna is located on the roof of a high building in a static position. Data recording starts when all operational IOV Galileo satellites are visible, and ends before the test slot is finished.
- Kinematic: The receiver antenna is attached to the roof of a car. The test is started by recording 25-30 minutes of data in a static open-sky location; after all operational IOV Galileo satellites are visible. Then the car starts following a route which slowly increases the severity of the signal reception conditions.

A feasibility study was carried out to find the most convenient tests slots which would guarantee visibility of all operational IOV satellites over GMV’s premises (Madrid). Based on this study, the test campaign schedule was agreed with ESA and Spaceopal, allocating 6-hour slots to the EPOC SIS tests on a weekly basis. Spreading Code Encryption was activated for 10 days, from 15th to 25th July. During this period three static tests were conducted to obtain as much information as possible.

The following paragraphs present the most relevant results of the SIS testing activities. Three tests have been selected; two static tests -with and without SCE enabled- and one kinematic test.

Static test results with SCE – 22/07/2014

Robustness of the E6 signal reception and encryption/decryption performance has been assessed in terms of data transmission. As Table 2 yields, the page-loss ratio is below 0.4% for E11 and E19, whereas for E12 it is raised to 2.7% due to low elevation at the end of the tracking period. This can be seen in Fig. 6, where crosses represent tracking losses at the end of the tracking period of E12.

<table>
<thead>
<tr>
<th>PRN</th>
<th>Expected</th>
<th>Received</th>
<th>Lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>E11</td>
<td>21000</td>
<td>20989</td>
<td>11</td>
</tr>
<tr>
<td>E12</td>
<td>16598</td>
<td>16150</td>
<td>448</td>
</tr>
<tr>
<td>E19</td>
<td>18833</td>
<td>18766</td>
<td>67</td>
</tr>
</tbody>
</table>

Table 2: Transmission performance
Fig. 6: Tracking profile

Authentication Error Rate (AER) has also been computed for the test. AER measures authentication performance in the absence of attacks, but in the presence of disturbances of the real transmission channel [4]. In Fig. 7 short-term AER, that is, the error rate of “Short-Term Authentication” computed every 30 seconds has been plotted along with E6 carrier noise (C/N0). There are no authentication errors except for those coincident with certain C/N0 dropouts around 23:30 UTC. These dropouts are also reflected in Fig. 6 as tracking losses. The overall short-term AER has been of 0.25% for E11, 3.4% for E12 and 0.75% for E19. It should be noted that, as the data were modulated on encrypted signals, no data authentication would have been necessary to consider the data authentic. Nevertheless the purpose of the EPOC test campaign was to characterize the performance of SIS data authentication in all cases.

Fig. 7: Short-Term AER for satellite E11

The data-authenticated PVT performance is presented in Fig. 8. The positioning error Root Mean Square (RMS) is below 0.35 m for the horizontal plane and 0.46 m for the vertical plane; including the convergence period. If the error RMS is computed for the stationary period, it is bounded by 0.25 m in all three components. Note that this accuracy has been achieved with orbit and clock predictions generated 42 hours in advance of the test slot, thus it is expected to obtain error RMS values below 20 cm using products generated with low latency.

Fig. 8: Static tests antenna location (left) and PVT positioning error (right)

Static test results without SCE – 28/08/2014

Transmission performance results are given in Table 3. Page losses are below 0.46% for satellites E12 and E19, whereas for satellite E11 losses are increased to 1.56% due to low elevation at the beginning of the tracking interval. This effect can be seen in Fig. 9, where a high number of tracking losses are registered before 18:15 UTC.
Table 3: Transmission performance

<table>
<thead>
<tr>
<th>PRN</th>
<th>Number of pages</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Expected</td>
<td>Received</td>
<td>Lost</td>
</tr>
<tr>
<td>E11</td>
<td>9059</td>
<td>8918</td>
<td>141</td>
</tr>
<tr>
<td>E12</td>
<td>10799</td>
<td>10765</td>
<td>34</td>
</tr>
<tr>
<td>E19</td>
<td>10798</td>
<td>10749</td>
<td>49</td>
</tr>
</tbody>
</table>

Fig. 9: Tracking profile

The overall short-term Authentication Error Rate has been of 2.25% for E11, 0.45% for E12 and 0.55% for E19, thus it can be stated that the tracking and authentication performances are similar with and without SCE enabled.

The data-authenticated PVT performance is depicted in Fig. 10. The positioning error RMS is reduced to 0.23 m North, 0.63 m East, 0.28 m Up if computed over the stationary period. Predictions for this test were generated 41 hours in advance of the test slot.

Fig. 10: PVT positioning error

Kinematic test results without SCE – 03/09/2014

This test was conducted in the surroundings of GMV’s premises at Tres Cantos (Madrid). The followed path traverses an expansion zone where there are numerous buildings under construction. The first half of the test (after the initial static 25 minutes) can be considered open-sky whereas the second half included several sections with buildings on one side of the street. All operational IOV satellites were over 25 degrees of elevation throughout the test.

Transmission performance is shown in Table 4, with a page-loss ratio below 0.38% for all three satellites. As depicted in Fig. 11, data losses are due to momentary track losses occurred during the test. The overall short-term AER is below 0.6% for all satellites.

Table 4: Transmission performance

<table>
<thead>
<tr>
<th>PRN</th>
<th>Number of pages</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Expected</td>
<td>Received</td>
<td>Lost</td>
</tr>
<tr>
<td>E11</td>
<td>3937</td>
<td>3922</td>
<td>15</td>
</tr>
<tr>
<td>E12</td>
<td>3925</td>
<td>3911</td>
<td>14</td>
</tr>
<tr>
<td>E19</td>
<td>3925</td>
<td>2638</td>
<td>7</td>
</tr>
</tbody>
</table>
Fig. 11: Tracking profile

Fig. 12 shows the data-authenticated PVT performance. The reference trajectory has been calculated using the magicGNSS suite of products. High-quality products have been obtained using magicODTS and used to compute a high-precision reference trajectory using magicPPP. As Fig. 12 yields, the positioning error RMS values are higher in this test than those obtained during static tests. However, if the convergence period is discarded (up to 14:20 UTC) the errors RMS are reduced to 0.66 m N, 0.61 m E and 0.15 m U. The HA data ageing is of 62 hours for this test.

Fig. 12: Test trajectory (left) and PVT positioning error (right)

CONCLUSIONS

The European Commission is betting on the Galileo Commercial Service, as one of the differentiators of Galileo with respect to other GNSS. As part of its efforts, the AALECS project has been launched to produce a CS Demonstrator platform to test services with the real Galileo SIS.

The first outcome of this project is the Early Proof-Of-Concept, which from mid-June to end of September 2014 has been testing E6-based navigation authentication and precise point positioning (PPP). The EPOC platform has been able prove the CS capabilities before the Galileo Early Service Declaration milestone.

ACKNOWLEDGEMENTS

We would like to thank to Jose María Almansa from GMV for his support during the EPOC experimentation phase; and the teams at Spaceopal, GSA and ESA that supported the real SIS transmission through the Galileo satellites.

REFERENCES