IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Space-Based Navigation Systems and Services (5)

Author: Dr. Ignacio Fernandez Hernandez
European Commission, Belgium

Mr. Giovanni Vecchione
Rhea Group, Belgium
Mrs. Flor Diaz Pulido
European Commission, Belgium
Mr. Marc Jeannot
European Commission, Belgium
Ms. Giedre Valentaite
European Commission, Belgium
Mr. Reinhard Blasi
European Union Agency for the Space Programme (EUSPA), Czech Republic
Mr. Joaquin Reyes
European Union Agency for the Space Programme (EUSPA), Czech Republic
Mr. Javier Simon
European Union Agency for the Space Programme (EUSPA), Czech Republic

GALILEO MESSAGE AND SIGNAL AUTHENTICATION SERVICES: A PROGRAM AND POLICY PERSPECTIVE

Abstract

In our society, information based on GNSS signals has become a commodity, a basic need for many of our daily activities as electricity or internet. However, civil GNSS signals have not been designed to be resistant to intentional attacks such as spoofing; a common receiver can be tricked to accept a non-authentic GNSS signal. It is important to assure that the message received by the end-user is identical to the transmitted one and that it has been generated by a trusted source.

In 2013, the implementation of authentication for Galileo was recommended by an independent expert group. On this basis, after a few-year feasibility study, the Programme decide to incorporate to its service baseline:

• A Navigation Message Authentication (NMA) service, which consists on the digital signature of the navigation data of the Open Service (OS), to ensure the data authenticity. • A Signal Authentication service. This service largely concerns critical applications, which consist on transmitting encrypted ranging codes to ensure signal authenticity.

NMA is a simple, yet long-desired feature for GNSS, identified and confirmed by user needs and market analyses over the last years. Its level of protection is commensurate with its target users (e.g. mobile location, road). While other GNSS like GPS have studied NMA but are not in a position to implement it due to their signal and message properties, Galileo implements authentication both on E1 and E6 frequencies offering a competitive advantage and making Galileo a pioneer in this field. Another driver for the addition of OSNMA is the regulatory framework, and in particular the Digital Tachograph Regulation. Being unique Galileo feature, OSNMA is indeed a strategic enabler for the taking-up of Galileo to this and other future EU regulations.

On the other side, Galileo Signal authentication service will be based on the full encryption of the

E6C signal, initially designed as a pilot tone for the Commercial Service data signal (E6B) and so far been called "CS Authentication". It will rely on an external provider that will manage its user base, and will offer the service at a fee. CS Authentication will provide the highest level of robustness possible for GNSS commercial users, protecting against most possible spoofing attacks.

This paper will present the two services, their applications, and implementation roadmap, mainly from a policymaking perspective, but also including some information on what is expected from the services in terms of functionality and performance.