Implementation and Testing of OSNMA for Galileo

Carlo Sarto, Oscar Pozzobon, Samuele Fantinato, Stefano Montagner, *QASCOM*
Ignacio Fernández-Hernández, *European Commission*
Javier Simon, *European GNSS Agency*
Jesus David Calle, Simón Cancela Díaz, *GMV*
Paul Walker, Daniel Burkey, *CGI*
Gonzalo Seco-Granados, *Universitat Autonoma de Barcelona*
Eckart Göhler, *IfEN*

BIOGRAPHIES

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

Oscar Pozzobon received a master degree in Telecommunication Engineering from University of Queensland, Australia, and a Ph.D. from University of Padua, Italy. He is CTO and founder of Qascom, and involved in several activities on space, GNSS and cybersecurity with ESA, EC, GSA, NASA. He is adjunct professor at the University of Padua.

Samuele Fantinato is a Radio Navigation Systems Engineer at Qascom. He received a Master's degree in Telecommunication Engineering from the University of Padova in 2007. He is currently leading several projects on advanced navigation technologies including GNSS Space SDR receivers, GNSS Simulation Test Beds for space and ground based interference monitoring and mitigation and the validation of authentication schemes for Galileo.

Stefano Montagner is a Radio Navigation System and DSP Engineer at Qascom. He has been involved in the design of GNSS authentication and spoofing mitigation techniques and the development and testing of interference monitoring systems.

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

Javier Simon is Service Design Engineer within the European GNSS Agency, currently contributing to the definition and design of the Galileo OSNMA and CS services. He holds a MSc. degree in Telecommunications Engineering from the Polytechnic University of Madrid, Spain. Before joining GSA he participated in several projects for the study and design of future GNSS algorithms and systems

David Calle holds a MSc. in Computer Engineering from the University of Salamanca. He joined GMV in 2008 and he has been working in the GNSS business unit involved in the design and development of GNSS algorithms, applications and systems. He is currently Head of GNSS Services Section coordinating the activities related to the Galileo Commercial Service, Open Service Authentication and High Accuracy provision services.

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

Paul Walker is the Solution Architect at CGI responsible for navigation authentication design and development projects. He received a PhD in Physics in 1996 and has been a software engineer in the space sector since 1999.

Dan Burkey is a Software Engineer at CGI, currently engaged on the EGNOS Check Set G2 project. He previously worked on the AALECS PTB project, and the IRIS precursor programme. He holds a PhD in Astronomy from the Royal Observatory Edinburgh.

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

Eckart Göhler received his Diploma in physics from the University Tübingen and his Ph.D. from the Institute for Astronomy and Astrophysics, Tübingen. He worked as a lead software engineer at IFEN GmbH in the receiver technology department. Today he is employed at OHB System AG in the instrument software group.

ABSTRACT

A candidate specification of the protocol for the Galileo Open Service navigation message authentication (hereinafter referred to as OSNMA) has been implemented as part of the AALECS project (Authentic and Accurate Location Experimentation with the Commercial Service). The protocol has been integrated into an end-to-end demonstrator in order to evaluate its performance. The purpose of this paper is to present the testing framework that has been adopted in the AALECS experimentation activities and to report the first end-to-end test results. This includes worldwide service volume analyses with realistic satellite visibility and availability of satellites connected to the Galileo Uplink Stations, in order to characterize the entire system performance by simulation of the Galileo Full Operational Capability (FOC). These results allow evaluating in advance the achievable performances of a future Galileo OSNMA user considering the full system capabilities. This paper also partly addresses the fundamental requirements to implement Galileo Open Service Navigation Messages Authentication in the current and next generation of GNSS receivers, based on the lessons learned in the AALECS project.

INTRODUCTION

The authentication of civil GNSS services, and in particular navigation message authentication, has been proposed and studied in the literature for more than a decade [1] [2] [3]. A candidate protocol for Galileo Open Service Navigation Message Authentication has been recently presented [4] and fine-tuned for future Galileo signal-in-space testing. It is based on an adaption of the original Timed Efficient Stream Loss-Tolerant Authentication (TESLA) [5], already proposed for GNSS in [2], with two main optimizations: cross-authentication of some satellites by others, and the use of a single TESLA key or key chain for all satellites. Such a configuration allows GNSS receivers to receive each key from any satellites in view, differently from the case where different key chain per transmitted is employed, highly improving TESLA performance. The advantages of TESLA are to allow authentication on broadcasting services such as GNSS with the constrains of low bandwidth consumption and packet loss tolerance. This is particularly needed in Galileo as the NAV data has been already allocated and authentication schemes must be implemented in the available I/NAV spare/reserved capacity as per the Galileo OS SIS ICD [6]. The AALECS consortium developed an OSNMA end-to-end demonstrator platform that allows the execution of end-to-end tests in real and simulated environments, evaluating the preliminary service functionalities and performance in both nominal and threat scenarios.

REQUIREMENTS AND DESIGN DRIVERS FOR OSNMA INTEGRATION IN GNSS RECEIVERS

This section describes the main blocks and requirements to implement the Galileo OSNMA service in GNSS receivers. These general advices derive from the experience gained in the AALECS project. Receivers willing to implement OSNMA shall support at least the function of storage of OSNMA public keys, processing of the OSNMA data for every channel, processing some specific cryptographic functions and report the authenticated navigation messages to the navigation filter.

16 OSNMA public keys can be preloaded from factory in the receiver, and managed by a Merkle tree whose leaves are stored in a persistent read-write memory area, allowing for the update of the public keys through the reception of a DSM-PKR (Digital Signature Message – Public Key Renewal) message. A public key is used to authenticate (with asymmetric cryptography) the key received in a DSM-KROOT (Digital Signature Message – Root Key) message which, in turn, authenticates the TESLA root key used to validate the key transmitted in the MACK (MAC and key) sections.

The keys in the DSM-KROOT and in the MACK messages belong to a chain of keys generated with a one-way function, so that each element of the chain can be generated by hashing the previous element. The chain is disclosed through the DSM-KROOT and MACK messages in inverse order and, as consequence, the authenticity of a key received in a MACK message can be verified against a previously disclosed and verified key (being a key received through a DSM-KROOT or a MACK message). The storage of the full chain is not required as the key verification process requires the availability of just the last verified key of the chain.

The MACK sections also contain a number of MACs (message authentication codes) which are authentication tags providing authentication of the navigation messages. The verification of a MAC requires the availability of the navigation data to be verified and of a specific verified key of the chain, which is disclosed after the MAC. Note that the required key can be also retrieved from other satellites transmitting OSNMA data and performing the required steps in the chain to obtain the required key index. Figure 1 below shows a chain of TESLA keys, whereby the DSM-KROOT authenticates a new *floating root key* on a daily basis, as proposed and further explained in [7].

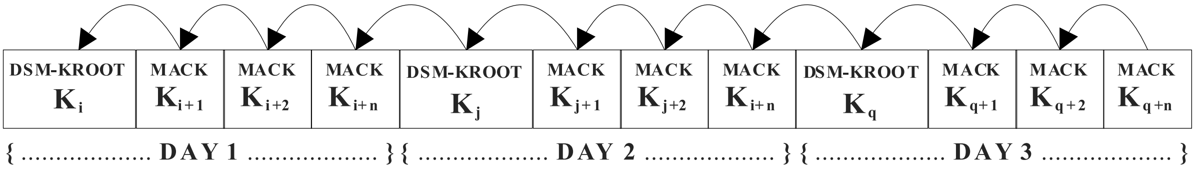


Figure 1: Chain of keys.

The routine for the decoding and processing of the OSNMA data can be executed in parallel with the receiver routine for the collection of the navigation messages, but with some constraints. Each received I/NAV page shall be processed by the OSNMA client in a sequential and time ordered manner (with knowledge of transmitting satellite and timestamp associated to each page). After checking the CRC, the OSNMA data (40 bits) can be extracted from the I/NAV page and then processed, in sequence, by a number of supporting sub-routines, outlined in Figure 2. The first step is for the extraction and processing of the HKROOT (Header and Root Key) data (available in the first 8 bits of each OSNMA 40 bits field). The second operation is the extraction and processing of the key (transmitted over the MACK section). The third step is the extraction and processing of the authentication tags. The last step is the verification of the received data with the authentication tags. Note that the extraction of the keys and tags does not require the full reception of the MACK section as keys and tags can be individually extracted from the available I/NAV pages, as soon as they are received. This approach considerably preserves the availability and performance of the service in degraded environment, where several pages might be affected by errors or not received at all.

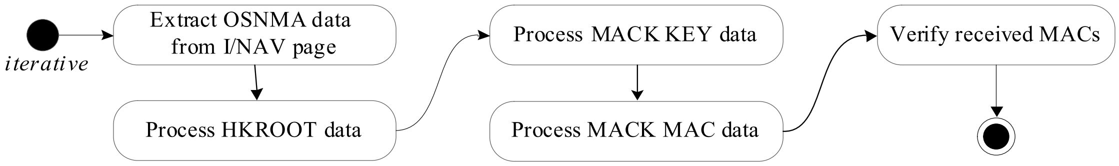
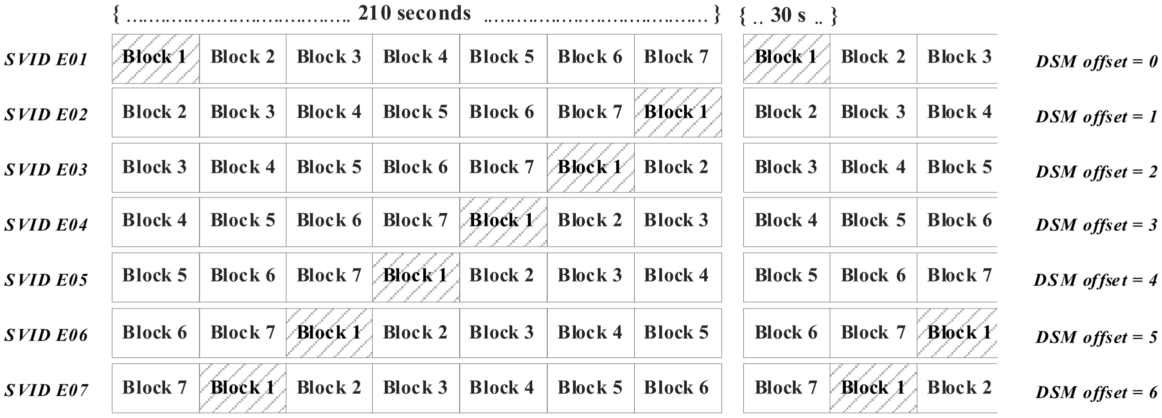


Figure 2: AALECS OSNMA data high level processing logic (UML activity notation).

The OSNMA protocol supports several signal-in-space configurations defined in terms of sizes and number of authentication tags, the size of the keys and the number of MACK sections transmitted in each I/NAV subframe. These parameters are required to start the decoding of the MACK sections and they are transmitted and authenticated with the DSM-KROOT message. A direct consequence is that the full reception of a DSM-KROOT message is required when the receiver is switch on for the first time or if the chain of keys (identified by the CID field) is changed. In accordance with the current OSNMA specification, during the validity period of the key chain, the DSM-KROOT message can be updated every day for the dissemination of a new, floating KROOT. Such a daily update of the KROOT would facilitate the first key verification process for power constrained receivers that have been switched off for a long time (e.g. days).

The DSM-KROOT message is split in multiple blocks, each transmitted over a I/NAV subframe (30 seconds). The total number of blocks composing the DSM-KROOT depends on the asymmetric algorithm in use (e.g. 7 blocks are required when using ECDSA P-256 [8]). In order to reduce the time required for the DSM-KROOT reception, the satellites transmit different blocks of the same DSM-KROOT according with a packet scheduling algorithm. At the time of writing this paper, the packet dissemination strategy implemented is based on a block offsetting algorithm [9] but optimizations are under study. The baseline algorithm defines that each satellite transmits the ordered sequence of packets, each satellite transmits the sequence with an offset known at the receiver (Figure 3 reports the configuration used in the experimentation: a relative offset corresponding to *mod(SVID – 1 , 7)* blocks is applied to each satellite). The offset between blocks transmitted by each satellite is known and as consequence the block ID, transmitted in the HKROOT section, can be inferred by just receiving the Block ID field from one of the satellite in view. Being the packet transmitted in incremental order, the past and future blocks transmitted by each satellite can be inferred by just receiving the BID field from one of the satellite in view. These considerations allow to implement the reception of the DSM-KROOT data on a per-byte basis, not requiring for the full reception of a full block and, as consequence, speeding up the reception process and at the same time ensuring acceptable performance in a degraded environment (where the reception of all the BID fields and in general of full I/NAV subframe might be difficult).



	{ …………………………………… 210 seconds						…………………………………… }	{ .. 30 s .. }			
SVID E01	Block 1	Block 2	Block 3	Block 4	Block 5	Block 6	Block 7	Block 1	Block 2	Block 3	*DSM offset = 0*
SVID E02	Block 2	Block 3	Block 4	Block 5	Block 6	Block 7	Block 1	Block 2	Block 3	Block 4	*DSM offset = 1*
SVID E03	Block 3	Block 4	Block 5	Block 6	Block 7	Block 1	Block 2	Block 3	Block 4	Block 5	*DSM offset = 2*
SVID E04	Block 4	Block 5	Block 6	Block 7	Block 1	Block 2	Block 3	Block 4	Block 5	Block 6	*DSM offset = 3*
SVID E05	Block 5	Block 6	Block 7	Block 1	Block 2	Block 3	Block 4	Block 5	Block 6	Block 7	*DSM offset = 4*
SVID E06	Block 6	Block 7	Block 1	Block 2	Block 3	Block 4	Block 5	Block 6	Block 7	Block 1	*DSM offset = 5*
SVID E07	Block 7	Block 1	Block 2	Block 3	Block 4	Block 5	Block 6	Block 7	Block 1	Block 2	*DSM offset = 6*

Figure 3: Scattered transmission of DSM-KROOT blocks using AALECS assumption on the packet scheduling algorithm.

OSNMA EXPERIMENTATION

AALECS provides a sophisticated testbed able to emulate the Galileo infrastructure involved in the OSNMA provisioning. The test campaign of the project is divided in two initial phases: the first phase is for the execution of laboratory tests; and the second phase has been designed to increase the realism of the simulation by using raw navigation data recorded from SIS.
In the first experimentation phase, an advanced simulation environment has been designed based on the project assets and the European Commission (EC)'s Joint Research Center (JRC) simulation capabilities in Ispra, Italy. It includes the emulation of satellite channel models that allow realistic simulation of different user environments (e.g. urban, suburban, open field, etc.). In the second experimentation phase, a novel working mode called Advance Replay Mode (ARM) has been implemented and presented in [10]. The ARM mode can evaluate the achievable user performance of future services without actually transmitting the data through the Signal in Space. This working mode can be considered as very representative of the real environment since the actual observed bit errors are injected in the future data (OSNMA in our case) generated by the AALECS Demonstrator. This approach allows performing tests in which the data demodulation errors, multipath effects and signal degradation is representative of what a future OSNMA users will experience. This phase has been specifically defined to allow the experimentation with real signals before the OSNMA Signal-in-Space (SIS) is available.

The ARM requires the simultaneous usage of two GNSS receivers located nearby. The first receiver shall be used as reference station (collecting error free I/NAV navigation messages). The second one is used as a rover, collecting observable and navigation messages affected by the user environment errors. Figure 4 depicts the ARM processing steps: the recorded data navigation messages of the two receivers are compared to detect the observed errors and create (1) a map of bit errors; the error free navigation messages are then used in combination with a given OSNMA configuration to generate (2) the OSNMA data; the bit errors map is then applied (3) to the OSNMA data which is finally injected (4) in the recorded rover navigation messages. The resulting output is a log file with the rover navigation messages including the OSNMA data but preserving the observed navigation messages availability and errors.

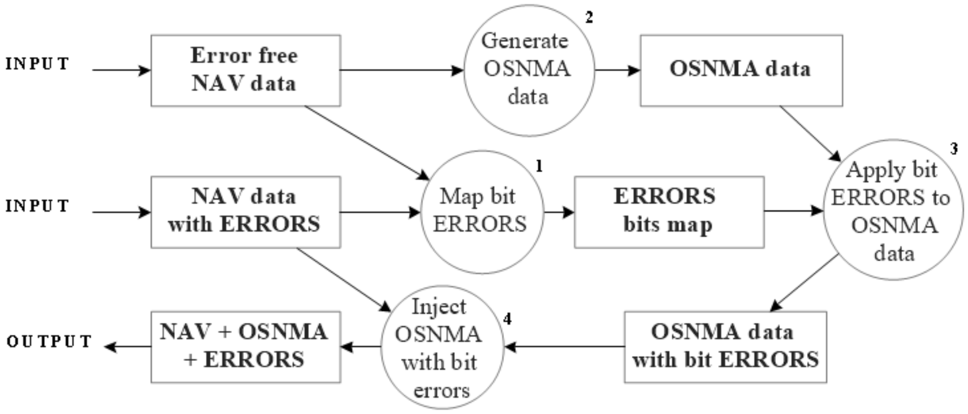


Figure 4: Advanced Replay Mode (data flow of navigation messages processing).

Test specification and performance metrics

The results reported in the following sections are generated using a baseline OSNMA configuration (reported in Table 1). This configuration allows for 4 MACs being hosted in each MACK section (a total of 8 MACs per I/NAV Subframe). MACs are used for authentication of Galileo satellites only, with cross-authentication option enabled.

Table 1: OSNMA configuration used for testing

OSNMA parameter [1]	**Description**	**Value**
DSF	Digital Signature Function	ECDSA P256
NB	Number of DS blocks	7
NMACK	Number of MACK sections	2
HF	Hash Function	SHA-256
MF	MAC Function	SHA-256
KS	Key Size	128 bits
MS	MAC Size	12 bits
NM	Number of MACs per MACK section	4
ADKD (authentication data and key delay) sequence	ADKD sequence of the MACs transmitted in a subframe	[0,0,0,0,0,0,4,0] 0: Words 1-5 are authenticated 4: Other data authenticated
Cross-authentication sequence	(“C0” stands for self-authentication, “N” for non-connected and the number refers to the sorted list of closer neighbors)	[N5,N4,N3,C0,N2,N1,N/A,C0]

The simulated tests use a constellation of 24 satellites. The tests using real data still assume a constellation of 24 satellites but only 16 satellites where actually usable for testing at the time the data has been recorded (June 19th and 21st 2017). The impact of the ground segment has been simulated with GSS and ULS stations placed in Kourou, Reunion, Svalbard, Noumea and Tahiti.

The metrics used to measure the performance were:

- PAF: Probability of authentication failure (%) is the percentage of failed data authentication verification events against the total number of data authentication verification events of a given satellite.
- SAF: Average satellite authentication period (s) is the average time elapsed between successful data authentication verification events of a given satellite.
- ADA-S: Authenticated data availability at satellite level (%) is the percentage of time, over the total time the satellite is in full tracking status, in which the user has authenticated data for that satellite. Satellite is declared available after the navigation data is authenticated, thus considering that authentication shall be performed only if authenticated data is not available (rising satellite case or cold start cases). It is assumed that if the IODnav changes the new set of data can be authenticated with some seconds delay (without affecting availability KPI).

- ADA-U: Authenticated data availability at user level (%) is the percentage of time, against total observation time, the user has authenticated data for at least 4 of the satellites being tracked. Authenticated data availability at user level is calculated considering as total observation time the period starting from the first authenticated fix till the scenario end.
- ATFFD-4: Average Time To First Fix Data is the average time, in seconds, required to successfully retrieve Word 1 to 5 data from I/NAV E1-B (thus only considering pages for which the CRC is successfully checked) for at least 4 satellites. The average is computed on the TTFFD calculated at different time into scenario. In the reported results, TTFFD is calculated by assuming a startup every 7 seconds, for approximately 500 times. The TTFFD value is also reported considering position fix possible even with 2 or 3 satellites (TTFFD-2 and TTFFD-3).
- ATFAFD-4: Average Time To First Authenticated Fix Data is the average time, in seconds, required to successfully retrieve Word 1 to 5 data from I/NAV E1-B (thus only considering pages for which the CRC is successfully checked) for at least 4 satellites and authenticate it (thus considering the successful reception of the required key and tag material). This KPIs is measured considering the applicable KROOT already available. The average is computed on the TTFAFD calculated at different time into scenario. In the reported results, TTFAFD is calculated by assuming a startup every 7 seconds, for approximately 500 times. As per the TTFFD, the TTFAFD is also reported considering position fix possible even with 2 or 3 satellites (TTFAFD-2 and TTFAFD-3).
- Average DSM reception time is the average time required to retrieve the DSM-KROOT message. The average is computed for DSM reception time at different time into scenario. In the reported results, the time into scenario for which the DSM reception time is calculated by assuming a startup every 7 seconds at each computation, for approximately 500 times.
- BER: Bit Error Rate is the number of bit errors per unit time.

Preliminary results obtained using real data

This section reports the results of two representative tests using navigation message and observables recorded in real environment (using the Advanced Replay Mode). The first test has been performed in a soft urban user environment while the second test in a harsh urban environment, as illustrated in Figure 5. The data has been recorded in two different days and as consequence the satellite in view and their geometries are different. The data of these scenarios have been recorded from an antenna placed on the roof of a vehicle moving in North Italy (near to Qascom headquarters) at a linear distance of approx. 240 Km from European Joint Research Center were the reference station, recording error free data, was located.

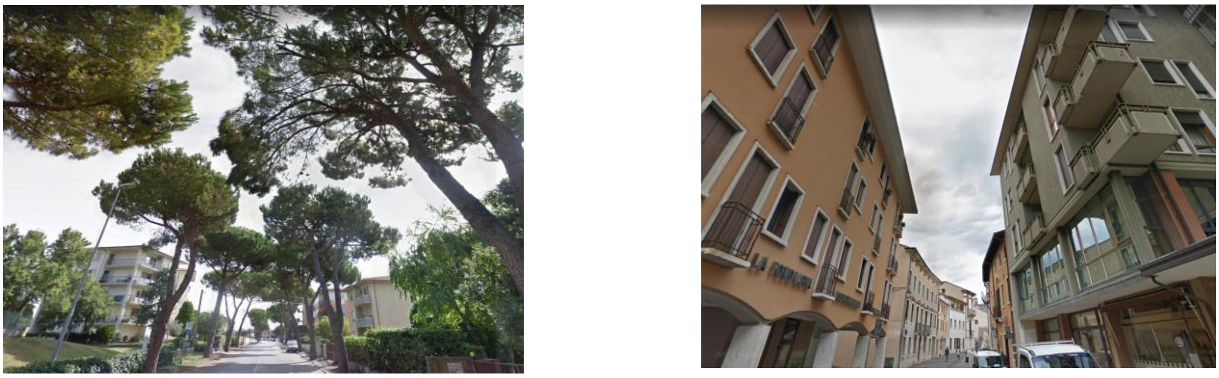
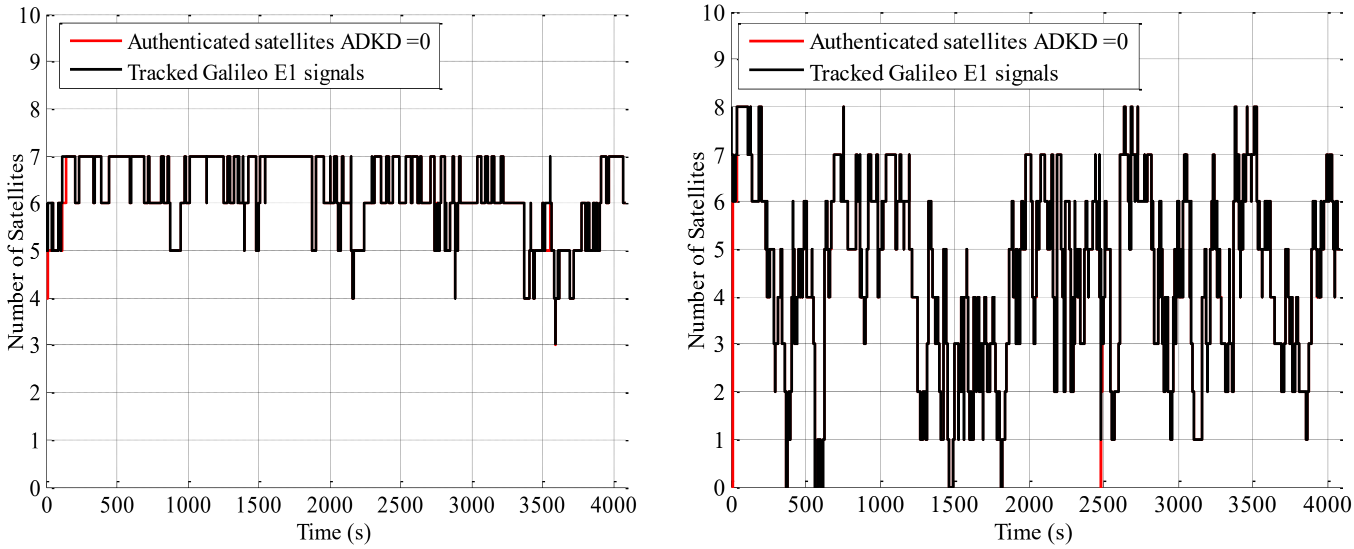


Figure 5: Example of soft-urban (left) and harsh-urban (right) scenarios, Qascom HQ surroundings.

During the soft urban scenario recording the number of visible satellites is generally between 5 and 7, and only for a short period of time below 4. The measured authenticated data availability at user level is of 99.92%, and it exactly matches the percentage of time there were at least 4 Galileo satellites being tracked. In this sense, no availability degradation has been observed due to the use of OSNMA. In the harsh-urban scenario only for the 67.73% of the time there were at least 4 satellites in view, navigation messages for at least 4 satellites were available for the 67.65% of the time, and authenticated navigation messages were available for the 67.65% of the time as well. Therefore, also in the harsh-urban environment no degradation due to OSNMA was observed. This is consistent with the expectations, as performance is mainly constrained by reception of the navigation data, and the addition of NMA interleaved with the navigation data, as per the current implementation, does not degrade performance even in hard environments.



(fig. A) (fig. B)

Figure 6: Number of tracked/authenticated channels for soft-urban (fig. A) and harsh-urban (fig. B).

In accordance with the results provided in Table 2 and Table 3, the OSNMA client was accepting as input only pages with integrity successfully validated by CRC. This means that under non-spoofing conditions, an authentication verification will be performed over CRC-corrected data and therefore the probability of authentication failure can be approximated to zero. From each stably-tracked satellite (i.e. excluding those satellites that have been tracked for less than 5 minutes), in average, every 30 seconds (corresponding to an I/NAV subframe) the client receives for each satellite 4.7 tags in soft-urban environment and 1.9 tags in urban environment. The values measured for the average authentication period metrics confirm the relevance of the cross-authentication feature that increases the redundancy of the authentication service. Still, excluding satellites that have been tracked for less than 5 minutes, the satellite availability is >99.8% for satellites both in soft-urban and harsh urban, thus confirming the packet loss tolerance feature of the TESLA protocol.

Table 4 shows the percentage of pages with all combinations of correct-incorrect navigation-authentication data. It shows that only between 3.4% and 6.7% of the messages would provide valid NMA data by ignoring the CRC. As mentioned above, only CRC-verified NMA data has been taken into account for the tests, and even in this configuration there is no availability degradation. The results prove that, in the analyzed environments and with the proposed configuration, it seems convenient to use NMA data that is verified by CRC.

Another relevant metric to measure is the delay introduced by the OSNMA service in the TTFFD-4, due to latencies introduced by the tag verification process that shall be performed in addition to the nominal navigation messages demodulation process. In the scope of the AALECS project, two approaches for the tag verification process have been experimented. The first approach, parallel processing, is designed to guarantee the best performances while the second one, called sequential processing, has been used to measure the performances of a less-optimized solution (that would generate the lower-bound performances). The parallel processing consists in the parallel demodulation of the navigation message and the corresponding authentication tags. The sequential processing consists in using only the authentication tags that have been received after the corresponding data to authenticate for a specific satellite. The sequential processing generates an intrinsic delay in the time the data becomes available, corresponding approximately to the average time required to retrieve the authentication material (tag and key). Activities parallel to the AALECS project are underway to consolidate the tags verification process considering the security requirements of the protocol.

As shown in Table 5, an average TTFFD-4 degradation of 0.53 seconds and 0.60 seconds in soft and harsh urban scenarios is observed, increasing respectively to 15 and 22 seconds when using sequential processing. However, the main latency peaks (affecting the average value) are observed whenever the IODnav changes. These peaks are caused by a limitation in the experimentation platform: the authentication tags can be generated (and then broadcasted) only after the new set of authentication navigation data is received from the satellite broadcasted E1-B navigation messages and thus introducing an intrinsic latency whenever the data changes. In a real implementation this effect is minimized, since the service provider would obtain I/NAV data to authenticate from both E1-B and E5-B, allowing to authenticate a new IODnav in the subframe it first appears.

Table 2: Key performance indicators (Soft-Urban).

SV ID	Elevation (decimal degrees)	BER	Number of decoded I/NAV page parts	Rate of decoded I/NAV page parts with errors	Probability of authentication failure	Average authentication period (s)	Authenticated data availability (%)
2	18 to 24	2.75E-02	3132	0.07567	0	6.43607	98.36066
4	19 to 41	2.65E-02	3485	0.07202	0	7.23022	99.78875
9	6 to 9	2.51E-02	185 *	0.08108	0	9.07143	80.66038
11	58 to 75	2.40E-03	4065	0.00812	0	5.76102	99.65686
12	64 to 45	4.24E-03	4038	0.01312	0	5.60552	100
14	32 to 12	2.33E-02	3124	0.06882	0	6.65139	100
19	32 to 35	1.13E-02	3829	0.03108	0	5.80571	100
24	27 to 6	2.58E-02	2104	0.07367	0	7.11752	100

Table 3: Key performance indicators (Harsh-Urban).

SV ID	Elevation (decimal degrees)	BER	Number of decoded I/NAV page parts	Rate of decoded I/NAV page parts with errors	Probability of authentication failure	Average authentication period (s)	Authenticated data availability (%)
2	30 to 49	5.36E-02	2932	0.14291	0	10.87332	100
3	34 to 13	6.61E-02	1674	0.16308	0	16.14516	100
5	10 to 5	4.48E-02	104 *	0.13461	0	46.52632	100
7	5 to 9	2.97E-02	316 *	0.06962	0	24.83871	73.4748
8	26 to 22	6.73E-02	1617	0.17069	0	18.85047	100
11	34 to 51	4.19E-02	2500	0.11640	0	12.45062	100
12	33 to 26	5.62E-02	1550	0.14968	0	21.12042	100
18	10 to 40	7.53E-02	1681	0.19631	0	16.46531	100
24	38 to 19	5.00E-02	1993	0.13698	0	14.00775	100

Table 4: Overall percentage of pages affected by errors.

NAV	OSNMA	Percentage of pages (%)	
		Soft-Urban	Harsh-Urban
Correct	Correct	93.14%	84.70%
Incorrect	Correct	3.40%	6.72%
Correct	Incorrect	0.013%	0.03%
Incorrect	Incorrect	3.442%	8.55%

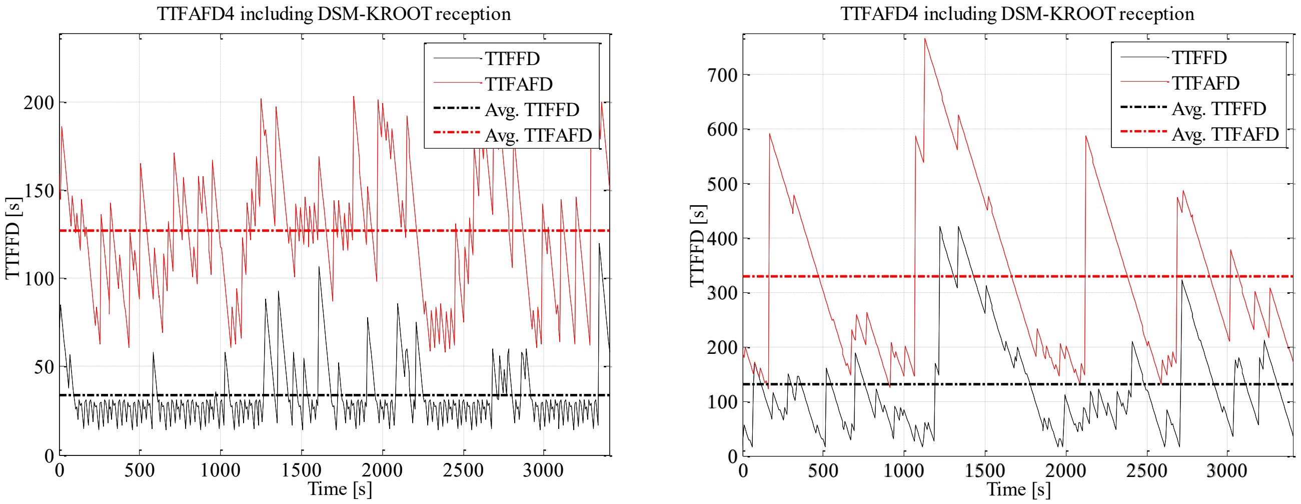
Table 5: Average Time-To-First-Fix Data.

TTFFD mode and user environment	2 SVs (seconds)	3 SVs (seconds)	4 SVs (seconds)
OS (Soft-Urban)	26.90656	28.77535	34.61233
OSNMA (Soft-Urban) parallel	27.01789	29.17296	35.14910
OSNMA (Soft-Urban) sequential	40.82424	42.68282	50.14949
OS (Harsh-Urban)	62.40606	89.79595	128.81818
OSNMA (Harsh-Urban) parallel	62.73333	89.98585	129.42222
OSNMA (Harsh-Urban) sequential	88.19595	118.5878	151.73535

The time it takes to obtain the DSM-KROOT message depends on several factors: the number of blocks composing the full message (which depends on the OSNMA configuration in use), the packet scheduling algorithm, the receiver implementation, and the number of visible connected satellites and on the presence of I/NAV page reception errors. The configuration used in these tests allows the reception of the full message in approximately 30 seconds in ideal conditions, consisting an open sky environment with 7 satellites in view, each transmitting a different block. Whenever DSM-KROOT reception is required when the receiver is switched on, a delay in the DSM-KROOT reception time might be observed (as reported in Table 6). Figure 7 shows that the TTFAFD-4 considering the DSM-KROOT reception follows the TTFFD-4 values calculated at different epoch in the scenario and thus confirming the expected effect of the user environment on the DSM-KROOT reception. In the harsh-urban scenario case two additional peaks caused by the limited number of satellites in view and high page error rate (as demonstrated by Figure 8) are observed at approximately 210 seconds and 2100 seconds of test time.

Table 6: Average DSM-KROOT reception time.

User environment	Average DSM reception time (seconds)	Average delay observed on TTFFD (seconds)
Open-Sky (ideal)	~30 (expected best value)	~3.1
Open-Sky	88.134 (average)	~62.6
Soft-Urban	128.818 (average)	~94.2
Harsh-Urban	329.143 (average)	~200,3



(fig. A)

(fig. B)

Figure 7: TTFAFD (average DSM-KROOT reception time) vs. TTFFD for soft-urban (fig. A) and harsh-urban (fig. B).

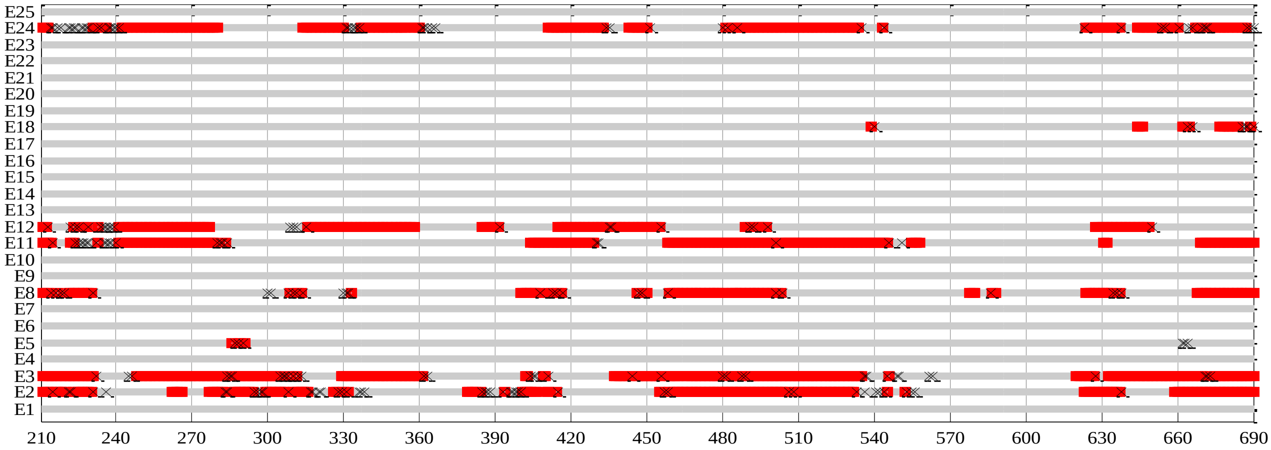


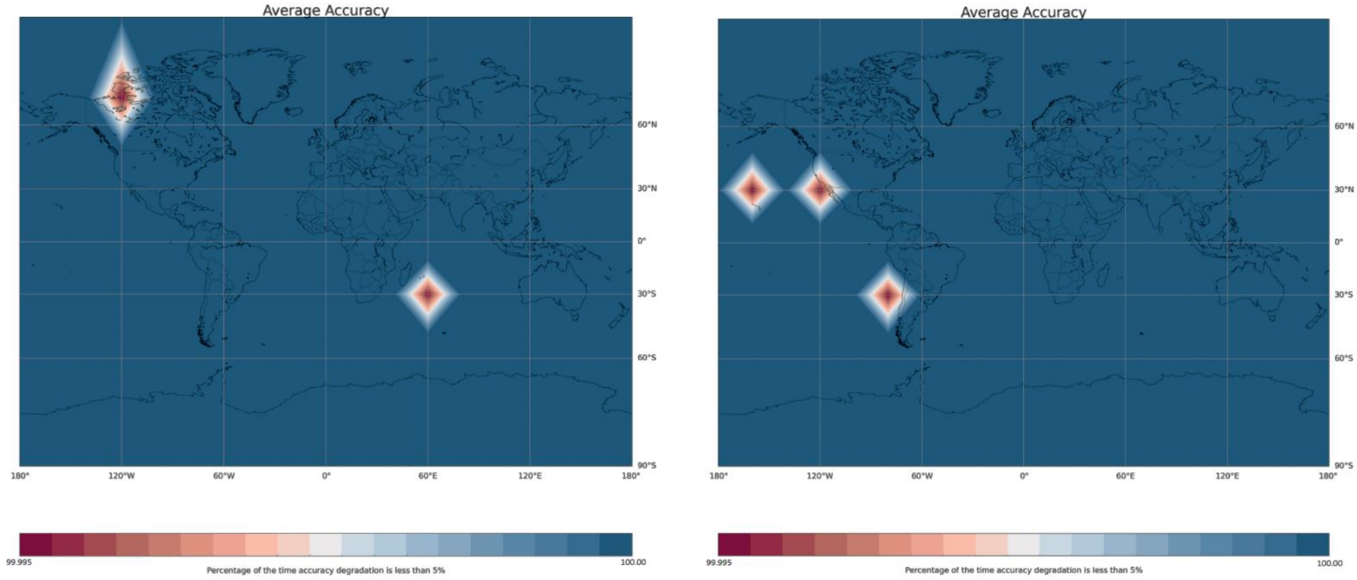
Figure 8: Availability of correct I/NAV pages (red lines) and pages with errors (black crosses) at 210-690 seconds into scenario (harsh-urban).

SERVICE VOLUME ANALYSIS

The results presented in the previous sections provide the service availability and performance for specific locations in urban environments. Nevertheless, when thinking about providing a global OSNMA service, the accuracy, time to first authenticated fix data and availability requirements shall be met for any user and in any location around the globe. In order to assess the fulfillment of these requirements, a service volume emulator has been developed within the AALECS project to simulate the satellite constellation, uplink stations, connectivity period using real or simulated contact plans, satellite visibility and data demodulation errors with different conditions (Bit error rate, Page error rate and masking angle). For this purpose, a two-stage experimentation campaign has been defined and executed. First step aimed at understanding the protocol behavior and singularities which might impact the service performance, the outcome of this first set of runs is the definition of the candidate configuration of the protocol settings. In the second stage a specific configuration (Table 1) was used to conduct a set of long run simulations covering up to 10 days with a processing step of 2-seconds (in line with the Galileo I/NAV page duration) to measure the differences between the Open Service and OSNMA service performances. The aspects under analysis in these tests were the accuracy, availability and average TTFAF.

The Galileo system configuration used for the test campaign is the nominal one expected for FOC 2020, consisting on 24 satellites and 5 uplink stations and 4 antennae per site having a total of 20 antennae. For the availability study, a set of scenarios with different outages of antenna and full uplink station are weighted according with a probability value that represents the time of the system in each state. Representative values for the Galileo system have been used in this analysis.

Accuracy performance is measured using the Dilution of Precision (DOP) for OS and OSNMA each point in the grid. In this analysis a five-day scenario with a nominal system configuration is used. The results are reported on a per-day basis for an open-sky user, as presented in Figure 9. The figures obtained show that the accuracy performances achieved using the OSNMA service are equal to the ones obtained by the Open Service for almost 100% of the time. There are only a few epochs, between two and six epochs which are equivalent to four-twelve seconds, on each day that on specific places of the Earth one satellite is not available to compute OSNMA position, while the satellite is usable for the open service. This issue affects the OSNMA dilution of precision (DOP), degrading OSNMA accuracy more than 5% with respect to the OS accuracy.



Day 2 (17/02/2016 to 18/02/2016)

Day 3 (18/02/2016 to 19/02/2016)

Figure 9: Average accuracy in the 2nd and 3rd day of the 5 days scenario, showing the percentage of the time that the accuracy degradation is above 5%

These slight degradations of few seconds on the whole day do not occur always in the same region of the Earth and are strictly related to the constellation navigation configuration (i.e. the geometry of the input constellation) and OSNMA protocol configuration (mainly ADKDs and the cross-authentication sequence).

The TTFAFD is analyzed over one subframe for the nominal system configuration. The results, reported in Table 7, show that TTFAFD, obtained with the authentication tags parallel processing, is always equal to TTFFD for the parallel case, with some seconds of degradation for the sequential case; the variations observed both in TTFFD and TTFAFD with the time is in line with the time a user start tracking and receiving the pages. As abovementioned, receiver guidelines are being developed allowing future receivers to protect against data forging threats while minimizing time to fix delay due to authentication: while the TESLA protocol foresees that the data to authenticate is authenticated before the delayed key release, secure receiver strategies currently under study may reduce waiting time in the receiver. Therefore, at this stage, the parallel and sequential TTFAFD results below can be understood as lower and upper bounds.

Availability of the OSNMA service is evaluated in a scenario of several days. In order to obtain the global availability, the accuracy metric for all the scenarios specified previously is calculated and the results obtained from each simulation are weighted according with the corresponding system state probability. The global availability of the OSNMA SIS is calculated and the result obtained is 99.20%, representing this figure the OSNMA availability over the nominal lifetime of the service.

Table 7: EMU OSNMA TTFFD/TTFAFD Results for parallel processing

First received subframe page	TTFFD	TTFAFD parallel	TTFAFD sequential
1st	26s	26s	46s
2nd	30s	30s	44s
3rd	30s	30s	42s
4th	28s	28s	40s
5th	26s	26s	38s
6th	24s	24s	36s
7th	22s	22s	34s
8th	20s	20s	32s
9th	18s	18s	30s
10th	16s	16s	28s
11th	14s	14s	26s
12th	30s	30s	38s
13th	30s	30s	52s
14th	30s	30s	50s
15th	28s	28s	48s

CONCLUSIONS

A full end-to-end Galileo OSNMA demonstrator has been implemented in the context of the AALECS project and based on current definition of the OSNMA service. The project consortium implemented tools, performance indicators and methodologies to evaluate the service performances in a representative way, also including methods to use SIS recoded data even before the service deployment. The analyses include experimentation of the performance experienced by a single user in lifelike environments as well as a worldwide service volume analysis based on a Galileo nominal configuration including realistic operational restrictions. Although some assumptions have been introduced for those aspects are not yet fixed (e.g. the DSM-KROOT dissemination strategies, receiver OSNMA algorithm implementation and OSNMA exact service configuration), the results provide a first overview of the performance. The experimentation tests show no measurable degradation in accuracy and availability due to the addition of OSNMA. Time to data-authenticated is not degraded due to the need to receive the authentication data in addition to the navigation data. However, it may be delayed by some seconds, depending on the protocol and receiver implementations, of which an upper bound is presented here. The work also highlights a number of aspects that should be addressed in future work, notably on the consolidation of OSNMA receiver implementations.

ACKNOWLEDGMENTS

We would like to thank all the members of the AALECS team (especially Vincent Rijmen and Tomer Ashur), Joaquim Fortuny-Guasch (from Joint Research Center of the European Commission) and Giovanni Vecchione for all their support.

DISCLAIMER

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

REFERENCES

[1] L. Scott, "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," *ION GPS,* 2003.

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

[3] K. Wesson, M. Rothlisberger and T. Humphreys, "Practical Cryptographic Civil GPS Signal Authentication,"

NAVIGATION, The Journal of the Institute of Navigation, February 2012.

[4] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simón, I. Rodríguez and J. D. Calle, "A Navigation Message Authentication Proposal for the Galileo Open Service," *NAVIGATION, the Journal of the Institute of Navigation,* 2016.

[5] A. Perrig, R. Canetti, J. Tygar and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," *IEEE Symposium on Security and Privacy*, pp. 56-73, May 2000.

[6] European Union, "Galileo OS SIS ICD: Open Service Signal In Space Interface Control Document v1.2," European Union, Nov 2015.

[7] P. Walker, V. Rijmen, I. Fernandez-Hernandez, J. Simón, D. Calle, O. Pozzobon and G. Seco-Granados, "Galileo Open Service Authentication: A Complete Service Design and Provision Analysis," in *Proceedings of ION GNSS+ 2015*, Tampa, 2015.

[8] National Institute of Standards and Technology, "FIPS PUB 186-4 - Digital Signature Standard (DSS)," U.S. Department of Commerce, 2013.

[9] I. Fernández-Hernández, J. D. C. Calle, S. Cancela, O. Pozzobon, C. Sarto and J. Simón, "Packet transmission through navigation satellites: A preliminary analysis using Monte Carlo simulations," in *ENC 2017*, Lausanne, CH, 2017.

[10] D. Calle, S. Cancela, E. Carbonell, I. Rodríguez, G. Tobías and I. Fernández-Hernández, "First Experimentation Results with the Full Galileo CS Demonstrator," in *ION GNSS+ 2016*, Portland, OR, 2016.