Galileo OSNMA: Join the Public Observation Test Phase and share your feedback!

Webinar Questions & Answers

Introduction

This document is a compilation of the questions that have been made during the EUSPA webinar '*Galileo OSNMA: Join the Public Observation Test Phase and share your feedback!*', held on February 2nd 2022. Inquiries which have been answered online, as well as those posed in the webinar's Q&A section which could not be answered directly by panellists, are addressed here.

Questions and answers

- **How can I share my feedback related to the OSNMA Public Observation Test Phase?**
  If you want to share your OSNMA testing feedback, as explained at the webinar (see slides from 36 to 47), give visibility to your '*OSNMA tested*' receiver/solution and eventually share your experience with the OSNMA community, you can use the functional mailbox MARKET@euspa.europa.eu.
  Through the same channel, the participants will also have the opportunity to get in touch directly with members from EUSPA Market & Downstream Innovation team to discuss any other market related questions.

- **Who can I contact in case of technical difficulties?**
  All service-related requests are to be sent to Galileo Help Desk. Dedicated support to the developers engaged in the OSNMA Public Observation Test Phase, concerning access to the OSNMA public keys, interaction, notifications, and information updates on the OSNMA service status, etc., is provided by the European GNSS Service Centre and accessible at the following link https://www.gsc-europa.eu/support-to-developers/osnma-public-observation-test-phase.

- **Do you have a list of OSNMA-enabled receivers, or a percentage of market OSNMA-enabled receivers?**
  Being the OSNMA currently provided in test mode, there are no commercially available OSNMA receivers yet. However, EUSPA has funded the development of a number of OSNMA receiver prototypes, which address a range of application areas such as automotive, mass market, maritime, drones, etc. The complete list of these projects can be found in Annex I of the OSNMA Info Note.

- **Could you share the schedule of the current step and the future steps of making the OSNMA operational?**
  The Public Observation Phase started in November 2021 and is planned to last throughout 2022. The initial OSNMA service declaration is foreseen in 2023.

- **Is there any period between the public observation test phase and the service provision phase in which OSNMA capability will not be available?**
  It is foreseen that the service provision phase will follow the Public Observation Test Phase without prolonged gaps in between them. Certain gaps could be expected due to the deployment of additional infrastructure supporting service phase.

- **Will the slides of this presentation be available?**
  Yes. The slides of the webinar presentation, as well as a list of the questions raised during the event and their appropriate answers will be shared with the participants per e-mail.

- **Are there any issues already identified in the test phase?**
  There is a very low probability that processing of broadcast OSNMA data can lead to failed authentication events. However, this probability must be considered since OSNMA is still in the test phase and certain aspects are to be fine-tuned. Corrections are being developed for the service provision phase.

- **How can the user be sure that the public key is the correct one?**
  During the test phase, the user shall retrieve the public key material solely from the GSC following the registration process to the OSNMA test phase. Additional mechanisms to ensure authenticity of OSNMA key material provided to the users through the GSC are being developed for the service provision phase.

- **What is the duration of the public key's validity?**
  As regards both the Public key and the TESLA chain, no expiration date is defined associated to the publication of new key material. The user shall be able to apply new cryptographic material from the time the previous one is renewed/revoked following the defined processes. However, for the Public Observation Test Phase, the renewal of key material is not foreseen. More information on the different flags related to this process can be found in Galileo OSNMA Receiver Guidelines for the Test Phase and Galileo OSNMA User Interface Control Document (ICD) for the Test Phase.

- **About the tag accumulation, does it mean that in current configuration we need to authenticate twice the same data to trust the authentication? In the receiver guidelines it is indicated that the tags shall be accumulated before performing the authentication all at once, so there is the need to keep in memory different tags obtained at different times with their corresponding GSTSF. However, wouldn't it be equivalent to authenticate each tag as you receive it and just keep count of the number of times?**
  Navigation data authentication is achieved after verifying a minimum number of tag bits, associated to the same navigation data sets. The value of the minimum equivalent tag length is currently equal to 80 bits. The broadcasted tags are 40 bits, therefore, two authentications are needed. If these two are valid, the data is considered as authenticated.

- **Is there available data or material for testing implementations such as examples (data streams) of authentication failures, attack attempts etc? Having those would be very beneficial for developers, to be included in e.g. unit/functional tests.**
  The Galileo OSNMA Receiver Guidelines for the Test Phase already includes a set of test vectors allowing to verify the OSNMA user implementation. Additional test vectors will be available in the format of data streams to the participants (see Part 2 - Corner test cases, in the webinar presentation). However, it is expected that they will be used for testing the correct implementation of the OSNMA rather than for testing of failures.

- **If OSNMA is not meant to affect the performance, why accuracy and velocity are suggested as KPIs? How can OSNMA affect accuracy?**
  The background of the performance analysis is connected to the proper implementation of the OSNMA functionality in the receiver. For instance, if the OSNMA algorithm is not implemented

correctly, certain performance parameters might be affected by that. Additionally, with these KPIs it will be possible to check whether the minimal additional computation needed for the OSNMA functionality affects the standard functionality of the GNSS receiver and/or GNSS-based system.

- **How do you foresee the rekeying process?**
  Rekeying may happen several times in the receiver lifetime (yet remain infrequent i.e. once a year/every few years) e.g. when the public key is being renewed or revoked. There are two methods to perform this operation:

  1. Through over-the-air rekeying (OTAR) transmitted as part of the SIS authentication data. In addition to this OTAR procedure, it is planned to broadcast the active public key with a low frequency, even when it is not renewed or revoked, allowing users that missed the previous key renewal process to retrieve the applicable material.
  2. For connected users, through contacting the OSNMA server in GSC, which will also keep the history of the public keys status.

- **About the GST mechanism, may you indicate an order of magnitude for the requested accuracy in synchronisation? Is there any public documentation available about this subject?**
  To ensure the security of the TESLA protocol and guarantee the authenticity of the data, the receiver must ensure it has received the navigation data and associated tag before the corresponding TESLA chain key is disclosed by the system. This implies that the receiver must be synchronised with a given accuracy to the Galileo System Time (GST) before receiving and processing OSNMA information. The time synchronisation requirement TL is set to 30 sec. If the receiver verifies this condition, all tags for all authentication types can be used. If the condition is not verified, slow MACs, i.e. messages whose associated TESLA chain key is transmitted with an extra delay, may be exploited. A receiver synchronised to GST with an accuracy better than TL + 300 *sec*, can process slow MAC with a 10 sub-frame delay. If none of the above conditions on the receiver time synchronisation to GST is verified, the OSNMA protocol shall not be used. For more details, please refer to section 2.1 of Galileo OSNMA Receiver Guidelines For The Test Phase.

- **Will all satellites always transmit the same key or is it planned for the constellation to transmit multiple at once?**
  The same key will be transmitted for all satellites at the same epoch. If no key can be retrieved from a certain satellite due to difficulties in the environment, it will be possible to retrieve the key from another satellite.

- **About OSNMA capabilities, its anti-spoofing capability is well known, but has it been assessed the anti-replay/meaconing protection capability of the OSNMA?**
  Anti-replay/meaconing protection is not the primary objective for the OSNMA service and its future service declaration. However, due to its characteristics, OSNMA signal provides a certain level of unpredictability that could be exploited at user level for increased robustness of the solution.

- **Are End of Chain, Chain Revoked, New public Key or Public key revoked events also sent during the test phase so that they can be tested? If so, are these events announced?**
  No TESLA chain or public key renewal or revocation processes are planned to be executed during the test phase. Such processes can be tested with the supporting test data (test vectors) that will be made available to the participants (see Part 2 - Corner test cases, in the webinar presentation).

In case these processes would be executed, provided that the user is registered and subscribed to receive OSNMA products notifications, he/she will receive an email whenever a new Public Key and/or Merkle Tree is published.
Users will also be able to review the list of previous Public Keys in the "Historical records" in the GSC including Past Renewed or Revoked Public Keys and past Merkle trees. The processes of public key renewal and revocation (as well as a TESLA chain renewal) are described in the Galileo OSNMA User Interface Control Document (ICD) for the Test Phase available on the GSC Web Portal.

- **Does new RINEX 4.0 format contain these Galileo I/NAV data?**
  Yes, it contains Galileo I/NAV data. However, at the time the OSNMA webinar was held (2nd February 2022), the current implementation of RINEX 4.0 according to IGS does not include Galileo OSNMA related topics. It is yet to be determined if this inclusion will take place once OSNMA is declared operational.

- **In the presentation it is stated "Need of a Network Connection: No", though in the receiver test guidelines it is stated that the Merkle tree root could be updated and in that case the receiver must connect to the OSNMA server. Is this a particularity of the public test phase or the Merkle tree root can also be updated in the operational service?**
  The Merkle tree root is expected to be valid for several years during service provision. In case of update of the Merkle tree root, the user shall connect to the OSNMA server to retrieve the new material. Nevertheless, this shall be expected to happen rarely during the service provision and not imposing the need of implementing a network connection on the receiver. The new Merkle tree root could be uploaded, for example, by means of operational procedures by the receiver operator. In addition, a planned update of the Merkle tree root will be communicated well in advance to the users.
  No update of the Merkle tree root is planned during the test phase.

- **Is it possible to foresee the OSNMA capability broadcast in E5b in order to have frequency diversity in case of L1 jamming/interference issue?**
  This is outside of the scope of the current OSNMA specification although might be considered for future service evolutions.

- **Will the final Galileo OSNMA be able to authenticate all satellites in view?**
  OSNMA data is transmitted only from a subset of satellites, currently up to 20, out of the total constellation. The OS data of the remaining satellites will be cross-authenticated through the satellites transmitting OSNMA. One of the OSNMA service targets is to provide the user with accuracy performance equivalent to the ones of the standard Open Service by frequently authenticating satellites in view to the user.

- **What is your recommendation towards using data that has not yet been authenticated?**
  Use of data that has not yet been authenticated will depend on the target application. From OSNMA service point of view such data shall not be considered authenticated.

- **Can you clarify the mentioned capability foreseen in E5a F/NAV? What is the added value in considering E5a in addition to E1-B? It is "only" channel redundancy or there is any other concept (e. g. increase KPI such as time between authentication, …)?**
  The OSNMA protocol authenticates selected Galileo I/NAV navigation data transmitted in E1-B and E5b-I and could as well authenticate F/NAV navigation data transmitted in E5a-I.

The authentication of F/NAV navigation data is outside of the scope of the current OSNMA specification although might be considered for future service evolutions.

- **My interest is integrating OSNMA in timing applications. How much of the OSNMA algorithm will be handled by the chip manufacturers and be implemented in firmware, and how much has to be handled be handled by the application system integrator?**
  This depends highly on system and application design. As an example not intended to be fully representative nor exhaustive, in systems/applications which follow a “loosely coupling” approach, the main computation usually is done by the chipset’s firmware. In systems/applications which follow “tight or ultra-tight coupling” approach, more and more of the computation can be shifted towards the rest of the system or towards the application.

- **Are there plans to add the possibility to authenticate GPS navigation data to the OSNMA in the future?**
  The authentication of GPS navigation data is outside of the scope of the current OSNMA specification although might be considered for future service evolutions.

- **Are the satellites going to send the same DSM ID?**
  At a given time all the satellites will broadcast blocks belonging to the same DSM, identified by its DSM ID. However, different DSM will be transmitted over time. The DSM ID field contained in the DSM Header shall be used to identify the DSM being transmitted in a given sub-frame.