Galileo's Commercial Service

Testing GNSS High Accuracy and Authentication

Galileo Up-Link Station (ULS) on Svalbard (Norway) showing the two uplink antennas, protected by a radome each.
ESA photo

In the near future, the Galileo program will decide on the design and implementation of a Commercial Service for civil applications that provides high-accuracy positioning and signal authentication. A team of authors involved in the program describes the evolution of this service, its current design, and the results of tests of its capabilities using actual signals in space.

IGNACIO FERNÁNDEZ HERNÁNDEZ
EUROPEAN COMMISSION

IRMA RODRÍGUEZ, GUILLERMO TOBÍAS, J. DAVID CALLE, ENRIQUE CARBONELL
GMV

GONZALO SECO-GRANADOS
UNIVERSIDAD AUTÓNOMA DE BARCELONA

JAVIER SIMÓN, REINHARD BLASI
EUROPEAN GNSS AGENCY (GSA)

After some years of concept studies and simulations, the Galileo Commercial Service is taking off. The journey has started toward what can be the most accurate and secure worldwide satellite-based navigation services for civil use.

Employing only GNSS signals, authenticated position fixes accurate to the decimeter level were achieved for the first time in the summer of 2014. Future prospects are for even better results. Although the journey is exciting, many challenges still lay ahead. This article presents the work accomplished thus far on the development of the Commercial Service and the first results of the Authentic and Accurate Location Experimentation with the Commercial Service (AALECS) project with real Galileo signals.

Galileo and the Commercial Service

Since its inception, the Galileo program has experienced several ups and downs, and the Commercial Service (CS) has been no exception. In the late 1990s, the European Union (EU) conceived Galileo and proposed a public-private partnership to share program development costs and risks. At that time, the Commercial

Service, named "Control-Access Service 2" or CAS-2, was one of the pillars of Galileo, intended to enable private partners to recover their investment. (CAS-1 is now known as the Public Regulated Service or PRS.)

This approach helped the EU Member States to make the important decision for Europe to develop its own satellite-based navigation system. However, the "added-value" services that Galileo could offer, on top of the ubiquitous, free, and already excellently performing GPS — especially after the removal of that system's civil accuracy–degrading Selective Availability feature in 2000 — remained unclear.

Perhaps the lack of a clear return on investment ultimately deterred prospective industrial concessionaires from accepting the risk of building Galileo with their own resources. After years of negotiations, the concession-based approach was discarded in the late 2000s, in favor of a fully EU-funded program. At that time, priorities were shifted to those services considered to be more critical for public or governmental uses, such as the PRS, the Open Service (OS), and the Safety-Of-Life (SOL) and Search-And-Rescue (SAR) services.

The evolving Galileo regulation that guided program development still mandated the existence of a commercial service with "improved performance and data with greater added value" than the other services. However, that "added value" was not concretized in any mission or system requirement, and the program budget was already fully allocated to other priorities. Early definition tasks identified high accuracy (HA) and authentication as the two most promising services, but it was not clear if and how the services could be provided, what their performance would be, and how they would be implemented and operated.

The *re-profiling* of the Galileo SOL in the early 2010s was an important event for the Galileo CS. SOL had been a major factor in defining the Galileo ground infrastructure and signal structure. Its original mission was to provide a worldwide integrity service, satisfying the stringent requirements of aviation communities, among others.

For several reasons, the Galileo program decided to re-profile the SOL into a lighter service, currently being defined, which will provide integrity in likely cooperation with other regions. Therefore, some Galileo features designed to provide the SOL service became available for other purposes. These features include:

- a high data bandwidth compared to other GNSS signals.
- the transmission of data with a latency of few seconds through satellites connected to Galileo ground uplink stations.
- an external real-time input channel initially expected to transmit integrity data from and to other regions in the world.

A Broader Scope

The "post-concessionaire" era has broadened the scope of the CS, and the objective of creating a source of revenue for Galileo in order to partly recover its operation costs has been balanced with other aims, in accordance with the Galileo program's new status as a public initiative. These aims have been summarized in the following five objectives:

- to maximize the public benefits offered by satellite navigation
- to create economic value, by creating new services, or enlarging the existing ones, with the related increase in economic activity
- to improve Galileo navigation performance
- to promote innovation by enabling new services, ideas and solutions
- and finally, to create a complementary revenue source for the EU satellite navigation programs.

With these objectives in mind, by early 2013, two parallel studies were launched to define the Commercial Service and its implementation in Galileo. The main premise for the studies was to offer the maximum value with the minimum modifications, if any, to the Galileo core infrastructure. This means no or minimal modifications to the Galileo ground infrastructure and the satellite on-board software, and no modifications at all to the satellite hardware, which implies that the current Galileo CS signal definition needs to be maintained.

The Galileo CS Signals

The Commercial Service signals define the capabilities that the Galileo CS will bring. As described in the Galileo OS SIS ICD, the CS signal is composed of a data (E6-B) component and a pilot (E6-C) component transmitted in the E6 band (1260–1300 MHz).

The signals are modulated with a binary phase shift keying BPSK(5) at a carrier frequency of 1278.75 MHz, which is used by all satellites and shared through a code division multiple access (CDMA) RF channel access method. Therefore, the signal main lobe and most of the signal power is in the 1273.75-1283.75 MHz band. **Figure 1** shows the CS and other signals from all satellite-based navigation systems operating in the same band.

Both E6-B and E6-C signals are modulated on the in-phase component, leaving the quadrature component to the E6-A signal, used in conjunction with the E1-A for the Public Regulated Service. **Table 1** summarizes the main properties of the E6-B and E6-C signal components.

A relevant feature of the CS signal is that the primary spreading codes of both components can be either encrypted or in the clear when transmitted. When encrypted, the spreading codes are replaced by an unpredictable bit-stream generated through a secret key, making the signal indistinguishable from noise for unauthorized receivers.

One of the challenges for the Galileo CS is that it will have to share the RF spectrum with other users. The 1240–1300 MHz band is currently used by several applications, and ensuring compatibility with some of them, such as aeronautical and land military radars or the amateur radio community, may require coordination and interference

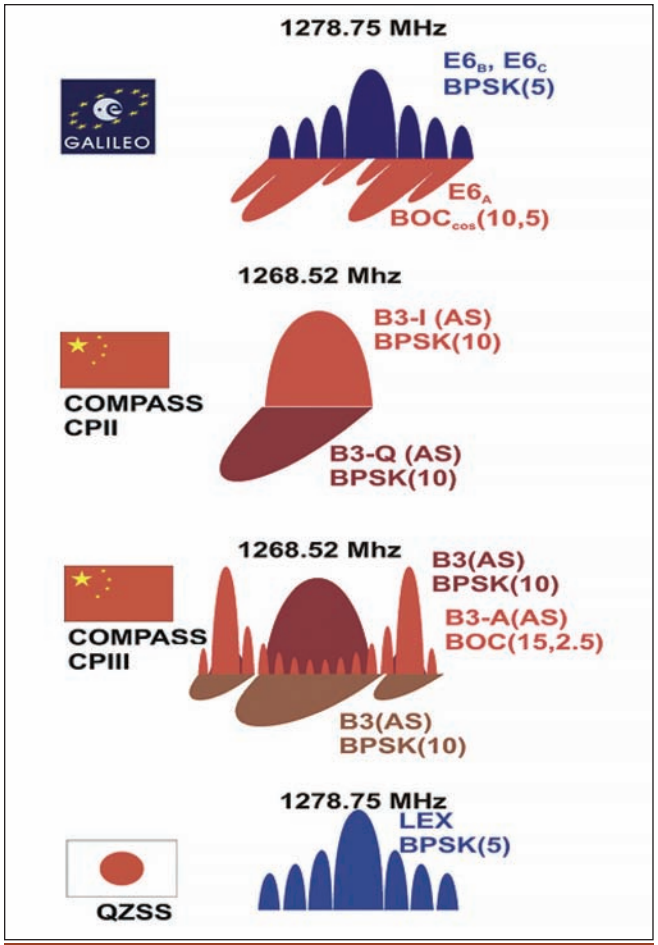


FIGURE 1 GNSS signals in the Galileo E6 band.
Source: www.navipedia.net

	E6B	E6C
Component	Data	Pilot
Carrier Frequency	1278.75 MHz	1278.75 MHz
Spreading Modulation	BPSK(5)	BPSK(5)
Chip Rate	5.115 Mcps	5.115 Mcps
Primary Code Length	5115 chips	5115 chips
Primary Code Duration	1 ms	1 ms
Secondary Code Length	N/A	100 chips
Secondary Code Duration	N/A	100ms
Symbol Rate	1000 sps	N/A
Data Rate	492 bps	N/A
Data Encoding	As per SIS ICD	N/A
Data interleaving (col. x row)	123 x 8	N/A
Spreading code encryption capability	Yes	Yes
Power sharing	50%	50%
Received Minimum Power (E6B + E6C)	-155 dBW	

TABLE 1. Galileo E6-B/C signal characteristics

Sync Symbols	Data Symbols			Total
16	984			1000 symbols
	Page type	**CS data**	CRC	Tail	492 bits
	16	**448**	24	6	

TABLE 2 Galileo CS E6B per-second data structure

mitigation in the vicinity of these systems' ground-based transmitters.

In addition to those applications, the E6 band is also used by the space research and satellite-based Earth exploration communities. Early CS tests involving real signals have shown satisfactory performance when no interferers are around but have suffered interference effects in the vicinities of transmitters.

The European Commission (EC) is pursuing actions to facilitate the use of the E6 for satellite-based radionavigation to the widest extent, and discussions with telecom regulators and user communities will continue over the next few years, in parallel with the experimentation of the services that Galileo CS aims to offer: high accuracy and authentication.

High Accuracy

High accuracy is generally understood as a positioning accuracy on the order of a few centimeters. Two primary approaches have been used in the past years to provide high accuracy: real time kinematic (RTK) and precise point positioning (PPP). The main advantage of using PPP instead of RTK is that it provides a global and absolute positioning and timing service without the need for nearby reference stations.

PPP is based on the use of accurate GNSS satellite orbits and clock data to estimate a user position based on carrier phase measurements, where the ionospheric delay is typically removed by performing the iono-free combination. The main disadvantage of PPP is the time needed to converge to a centimeter-level accuracy, which currently takes about 15–30 minutes to achieve, while RTK is almost instantaneous. The most common and optimized technique in terms of bandwidth for real-time PPP is to send orbits and clock corrections to the navigation message, allowing the reconstruction of the accurate values in the receiver.

The Galileo E6-B channel is well suited to transmit PPP information. Various analyses have shown that the available rate of 448 bps per satellite allows the transmission of satellite orbits and clock data at an adequate update rate to provide accuracy at the centimeter level. (See **Table 2**.)

The data update rate is especially relevant for satellite clock corrections, which are not as stable in the medium and long term as the orbits. In order to obtain the highest accuracy, corrections must be updated every few seconds, especially for the satellites with less stable clocks.

Figure 2, generated for GALCS ("Galileo Commercial Service definition"), one of the two parallel studies mentioned

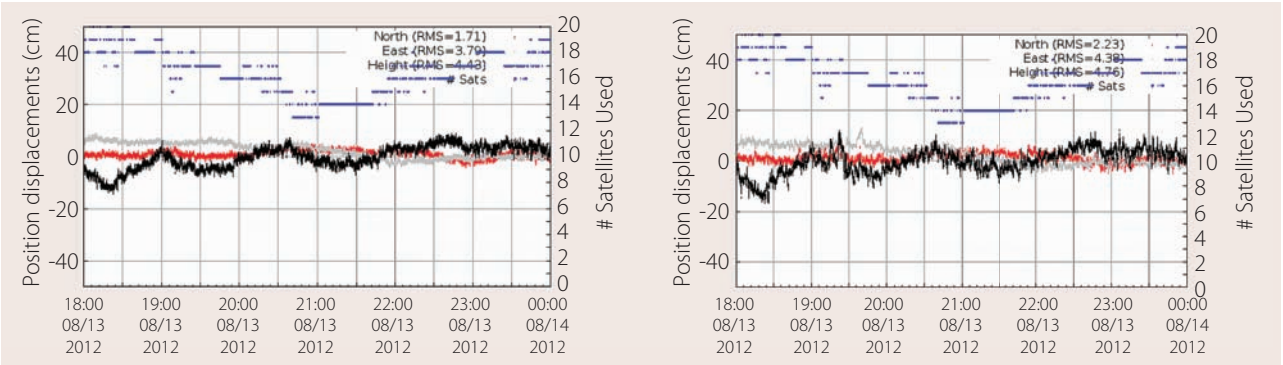


FIGURE 2 High-accuracy performance simulation with a 5-second clock update rate (left) and a 30-second clock update rate (right)

previously, shows the evolution of the 3D position error and the corresponding root mean square (RMS) for a static GNSS receiver after convergence on a position solution. The reference products were computed by means of a network of 50 worldwide GPS and GLONASS stations. The corrections used below 400 bps, which is compatible with the CS. The panel on the left of Figure 2 shows the PPP positioning error with a 5-second clock update rate, while the panel on the right shows the error with a 30-second clock update rate. The system latency was configured to 5 seconds, understanding latency as the time between when the system processes the satellite measurements and when corrections based on these measurements are transmitted.

Both latency and clock update rates contribute to the age of data of the clock corrections applied at a given time, which have an impact on the PPP accuracy. As the CS allows for the transmission of different bits from different satellites, the total bandwidth can be highly increased leading to a better performance that, when combined with other factors may reduce the PPP receiver convergence time.

Spreading Code Encryption

Due to their low power, GNSS signals can be easily jammed, and because of the lack of authentication, they could also be forged or "spoofed" with the appropriate equipment. Therefore, protecting GNSS has become one of the major topics of interest for GNSS.

In addition to other technical and regulatory measures, features in the GNSS signals allowing authentication are undoubtedly a major building block of location security. GNSS authentication is different from information authentication, as its objective is not only to authenticate the information encoded in the signal but also to authenticate the signal time of arrival, at least against certain threats and with a certain confidence level. Both factors are required for a trustworthy position and time estimation.

With this in mind, Galileo is a good candidate to offer authentication services to civil communities for two main reasons. The first is that Galileo E6-B and E6-C signal spreading codes can be encrypted, which provides spreading code authentication for receivers (or server-receiver architectures) having the encryption keys. Also, the fact that the keys are not used for military purposes implies that they can be shared under certain conditions with certain users, providing additional flexibility. The second reason is that the available bandwidth in both E6-B and E1-B Galileo signals permits the transmission of authentication and re-keying data while guaranteeing full backward-compatibility.

Navigation Message Authentication

As mentioned earlier, the CS objectives go beyond obtaining revenues. In addition to an access-controlled E6-based authentication service, The Galileo program is working to offer an open navigation message authentication (NMA) service. The latter service can use the E1 signal for data transmission through an underlying architecture similar to that for E6-B.

Some work already performed shows that Galileo can achieve very good performance, including the possibility to authenticate the navigation messages of other constellations. (For further discussion of this point, see the article by I. Fernández-Hernández *et alia* (2014a) listed in the Additional Resource section near the end of this article.)

Putting It All Together

The exact definition and implementation of the HA and authentication services is yet to be finalized and will depend on EU member states' agreement and the involvement of external providers. Nevertheless, we can already envision the following service bundle:

- a commercial high-accuracy service on the E6-B signal, transmitted unencrypted at spreading code level and whose access is controlled at data level.
- two authentication services — an open authentication service based on Galileo E1-B for applications requiring a medium security level and a commercial authentication service based on encrypted spreading-codes on the E6-C pilot tone, the data authentication on E1-B and some additional E6-B data for spreading code re-keying.

Conceptually, the provision by Galileo of different authentication services (PRS, CS, OS) seems coherent with general security principles, whereby the

level of security is commensurate with the criticality of the assets to protect.

Galileo CS Architecture

As said before, the CS is designed to be as respectful as possible of the current Galileo core system infrastructure. To achieve this, CS will be provided through an external interface already built into the core system. This scheme, once accredited, will offer a high flexibility and fit very well with the premise that Galileo is eminently a civil system for civil purposes.

Figure 3 shows the CS data transmission process, which consists of the following steps:

- The data is generated by an external source, for example, a high accuracy service provider with its own network of monitor stations. These data are formatted and transmitted to the European GNSS Service Center (GSC), located in Torrejón de Ardoz, Spain.
- The GSC ensures the integrity and authenticity of the data, and after the required security verifications it relays data to the operational Galileo Ground Control Center (GCC) in Oberpfaffenhofen (Germany) or Fucino (Italy).
- The GCC incorporates the CS data into the messages that contain all other mission and navigation data and sends them to the five up-link stations (ULS) located at Papeete (French Polynesia), Kourou (French Guyana), Svalbard (Norway), Reunion (France) and Noumea (New Caledonia, France), for the transmission to the satellites.
- At each ULS site, uplink antennas pointing at Galileo satellites transmit the data. Currently two antennas per site are available, but more may be deployed soon. Only the satellites pointed by a ULS antenna can transmit real-time data; so, the uplink connections are also one of the drivers of the CS performance.
- Each ground-connected satellite receives its own 448-bit data page and incorporates it into the E6-B data structure. Users and ground monitor stations worldwide receive the signals with the CS data, closing the loop.

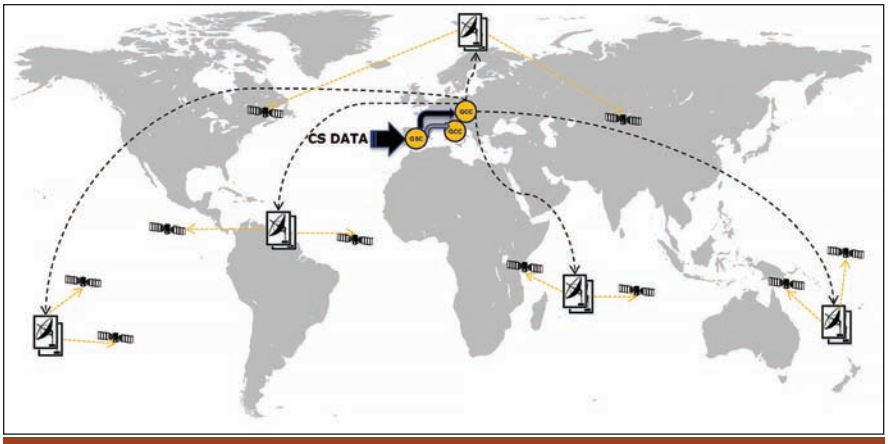


FIGURE 3 Galileo Commercial Service Architecture

This scheme not only allows transmission of CS data in the E6-B but also transmission of data in the E1 I/NAV "Reserved 1" field as per the OS SIS ICD.

The AALECS Project: Three Steps Ahead

The CS definition work started ramping up in mid-2012, but by the end of 2013 it still was based on concept studies and simulations. In January 2014, the EC Directorate-General for Enterprise and Industry (DG ENTR), in charge of the definition and management of the CS, launched the Authentic and Accurate Location Experimentation with the Commercial Service (AALECS) project, with the aim of experimenting with the real architecture and satellite signals.

The project, carried out by a consortium composed of GMV, CGI, Qascom, IfEN, KUL, and Veripos, will run until 2016 and is composed of three phases. Firstly, it has developed an *early proof-of-concept* (EPOC) platform for initial testing, the results of which will be reported later in this article. Secondly, the AALECS project is developing a distributed platform across Europe to transmit and receive real-time CS data through the Galileo satellites. The platform is composed by four receivers located in UK, Italy, Germany and Spain, as well as two core platforms in Spain and Italy, as shown in **Figure 4**.

In addition, the platform will integrate EC Joint Research Center's simulation capabilities. Finally, in its last phase, AALECS will support potential external providers to test their applications and solutions with Galileo.

The EPOC: AALECS's First Step

During the summer of 2014 the EPOC tested the E6 external data transmission. Given the unique opportunity to use the real CS signals and the flexibility provided by the platform, the European Commission and the AALECS team agreed to make the tests as realistic as possible within the limits of the architecture. This included the generation of high-accuracy satellite orbit and clock predictions and data authentication, both with and without the spreading code signals encrypted. The EPOC experimentation activities with real signals in space started in July and finished in late September, although an extension of the testing is under discussion.

As shown in **Figure 5**, the EPOC platform is composed of three independent hardware and software items: the CS Receiver, the receiver platform (RXP) host and the EPOC-host. The CS receiver is a modified multi-frequency commercial receiver capable of performing E6 ranging with and without spreading code encryption (SCE) and can decode data from the E6-B channel.

The RXP-host commands the CS receiver and includes the authentication and position/velocity/time (PVT) software modules that process the received CS data together with the observations gathered from Galileo and GPS satellites. The EPOC-host generates the authenticated high-accuracy data to be broadcast

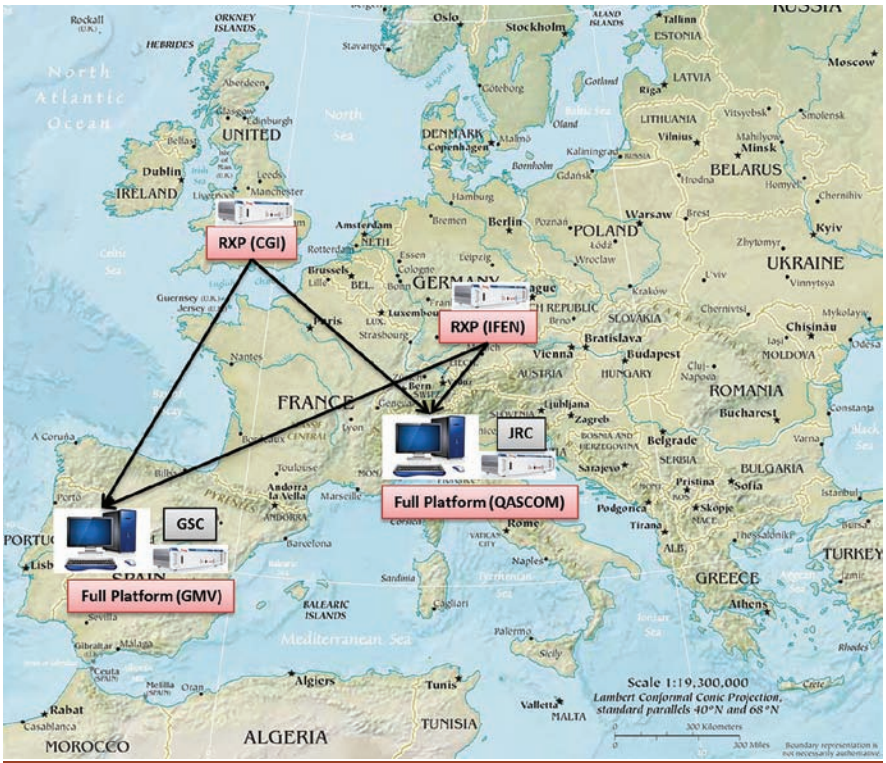


FIGURE 4 AALECS in the field

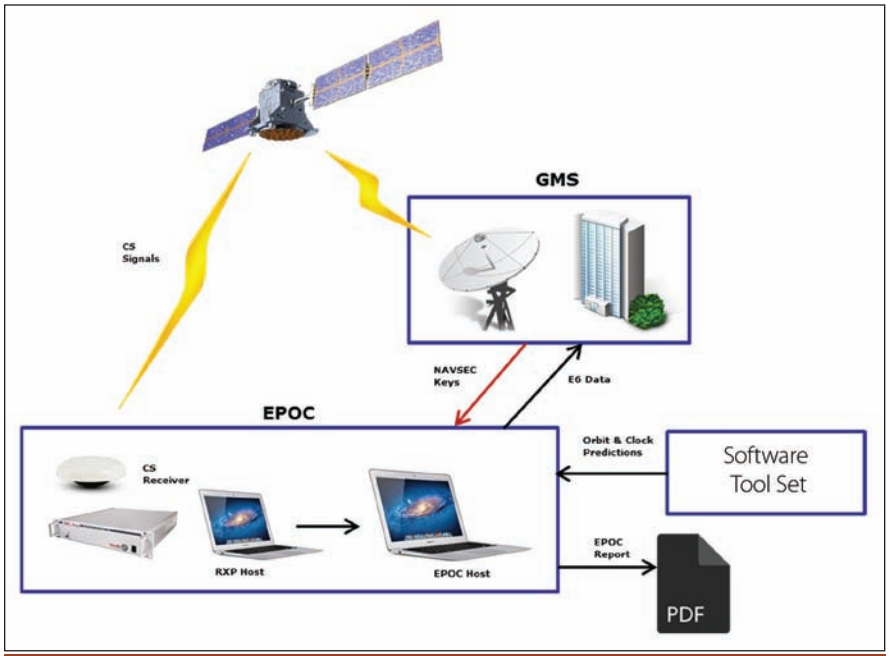


FIGURE 5 EPOC tests data flows

in the E6 signal. It also includes the historical archive, where the generated and received data is stored, and a software tool that analyzes the received data.

Each EPOC test consists of the following steps:

- A commercial, off-the-shelf software product — consisting of a set of software tools that supports a wide variety GNSS performance and accuracy analyses — generates satellite orbit and clock predictions for the desired testing period. (See "Manufacturers "section near the end of this article for more details. Note that the AALECS project does not finance or call for the development or adaptation of any high accuracy technologies.)
- Based on the software tool set's predictions, the EPOC generates CS data files in the E6-B message structure format and sends them to the GCC operator.
- The GCC operator performs the required "sanitization" activities to insure that the files are correct and their incorporation into the navigation message does not pose a risk to the system. The CS data is uploaded to the satellites via an uplink station and injected into the signals; then the Galileo satellites start broadcasting the E6-B data.
- During the periods of transmission, the EPOC collects the data in the receiver. Then, in post-processing, it obtains the transmission metrics, the authentication solution, and the PVT solution, producing a comprehensive report with the most relevant information.

In addition to the foregoing, for tests with SCE enabled, the EPOC operator needs to install the NAVSEC key (i.e., the key used to encrypt the E6-B/C components) in the receiver, to enable decryption of the spreading code.

Generating High Accuracy and Authentication Data

Figure 6 shows the format of the HA and authentication data transmitted in the EPOC tests. The HA data generated by the software tool set is formatted in 160-bit messages, each of which contains the predicted XYZ position and clock bias of a given satellite at a given epoch. These 160-bit messages are authenticated and packed together to fit in the 448 bps available in the E6 pages.

The current format allows for 8 HA sections every 5 seconds, for a total of 48 HA sections every 30 seconds. All Galileo satellites synchronously transmit the same 30-second sequence of authenticated HA data for 32 GPS + 3 Galileo satellites. The remaining HA sections are left empty.

Data obtained from the International GNSS Service (IGS) Multi-GNSS Exper-

iment (MGEX) station network feeds the software tool set in order to generate the satellite ephemerides and clock products. One of the major limitations of the EPOC compared with a future operational CS is the data latency: Satellite orbit and clock predictions had to be generated and transmitted to the Galileo operator about two days in advance of the planned test; therefore, the age of the predicted products — and associated decorrelation of real-time and predicted data — limited EPOC's achievable PVT performance.

The authentication solution used for the EPOC is an adaptation of the Timed-Efficient Stream Loss-tolerant Authentication (TESLA) algorithm described in the article by A. Perrig *et alia* listed in the Additional Resources section near the end of this article. TESLA seems more bandwidth-efficient compared to other solutions, such as standard digital signatures.

The proposed TESLA implementation is based on a single one-way chain of 256-bit keys for data authentication. An initial random seed key (K_n) generates this chain by performing a given number of hashes using the SHA-256 algorithm. The key-chain is generated from K_n to K_0, but keys are disclosed to the user from K_0 (certified as correct through non-SIS means in this implementation) to K_n, as shown in **Figure 7**.

This approach enables the user to recover an old key from a recently disclosed one, while insuring that future keys cannot be inferred from disclosed ones. As shown in Figure 6, out of five seconds of the data message, four are devoted to authenticated HA data and one to the authentication key, plus a bit pattern to differentiate key pages from HA pages, and a *message authentication code* (MAC) of the preceding HA packet (HAP) authenticated with a key delivered 30 seconds later. This MAC is intended to resist data spoofing attacks to receivers with very inaccurate clocks using already disclosed keys, and is called "Long Term Authentication" by the EPOC developers (as opposed to "Short Term Authentication," which refers to all other cases).

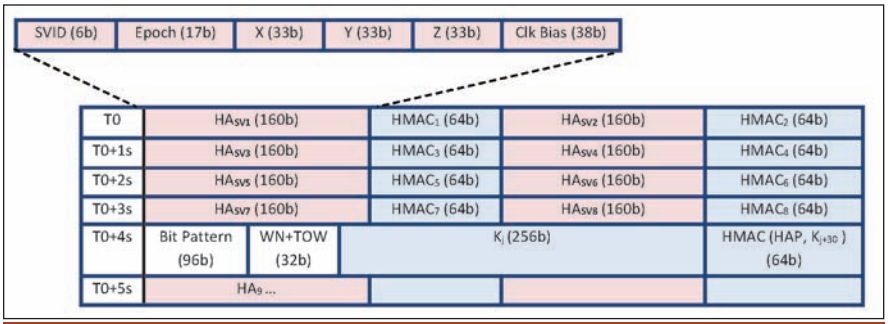


FIGURE 6 EPOC high accuracy and authentication data format

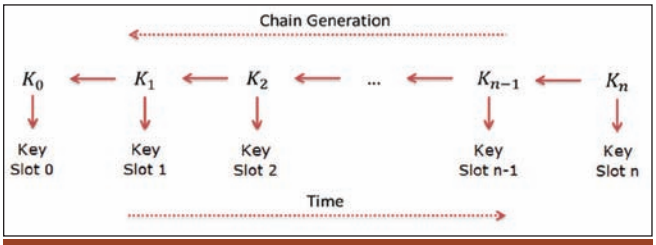


FIGURE 7 TESLA key chain generation/key slot description

The keys are used to authenticate the HA 160-bit data through a hash-based MAC (HMAC) function truncated to 64 bits. The receiver can then verify the authenticity of the HA data by comparing the MAC generated from the HA data and the later disclosed key, with the previously received MAC.

In the Additional Resources section, further details on the authentication solution implemented in the EPOC can be found in the article by D. Calle *et alia*, and additional details about TESLA-based implementations for satellite-based navigation in the articles by C. Wullems *et alia,* S. Lo and P. Enge, and J. T. Curran *et alia*.

We must emphasize that *this message structure and data definition have been implemented for testing purposes only* and are not bandwidth-optimized, neither for high accuracy nor for authentication. We must also highlight the fact that future HA and authentication services are expected to be provided separately, although they may be combined in the receiver.

EPOC Testing

The EPOC Signal-In-Space (SIS) test campaign had two main objectives. The first was to check that the Galileo system and signals were capable of delivering the future CS. This implies testing the E6-B data transmission, including synchronization aspects, the satellite uplink process, potential data glitches or duplications, spreading code encryption and decryption, and correct signal transmission in terms of power and modulation. The second objective was to evaluate the potential of Galileo-based high accuracy and authentication applications, including open sky/urban and static/dynamic use cases.

Test slots were predicted that would guarantee the best visibility of the three available Galileo in-orbit validation (IOV) satellites over GMV's premises in Madrid. Based on these predictions and other operational constraints, six-hour slots were allocated to the EPOC SIS tests on a weekly basis.

The test campaign began on June 12 and finished on September 30, 2014, with the following main outcomes:

- A total of 18 tests were executed: 4 "dry runs" involving no data transmission, 10 static/open-sky tests, and 4 dynamic tests in open-sky and urban conditions.
- Out of the 10 static tests, E6-B/C spreading code encryption was activated for 3 of them, between July 15 and 25. These were reflected in Notice Advisories to Galileo Users (NAGUs). The signals were transmitted in the clear the rest of the time.
- More than 83 hours of generated, transmitted, and received E6 data from the available IOV satellites were recorded.

- A GPS L1/L2 + Galileo E1/E5 PPP solution based on E6-B corrections was implemented. As satellite E20 was not available, Galileo-only PVT could not be calculated.

The following sections describe the results obtained in terms of data transmission, authentication, and high accuracy. We will analyze the test performed on July 22 in detail as it illustrates the results obtained under nominal conditions in most of the other tests.

Data Transmission Results

Figure 8 shows the *tracking profile* for satellites E11, E12, and E19 for the July 22 test, which was performed with SCE activated. The figure shows that dummy messages (broadcast when no data is uplinked) were transmitted due to a scheduled uplink station handover for E12 and E19 at around 19:40 UTC. A similar event is observed for E19 around 23:15 UTC. Two repeated-or-missing messages of two seconds each occurred for E19 between 21:30 UTC and 22:00 UTC. This is due to the current data uplink process, which is based on data files of some minutes' duration and will be replaced in future Galileo versions by a continuous data stream.

As expected, some tracking losses were observed at the end of the satellite pass, principally when satellites were at a 5/7-degree elevation. A few other tracking losses were observed due to receiver or environmental issues, but overall the page-loss ratio was below 0.5 percent.

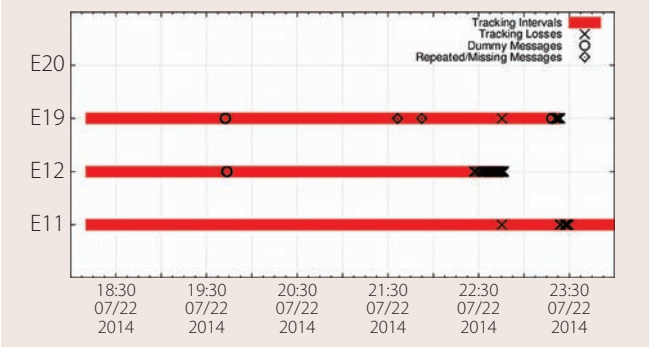


FIGURE 8 E6-B tracking profile (SCE-enabled) from July 22, 2014

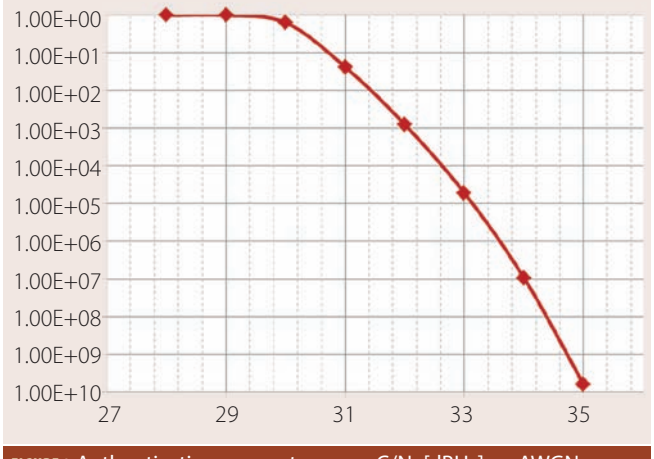


FIGURE 9 Authentication error rate versus C/N_0 [dBHz] on AWGN channel

Other tests confirmed this good data transmission performance and also showed that SCE and decryption at the receiver are correctly implemented.

These results demonstrate that a seamless synchronization was achieved during almost all of the several hours of tests. This feature is very important not only for the HA data transmission but also for the TESLA-based authentication requirements, which require fully synchronized messages. In summary, the field testing has demonstrated the correct transmission of external data through the E6 signal. Given that the Galileo system is still under deployment and the performance is expected to improve, we consider the data transmission results to be very good.

Authentication Results

Before presenting the results, we can characterize the authentication performance theoretically in terms of *authentication error rate* (AER), *time between authentications* (TBA) and *time to first authenticated fix* (TTFAF) as described in the article by I. Fernández Hernández *et alia* (2014a).

TBA is five seconds without SCE and zero seconds with SCE, as the receiver can navigate with previously authenticated data and continuously re-authenticated spreading codes. TTFAF is around 30 seconds (the time to receive from E6 all the HA data, excluding the time for a PPP algorithm to converge and the potential need to extrapolate from two XYZ given satellite datasets). As regards AER, it is calculated as follows:

$$AER + 1 - (1 - BER)^{NNA} \quad [1]$$

where BER is the bit error rate, calculated according to the method described in the book by E. Kaplan and C. Hegarty (see Additional Resources), and NNA is the number of bits for navigation and authentication, which for a given authentication verification are 480 bits (160 + 64 + 256), as per Figure 6. **Figure 9** characterizes AER versus the carrier-to-noise power spectral density ratio (C/N_0) analytically for an additive white Gaussian noise (AWGN) channel.

By way of example, **Figure 10** shows the actual (short-term) AER versus C/N_0 results from the July 22 test for E11, E12, and E19. AER was measured every 30 seconds, i.e., it was the percentage of failed data authentications per satellite every 30 seconds out of the total expected authentications. Some spikes observed for E12 and E19 at around 19:40 UTC are related to the previously mentioned uplink transition.

Some smaller spikes observed for E19 between 21:30 UTC and 22:00 UTC are related to the aforementioned data file desynchronization. This latter event affected TESLA synchronization leading to failed authentications. All other AER spikes are related to C/N_0 drops. The figures show that, at a C/N_0 below 40 dBHz, AER starts to increase. Further analyses are ongoing to understand the discrepancy with respect to the theoretical

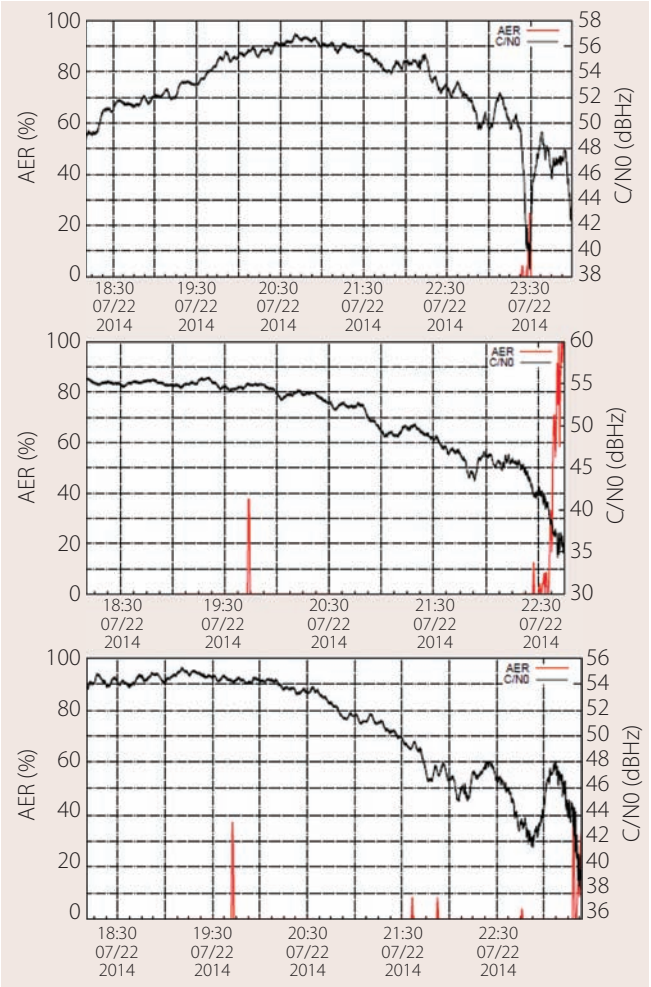


FIGURE 10 Five-second authentication error rate versus C/N_0 for E11 (top panel), E12 (middle), and E19 (bottom)

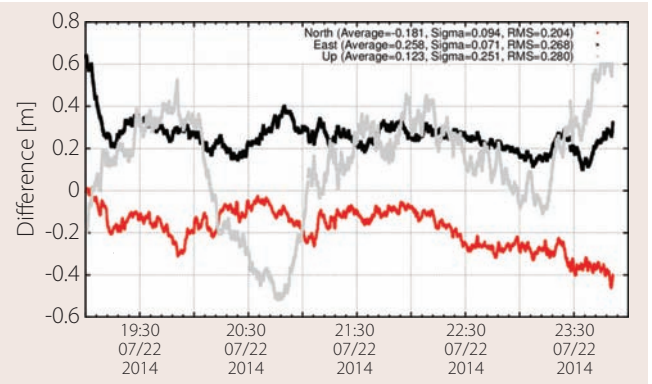


FIGURE 11 Data-authenticated PVT positioning error 22/07/2014 – static open sky

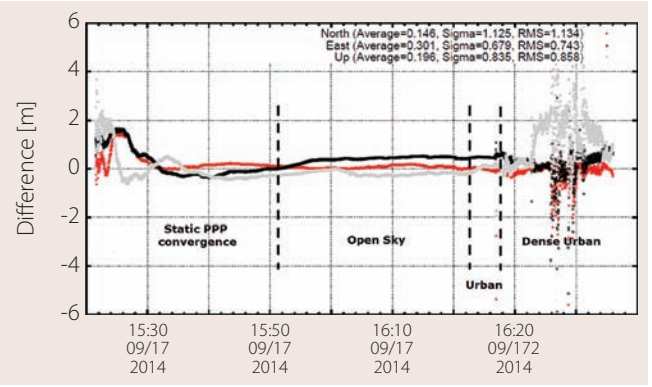


FIGURE 12 Data-authenticated PVT positioning error September 17, 2014, dynamic open sky/urban test

values, and C/N_0 higher than expected, which seem due to a C/N_0 overestimation in the receiver.

All in all, these valuable results show how asymmetric authentication can work in a real satellite navigation system. They also confirm the feasibility of data authentication through Galileo, which can be extremely valuable in thinking of future data-based and even spreading-code–based open authentication services for future Galileo generations. One could, for example, foresee a scheme whereby spreading codes are watermarked with a TESLA key and transmitted some time before the key is disclosed.

High Accuracy Results

This section presents some data-authenticated high accuracy results. As only three Galileo satellites were available during the tests, positioning was calculated using signals from GPS as well as Galileo. **Figure 11** shows the 3D accuracy obtained in a July 22 static open-sky test with data-authenticated corrections sent by Galileo satellites E11, E12, and E19 through E6-B. HA data was transmitted 48 hours after its generation by the software tool set.

The performances are remarkably good given the age of corrections and show accuracies on the order of decimeters. So, the CS performance appears promising, especially taking into account that the target data latency for Galileo is on the order of seconds rather than days.

Figure 12 shows the authenticated high-accuracy performance on September 17 during a kinematic test, including open-sky and deep urban environments, as well as around GMV's premises in Tres Cantos, Madrid. **Figure 13** shows the trajectory followed.

For this test, HA data was transmitted 15 hours after its generation. The solution remains stable after the convergence period (due to good modeling of satellite clock behavior) and is only destabilized when the environmental conditions go beyond a certain level of severity. The first signs of instability are seen at 16:25 UTC, and then the position solution is definitely destabilized by 16:35 UTC.

Although the accuracy results are not as good as in other cases, due to a higher error in the clock predictions for this particular test, they are still very good and — to the knowledge of the authors — better than the accuracy provided to date by the navigation message of any global navigation system. (Note that the user error includes not only the orbital and clock error but also propagation and receiver effects.) We should also point out that, even under harsh urban conditions, the AER of E12,

FIGURE 13 Data-Authenticated PVT trajectory from a kinematic test of the Galileo Commercial Service (Tres Cantos, Madrid; green: open sky; yellow: urban – dense urban)

the only satellite visible, remained very low, leading to almost no degradation of the authenticated versus non-authenticated performance, as shown in **Figure 14**.

These results, we conclude, demonstrate the feasibility of obtaining high accuracy from the Galileo Commercial Service, even with the substantial latency imposed by the test design. When this latency is reduced, we expect the achievable performance can be much higher — down to the centimeter-level error of state-of-the-art, high-accuracy services.

Conclusions and Next Steps

This article has presented the Galileo Commercial Service as it stands now, including its brief history, its signals, its anticipated services, architecture, and early field testing.

Galileo, through the Commercial Service, presents relevant differentiators with respect to other systems, such as an external data transmission channel and spreading code–encrypted signals for purely civil purposes. These capabilities, even if limited for the time being, have demonstrated accurate positioning and authentication, as shown in detail for the first time in this article. The test results are remarkable, considering that an accuracy at the decimeter level has been achieved by a standalone receiver with two-day-old orbit and clock predictions. Further, data and code authentication schemes over civil GNSS signals have been tested for the first time, to the knowledge of the authors.

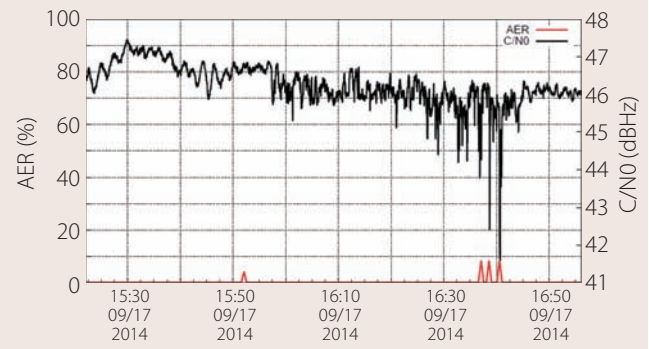


FIGURE 14 ST AER versus C/N_0 of E12, 17/9/2014

In the years to come, Galileo has a great opportunity to deliver highly accurate and robust services worldwide. In spite of the many challenges ahead, the authors believe that the Galileo program will be capable of turning the test results of today into the operational services of tomorrow for the benefit of industries and citizens.

Acknowledgments

The authors would like to thank the people that made possible the transmission of the E6-B signal-in-space data, principally Spaceopal and ESA teams, all of the people involved in the AALECS project, and GSA Communications Department.

Manufacturers

The EPOC test set up used magicGNSS from **GMV,** Tres Cantos, Madrid, Spain, to generate satellite orbit and clock predictions, and a NAVX-NTR receiver from **IFEN GmbH,** Poing, Germany. The map data in Figure 13 came from **Google Inc.**, Mountain View, California USA; **CNES/Spot,** Toulouse, France; **Digital Globe,** Longmont, Colorado; and **Terrametrics, Inc.**, Littleton, Colorado, USA.

Additional Resources

[1] Calle, D., and E. Carbonell, I. Rodriguez, G. Tobias, E. Göhler, O. Pozzobon, M. Canale, and I. Fernández Hernández, "Galileo Commercial Service from the Early Definition to the Early Proof-Of-Concept," *Proceedings of the ION GNSS 2014+,* Tampa, Florida USA

[2] Curran, J.T., and M. Paonni and J. Bishop, "Securing the Open-Service: A Candidate Navigation Message Authentication Scheme for Galileo E1 OS," *Proceedings of ENC 2014,* European Navigation Conference, Rotterdam, Netherlands

[3] European Union, European GNSS (Galileo) Open Service Signal In Space Interface Control Document, 2010

[4] European GNSS Service Center, Notice Advisories to Galileo Users <http://www.gsc-europa.eu/system-status/user-notifications-archive>

[5] European Union, "Regulation (EU) No 1285/2013 of the European Parliament and of the Council," Brussels: *Official Journal of the European Union,* 2013

[6] Fernández-Hernández, I. (2014a), and V. Rijmen, G. Seco-Granados, J. Simón, I. Rodríguez, J. David Calle, "Design Drivers, Solutions and Robustness Assessment of Navigation Message Authentication for the Galileo Open Service," *Proceedings of the ION GNSS 2014+,* Tampa. Florida USA

[7] Fernández Hernández, I., (2014b) and J. Simón, R. Blasi, C. Payne, T. Miquel, and J. P. Boyero, J. P. (2014). "The Galileo Commercial Service: Current Status and Prospects," *Coordinates,* July 2014, pp. 18–25

[8] Kaplan, E., and C. Hegarty, *Understanding GPS: Principles and Applications,* 2nd Edition, Artech House, 2005

[9] Lo, S., and P. Enge, "Authenticating Aviation Augmentation System Broadcasts," IEEE/ION Position Location and Navigation Symposium (PLANS), Indian Wells, California USA, 2010

[10] National Telecommunications and Information Administration, U.S. Department of Commerce, "1240-1300 MHz," *NTIA Publications,* 2014

[11] Parkinson, B., "Assured PNT - What actions can/should be taken to reduce vulnerability and ensure PNT availability?" *Proceedings of ENC 2014,* European Navigation Conference, Rotterdam, Netherlands

[12] Perrig, A., and R. Canetti, J. D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," *CryptoBytes*, 5:2, Summer/Fall 2002, pp. 2-13

[13] Pozzobon, O., and C. Sarto, A. Pozzobon, D. Dötterböck, B. Eissfeller, E. Pérez, D. Abia , "Open GNSS Signal Authentication Based on the Galileo Commercial Service (CS)," *Proceedings of the 26th ION GNSS+ 2013,* September 16–20, 2013, Nashville, Tennessee USA

[14] Wullems, C., and O. Pozzobon and K. Kubik, "Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems," in *Proceedings of the 2005 European Navigation Conference GNSS,* Munich, Germany

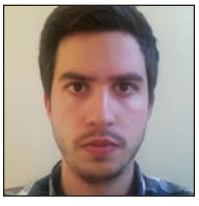
Authors

Ignacio Fernández Hernández is the manager and design lead of the Galileo Commercial Service at the European Commission, DG ENTR, since 2012. He also chairs the Galileo CS EU Working Group. Previously, he coordinated the GNSS user segment activities at the European Commission DG TREN and the European GNSS Agency, where he supervised several R&D and standardization projects and co-chaired the U.S.-EU ARAIM technical group. Prior to that, he was involved in the EGNOS program as system engineer and system test manager. He holds a MSc degree in electronic engineering from ICAI, Madrid, and a MBA from London Business School, United Kingdom.

Irma Rodríguez is head of the GNSS Algorithms, Products and Services Division within the GNSS Business Unit of GMV. After working in the development, validation, and testing of the Galileo OSPF (orbit and synchronization processing facility) and integrity algorithms, she was the managerial and technical responsible for several projects and studies related to GNSS algorithms. In 2013, she was the project manager for one of the two parallel studies launched by the European Commission for the definition of the Galileo Commercial Service. She is now the responsible for a division in charge of, among other activities, the GMV's *magicODTS* and *magicPPP* services and the Galileo CS Demonstrator.

Guillermo Tobías holds an MSc in telecommunication engineering from the University of Zaragoza. He has more than seven years of experience in GNSS, notably in the area of precise orbit determination and clock synchronization, and precise point positioning (PPP), including contributions to the Galileo program and the International GNSS Service (IGS). He has been the GMV's responsible for the *magicGNSS* suite in recent years and for GMV's contribution to the Real-Time IGS Service. He is currently coordinating R&D activities related to PPP services and is the project manager for the development of the Galileo Commercial Service Demonstrator.

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



Enrique Carbonell has a master of science degree in aerospace from the Universidad Politécnica de Valencia (Spain) and Cranfield University (UK). He joined GMV in early 2014 and he has been working in the GNSS business unit designing and developing algorithms and applications. He is currently the responsible for the early proof-of-concept in the Galileo Commercial Service Demonstrator.

Gonzalo Seco-Granados received a Ph.D. degree in telecommunications engineering from Universidad Politècnica de Catalunya and an MBA from IESE, the graduate business school of the University of Navarra. From 2002 to 2005, he was with the European Space Agency, Netherlands. Since 2006, he is an associate professor at the Universidad Autònoma de Barcelona, where he coordinates the SPCOMNAV (Signal Processing for Communications and Navigation) group. His research interests include signal-processing techniques for advanced features of GNSS receivers and localization using next-generation wireless communications networks.

Javier Simon is a service design engineer within the European GNSS Agency (GSA), currently contributing to the definition and design of the Galileo Commercial Service. He holds a MSc. degree in telecommunications engineering from the Polytechnic University of Madrid, Spain. Before joining GSA he participated in several projects for the study and design of future GNSS algorithms and systems.

Reinhard Blasi is the market development officer at GSA in charge of the EGNOS and Galileo market entry in the professional high-precision market. He gained his management experience as a strategy consultant during national and international assignments at innovation projects in various industries. He holds a degree in business administration and master's degree in international business studies conducted in the Universities of Paderborn (Germany), Lille (France), and Bologna (Italy). IG