NAVIGATION SOLUTIONS POWERED BY EUROPE

GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OSNMA) USER ICD FOR THE TEST PHASE

Issue 1.0, November 2021

TERMS OF USE AND DISCLAIMERS

1. Authorised Use and Scope of Use

The European GNSS (Galileo) Open Service Navigation Message Authentication (OSNMA) User Interface Control Document for the Test Phase Issue 1.0 (hereinafter referred to as OSNMA User ICD for the Test Phase) and the information contained herein is made available to the public by the European Union (hereinafter referred to as Publishing Authority) as part of the OSNMA Test Phase for information, standardisation, research and development and commercial purposes for the benefit and the promotion of the European Global Navigation Satellite Systems programmes (European GNSS Programmes) and according to terms and conditions specified thereafter.

2. General Disclaimer of Liability

With respect to the OSNMA User ICD for the Test Phase and any information contained in the OSNMA User ICD for the Test Phase , neither the EU as the Publishing Authority nor the generator of such information make any warranty, express or implied, including the warranty of fitness for a particular purpose, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information hereby disclosed or for any product developed based on this information, or represents that the use of this information would not cause damages or would not infringe any intellectual property rights. No liability is hereby assumed for any direct, indirect, incidental, special or consequential damages, including but not limited to, damages for interruption of business, loss of profits, goodwill or other intangible losses, resulting from the use of the OSNMA User ICD for the Test Phase or of the information contained herein. Liability is excluded as well for consequences of the use and / or abuse of the OSNMA User ICD for the Test Phase or the information contained herein.

3. Intellectual Property Rights

The information contained in the OSNMA User ICD for the Test Phase, including its Annexes, is subject to intellectual property rights (hereinafter referred to as IPR).

Copyrights

The OSNMA User ICD for the Test Phase is protected by copyright. Any alteration or translation in any language of the OSNMA User ICD for the Test Phase as a whole or parts of it is prohibited unless the Publishing Authority provides a specific written prior permission. The OSNMA User ICD for the Test Phase may only be partly or wholly reproduced and/or transmitted to a third party in accordance with the herein described permitted use and under the following conditions:

- the present “Terms of Use and Disclaimers”, as well as the terms of Annex G, are accepted, reproduced and transmitted entirely and unmodified together with the reproduced and/or transmitted information;
- the copyright notice “© European Union 2021” is not removed from any page.

Industrial Property Rights

The use of the information contained in the OSNMA User ICD for the Test Phase is authorised under the terms and conditions stated in Annex G. The use of the Galileo related trademarks that EU owns is authorised under the terms and conditions stated in Annex H.

4. Miscellaneous

No failure or delay in exercising any right in relation to the OSNMA User ICD for the Test Phase or the information contained therein shall operate as a waiver thereof, nor shall any single or partial exercise preclude any other or further exercise of such rights. The disclaimers contained in this document apply to the extent permitted by applicable law.

5. Updates

The OSNMA User ICD for the Test Phase is expected to be subject to modification, update and variations. Those modification, updates and variations will reflect, between others, the result of the execution of the OSNMA Test Phase.

The publication of updates will be subject to the same terms as stated herein unless otherwise evidenced.

Although the Publishing Authority will deploy its efforts to give notice to the public for further updates of OSNMA User ICD for the Test Phase, it does not assume any obligation to advise on further developments and updates of the OSNMA User ICD for the Test Phase, nor to take into account any inputs, comments proposed by interested persons or entities, involved in the updating process.

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1. Document Scope

The present Galileo Open Service Navigation Message Authentication (OSNMA) User Interface Control Document (ICD) for the Test Phase contains all information on the OSNMA protocol that is relevant for the user segment during the Test Phase. The document is intended for use by the Galileo user community and specifies the interface between the Galileo Space Segment and the Galileo User Segment and the interface between the Galileo Service Centre (GSC) OSNMA Server and the Galileo User Segment for what matters the use of Galileo OSNMA.

The current version of the OSNMA User ICD still contains some TBD and TBC values that will be consolidated during the OSNMA Test Phase and fixed in successive updates of the document.

1.2. Structure of the Document

The document is structured as follows:

- Chapter 2 describes the OSNMA Message Structure;
- Chapter 3 and 4 provide all the details on the HKROOT and the MACK messages, respectively;
- Chapter 5 details various elements related with the distribution and the sequencing of OSNMA;
- Chapter 6 describes the receiver cryptographic operations.

1.3. Applicable Documents

[AD.1] European GNSS (Galileo) Open Service, Signal-In-Space Interface Control Document, Issue 2, 2021

[AD.2] European GNSS (Galileo) Open Service, OSNMA Receiver Guidelines for the Test Phase, Issue 1.0

1.4. Galileo Open Service Navigation Message Authentication Overview

The Galileo programme will provide cryptographic data with the purpose of authenticating its Open Service navigation messages [1] [2]. The authentication protocol here described is based on the TESLA protocol [3][4][5] and specifically tailored for Galileo Open Service. The TESLA protocol uses message authentication codes generated with a key that is broadcast with some delay. This key is part of a pre-generated one-way chain whose root is public, known in advance by the user, and which is transmitted in reverse order with respect to its generation. The root key is authenticated by a digital signature (ECDSA) [6], and the digital signature public key can be renewed by a Merkle tree [7]. It is optimized for Galileo by using the same key chain for all satellites, and allowing the authentication of data transmitted by other satellites from a given satellite (cross-authentication).

The Open Service Navigation Message Authentication (OSNMA) protocol data are transmitted within the Galileo I/NAV navigation message transmitted in the E1-B Galileo Open Service signal. 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. The OSNMA protocol can authenticate selected Galileo I/NAV navigation data transmitted in E1-B and E5b-I as well as F/NAV navigation data transmitted in E5a-I, as per [AD.1].

2. OSNMA Message Structure

Galileo OSNMA protocol data are transmitted within the odd pages of the nominal E1-B I/NAV message.

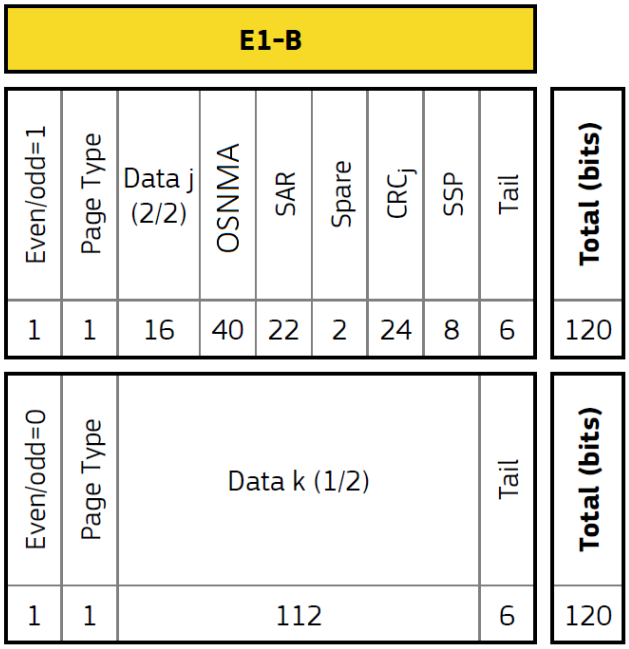


Figure 1. E1-B I/NAV Nominal Page with bits allocation, including OSNMA data

Figure 1 displays the layout of the E1-B I/NAV nominal page, as per [AD.1]. The OSNMA data is transmitted within the “OSNMA" field, corresponding to the "Reserved 1" in [AD.1]. All data fields of the E1-B I/NAV nominal page are described in [AD.1]. It is important to recall that the OSNMA field is also protected by the CRC, as described in [AD.1].

As discussed in Chapter 5, OSNMA data are distributed only by a subset of the Galileo satellites and, for the satellites that are not transmitting OSNMA data, the I/NAV OSNMA message will contain a 40-bit sequence of zeros. The subset of satellites distributing the OSNMA data is changing dynamically over time and the user has no means to know in advance which satellites are distributing OSNMA data and which not. OSNMA receivers will have to be designed accordingly.

OSNMA is not provided in I/NAV Dummy Messages or in I/NAV Alert Pages. Any data retrieved from the OSNMA field of Dummy or Alert Pages shall be therefore discarded. Both I/NAV dummy message and alert page are described in [AD.1].

Within each E1-B I/NAV nominal odd page part an OSNMA message is transmitted and having the following structure:

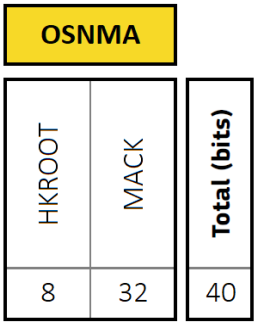


Figure 2. OSNMA data message

Two sections compose the OSNMA message: the HKROOT section (first 8 bits) and MACK section (next 32 bits). The HKROOT and the MACK messages are described within Chapter 3 and Chapter 4, respectively, where a description of the message structure and the message data contents is provided, including semantics, formats and specific characteristics.

Within an E1-B I/NAV nominal sub-frame, 15 pages are transmitted every 30 seconds, with the OSNMA data message included within the odd part of the page. This means that 15 OSNMA data messages as the one represented in Figure 2 are transmitted over 30 seconds. As a consequence, a 120-bit HKROOT message and a 480-bit MACK message are also transmitted every 30 seconds. Both HKROOT and MACK messages are split into 15 portions of equal size (8 or 32 bits) and transmitted within each 40-bit OSNMA data message.

2.1. OSNMABit and Byte Ordering Criteria

All data values are encoded using the same ordering criteria defined in [AD.1]:

- For numbering, the most significant bit/byte is numbered as bit/byte 0;
- For bit/byte ordering, the most significant bit/byte is transmitted first;
- Except when noted, all fields are represented as unsigned integers.

3. HKROOT Message

The HKROOT message is 120 bits long and is transmitted once every 30 seconds, i.e. within each E1-B I/NAV sub-frame. The HKROOT message is transmitted in 15 sections of 8 bits each within every 40-bit OSNMA data message.

The HKROOT message begins always with an 8-bit NMA Header field, followed by a 112-bit Digital Signature Message (DSM) field, constituted by a DSM Header and a DSM block. The structure of the HKROOT message is represented in the following figure.

NMA Header	DSM Field														
1/15	2/15	3/15	4/15	5/15	6/15	7/15	8/15	9/15	10/15	11/15	12/15	13/15	14/15	15/15	**Total (bits)**
NMA Header	DSM Header	DSM Block *n*													
8	8	104													120

Figure 3. HKROOT Message

Several DSM blocks, transmitted through successive subframes, form a complete DSM message whose content is interpreted as per section 3.2. Each block is transmitted within the DSM field of the HKROOT message with the corresponding DSM Header (described in section 3.2.1). Different satellites can transmit different blocks of the same DSM at a given sub-frame. Details on the sequencing and the transmission of the DSM blocks are provided in section 5.3. NMA Header and DSM fields are described in sections 3.1 and 3.2, respectively.

3.1. NMA Header

The NMA Header defines the status of the NMA service. The structure of the NMA Header is represented here below:

NMA Header				
NMAS	CID	CPKS	Reserved	**Total (bits)**
2	2	3	1	8

Figure 4. NMA Header

The contents, format and semantic of the NMAS, CID and CPKS fields are described in the three following sub-sections, respectively. The last bit of the NMA Header is reserved for future use.

3.1.1. NMA Status (NMAS)

The 2-bit NMAS field presents the overall status of the OSNMA. NMAS can assume the values from 0 to 3, and in the following table the definition and the corresponding semantic for each value are defined.

NMAS	Definition	Semantic
0	Reserved	
1	**Test**	OSNMA is provided without any operational guarantees.
2	**Operational**	OSNMA is provided according to the specifications.
3	**Don't use**	Navigation data shall not be authenticated with the provided OSNMA information.

Table 1. NMAS values and corresponding semantic

3.1.2. Chain ID (CID)

The 2-bit CID field represents the ID of the key chain in force. Its value is incremented every time a new chain enters into force. Supported values are 0 to 3, after which the CID rolls over.

3.1.3. Chain and Public Key Status (CPKS)

The 3-bit CPKS field provides the status of the key chain and public key in force. The CPKS can assume values from 0 to 7, and in the following table the definition and the semantic of each possible status value is provided.

CPKS	Definition	Semantic
0	*Reserved*	
1	**Nominal**	The status of the chain in force (identified by CID, described in 3.1.2) and the public key in force (identified by PKID within the DSM-KROOT, defined in 3.2.3.2) is nominal (i.e., no public key/chain renewal nor revocation).
2	**End of Chain (EOC)**	The current chain (associated with the transmitted CID, described in 3.1.2) is coming to an end. A DSM-KROOT (described in 3.2.3) with the root key of the next chain is regularly transmitted.
3	**Chain Revoked (CREV)**	A chain is or has been revoked: • If NMAS is set to "Don't Use", then the current chain (associated with the transmitted CID) is revoked. • If NMAS is set to "Operational", then a previous chain (associated with a previous CID) has been revoked.
4	**New Public Key (NPK)**	The public key in force is being renewed. A DSM-PKR (defined in 3.2.2) with a new public key is transmitted.
5	**Public Key Revoked (PKREV)**	A public key is or has been revoked: • If NMAS is set to "Don't Use", then the current public key (identified by PKID in DSM-KROOT, defined in 3.2.3.2) is revoked. • If NMAS is set to "Operational", then a past public key, not anymore in force, has been revoked.
6	*Reserved*	
7	*Reserved*	

Table 2. Chain and Public Key Status (CPSK) values

Further details on renewal and revocation of chains and public keys are provided in sections 5.5.3 and 5.4.1, respectively.

3.2. Digital Signature Message (DSM)

As described in Figure 3, within each HKROOT message, a DSM Header (8 bits) and a DSM block (104 bits) are transmitted. A sequence of DSM blocks forms a DSM, whose length depends on the type of DSM and the cryptographic parameters in use.

There are two different types of DSM:

- DSM-PKR, providing the public key for the verification of the root key of the TESLA chain (described in section 3.2.2). The verification of the DSM-PKR is described in section 6.2.
- DSM-KROOT, providing a digitally signed KROOT for a TESLA chain (described in section 3.2.3). The verification of the DSM-KROOT is described in section 6.3.

In the following three sub-sections the DSM Header, the DSM-KROOT and the DSM-PKR messages are described in detail.

3.2.1. DSM Header

The DSM Header provides information about the DSM block being transmitted in the sub-frame. The structure of the DSM Header is represented here below:

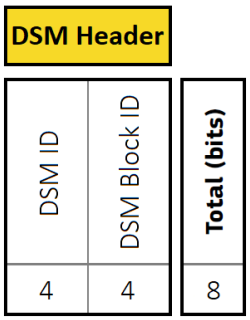


Figure 5. DMS Header

A DSM message is identified unambiguously by its DSM ID, which is associated also to each block of that DSM message. Then, each block of the same message is identified unambiguously with a DSM Block ID (BID). The contents, format and semantic of the DSM ID and DSM Block ID fields are described in the two following sub-sections, respectively.

3.2.1.1. DSM ID

The DSM ID field is a 4-bit identifier of the DSM. As a DSM is transmitted in several blocks (one block per I/NAV sub-frame), the DSM ID identifies the DSM associated with the current block. The DSM ID can take values from 0 to 15.

DSM ID values from 0 to 11 are allocated to DSM-KROOT messages, while DSM ID values from 12 to 15 are allocated to DSM-PKR.

3.2.1.2. DSM Block ID (BID)

The 4-bit DSM Block ID (BID) field encodes the ID of the DSM block sent by the transmitting satellite in the current sub-frame. The BID can take values from 0 to 15 and identifies the position of the block in the overall DSM message: the first block is identified by BID = 0, the second block by BID = 1, and so on, up to a maximum of 16 blocks (with the last block identified by BID = 15). In order to retrieve a full DSM, all the different blocks have to be recombined in the order indicated by the BID. The total number of blocks of a DSM is indicated within the Block 0 of the DSM, as described later, both for DSM-KROOT and DSM-PKR.

3.2.2. DSM-PKR

A DSM-PKR includes the elements for the provision and the verification of public keys for DSM-KROOT authentication, either for the key in force or for a new key in the case of a Public Key renewal or revocation. Details on the public key provision are provided in Chapter 5. The DSM-PKR structure is represented here below. A DSM-PKR can also be used to transmit an OSNMA Alert Message (OAM, see section 3.2.2.4).

DSM-PKR							
NB_{DP}	MID	ITN	NPKT	NPKID	NPK	P_{DP}	**Total (bits)**
4	4	1024	4	4	l_{NPK}	l_{PDP}	l_{DP}

Figure 6. DSM-PKR Message

The contents of DSM-PKR are verified as described in Chapter 6.

The total length l_{DP} (expressed in bits) of the DSM-PKR message corresponds to:

Eq. 1
$$l_{DP} = 104 \left\lceil \frac{(1040 + l_{NPK})}{104} \right\rceil$$

Where:

- l_{NPK} is the length of the NPK field, expressed in bits;
- 1040 is the size in bits of all the other fields within the DSM-PKR (NB_{DP}, MID, ITN, NPKT, and NPKID);
- [n] is the ceiling operator, indicating the least integer greater than or equal to n.

Following the above, the total length of the DSM-PKR message l_{DP} is always an integer multiple of 104, which is the DSM block length. Padding bits are added to the DSM-PKR if needed (P_{DP} field in Figure 6), as explained in section 3.2.2.7.

The contents, format and semantic of the various DSM-PKR fields are described in the following sub-sections.

3.2.2.1. Number of DSM-PKR Blocks (NB_{DP})

The NB_{DP} field identifies the number of blocks of the DSM-PKR, which will always be the minimum possible. A DSM block corresponds to the 104 bits of DSM that are transmitted in a given I/NAV sub-frame, as per Figure 3 above. The 4-bit NB_{DK} value is the entry of a look-up table that is used to define the number of blocks. The look-up table is provided in the following table, where for each NB_{DP} value the corresponding number of blocks and the total DSM-PKR length l_{DP}, expressed in bits, are also provided.

NB_{DP} value	Number of Blocks	DSM-PKR total length, l_{DP} [bits]
0-6	Reserved	n/a
7	13	1352
8	14	1456
9	15	1560
10	16	1664
11-15	Reserved	n/a

Table 3. NB_{DP} values, with corresponding Number of Blocks and DSM-PKR total length l_{DP}

3.2.2.2. Message ID (MID)

The MID field identifies which leaf of the Merkle tree is provided, as per Table 4, and the nodes transmitted in the Intermediate Tree Nodes field (see section 3.2.2.3). Details on the Merkle tree are provided in Section 6.2.

MID value	Merkle Tree Leaf	Intermediate Three Nodes			
0	m_0	$x_{0,1}$	$x_{1,1}$	$x_{2,1}$	$x_{3,1}$
1	m_1	$x_{0,0}$	$x_{1,1}$	$x_{2,1}$	$x_{3,1}$
2	m_2	$x_{0,3}$	$x_{1,0}$	$x_{2,1}$	$x_{3,1}$
3	m_3	$x_{0,2}$	$x_{1,0}$	$x_{2,1}$	$x_{3,1}$
4	m_4	$x_{0,5}$	$x_{1,3}$	$x_{2,0}$	$x_{3,1}$
5	m_5	$x_{0,4}$	$x_{1,3}$	$x_{2,0}$	$x_{3,1}$
6	m_6	$x_{0,7}$	$x_{1,2}$	$x_{2,0}$	$x_{3,1}$
7	m_7	$x_{0,6}$	$x_{1,2}$	$x_{2,0}$	$x_{3,1}$
8	m_8	$x_{0,9}$	$x_{1,5}$	$x_{2,3}$	$x_{3,0}$
9	m_9	$x_{0,8}$	$x_{1,5}$	$x_{2,3}$	$x_{3,0}$
10	m_{10}	$x_{0,11}$	$x_{1,4}$	$x_{2,3}$	$x_{3,0}$
11	m_{10}	$x_{0,10}$	$x_{1,4}$	$x_{2,3}$	$x_{3,0}$
12	m_{12}	$x_{0,13}$	$x_{1,7}$	$x_{2,2}$	$x_{3,0}$
13	m_{13}	$x_{0,12}$	$x_{1,7}$	$x_{2,2}$	$x_{3,0}$
14	m_{14}	$x_{0,15}$	$x_{1,6}$	$x_{2,2}$	$x_{3,0}$
15	m_{15}	$x_{0,14}$	$x_{1,6}$	$x_{2,2}$	$x_{3,0}$

Table 4. *MID field and associated Merkle Tree leaves and intermediate nodes*

3.2.2.3. *Intermediate Tree Nodes (ITN)*

The Intermediate Tree Nodes (ITN) field provides the four Merkle tree nodes necessary to authenticate the message identified by the Message ID (MID) field. Each node is 256 bits long, for a total field size of 1024 bits. The nodes are sent following the order defined in Table 4 (e.g. for MID=0, ITN=($x_{0,1}||x_{1,1}||x_{2,1}||x_{3,1}$), where (X||Y) indicates the concatenation of X and Y).

3.2.2.4. *New Public Key Type (NPKT)*

The New Public Key Type (NPKT) field represents the signature algorithm associated with the public key provided in the DSM-PKR message, as per the following table.

NPKT value	Message
0	*Reserved*
1	*ECDSA P-256*
2	*Reserved*
3	*ECDSA P-521*
4	*OSNMA Alert Message (OAM)*
5-15	*Reserved*

Table 5. *NPKT field and corresponding message*

As indicated in the previous table, NPKT=4 indicates that an OSNMA Alert Message (OAM) is being transmitted. If this is the case and once the DSM-PKR has been verified (see section 6.2), the receiver is requested to stop processing OSNMA data and connect to the GSC OSNMA Server for further updates (see Annex D for the interface to the GSC OSNMA Server).

3.2.2.5. *New Public Key ID (NPKID)*

This field represents the ID of the new public key. Note that, if NPKT is set to 4 (corresponding to "OSNMA Alert Message (OAM)", see Table 5), NPKID is set to 0. NPKID are provided in increasing order during service provision.

3.2.2.6. *New Public Key (NPK)*

This field provides the new OSNMA public. Keys are provided as compressed Elliptic Curve Digital Signature Algorithm (ECDSA) keys, including the sign field and rounded up to a whole number of bytes, as per [6].

The length of the NPK field l_{NPK} will depend on the key type indicated within the NPKT field as indicated in the following table:

Key Type	NPK size, l_{NPK} [bits]
ECDSA P-256	264
ECDSA P-521	536

Table 6. *Size of the NPK field for different key types*

Note that, in the case of an OSNMA Alert Message (field NPKT set to 4, see Table 5), the NPK field will contain a random sequence of bits allowing the authentication of the message, following the verification steps described in chapter 6 for the DSM-PKR. In this specific case

the length of the NPK field will be such that the whole DSM-PKR message fits in the number of blocks indicated by the NB_{DP} field and therefore, following Table 3 and Eq. 1:

Eq. 2
$$l_{PK\_OAM} = l_{DP} - 1040$$

Where l_{PK_OAM} is the length of the NPK field when an OSNMA Alert Message is provided.

3.2.2.7. DSM-PKR Padding (P_{DP})

The field P_{DP} includes padding bits added to the DSM-PKR, when required, in order to reach a total length l_{DP} that is a multiple of one DSM block, as per Table 3. This means that, following Eq. 1, the length of the padding bits sequence can be computed as follows:

Eq. 3
$$l_{PDP} = l_{DP} - 1040 - l_{NPK}$$

The content of the P_{DP} padding field is computed as follows:

Eq. 4
$$P_{DP} = \text{trunc}\left(l_{PDP}, \text{hash}_{H256}\left(x_{4,0} \| m_i\right)\right)$$

Where:

- the operator trunc(*L*,*I*) retains the *L* most significant bits of the input *I*;
- $x_{4,0}$ is the Merkle tree root and m_i is the tree leaf, as defined in 6.2;
- hash_{H256} is the SHA-256 hash operation function [8].

3.2.3. DSM-KROOT

The DSM-KROOT message provides the root key of the chain in force, or that of the next chain, and the means to authenticate those keys using the public key in force. Within the DSM-KROOT, the chain cryptographic functions, the key and tag sizes, as well as other parameters that are fixed for each given chain, are provided. The DSM-KROOT structure is represented here below. Details on the provision of DSM-KROOT are provided within section 5.5

DSM-KROOT																
NB_{DK}	PKID	CIDKR	Reserved1	HF	MF	KS	TS	MACLT	Reserved	WN_K	$TOWH_K$	α	KROOT	DS	P_{DK}	**Total (bits)**
4	4	2	2	2	2	4	4	8	4	12	8	48	l_K	l_{DS}	l_{PDK}	l_{DK}

Figure 7. *DSM-KROOT Message*

The total length of the DSM-KROOT message l_{DK} (expressed in bits) corresponds to:

Eq. 5
$$l_{DK} = 104\left\lceil 1 + \frac{l_K + l_{DS}}{104} \right\rceil$$

Where:

- l_K is the length of the KROOT field, expressed in bits;
- l_{DS} is the length of the DS field, expressed in bits;
- 104 is the total size in bits of all the other fields within the DSM-KROOT (NB_{DK}, PKID, CIDKR, Reserved1, HF, MF, KS, TS, MACLT, Reserved, WN_K, $TOWH_K$, α);
- $\lceil n \rceil$ is the ceiling operator, indicating the least integer greater than or equal to *n*.

The Reserved1 and Reserved fields are reserved for future use.

Following the above, the total length of the DSM-KROOT message l_{DK} is always an integer multiple of 104, which is the DSM block length. Padding bits are added to the DSM-KROOT if needed (P_{DK} field in Figure 7), as explained in section 3.2.3.13.

The contents, format and semantic of the various DSM-KROOT fields are described in the following sub-sections.

3.2.3.1. Number of DSM-KROOT Blocks (NB_{DK})

The NB_{DK} field identifies the number of blocks of the DSM-KROOT, which will always be the minimum possible. A DSM block corresponds to the 104 bits of DSM that are transmitted in a given I/NAV sub-frame, as per Figure 3 above. As in the case of the DSM-PKR, the 4-bit NB_{DK} value is the entry of a look-up table that is used to define the number of blocks. The look-up table is provided in the following table, where for each NB_{DK} value the corresponding number of blocks and the total DSM-KROOT length l_{DK}, expressed in bits, are also provided.

NB_{DK} value	**Number of Blocks**	**DSM-KROOT total length, l_{DK} [bits]**
0	*Reserved*	n/a
1	7	728
2	8	832
3	9	936
4	10	1040
5	11	1144
6	12	1248
7	13	1352
8	14	1456
9-15	*Reserved*	n/a

Table 7. *NB_{DK} values, with the corresponding Number of Blocks and the DSM-KROOT total length*

3.2.3.2. Public Key ID (PKID)

The 4-bit PKID field represents the ID of the Public Key (PK) used to verify the signature of the DSM-KROOT. Details on the Public key provision are provided in Chapter 5. The cryptographic operations to be performed by the receiver are described in Chapter 6.

3.2.3.3. KROOT Chain ID (CIDKR)

The 2-bit CIDKR field identifies the chain to which the signed KROOT belongs. Note that CIDKR may not be the same as the Chain ID (CID) in the NMA Header (defined in section 3.1.2), for example when a chain renewal process takes place (see 5.5.3).

3.2.3.4. Hash Function (HF)

The 2-bit HF field identifies the hash function used for the chain. It is to be interpreted as follows:

HF value	Hash Function
0	SHA-256
1	*Reserved*
2	SHA3-256
3	*Reserved*

Table 8. *HF values and corresponding Hash functions*[1]

3.2.3.5. MAC Function (MF)

The 2-bit MF field identifies the MAC function used to authenticate the navigation data. It is to be interpreted as follows:

MF value	Hash Function
0	HMAC-SHA-256
1	CMAC-AES
2	*Reserved*
3	*Reserved*

Table 9. *MF values and corresponding Hash functions*[2]

1. SHA-2 family hashes (SHA-256) are defined in the latest FIPS publication [8]. SHA-3 family is implemented according to the Keccak algorithm [9].

2. HMAC-SHA-256 is standardized in [10] and CMAC-AES is standardized [11] and [12].

3.2.3.6. *Key Size (KS)*

The 4-bit KS field identifies the entry of a look-up table indicating the length l_K of the keys of the chain, expressed in bits. The look-up table is provided here:

KS value	Key length, l_K [bits]	KS value	Key length, l_K [bits]
0	96	5	160
1	104	6	192
2	112	7	224
3	120	8	256
4	128	9-15	Reserved

Table 10. *KS values and corresponding key length [bits]*

3.2.3.7. *Tag Size (TS)*

The 4-bit TS field identifies the entry of a look-up table indicating the tag length l_t, expressed in bits. The look-up table is provided here:

TS value	Tag length, l_t [bits]
0-4	Reserved
5	20
6	24
7	28
8	32
9	40
10-15	Reserved

Table 11. *TS values and corresponding Tag length [bits]*

3.2.3.8. *MAC Look-up Table (MACLT)*

The MACLT is an 8-bit field which corresponds to the entry of a look-up table specifying the Authentication Data & Key Delay (ADKD) type sequence for the tags provided within the MACK message. The look-up table can specify a sequence for 1 or 2 MACK messages. More details about ADKD can be found in section 4.2.1.2.

The look-up table can identify up to 256 sequences. Each sequence specifies the positions that are fixed with the associated ADKD type, and the positions whose ADKD type is flexible, which will be dynamically allocated on every MACK message and authenticated through MACSEQ field (see section 4.1.2). The MACLT field is constant when a TESLA chain is in

force. Annex C provides the MAC Look-up Table bit interpretation and defines the currently available ADKD sequences.

3.2.3.9. KROOT Week Number and Time of Week (WNK and TOWHK)

The 12-bit KROOT Week Number (WN_K) and the 8-bit Time of Week (expressed in Hours, $TOWH_K$) parameters provide the time associated with a KROOT referred to Galileo System Time (GST), as explained in section 5.5.1.

3.2.3.10. Random Pattern α

The 48-bit α field includes the random pattern to be included in the hashing process of the chain, as per section 6.3.

3.2.3.11. KROOT

KROOT is the root key associated with KROOT Time (WN_K and $TOWH_K$) and signed, together with the chain information, in the DSM-KROOT.

The length of KROOT is fixed, equals the key size l_K and it is provided within the KS field (see section 3.2.3.6).

3.2.3.12. Digital Signature (DS)

The DS field includes the digital signature of the DSM-KROOT of length l_{ds}. The DS length for the supported ECDSA functions is provided in Table 15 within section 6.1.

The DS verification is performed according to the digital signature function associated with the key identified by PKID, as per section 6.3.

3.2.3.13. DSM-KROOT Padding (P_{DK})

The field P_{DK} includes padding bits added to the DSM-KROOT, when required, in order to reach a total length l_{DK} that is a multiple of one DSM block, as per Table 7. This means that, following Eq. 5, the length of the padding bit sequence can be computed as follows:

Eq. 6
$$l_{PDK} = l_{DK} - 104 - l_K - l_{DS}$$

The content of the P_{DK} padding field is computed as follows:

Eq. 7
$$P_{DK} = \text{trunc}\left(l_{PDK}, \text{hash}_{H256}(M \| DS)\right)$$

Where:

- the operator trunc(***L,I***) retains the ***L*** most significant bits of the input ***I***;
- ***M*** and ***DS*** are the message and the digital signature, as they are defined in Chapter 6;
- hash_{H256} is the SHA-256 hash operation function.

4. MACK Message

The MACK message is 480 bits long and is transmitted once every 30 seconds, i.e. within each E1-B I/NAV sub-frame. As already discussed in Chapter 2, the MACK message is transmitted in 15 sections of 32 bits each within every 40-bit OSNMA data message.

Each MACK message contains several truncated Message Authentication Codes (MACs), or tags, with associated specific information data (Tag-Info), and a TESLA key. The tags are obtained by generating a certain MAC, following the specific information within the Tag-Info field (see section 4.2.1), and then truncating it (starting from the MSB) to the length defined by the Tag Size (TS) field within the DSM-KROOT of the chain in force (see section 3.2.3.7). Within each MACK message one or more tags with associated information are transmitted within the Tags&Info message section. The MACK message also includes a MACK Header, described in section 4.1.

The structure of the MACK message is represented in the following figure.

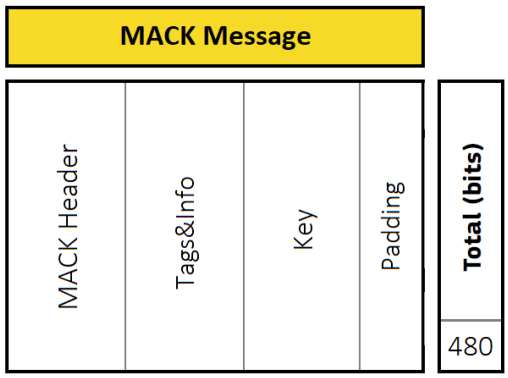


Figure 8. *MACK Message*

As represented in the figure above, a zero-padding sequence is added at the end of each MACK message in order to match the length of 480 bits.

The size, contents, format and semantic of the various sections of the MACK message represented above are discussed in the following sections.

4.1. MACK Header

Within the MACK Header, the Tag0 and the MACSEQ are transmitted. The structure of the MACK Header is represented here below:

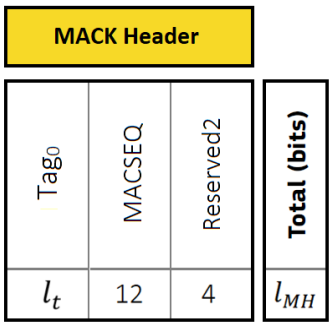


Figure 9. *MACK Header*

The Reserved2 field is reserved for future use. The format and content of the fields of the MACK Header are described in the following sections.

4.1.1. Tag_0 Field

The Tag_0 field contains a tag obtained by truncating a MAC of type "ADKD=0" for the satellite transmitting the OSNMA data. ADKD is defined in section 4.2.1.2. As for any tag, the length of the Tag_0 field l_t is identified by the Tag Size (TS) field within the DSM-KROOT of the chain in force (see section 3.2.3.7).

The verification of the Tag_0 field is described in section 6.7.

4.1.2. MACSEQ

MACSEQ is a 12-bit field that allows the receiver to authenticate the Tag-Info field for the tags whose ADKD type is identified as flexible within the MAC Look-up Table (see section 3.2.3.8).

The generation and verification of the MACSEQ field is described in section 6.6.

4.2. Tags&Info

The Tags&Info section contains a sequence of tags and associated Tag-Info, which are needed for the generation of the tags, as represented in the following figure.

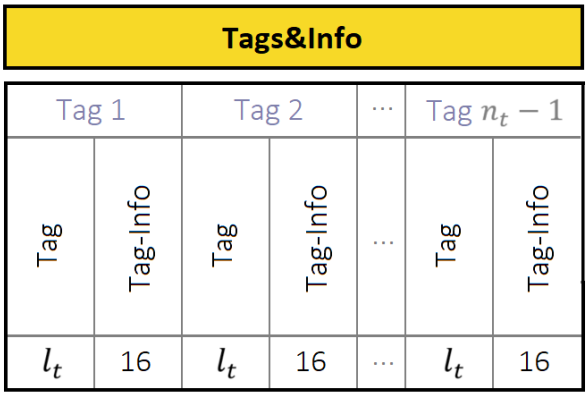


Figure 10. *Tags&Info Message*

The number of tags per MACK message n_t is the maximum possible and can be calculated as follows:

Eq. 8
$$n_t = \left\lfloor \frac{480 - l_K}{l_t + 16} \right\rfloor$$

Where:

- l_K is the key length (see section 3.2.3.6);
- l_t is the tag length (see section 3.2.3.7);
- $\lfloor n \rfloor$ is the floor operator, indicating the greatest integer less than or equal to n.

Considering the above and referring to Figure 10, the last tag would be the tag n_t -1, as the Tag_0 within the MACK Header needs also to be accounted within the n_t tags.

4.2.1. Tag-Info

The 16-bit Tag-Info section contains the necessary information to generate a tag and to identify the corresponding authenticated data. The Tag-Info section is represented in the following figure:

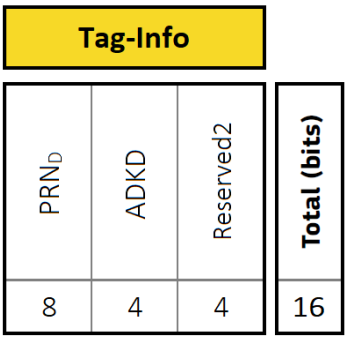


Figure 11. *Tags&Info Message*

The contents, format and semantic of various Tag-Info fields are described in the following sub-sections.

4.2.1.1. PRN_D

The PRN_D field identifies the satellite transmitting the navigation ***data*** which is authenticated by the tag. The OSNMA protocol is designed with the capability to authenticate data from Galileo as well as from other systems. The convention used for the PRN_D field for Galileo and the other systems is indicated in Table 12.

PRND Field value	Assignment
0	Reserved
1-36	Galileo SV_{ID} 1-36 (see note[3])
37-254	Reserved
255	Galileo constellation-related information (not satellite specific)

Table 12. *Assignment for the PRN_D field*

Note that the value 255 is introduced to identify Galileo constellation-related information that is not satellite specific. This might refer to the case of a common set of data being transmitted by all satellites and therefore in principle can be authenticated independently of the specific satellite that transmitted it.

In order to verify the tag as described in section 6.7, the notion of which satellite is providing the authentication information (e.g. tags, Key, ...) is required, as is the satellite transmitting the data to be authenticated and identified by PRN_D. In section 6.7, the satellite transmitting the authentication information is identified with the PRN_A parameter. Considering that authentication information can only be provided by Galileo satellites, PRN_A will take the value of the SVID of the Galileo satellite transmitting the *authentication* information, from 1 to 36, as per Table 12. In the following table, PRN_D and PRN_A definitions are recalled for clarity and referring to the tag verification process described in section 6.7.

3. SV_{ID} parameter transmitted within the Galileo I/NAV Word Type 4 and assuming values from 1 to 36, as specified in [AD.1]

Parameter	Definition	Possible values
PRN_D	Identifies the satellite transmitting the navigation *data* to be authenticated by a specific tag. It is provided within the corresponding Tag-Info section	0-255
PRN_A	Identifies the satellite transmitting the *authentication* information (e.g. tag, Key, …). It is not transmitted within the OSNMA message and it assumes always the value of the SVID of the Galileo satellite transmitting the information	1-36

Table 13. *PRN_D and PRN_A definition*

4.2.1.2. Authentication Data and Key Delay (ADKD)

The 4-bit ADKD field describes the authenticated navigation data, used to generated the associated tag. ADKD can assume values from 0 to 15, and for each of those values the corresponding authenticated data and PRN_D are provided in the following table for Galileo PRNs. The exact format of the authenticated data and their concatenation is shown in Annex B.

ADKD	Galileo Authenticated Data	PRN_D
0	**Galileo I/NAV Ephemeris, Clock and Status** The tag authenticates I/NAV data from Word Types 1 to 5, retrieved from either E1-B or E5b-I, including: • IODnav, Ephemeris, SISA(E1,E5b), SVID, Clock correction, Ionospheric correction, BGDs, HS and DVS flags.	SV_{ID} of the Galileo satellite transmitting the data to be authenticated
1-3	*Reserved*	
4	**Galileo I/NAV Timing Parameters** The tag authenticates the following I/NAV data from the last Word Types 6 and 10 (retrieved from E1-B only): GST-UTC conversion parameters (Word Type 6), TOW[4] (Word Type 6) and GST-GPS conversion parameters (Word Type 10).	255[5]
5-11	*Reserved*	
12	**Slow MAC (additional 10 sub-frame delay, see section 5.6.2) - Galileo I/NAV Ephemeris, Clock and Status** The tag is generated as per ADKD=0 definition, but using a key that is published with an additional 10 sub-frames delay (5 minutes).	Same as ADKD=0
13-15	*Reserved*	

Table 14. *Galileo Authenticated Data with corresponding ADKD and PRN_D information*

4. TOW will be removed from the ADKD4 bit mask in a following version of this document.

5. PRN 255 will be replaced by the SV_{ID} of the Galileo satellite transmitting the data to be authenticated in a following version of this document.

4.2.2. Tag

The tag field contains the truncated MAC starting from the MSB, of length l_t, as defined in the Tag Size (TS) field of the DSM-KROOT of the chain in force. The link between a tag and the data it authenticates is described in Section 5.6.1.

4.3. Key

The key field contains the TESLA chain key. The specific key transmitted by a certain satellite within each MACK message and its position in the chain depends on the applicable time, as defined in section 5.5.

5. OSNMA Data Provision

Within this chapter, elements related with the distribution of the data previously described are discussed. The chapter deals in particular with the sequencing across the different satellites of the Galileo constellation and across time. It also presents the public key and TESLA chain management processes.

5.1. OSNMA Test Mode

As specified in section 3.1.1, OSNMA data might be provided in test mode. Such status is notified to the users through the NMA Status flag (NMAS). When OSNMA data is provided in test mode:

- NMAS is set to "Test" in all cases in which NMAS would be configured to "Operational", as per the other sections of this document (e.g. step 2 of the public key revocation process). More specifically, NMAS is never broadcast as "Operational" while the service is operated in test mode.
- NMAS status "Don't Use" is used as specified in this document. Test mode does not change behaviour of "Don't Use" status flag (e.g. step 1 of public key revocation process).
- CID and CPKS flags are used as specified in this document. Test mode does not change behaviour of CID and CPKS flags.

5.2. Distribution of OSNMA Data through Galileo Satellites

The OSNMA data message described in Chapter 2 is distributed only by a subset of the Galileo satellites, and for the satellites that are not transmitting OSNMA, the I/NAV OSNMA message of Figure 2 will contain a 40-bit sequence of zeros.

The subset of satellites distributing the OSNMA data is changing dynamically over time and the user has no means to know in advance which satellites are distributing OSNMA data and which not. OSNMA receivers will have to be designed accordingly.

The OSNMA protocol is built such that, even if OSNMA data are transmitted only by a subset of the satellites of the Galileo constellation, the data from all satellites can be authenticated. This is realised by means of the so-called cross-authentication: the satellites transmitting OSNMA data can distribute tags authenticating the navigation data from other satellites.

5.3. DSM Block Sequencing and Transmission

As explained in section 3.2, the DSM message is transmitted over several DSM blocks, identified by their DSM Block ID (BID, see section 3.2.1.2). These blocks are scattered across different satellites and each satellite is transmitting the blocks sequentially (i.e. BID=0, BID=1, …). This allows a receiver to determine the preceding and/or incoming DSM block for each satellite. A receveir can reconstruct the DSM combining the blocks from one or multiple satellites.

Within a given sub-frame, all satellites transmit blocks belonging to the same DSM message, identified by its DSM ID (section 3.2.1.1). A DSM associated with a given DSM ID is transmitted entirely and at least once before the transmission of another DSM.

Different DSM messages may be transmitted by the system, in an alternating manner, as shown in the following sections 5.4 and 5.5. In such a case, a DSM associated with a given DSM ID is transmitted in its entirety before the transmission of another DSM message[6]. Alternating DSM messages always have different DSM ID.

6. During the Test Phase, DSM messages may not be transmitted entirely while being alternated during renewal and revocation operations.

During the transmission of a DSM-KROOT, the NMA Header remains constant, and it coincides with the NMA Header information authenticated by the DSM-KROOT.

5.4. Public Key Provision

The public key in force, together with its ID and signature algorithm, is provided in the DSM-PKR message (see section 3.2.2) at defined times (TBD) and also published in the OSNMA server (see Annex D for the interface to the GSC OSNMA server), together with the relevant information required to verify that (as described in 6.2).

Note that only one public key is in force at any time, corresponding to the one with the highest PKID, which is also provided within the DSM-KROOT. Public Keys are published with increasing PKID values.

Even though a public key is expected to be in force for several years, a public key renewal process mechanism is foreseen in this specification. The processes of public key renewal and revocation are described in the following section. Note that a public key renewal does not imply a TESLA chain renewal (discussed in section 5.5.3).

5.4.1. Public Key Renewal and Revocation

The public key renewal mechanism is depicted in Figure 12 and comprises the following steps:

- Step 1: the *NMAS* flag remains set to "Operational" but the CPKS flag is set to "New Public Key" (NPK), reporting that the public key in force p is going to be replaced. During this step, which has a maximum duration of 24 hours [TBC], the DSM alternates two messages with different DSM IDs: a DSM-KROOT verifiable with p, KROOT(i,p), and DSM-PKR for the new public key p', PKR(p'), where PKID(p')>PKID(p).
- Step 2: p' enters into force with the transmission of a new DSM-KROOT verified with p', KROOT(i,p'). The DSM alternates the new DSM-KROOT with PKR(p') from Step 1. In Step 2, CPKS is maintained as NPK for a maximum duration of 24 hours [TBC]. When p' enters in force, p and any other public key with a PKID < PKID(p') is declared not in use, so at a given time only one public key is in force. From this time, the receiver must discard any previously stored public key.
- Step 3: CPKS is set back to "Nominal", and only the DSMs of KROOT(i,p') are transmitted.

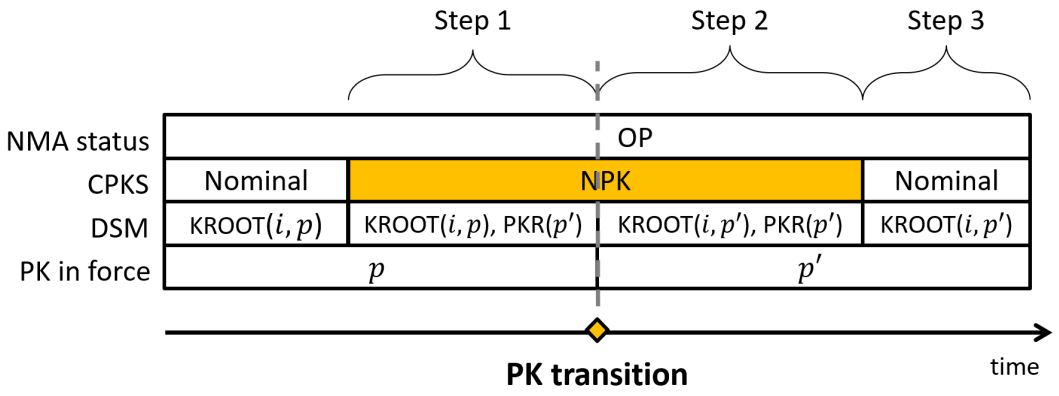


Figure 12. *Public Key renewal*

The public key revocation process is followed only when the public key in force is revoked.It is not expected to occur in nominal operation. The public key revocation process is depicted in Figure 13 and comprises the following steps:

- Step 1: The *NMAS* flag is set to "Don't Use" (DU) and the CPKS flag is set to "Public Key Revoked" (PKREV) for a duration of 2 hours [TBC], reporting that the public key *p* is revoked. A DSM-PKR with the new public key *p'* and a new DSM-KROOT with a root key for a new chain *i'*, authenticated with *p'*, start to be broadcast. By transmitting KROOT(*i'*,*p'*), the new key *p'* enters into force.
- Step 2: The *NMAS* is set back to "Operational" (OP). The PKREV flag reports that the previous public key has been revoked and remains set for 22 hours [TBC]. The chain *i'* enters into force at the same time. From this time on, the receiver shall discard any previous public key and any KROOT associated with the previous TESLA chain.
- Step 3: CPKS is set back to "Nominal" and the DSM-PKR stops being transmitted.

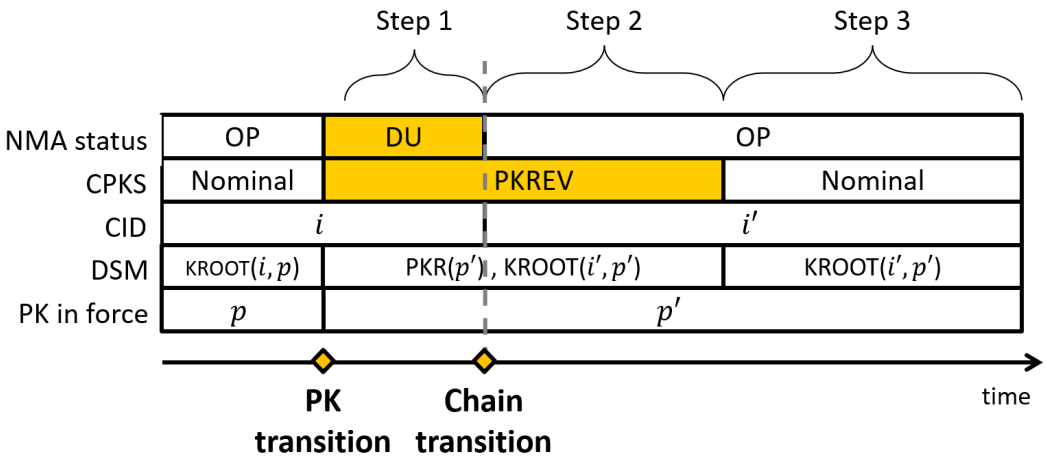


Figure 13. *Public Key revocation*

Note that the receiver shall prevent any key that has been subject to a renewal or revocation process from being further used.

5.5. TESLA Chain Provision

Within this section, various elements related with the provision of the TESLA chain are described.

5.5.1. Time of Applicability

The TESLA chain is associated to a time of applicability, GST_0. This time is provided with the root key of the TESLA chain, KROOT, in the DSM-KROOT message (see section 3.2.3). The time of applicability GST_0 is provided in the form of Week Number (WN_K) and Time Of Week (expressed in Hours, $TOWH_K$), as explained in section 3.2.3.9. These parameters are defined as follows:

- KROOT Week Number (WN_K) is represented with 12 bits and is defined, as in the case of Galileo GST defined in [AD.1], as an integer counter that gives the sequential week number from the GST start epoch;
- KROOT Time Of Week (expressed in Hours, $TOWH_K$) is defined as the number of hours that have elapsed since the transition from the previous to the current week. The $TOWH_K$

covers an entire week from 0 to 167 hours and is reset to zero at the beginning of the week.

WN_K and $TOWH_K$ are relative to the GST start epoch as specified in [AD.1].

KROOT is the key immediately preceding the first key of the chain and is nominally associated with the sub-frame starting at GST_0-30 sec. Thus, it will never be used for MAC/tag production, as it relates to a time before the chain enters into force. The time of applicability of the chain GST_0 is associated to the first key of the chain.

In order to facilitate the key verification process, the concept of floating KROOT is included in the OSNMA protocol. This concept allows transmitting several KROOTs, associated with different times of applicability, while a chain is in force. This facilitates the authentication of TESLA keys and allows users to verify reception of updated DSM messages.

Following the above, a new floating KROOT will be provided at least once per day and at most once per hour[7]. This means that, in nominal operation conditions, no DSM-KROOT with an applicability time GST_0 dating back more than 1 day (TBC) will be transmitted.

5.5.2. Key Sequencing

The TESLA keys, transmitted while the CID (section 3.1.2) remains constant, belong to a chain that is common to all the Galileo satellites providing OSNMA. Also, all satellites transmit the same key at the same epoch.

TESLA keys are provided in the MACK message (see Chapter 4). They are transmitted in reverse order with respect to their generation, as per the TESLA protocol [3].

5.5.3. TESLA Chain Renewal and Revocation

Similarly to the public key, the TESLA chain can be renewed or revoked as explained in the following lines. The chain renewal process is the usual process to follow when a TESLA chain is coming to an end. The chain renewal process is depicted in Figure 14 and comprises the following steps:

- Step 1: the Chain and Public Key Status (CPKS) flag (section 3.1.3) is set to “End of Chain” (EOC), reporting that the current chain *i* is coming to an end. A new DSM-KROOT for the new chain *i'* is transmitted. During this step, the DSM alternates two DSM-KROOTs: the one for the chain currently in force KROOT(*i,p*), where p is the public key in force, and the one for the next chain, KROOT(*i',p*). This step has a duration of 24 hours [TBC].
- Step 2: At the transition time, the new chain *i'* comes into force. The CPKS is set to “Nominal”, the Chain ID (CID) (section 3.1.2) is set to *i'* and the DSM transmits only the DSM-KROOT for the new chain KROOT(*i',p*). The previous chain *i* is considered expired and the receiver shall discard any parameter related to the previous chain.

7. During the Test Phase, floating KROOT will not be provided when a renewal or revocation process is taking place.

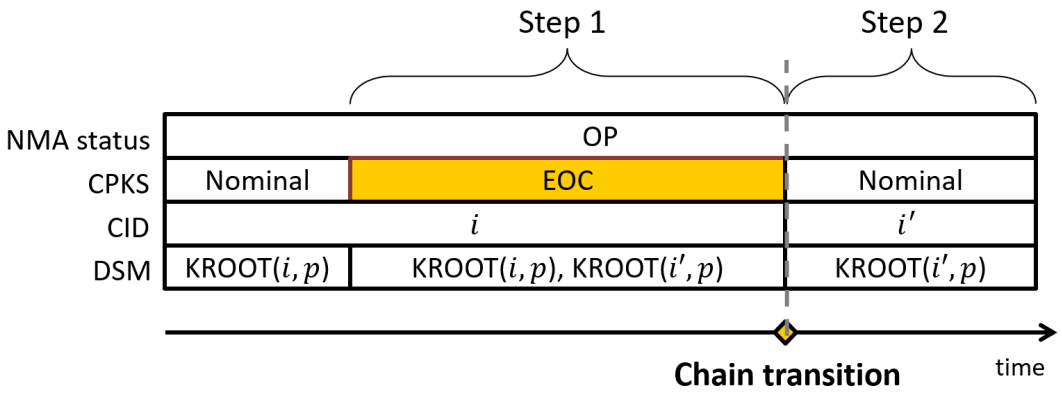


Figure 14. *TESLA chain renewal*

The chain revocation process is followed only when the chain in force is revoked. It is not expected to occur in nominal operations. The chain revocation process is depicted in Figure 15 and comprises the following steps:

- Step 1: the *NMAS* flag (section 3.1.1) is set to "Don't Use" (DU) and the CPKS is set to "Chain Revoked" (CREV), reporting that the chain in force *i* is revoked. This step has a duration of 2 hours [TBC]. A new DSM-KROOT(*i'*,*p*), with the root key of a new chain *i'* is transmitted. Its WN_K / $TOWH_K$ fields may refer to a time in the past, even though the chain is not yet in force because the CID has not yet been updated. The receiver may store the new KROOT but it must wait until the new chain comes into force in Step 2. The receiver must discard any KROOT related to the previous chain *i*.
- Step 2: The CID is set to *i'*, reporting that the new chain is in force. The *NMAS* flag is set back to "Operational" (OP). The CPKS is maintained as CREV for a duration of 22 hours [TBC], to report (in combination with the *NMAS*, as described in 3.1.3) that the previous chain has been revoked. The receiver can start the NMA service. For that, it must perform the required number of chain steps to authenticate the new keys with the newly received KROOT, as explained in Section 6.3.
- Step 3: The CPKS flag is set to "Nominal".

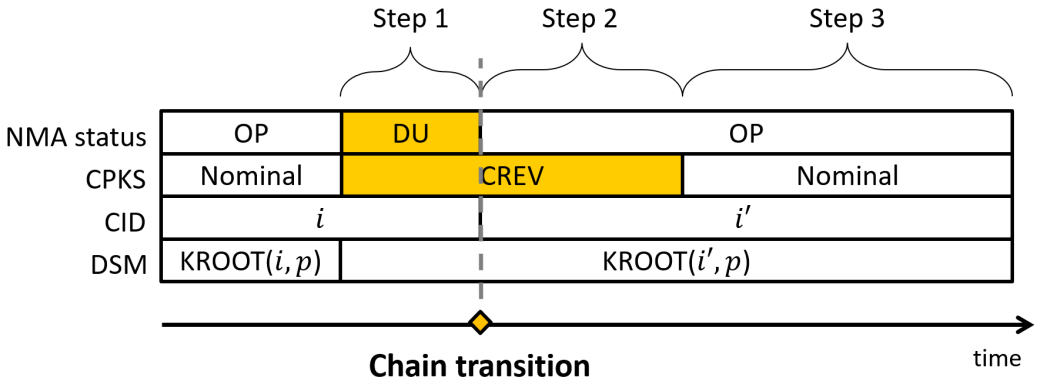


Figure 15. *TESLA chain revocation*

5.6. Tags Distribution

Within this section a number of aspects related with the distribution of the tags are discussed.

5.6.1. Tag Identification and Accumulation

A tag retrieved in a sub-frame transmitted at the time GST_{SF} is associated to navigation data transmitted in the previous sub-frame, transmitted at the time (GST_{SF} – 30 sec). As explained in Chapter 4, tags are transmitted together with their related Tag-Info fields, and therefore a certain tag is also associated to a specific data mask (ADKD) and satellite (PRN_D).

Defining a minimum equivalent tag length L_t^{min} as the minimum number of tag bits that are required to authenticate a certain data, the authentication of that data can be obtained by verifying a tag of length L_t such that

Eq. 9

$$l_t \geq L_t^{min}$$

Alternatively, several (shorter) tags can be accumulated in order to reach the minimum equivalent tag length such that

Eq. 10

$$l_t \cdot N_t \geq L_t^{min}$$

Where N_t is the number of tags of length L_t, associated to the same data, to be accumulated in order to perform authentication.

The concept of tag accumulation is further discussed in [AD.2], where a requirement in terms of minimum equivalent tag length necessary to perform authentication is also provided.

5.6.2. Applicable Keys for Tags Verification

An offset of one MACK message is introduced between the tags and the associated keys (to be used for their verification). This means that the tags received within a certain MACK message have to be verified with the key broadcast in the next MACK message.

In the specific case of ADKD = 12 (see section 4.2.1.2), the tag transmitted by the system is generated with a key that is broadcast with an additional 10 sub-frames delay. This is labelled also as “Slow MAC”. As a consequence, an additional delay of 10 sub-frames shall be taken into account when selecting the key to be used for a tag with an ADKD=12.

6. Receiver Cryptographic Operations

Within this chapter the various steps to be performed in order to verify the different cryptographic elements are described. Further details including conditions and requirements at user receiver level necessary to perform OSNMA as well as complementary guidelines are provided in [AD.2]. Notation, functions and operators that are common to the various sections within the chapter are introduced within section 6.1.

6.1. Common Cryptographic Functions and Operators

In order to improve the readability of the chapter, common functions, operators and notation are introduced within this section and are to be considered valid for the entire chapter.

6.1.1. Main Cryptographic Functions

The following are the main cryptographic functions used within the chapter:

- $\text{hash}_{H256}(m)$ is the SHA-256[8] hash operation function applied to the input message *m*.
- $\text{hash}_{chain}(m)$ is the specific hash function used for the TESLA chain as indicated in the HF field of the DSM-KROOT (see section 3.2.3.4).
- mac*(K,m)* is the MAC function used for the chain in force, as indicated in the MF field of the DSM-KROOT (see section 3.2.3.5), where *K* is the key from the TESLA chain used for the MAC generation and *m* is the input message.

Note that for the three functions above the length of the input message *m* has to fit an integer number of bytes, and if this is not the case it needs to be right zero-padded.

- signature*(x)* is the specific digital signature algorithm chosen for the protocol, which is ECDSA [6], supporting different signature lengths and public key lengths, as described in Table 15. These parameters are statically and unambiguously associated with the Public Key ID in force, and defined by the Public Key Type. The applicable function is specified in the New Public Key Type (NPKT) field of the DSM-PKR message and is also provided on the GSC OSNMA server (as described in Annex D) in case the public key is retrieved there. The key to be used as an input to the signature algorithm is the unsigned and unpadded value retrieved in the NPK field whose length is indicated in Table 15.

ECDSA Curve and hash function	Signature length l_{DS} [bits]	Key length [bits]
P-256/SHA-256	512	256
P-521/SHA-512	1056 [9]	521

Table 15. *Supported ECDSA algorithm*

For the time being, and according to current standards [6], Elliptic Curve Digital Signature Algorithm (ECDSA) with different key lengths is considered for the DSM generation. Future revisions might consider additional signature algorithms. Note that the length of the input to the signature algorithm *x* has to fit an integer number of bytes, and if this is not the case it needs to be zero-padded.

8. SHA-256 belongs to the SHA-2 family hashes, which are defined in [8]
9. In the case of ECDSA P-521, the digital signature is composed of a pair of 66-bytes signatures, being transmitted consecutively over 528-bits each. The elliptic curve point coordinate is represented by the 521 least significant (rightmost) bits, as per [14].

6.1.2. Operators

The following are the main operators used within the chapter:

- *trunc(L,I)* is the truncation function retaining the *L* most significant bits (MSB) of the input *I*;
- (*X*||*Y*) concatenates bitset *X* to bitset *Y*, with *X* at the MSB.

6.2. DSM-PKR Verification

The user is required to authenticate the ECDSA public key or service message received in the DSM-PKR, against a Merkle root, using the hashing algorithm that was used for the tree generation (currently being SHA-256). The system might use in future SHA3-256 for the tree generation. The Merkle root can be loaded in the receiver in the factory or retrieved from the OSNMA server with the associated information of what algorithm is to be used for the tree generation.

The Merkle tree leaf m_i, identified by the Message ID (see section 3.2.2.2), is generated as follows:

Eq. 11
$$m_i = (NPKT \| NPKID \| NPK)$$

Where *NPKT, NPKID* and *NPK* are described in section 3.2.2.

The Galileo OSNMA protocol uses a Merkle tree that can authenticate $N = 16$ leaves (m_0, …, m_{15}), as represented in Figure 16. A Merkle tree leaf m_i is validated against the Merkle root, $x_{4,0}$, by means of the intermediate tree nodes $x_{i,j}$ (see section 3.2.2.3). Further details on the Merkle tree can be found in [AD.2].

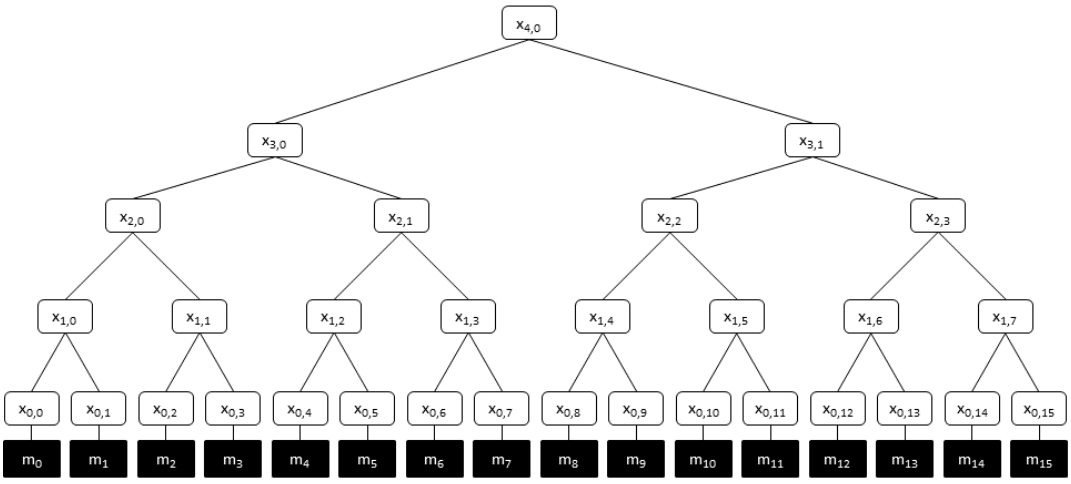


Figure 16. *Galileo OSNMA Merkle-tree*

The base nodes of the tree x_(0,i) can be computed as follows:

Eq. 12
$$x_{0,i} = \text{hash}_{H256}(m_i)$$

With *i=0,…,N*-1

The other nodes $x_{j,i}$ are computed as follows:

Eq. 13
$$x_{j,i} = \text{hash}_{H256}\left(x_{j-1,2i} \middle\| x_{j-1;2i+1}\right)$$

With:

- j=1,…,4 denotes the level in the tree;
- i=0,…,2^{4-j}-1, for each j.

To verify the Merkle tree leaf m_i, the nodes have to be computed until reaching the root $x_{4,0}$, then the obtained value shall be compared with the stored one. Additional details and examples of the DSM-PKR verification can be found in [AD.2].

6.3. DSM-KROOT Verification

The DSM-KROOT digital signature is produced generating a message *M*, concatenating the various DMS-KROOT fields as described below:

Eq. 14
$$M = \begin{pmatrix} NMA\ Header \| CIDKR \| Reserved1 \| HF \| MF \| KS \| TS \| MACLT \| \dots \\ \dots Reserved \| WN_K \| TOWH_K \| \alpha \| KROOT \end{pmatrix}$$

Where:

- *NMA Header* corresponds to the 8-bit NMA Header field as per section 3.1,
- The remaining fields are described in section 3.2.3.

The digital signature *DS* is generated as follow:

Eq. 15
$$DS = signature(M \| P)$$

Where *P* is a zero-padding sequence such that the length of the input for the signature algorithm fits an integer number of bytes.

6.4. TESLA Key Verification

The TESLA keys belong to a chain that starts with a random seed key K_N, which is only known by the OSNMA provider, and ends with a root key K_0 that is public and certified through the DSM-KROOT.

The seed key K_N and the root key K_0 are related to each other through a function *F* such that:

Eq. 16
$$K_0 = F^N(K_N)$$

Where F_N means recursively applying *N* times the function *F*, so that each element of the chain can be constructed by applying *F* to the previous element, as follows:

Eq. 17
$$K_I = F(K_{I+1}) = trunc\left(l_k, \text{hash}_{\text{chain}}\left(K_{I+1} \| GST_{SF\_I} \| \alpha\right)\right)$$

Where:

- I is the index of the key in the chain as from section 5.5.2;
- l_k is the key size as from section 3.2.3.6;
- α is the unpredictable chain pattern identified in section 3.2.3.10;
- $GST_{SF,I}$ is the Galileo System Time at the start of the 30-second sub-frame in which the key K_I is transmitted and is represented as a 32-bit unsigned integer as per [AD.1]. For Galileo E1 I/NAV, this is the E1 sub-frame start time minus 1 second. Note that for evaluating K_0 the following applies:

Eq. 18
$$GST_{SF,I} = GST_0 - 30 \text{ [seconds]}$$

where GST_0 is the time of applicability associated with the chain as per 3.2.3.9.

A Tesla key K_I can be verified against the root key K_0 , by computing $F^I(K_I)$ and comparing the result with K_0. The number of hashes to be performed to verify K_I versus K_0 is given by the following equation.

Eq. 19
$$I = \frac{GST_{SF,I} - GST_0}{30} + 1$$

Similarly, it can also be verified against a previously authenticated key from the same chain K_j, such that ($J<I$), by computing $F^{I-J}(K_I)$ and comparing the results with the stored K_j.

6.5. MAC Look-up Table Verification

The tag ADKD sequence can be partially or totally fixed for each chain through the MAC look-up table, as defined in section 3.2.3.8. When fixed, the ADKD type of the tag being verified shall match the one indicated in the look-up table.

6.6. MACSEQ Verification

The 12-bit MACSEQ authenticates the Tag-Info fields of those tags received in the MACK message and whose ADKD type is flexible as per the tag sequence (see MACLT field). The MACSEQ is generated with the same key and MAC function as the rest of the MACs in the same MACK message and it is verified by comparing the received value (see section 4.1.2) with a value computed locally as follows:

Eq. 20
$$MACSEQ = trunc\big(12, mac(K, m)\big)$$

Where K is the key from the TESLA chain used for the Tag_0 generation (see section 5.6.2) and m is computed as follows:

Eq. 21
$$m = (PRN_A \| GST_{SF} \| MFLEX_1 \| MFLEX_2 \| \ldots \| MFLEX_N)$$

with

- PRN_A is an 8-bit unsigned integer that identifies the satellite transmitting the authentication information and it takes always the value of the SV_{ID} of the Galileo satellite transmitting the information (see section 4.2.1.1);
- GST_{SF} is defined as the start of the 30-second sub-frame in which the MACSEQ field is transmitted and is represented as a 32-bit unsigned integer as per [AD.1];
- $MFLEX_i$, with $_i$=[1…$_N$] are the Tag-Info fields to be authenticated. $MFLEX_1$ represents the Tag-Info field (as per section 4.2.1) of the first tag in the current MACK message defined as flexible in the sequence provided by the MAC Look-up Table. $MFLEX_N$ represents the Tag-Info field of the last tag in the current MACK message defined as flexible within the sequence provided by the MAC Look-up Table.

In the case there are no tags defined as flexible in MACLT entry, the following simplified expression applies

Eq. 22 $$m = (PRN_A \| GST_{SF})$$

6.7. Tag Verification

The tags provided in the MACK message are generated as follows. For tags other than Tag_0, the *tag* is generated as:

Eq. 23 $$tag = trunc\big(l_t, mac(K, m)\big)$$

Where:

- l_t is the length of the tag as defined in 3.2.3.7;
- *K* is the key from the TESLA chain used for the tag generation identified as discussed in section 5.6.2;
- *m* is computed as follows:

Eq. 24 $$m = (PRN_D \| PRN_A \| GST_{SF} \| CTR \| NMAS \| navdata \| P)$$

Where

- PRN_D identifies the satellite transmitting the navigation data to be authenticated and is provided within the corresponding Tag-Info section (see section 4.2.1.1). In the case PRN_D is set to the value “255” (e.g. ADKD=4), PRN_D=PRN_A shall be used for the computation of *m* as from Eq. 25;
- PRN_A is defined in the section 6.6 above;
- GST_{SF} is defined as the start of the 30-second sub-frame in which the tag is transmitted and is represented as a 32-bit unsigned integer as per [AD.1];
- *CTR* is an 8-bit unsigned integer identifying the position of the tag within the MACK message; it has a value of ‘1’ for the first tag in the tag sequence, incrementing by one for each subsequent tag of that message;
- *NMAS* is transmitted within the NMA Header (see section 3.1.1);

- *navdata* is the concatenation of the navigation data from the previous sub-frame being authenticated, obtained as indicated in 4.2.1.2 and Annex B for the corresponding ADKD indicated within the Tag-Info field;
- *P* is a zero-padding sequence such that the length of *m* fits the minimum number of integer bytes.

The message *m* is unique for each tag.

Similarly to the above, in the case of Tag_0, the computation becomes:

Eq. 25 $$Tag_0 = trunc\left(l_t, mac(K, m_0)\right)$$

Eq. 26 $$m_0 = (PRN_A \| GST_{SF} \| CTR \| NMAS \| navdata \| P\ )$$

Where CTR equals 1, as Tag_0 is always the first tag of the MACK message. Similarly, the tags can be locally generated by the receiver and verified by comparing them with the received values.

Additional References

[1] European Commission, COMMISSION IMPLEMENTING DECISION (EU)2017/224, 8 February 2017 (CS Implemeting Act), 2017.

[2] European Commission, COMMISSION IMPLEMENTING DECISION (EU)2018/321, 2 March 2018 amending Implementing Decision (EU) 2017/224 (CS Implemeting Act), 2018.

[3] International Organization for Standardization, "ISO/IEC 29192-7:2019(E), Information security- Lightweight cryptography- Part 7: Broadcast authentication protocols," 2019.

[4] Method and system to optimise the authentication of radionavigation signals, Patent application, PCT/EP2015/056120, 23/03/2015, European Union represented by European Commission

[5] Digitally-signed satellite radio-navigation signals, Patent application PCT/EP2014/064285, 04/07/2014, European Union represented by European Commission

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

[7] National Institute of Standards and Technology, "NIST Special Publication 800-208: Recommendation for Stateful Hash-Based Signature Schemes." 2020.

[8] National Institute of Standards and Technology, "FIPS PUB 180-4: Secure Hash Standard (SHS)," 2012.

[9] National Institute of Standards and Technology, "FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," 2015.

[10] National Institute of Standards and Technology, "FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC)," 2008.

[11] International Organization for Standardization, "ISO/IEC 9797-1:2011: Information technology - Security techniques - Message Authentication Codes (MACs)- Part 1: Mechanisms using a block cipher," 2011.

[12] National Institute of Standards and Technology, "NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode forAuthentication," 2004.

[13] US Government, "GPS Interface Specification IS-GPS-200K", 06.05.2019.

[14] ISO/IEC 15946-1:2016, Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General

Annex A - List of Acronyms

ADKD	Authentication Data & Key Delay
AES	Advanced Encryption Standard
BID	Block ID
CID	Chain ID
CMAC	Cipher-based Message Authentication Code
CPKS	Chain and Public Key Status
CREV	Chain Revoked
DSM	Digital Signature Message
DSM-KROOT	DSM for a KROOT
DSM-PKR	DSM for a PKR
DU	Don't Use
ECDSA	Elliptic Curve Digital Signature Algorithm
EOC	End Of Chain
GSC	European GNSS Service Centre
GST	Galileo System Time
HF	Hash Function
HKROOT	Header and KROOT
HMAC	Hash-based Message Authentication Code
ICD	Interface Control Document
IOD	Issue of Data
ITN	Intermediate Tree Node
KROOT	Root Key
MAC	Message Authentication Code
MACK	MAC and Key
MACLT	MAC Look-up Table
MACSEQ	MAC Sequence
MF	MAC Function
MID	Message ID
MSB	Most Significant Bit
NB	Number of Blocks
NMA	Navigation Message Authentication
NPK	New Public Key
NPKID	New Public Key ID
NPKT	New Public Key Type
OP	Operational
OS	Open Service
PK	Public Key
PKID	Public Key ID
PKR	Public Key Renewal
PKREV	Public Key Revocation
PRN	Pseudo Random Noise
SHA	Secure Hash Algorithm
SIS	Signal In Space
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
TOW	Time of Week
WN	Week Number

Annex B - Authenticated Data Concatenation Format

Within this annex, the exact format of the authenticated data for each entry of Table 14 is described. For each set of data a bit mask to extract the data from the corresponding I/NAV word is provided within [AD.2].

B.1 Galileo I/NAV Ephemeris, Clock and Status (ADKD=0 and ADKD=12)

The format of the authenticated data for the cases ADKD=0 and ADKD=12 for Galileo is provided in the following figure, where selected data from I/NAV Word Types 1 to 5 are concatenated.

data from Word Type 1						data from Word Type 2						data from Word Type 3								data from Word Type 4								data from Word Type 5													
	Ephemeris (1/4)						Ephemeris (2/4)						Ephemeris (3/4)								Ephemeris (4/4)		Clock Correction				Ionospheric correction													
IOD_{nav}	t_{0e}	M_0	e	$A^{1/2}$		IOD_{nav}	Ω_0	i_0	ω	$\bullet i$		IOD_{nav}	$\bullet \Omega$	Δn	C_{UC}	C_{US}	C_{RC}	C_{RS}	SISA(E1,E5b)		IOD_{nav}	SVID	C_{ic}	C_{is}	t_{0c}	a_{f0}	a_{f1}	a_{f2}	a_{i0}	a_{i1}	a_{i2}	Region 1	Region 2	Region 3	Region 4	Region 5	BGD(E1,E5a)	BGD(E1,E5b)	$E5b_{HS}$	$E1B_{HS}$	$E5b_{DVS}$	$E1B_{DVS}$	Total (bits)
10	14	32	32	32		10	32	32	32	14		10	24	16	16	16	16	16	8		10	6	16	16	14	31	21	6	11	11	14	1	1	1	1	1	10	10	2	2	1	1	549

Figure 17. *Concatenated Authenticated Data for ADKD=0 and ADKD=12*

It is recalled that, following [AD.1], the information contained within Word Types 1-4 can be recovered also using Reed-Solomon outer enconding and the parity words provided within the Word Types 17-20. As specified within [AD.1], the condition to be respected is that the concerned Words 1-4 and the parity words 17-20 are all identified with the same IOD_{nav}.

B.2 Galileo I/NAV Timing Parameters (ADKD=4)

The format of the authenticated data for the case ADKD=4 for Galileo is provided in the following figure, where selected data from the last I/NAV Word Types 6[10] and 10 (retrieved from E1-B only) are concatenated.

data from Word Type 6									data from Word Type 10				Total (bits)
GST-UTC conversion parameters								TOW	GST-GPS conversion parameters				
A_0	A_1	Δt_{LS}	t_{ot}	WN_{0t}	WN_{LSF}	DN	Δt_{LSF}		A_{0G}	A_{1G}	t_{0G}	WN_{0G}	
32	24	8	8	8	8	3	8	20	16	12	8	6	**161**

Figure 18. *Concatenated Authenticated Data for ADKD=4*

10. TOW will be removed from the ADKD4 bit mask in a following version of this document.

Annex C – MAC Look-up Table

The OSNMA protocol allows the receiver to authenticate different data from different satellites. The tag sequence is partially fixed for each chain through a look-up table, whose entry is provided in the MACLT field, described in 3.2.3.8. Table 16 defines the MAC look-up table with the associated ADKD sequences. New sequences might be added in future updates of this ICD.

The first column (ID[11]) is the entry value to the table as per the DSM-KROOT MACLT field defined in 3.2.3.8. It is maintained for the duration of the chain. The second column (Msg) specifies the number of MACK messages (1 or 2) for which the sequence is defined. When it is equal to 2, the sequence starts with the MACK message transmitted in the first 30 seconds of a GST minute. The third column (*nt*) is the number of tags per MACK message, as defined in 4.2. The last column specifies the tag slot sequence, and should be interpreted as follows.

Every slot is represented by three characters:

- Flexible slots are represented as 'FLX'. They are not fixed in the look-up table and their Tag-Info data is authenticated as per 6.6.
- All other slots are fixed. Their first 2 characters define the ADKD (as per 4.2.1.2) and the last character means 'S' for Self-authentication and 'E' for Galileo cross-authentication. For example, '12S' means ADKD = 12, self-authentication; and '00E' means ADKD = 0, Galileo cross-authentication. The first element of the sequence is always fixed to '00S' and corresponds to Tag0, as described in 4.1.1.

ID	Msg	nt	Sequence	
27	2	6	00S, 00E, 00E, 00E, 12S, 00E	00S, 00E, 00E, 04S, 12S, 00E
28	2	10	00S, 00E, 00E, 00E, 00S, 00E, 00E, 12S, 00E, 00E	00S, 00E, 00E, 00S, 00E, 00E, 04S, 12S, 00E, 00E
31	2	5	00S, 00E, 00E, 12S, 00E	00S, 00E, 00E, 12S, 04S
33		6	00S, 00E, 04S, 00E, 12S, 00E	00S, 00E, 00E, 12S, 00E, 12E

Table 16. *MAC Look-up Table*

11. The IDs specified in this version of the document are the ones supported for the Test Phase.

Annex D – Interface with the European GNSS Service Centre (GSC) OSNMA Server

The aim of this annex is to explain how a user can retrieve the OSNMA crypto material from the GSC web portal. Additionally, the GSC web portal will provide information on recovery actions in case an OSNMA Alert Message is broadcast.

D.1. Accessing the Web Portal

Users can access the web portal via: https://www.gsc-europa.eu

D.2. GSC Registration Process

In the landing page, users need to click on the top link “REGISTER”.

Figure 19. *GSC web portal page*

After that, users need to fill out the registration form.

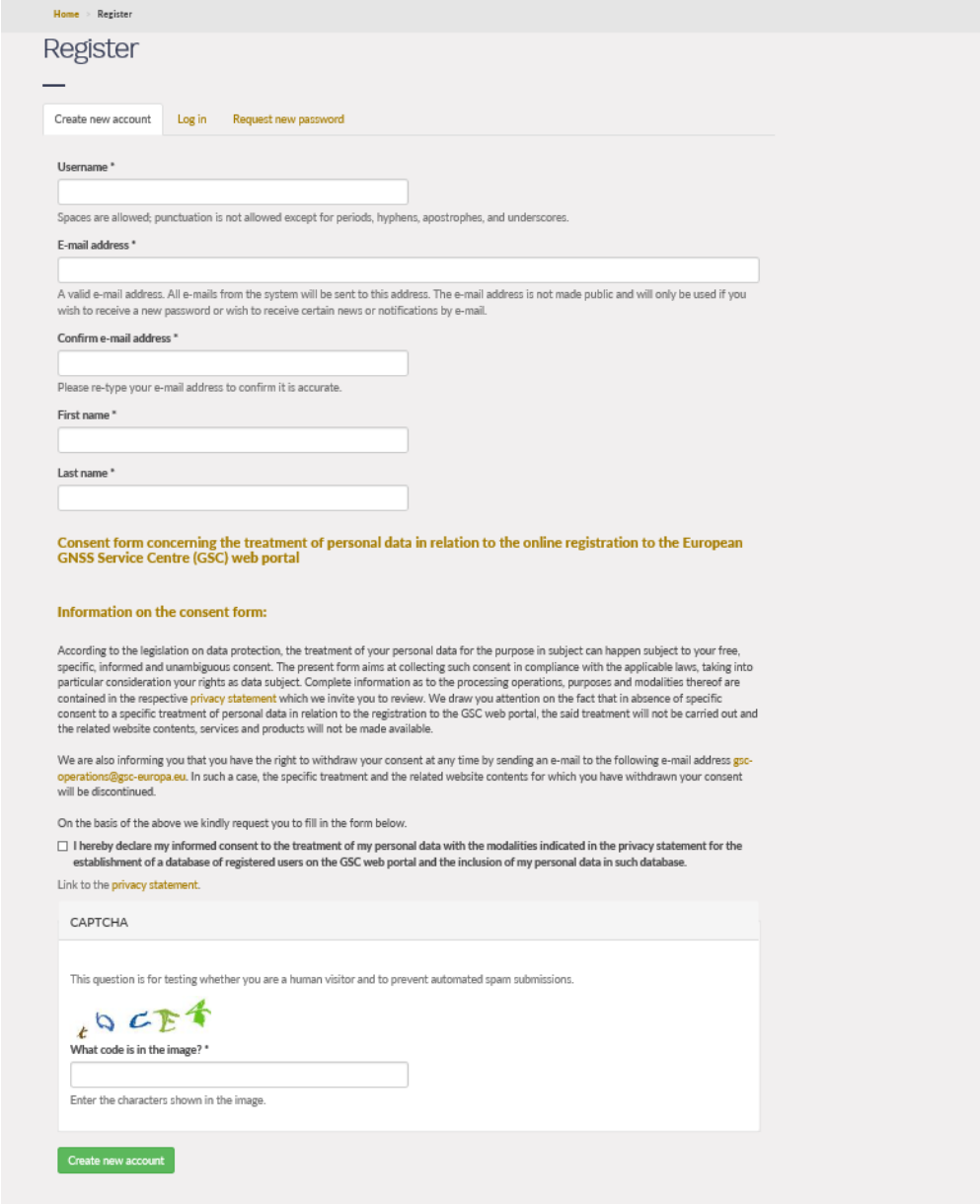


Figure 20. *User registration form*

D.3. GSC User Login

In the top menu, a user can access the login form via the “LOGIN” link (Figure 21).

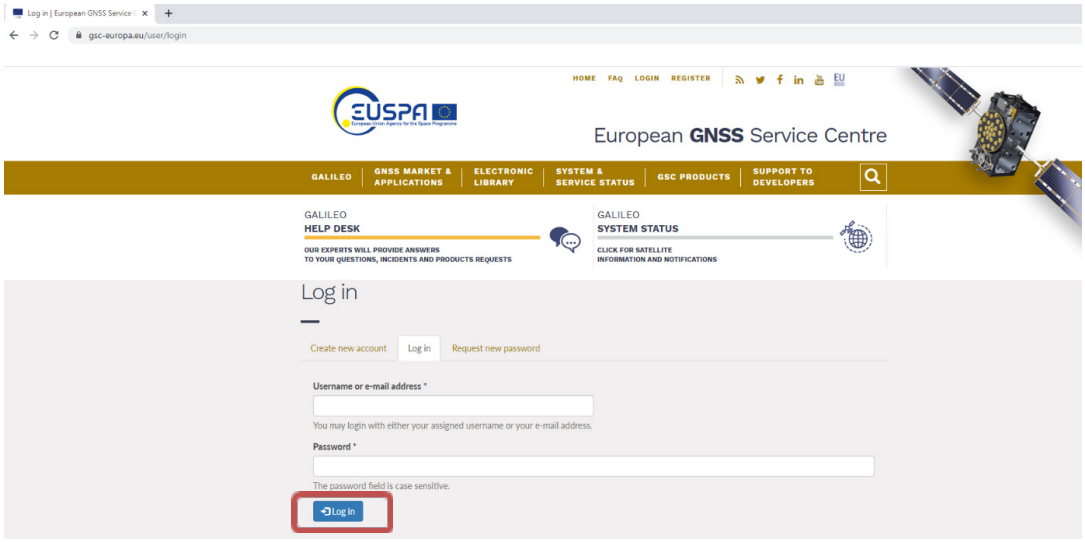


Figure 21. *Login menu*

D.4. Registration to the OSNMA Test Phase

After successful login in the GSC webportal, and in order to receive the key material needed to process the OSNMA test SIS, the user shall register to the OSNMA Test Phase. This is achived by clicking in “OSNMA PUBLIC OBSERVATION TEST PHASE” under “SUPPORT TO DEVELOPERS” menu and the subsequent steps, as shown in the following figures.

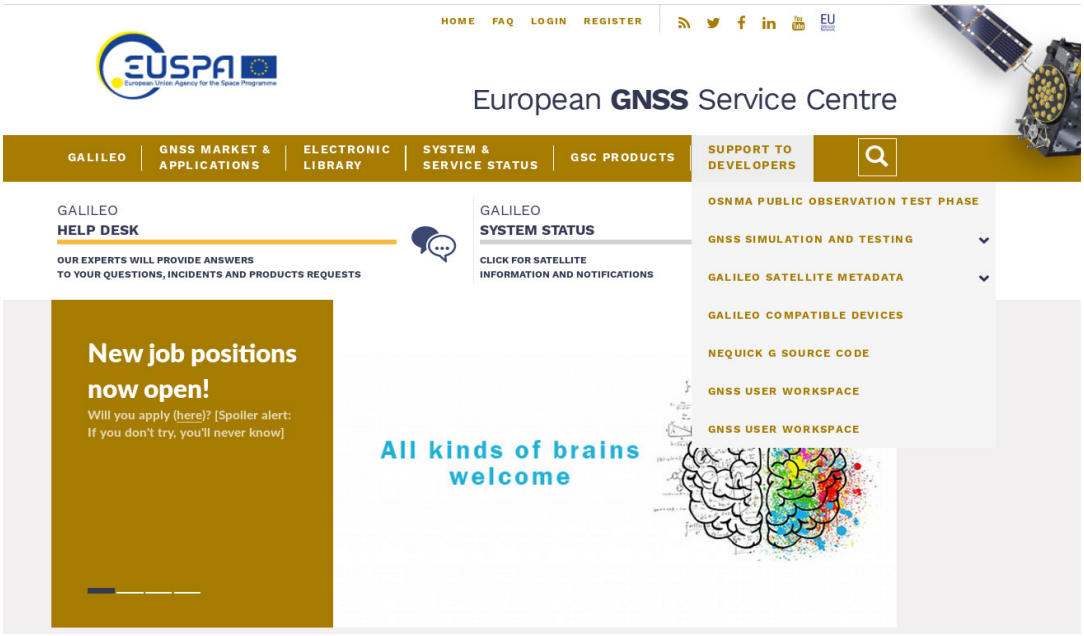


Figure 22. *Support to developers menu*

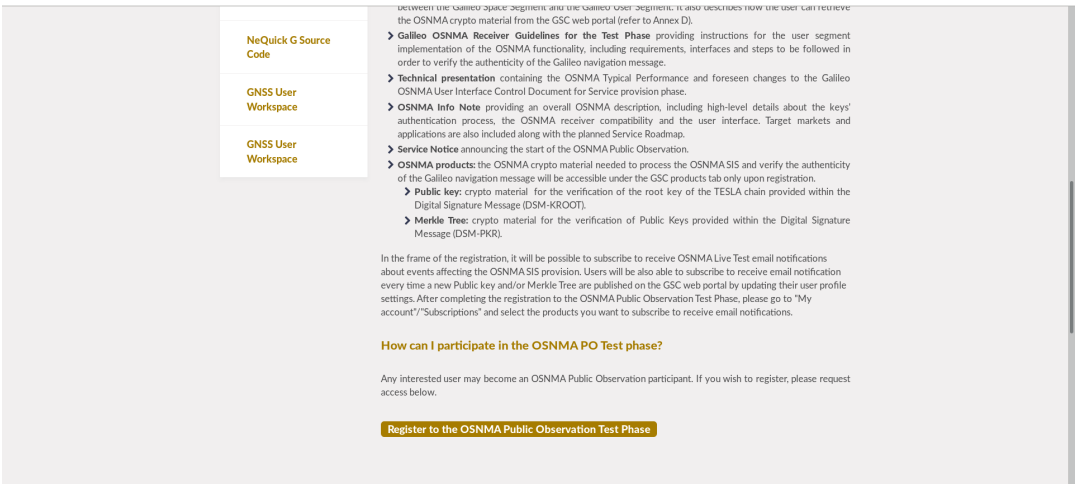


Figure 23. *OSNMA Test Phase registration*

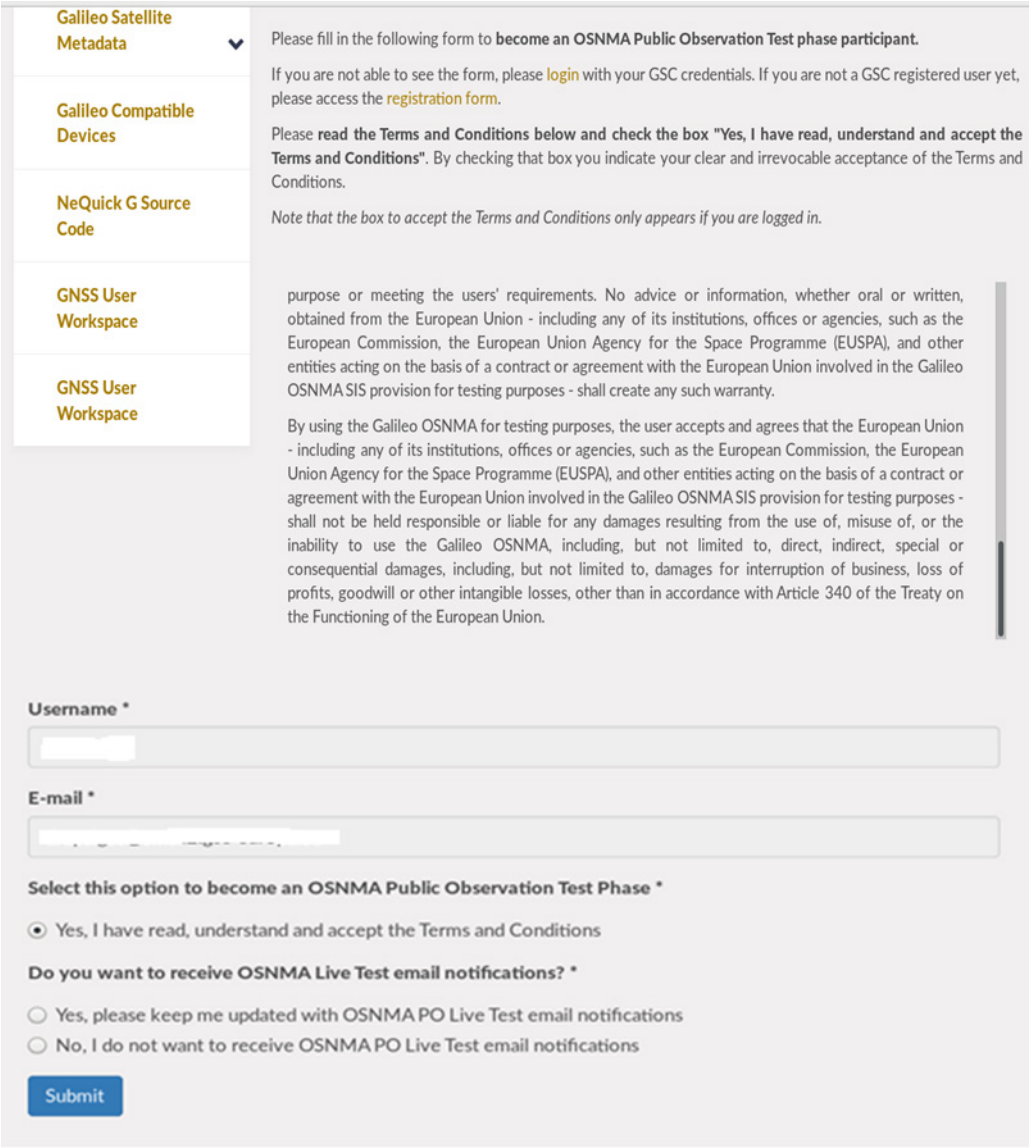


Figure 24. *OSNMA Public Observation Test Phase registration form*

Under the registration page, the Terms and Conditions applicable to the OSNMA Public Observation Test Phase will be displayed along with the user registration form. The user will need to fill in the form and to accept the Terms and Conditions.

To complete the registration, users will be able to subscribe to receive OSNMA Live Test email notifications about events affecting the OSNMA SIS provision.

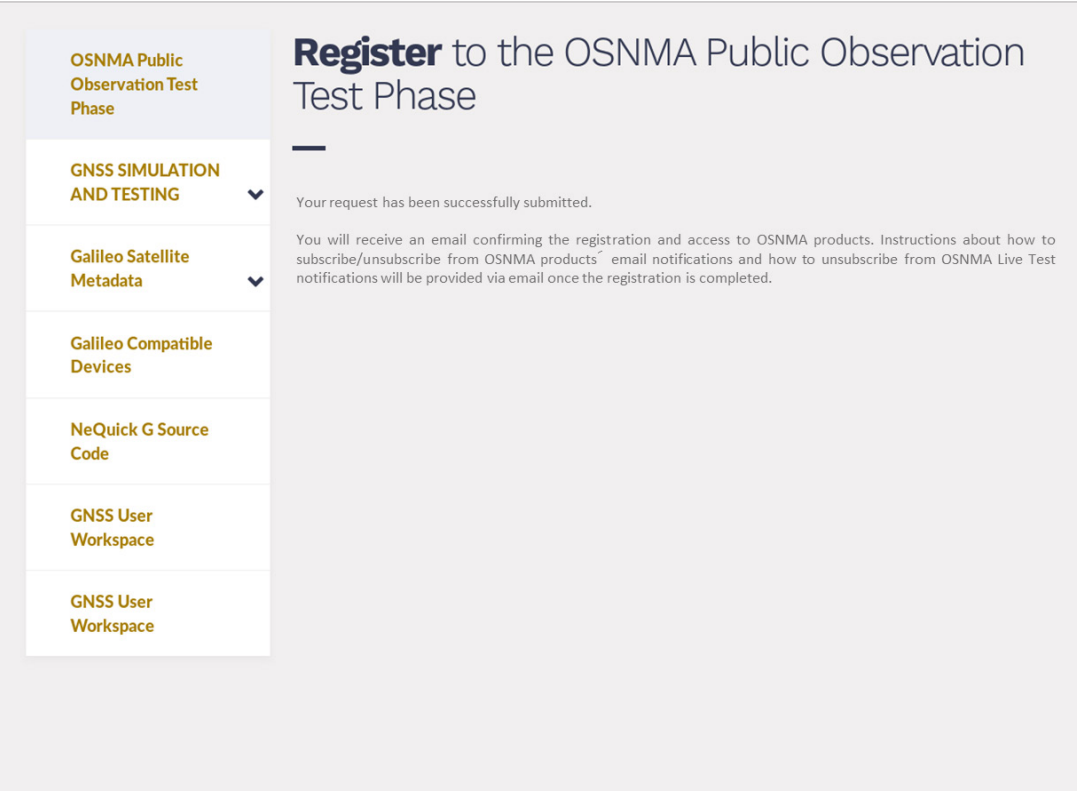


Figure 25. *OSNMA Public Observation Test Phase registration submission*

D.5. Subscription to OSNMA Products email notifications

Upon registration to the OSNMA Public Observation Test Phase, a user may subscribe to receive OSNMA products email notifications.

After a user is logged in, a new menu in “MY ACCOUNT” will be visible where they can click on “Subscriptions” to update its email notification preferences.

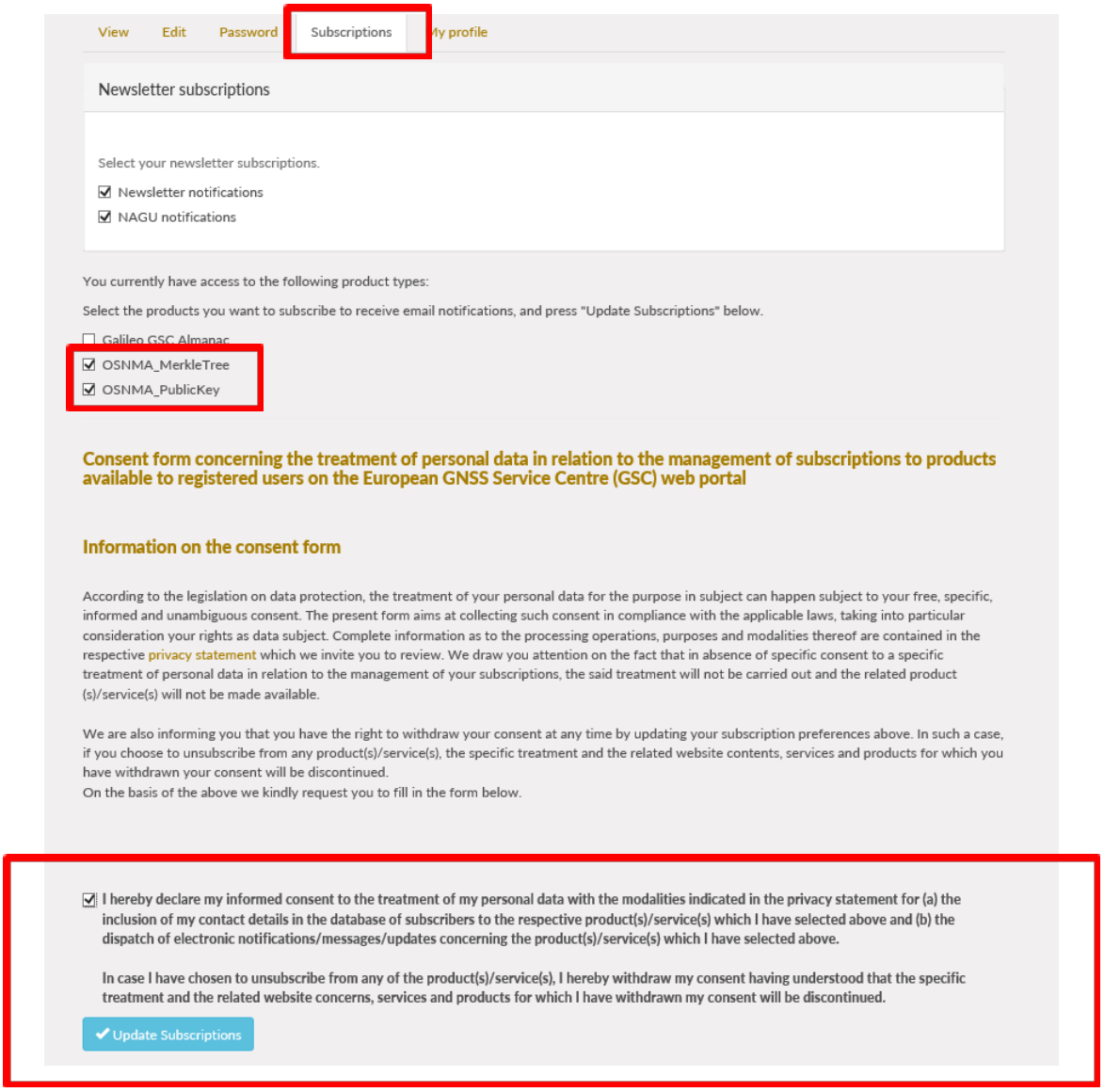


Figure 26. *Enabling email notifications*

After subscription, the user will receive OSNMA products notifications. An email will be received whenever a new Public Key and/or Merkle Tree is published. The subscription to these products is not mandatory to use the OSNMA service.

D.6. Accessing OSNMA Products

After receving confirmation for the registration to the OSNMA Test Phase users will see in the drop-down menu “GSC Products” the OSNMA products.

Note that all products need to be assigned audiences by operators, which may be configured as

- public,
- audience-based (only members of set of approved audiences),
- per user.

Only members of the appropriate audience can access the OSNMA products.

Additionally, product access may be configured as

- awareness: audience users will be made aware of the product type existence but access must be granted explicitly for each user.
- access: all members of the product's audience can access the product.

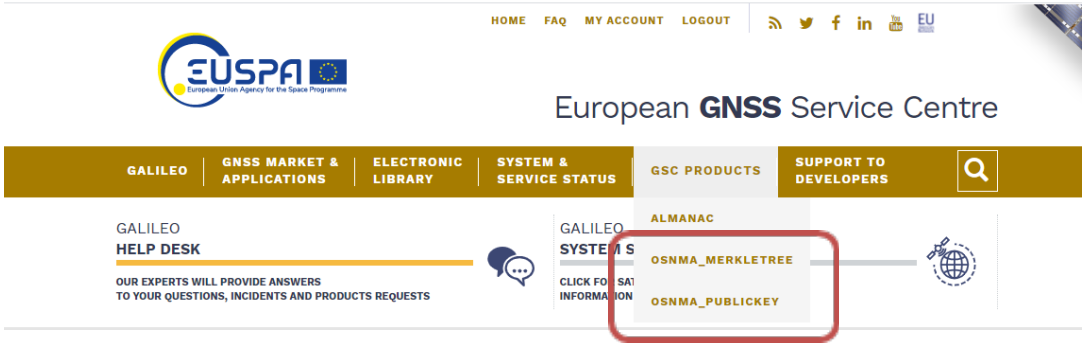


Figure 27. *Product selection menu*

D.7. OSNMA Public Key Products

A user allowed to see OSNMA Public Key products can check the current Public Key in force parameters in "GSC-Products > OSNMA_PublicKey". In addition, the user can download the Public Key in PEM or XML format. For each file, its MD5 checksum is also available for download.

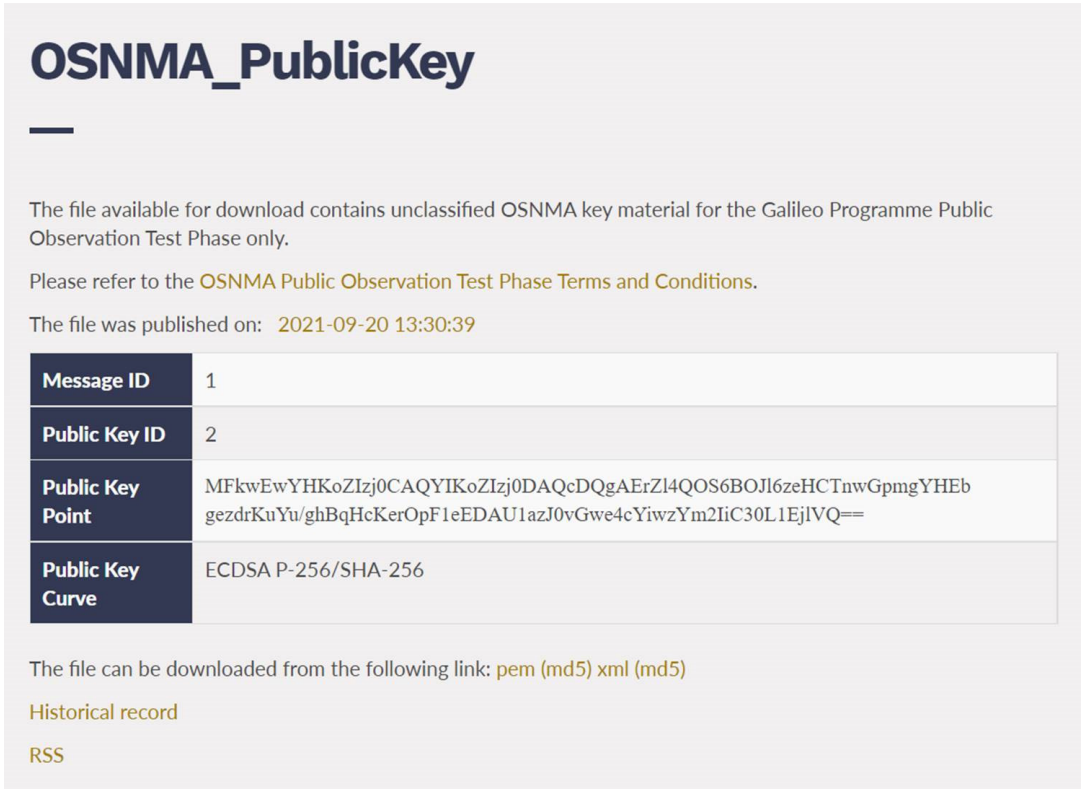


Figure 28. *OSNMA_PublicKey product view*

D.8. Public Key Product Description

The “pem” option allows the user to download a PEM-encoded file. PEM is a text-based format for public key exchange compatible with `openssl ecparam`[12].

In addition, the Public Key can be downloaded in XML format with the “xml” link. The XML has the standard signal structure:

- signalData : contains a header element and a body element.
    - header: contains a standard GAL header.
    - body: contains a single PublicKey element.

A PublicKey element contains:

- i: an integer. Indicates the position of the Public Key in the Tree.
- PKID: an integer. It is the unique ID of the Public Key.
- point: the compressed public point encoded in base16[13] .
- PKType: a string. It indicates the type of the Public Key.

D.9. Accessing Past Renewed or Revoked Public Keys

A logged-in user can review the list of previous Public Keys in the “Historical records” view (see following figure).

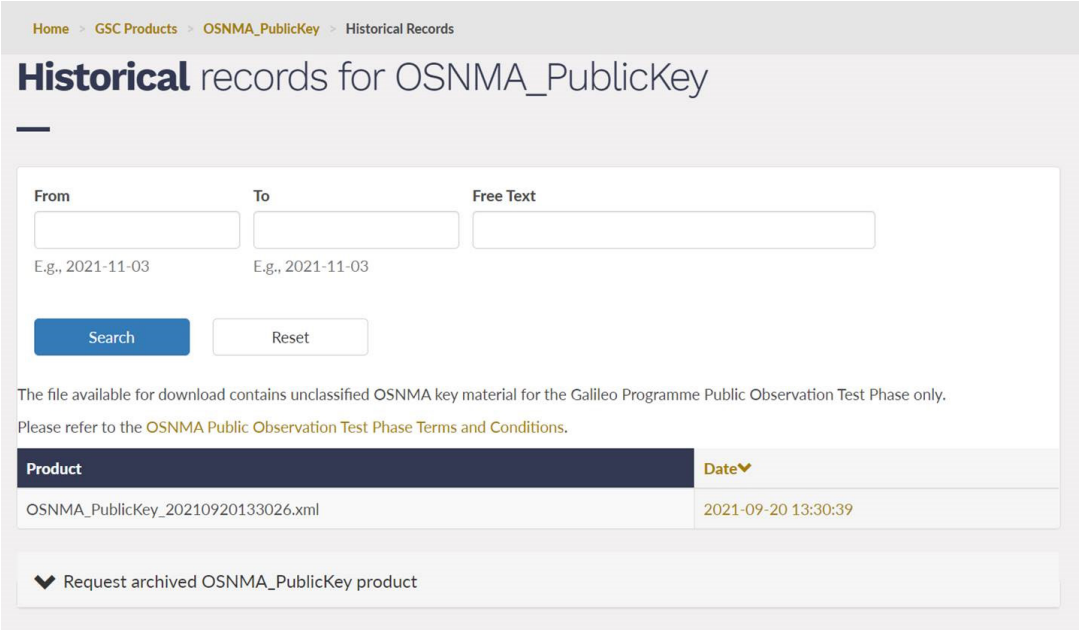
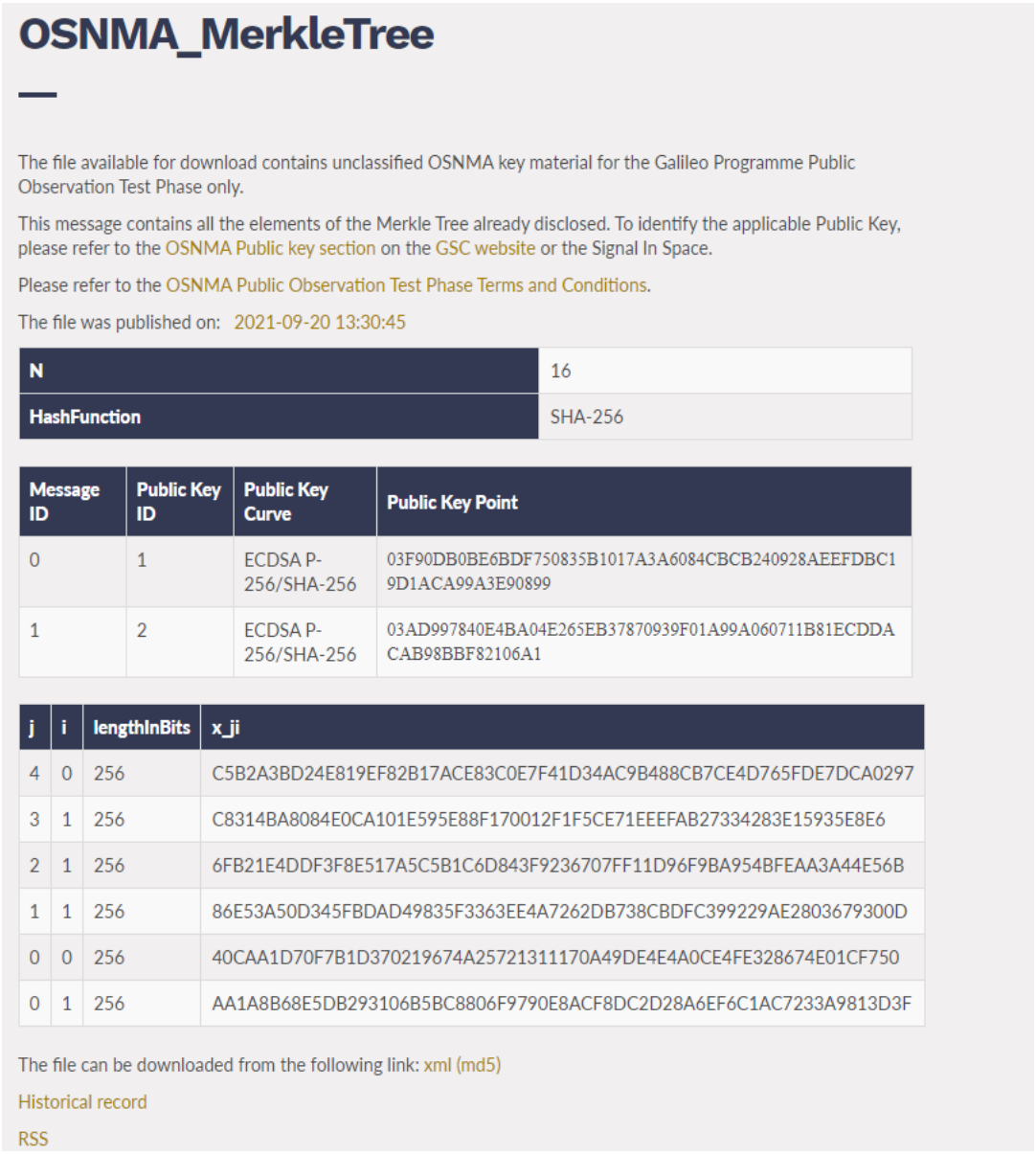


Figure 29. *Accessing historical records for OSNMA_PublicKey products*

12. https://www.openssl.org/docs/man1.0.2/man1/ecparam.html
13. https://tools.ietf.org/html/rfc4648

D.10. OSNMA Merkle Tree Product

A user allowed to see OSNMA MerkleTree products can check the current MerkleTree in force parameters in “GSC-Products > OSNMA_MerkleTree”. In addition, the user can download the Merkle Tree in XML format or the MD5 checksum of the XML file.



OSNMA_MerkleTree

The file available for download contains unclassified OSNMA key material for the Galileo Programme Public Observation Test Phase only.

This message contains all the elements of the Merkle Tree already disclosed. To identify the applicable Public Key, please refer to the OSNMA Public key section on the GSC website or the Signal In Space.

Please refer to the OSNMA Public Observation Test Phase Terms and Conditions.

The file was published on: 2021-09-20 13:30:45

N	16
HashFunction	SHA-256

Message ID	Public Key ID	Public Key Curve	Public Key Point
0	1	ECDSA P-256/SHA-256	03F90DB0BE6BDF750835B1017A3A6084CBCB240928AEEFDBC19D1ACA99A3E90899
1	2	ECDSA P-256/SHA-256	03AD997840E4BA04E265EB37870939F01A99A060711B81ECDDACAB98BBF82106A1

j	i	lengthInBits	x_ji
4	0	256	C5B2A3BD24E819EF82B17ACE83C0E7F41D34AC9B488CB7CE4D765FDE7DCA0297
3	1	256	C8314BA8084E0CA101E595E88F170012F1F5CE71EEEFAB27334283E15935E8E6
2	1	256	6FB21E4DDF3F8E517A5C5B1C6D843F9236707FF11D96F9BA954BFEAA3A44E56B
1	1	256	86E53A50D345FBDAD49835F3363EE4A7262DB738CBDFC399229AE2803679300D
0	0	256	40CAA1D70F7B1D370219674A25721311170A49DE4E4A0CE4FE328674E01CF750
0	1	256	AA1A8B68E5DB293106B5BC8806F9790E8ACF8DC2D28A6EF6C1AC7233A9813D3F

The file can be downloaded from the following link: xml (md5)

Historical record

RSS

Figure 30. *OSNMA_MerkleTree product view*

D.11. Merkle Tree Product Description

The Merkle Tree XML has the standard signal structure:

- signalData:contains a header element and a body element.
    - header: contains a standard GAL header.
    - body: contains a single MerkleTree element.

A MerkleTree element contains:

- N: an integer. It is the number of Public Keys in the base of the Merkle Tree.

- HashFunction: a string. It allows the user to know which hash function was used to compute the Merkle Tree nodes.
- PublicKey elements (please refer to section D.65. The number of keys depends on the number of elements already disclosed from the Merkle Tree).
- The necessary TreeNodes. A TreeNode contains:
    - j: an integer. It is the height of the node in the Merkle Tree according to OSNMA Spec.
    - i: an integer. It is the position of the node in the Merkle Tree level according to OSNMA Spec.
    - lengthInBits: the length in bits of the hash in the x_ji element.
    - x_ji: a string with the base16 encoded hash of the Merkle Tree node.

D.12. Accessing Past Merkle Trees

A logged-in user can review the list of previos Public Keys in the “Historical record” view (see sample in the following figure).

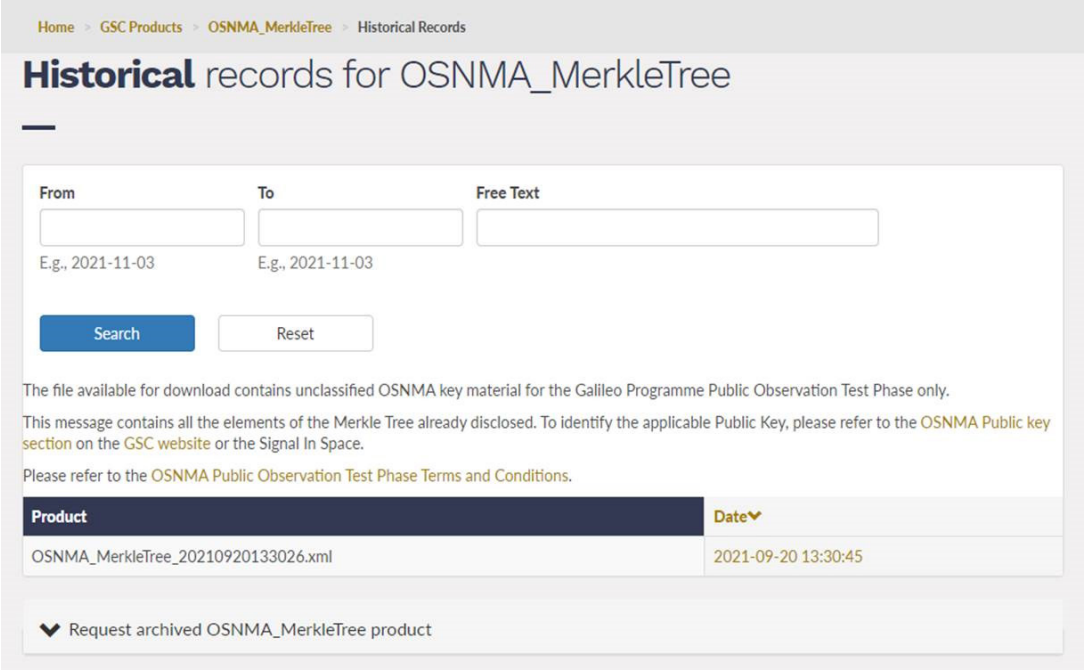


Figure 31. *Accessing historical records for OSNMA_MerkleTree products*

D.13. OSNMA Products Structure

The following file provide the xsd files used to generate the xmls downloaded by the user. Those files can help the users to code their own tools to read the provided xmls.

14. European Commission, Galileo Navigation Message Authentication Specification for Signal-In-Space Test – v1.1, ARES Ref. grow. ddg3.j.1(2018)1670062

Annex E – Traceability Matrix between this OSNMA User ICD for Test Phase and OSNMA Specifications v1.1[14]

This document supersedes the Galileo OSNMA specification v1.1 for what matters the definition and development of OSNMA receivers and processing. This annex is meant to support users who used the OSNMA specification v1.1 for development of prototypes to make a full traceability between the elements of the OSNMA specification v1.1 and those presented in this ICD.

This annex is meant to be used only during the Test Phase and should be removed before this ICD is released for public use.

Specs v1.1	OSNMA ICD	Description
2	2	Updated to reflect relevant aspects to users and to comply with [AD.1]
3	3	"HKROOT Section" renamed as "HKROOT Message"
3.1	3.1	"NMA Status" renamed as "NMAS"
3.1.1	3.1.1	NMA Status definition and semantic updated. Meaning of "Don't use" flab has been further clarified
3.1.2	3.1.2	No change
3.1.3	3.1.3	No change
-	3.2	New section created for the digital signature message (DSM)
3.2	3.2.1	Clarification about DSM message and DSM ID inserted
3.2.1	3.2.1.1	Description simplified and table 5 removed
3.2.2	3.2.1.2	Table 6 removed
3.3	3.2.3	DSM-KROOT Message description improved. New parameters for KROOT, Digital Signature (DS) and Padding (now labelled as PDK) lengths introduced. Expression for the DSM-KROOT message total length introduced. MACK Offset removed. Consequently, the reserved bits in the DSM-KROOT are 4.
3.3.1	3.2.3.1	Number of Blocks has been differentiated for the DSM-KROOT (NBDK) and DSM-PKR (NBDP) and specific tables (with applicable values) are provided in sections 3.2.3.1 and 3.2.2.1, respectively.
3.3.2	3.2.3.2	Contents have been reduced. Details on the Public key provision are provided in Chapter 5. The cryptographic operations to be performed by the receiver are described in Chapter 6.
3.3.3	3.2.3.3	No Change
3.3.4	N/A	NMACK is fixed to one, the NMACK field is set to Reserved1.
3.3.5	3.2.3.4	SHA3-224 removed from the possible HASH functions (HF=1 set to Reserved)

Specs v1.1	OSNMA ICD	Description
-	4.2	Tags&Info section introduced, consisting of a sequence of Tag and Tag-Info fields. Definition of “number of tags per MACK block”, nM introduced.
4.1.3	4.2.2	“MAC” relabelled as “Tag”. Tag definition provided at the beginning of Chapter 4.
4.1.4	4.2.1	“MAC-Info” relabelled as “Tag-Info”.
4.1.4.1	4.2.1.1	“PRN” field relabelled as “PRND”. All PRND field values in the range 37-254 (corresponding to GPS, Glonass, BDS and SBAS) have been marked as reserved. Computation of PRN for SAR RLM data has been removed as the corresponding ADKD=7 is not defined in the User ICD. Definition of “PRNA” introduced as the parameter identifying the satellite transmitting the authentication information.
4.1.4.2	4.2.1.2	Description of ADKD has been simplified. Galileo ADKDs 2,3,5,6,7,11 as well as some ADKDs marked as for future implementation have been set as reserved. For each ADKD the applicable PRND descriptions are provided. The exact format of the authenticated data and their concatenation is shown in Annex B. Link between navigation data and related tag updated, in particular affecting sentences in page 19 for ADKD#4 (“GST-UTC conversion parameters (WT6), TOW (WT6) and GST-GPS (WT10) authenticated as per the last WT6 and WT10 provided by the transmitting satellite in the E1-B I/NAV”) and 22 for ADKD#0 (“The WT5 authenticated corresponds to the last one transmitted in the I/NAV E1-B before the MAC (TBC)”).
4.1.4.3	N/A	Issue of Data is set to Reserved2.
4.1.5	4.3	No change
5	6	The elements are moved to Chapter 6. In a new section 6.1 cryptographic functions and operators that are common to the entire chapter are provided. SHA-224 and SHA-384 removed from the table of supported ECDSA algorithms. Further elements are covered in [AD.2].
5.1	6.3	Minor updates. Description of padding field computation moved to section 3.2.3.13. Further elements are covered in [AD.2]
5.2, 5.3	6.2	Notation slightly updated. Notion that the system might use in future SHA3-256 for the tree generation is introduced. Computation of padding moved to section 3.2.2.7. Further elements are covered in [AD.2]
5.4	6.4	Notation updated. Index of the key in the chain described in section 5.5.2. Further elements are covered in [AD.2]
-	6.5	Short section detailing the verification of the MAC Lookup Table is introduced. Further elements are covered in [AD.2]
5.5	6.7	Notation updated. Caveat on the verification of tags in the case PRN_D is set to the value “255” (e.g. ADKD=4) is introduced. Further elements are covered in [AD.2]. Applicable Key Index introduced in section 5.6.2
5.6	6.6	Notation updated
6	-	A specific document has been generated providing guidelines for the implementation of OSNMA receivers ([AD.2]). However, many elements of specs v1.1 chapter 6 are covered in Chapter 5, as described below

Specs v1.1	OSNMA ICD	Description
3.3.6	3.2.3.5	No change
3.3.7	3.2.3.6	New parameter introduced for the Key length, l_K
3.3.8	3.2.3.7	"MAC size" parameter is relabelled as "Tag size". Such change is consistently propagated all along the document. Tag Size values 1-4, corresponding to Tag lengths 10-18, have been set as reserved
3.3.9	3.2.3.8	Minor updates
3.3.10	-	Removed
3.3.11	-	MACK Offset Removed
3.3.12, 3.3.13	3.2.3.9	WN and TOWN relabelled as WNK and $TOWH_K$. Description moved to new section 5.5.1. Start epoch aligned with [AD.1].
3.3.14	3.2.3.10	No change
3.3.15	3.2.3.11	Notion of floating KROOT moved to Chapter 5
3.3.16	3.2.3.12	Relevant DS length for the supported ECDSA functions provided in Table 15 within section 6.1
3.3.17	3.2.3.13	Padding P1 relabelled as PDK. Description extended to improve clarity
3.4	3.2.2	DSM-PKR description improved. Details on the public key provision given in Chapter 5. Acronyms for most of the DSM-PKR fields introduced. New parameters for NPK and Padding (now labelled as PDP) lengths introduced. Expression for the DSM-PKR message total length introduced
3.4.1	3.2.2.1	Specific contents for Number of DSM-PKR Blocks (NBDP) introduced
3.4.2	3.2.2.2	No change
3.4.3	3.2.2.3	Minor updates
3.4.4	3.2.2.4	"Emergency Service Message" relabelled to "OSNMA Alert Message (OAM)"
3.4.5	3.2.2.5	No change
3.4.6	3.2.2.6	Description improved. Parameters for length of the NPK field in case of OSNMA Alert Message relabelled as l_(PK_OAM) and definition updated
3.4.7	3.2.2.7	Padding P2 relabelled as PDK. Description extended to improve clarity
4	4	Overall no substantial change in the protocol. However, description and representation of MACK section (now labelled as "MACK Message") heavily changed to improve clarity and consistency. New MACK Header and Tags&Info (sequence of Tag and Tag-Info fields) sections introduced with mostly updated fields names and definitions. NMACK is fixed to one, though the notion of NMACK block is removed and NMACK message is used instead.
-	4.1	MACK Header section introduced, including Tag0 and MACSEQ. IODtag field is replaced by Reserved2. It is replaced by a fixed link between the navigation data to be authenticated and the tag, as explained in section 5.6.1.
4.1.1	4.1.1	MAC0 relabelled as Tag0
4.1.2	4.1.2	No change

Specs v1.1	OSNMA ICD	Description
6.1	2, 5.2	The elements discussed in 6.1 of the specs v1.1 are introduced in sections 2 and 5.1.
6.2	5.3	Section 5.3 presents elements on the DSM block sequencing and transmission. Other elements are provided in [AD.2]
6.3	5.5	Some elements about floating KROOTs are discussed in section 5.5. Other elements are provided in [AD.2]
6.4	5.5.3	TESLA chain renewal and revocation are discussed in section 5.5.3 and in [AD.2]. Clarified that KROOT date is not synchronized with time of chain transition during chain renewal process. User can detect transition by monitoring NMA status and CPKS flags.
6.5	5.4.1	Public Key renewal and revocation are discussed in section 5.4.1 and in [AD.2]. Some new elements are introduced, e.g. the duration for certain steps, provisionally marked as TBC.
6.6	3.2.2.4	"Emergency Service Message" relabelled to "OSNMA Alert Message (OAM)"
6.7	[AD.2]	Alarm conditions are reformulated and described in [AD.2]
6.8	[AD.2]	Chain crypto period and lengths are described in [AD.2]
6.9	-	MACK Offset removed
6.10	5.6.1, [AD.2]	• Use of I/NAV CRC is discussed in [AD.2]. • Tag accumulation is discussed in 5.6.1 and in [AD.2]
6.11, 6.12,	[AD.2]	Elements of section 6.11 and 6.12 are discussed in [AD.2]
6.13	5.3	DSM block sequencing and transmission are described in section 5.3
7	5.5.2, 5.6.2, [AD.2]	• NS fixed to 1 • MAC Block Offset set to 1 and removed as a parameter from the User ICD. The notion of the one MACK block offset introduced between the tags and the associated keys introduced within the new section in 5.6.2
Annex B	Annex B, [AD.2]	Bitmasks are defined in Annex B. Test vectors are introduced in [AD.2]
Annex C	Annex C	MAC Look-up table and description updated. Any sequence from Specs v1.1 not provided here is to be considered as removed.

Annex F – Authorisation Concerning the OSNMA User ICD for the Test Phase IPRs

By practicing, using or copying the OSNMA User ICD for the Test Phase IPRs or any portion thereof, YOU ACCEPT ALL TERMS AND CONDITIONS OF THIS AUTHORISATION, including in particular the limitations on use, warranty and liability. If you are acting on behalf of a company or other legal entity, you represent and warrant that you have the legal authority to bind that company or legal entity to these terms and conditions. IF YOU DO NOT HAVE SUCH AUTHORITY OR IF YOU AND/OR THAT COMPANY OF LEGAL ENTITY DO NOT WISH TO BE BOUND TO THESE TERMS DO NOT PRACTICE, USE OR COPY THE OSNMA User ICD for the Test Phase IPRs OR ANY PORTION THEREOF.

The European Union (hereinafter "the EU") is the owner of, holds the right over, and/or controls the intellectual and industrial property rights to, the OSNMA User ICD for the Test Phase IPRs listed in section G.12.

In the interest of facilitating and encouraging the adoption of technologies using the EU GNSS, the EU represented by the European Commission hereby issues the Authorisation (as defined in Section 1 below) concerning the OSNMA User ICD for the Test Phase IPRs towards any individual, corporation or other natural or legal person worldwide, subject to the terms, conditions and limitations described herein. The Authorisation is non- exclusive and royalty-free.

The Authorisation is issued in the context where other GNSS providers provide open and free access to the information necessary to build equipment using civil GNSS signals.

F.1. Definitions

The under mentioned terms printed with an initial capital letter shall have herein the following meanings unless the context otherwise requires:

"Authorisation" – shall mean the EU's covenant that it shall not assert, seek to assert and/or enforce any of the rights and claims it has in relation to the OSNMA User ICD for the Test Phase IPRs against the practicing, using or copying thereof, subject to the terms, conditions and limitations described herein.

"Authorised Person" – shall mean the natural or legal person that benefits from the Authorisation under the terms, conditions and limitations described herein.

"Export Controls" – shall mean any international or national export control law or regulation applicable to activities carried out under the OSNMA User ICD for the Test Phase IPRs that regulates, embargoes or sanctions the export of products, information and/or technology in any way.

"Field of Use" – shall mean research and development on, manufacturing, commercialisation, distribution, sale, supply and maintenance of, the Products.

"GNSS" – shall mean Global Navigation Satellite System.

"OS Signal" – shall mean the open signal broadcasted by the infrastructure developed under the European GNSS Programme.

"OSNMA User ICD for the Test Phase" – shall mean the Galileo Open Service Navigation Message Authentication (OSNMA) User Interface Control Document for the Test Phase in

the version as of the date of issuance of this Authorisation and/or, as the case may be, as modified after that date (available at https://www.gsc-europa.eu).

"OSNMA User ICD for the Test Phase Copyright" – shall mean the copyright on and to the OSNMA User ICD for the Test Phase document and/or its content.

"OSNMA User ICD for the Test Phase IPRs" – shall mean the intellectual or industrial property rights listed in section G.12, including Patents and OSNMA User ICD for the Test Phase ICD Copyright. For the purpose of this Authorisation, OSNMA User ICD for the Test Phase IPRs also include any and all intellectual or industrial property rights and other proprietary rights on and to the Technical Data of the OSNMA User ICD for the Test Phase ICD.

"Patents" – shall mean any and all patents and/or patent applications mentioned in section G.12, including the inventions described and claimed therein as well as any divisions, continuations, continuations-in-part, re-examinations and reissues thereof, and any patents issued from said patent applications.

"Products" – shall mean software, electronic devices (e.g., chipsets and receivers) and Value Added Services that are developed – directly or indirectly – by the Authorised Person and that are making use of the OSNMA Signal.

"Technical Data of the OSNMA User ICD for the Test Phase" – shall mean the data related to: Galileo Signal characteristics, the Galileo Spreading Codes characteristics, Galileo Message Structure, Message Data Contents and E1 and E5 Memory Codes, as such terms are used in the OSNMA User ICD for the Test Phase.

"Territory" – shall mean, with respect to each OSNMA User ICD for the Test Phase IPRs individually, and subject to Export Controls, the territories covered by said individual OSNMA User ICD for the Test Phase IPR.

"Value Added Services" – shall mean any service developed based on, or by using, the OSNMA SIS ICD IPRs and delivering different or additional capabilities with respect to the OSNMA Signal.

F.2. Ownership of Rights

Ownership and/or control of the OSNMA User ICD for the Test Phase IPRs shall remain with the EU and therefore, no title of any intellectual property right on the OSNMA User ICD for the Test Phase IPRs under the Authorisation shall be acquired by the Authorised Person, whether by implication, estoppel or otherwise.

The Authorisation shall be withdrawn and shall not apply against any individual, corporation or other natural or legal person that challenges the validity of any of the OSNMA User ICD for the Test Phase IPRs or participates in such a challenge, or encourages or supports any third parties in such a challenge.

F.3. Scope of Authorisation

The scope of the Authorisation is limited to the Territory and Field of Use.

The Authorisation is non-transferable and non-licensable. The Authorised Person shall not assign, transfer or license any of the rights granted under the Authorisation.

The Authorised Person shall practice, use and/or copy the OSNMA User ICD for the Test Phase IPRs in the Field of Use under the Authorisation in a manner so as not to harm the security interests of the EU or its Member States as set forth of the Regulation (EU) No 2021/696 of the European Parliament and of the Council of 28th April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and

Decision No 541/2014/EU..

The commercial exploitation of the Products in the Field of Use under the Authorisation shall be under the sole responsibility of the Authorised Person.

The Authorised Person shall not state or imply in any promotional material or elsewhere that the Products were developed by, are used by or for or have been approved or endorsed by the EU or by the owner of any of the Patents.

Pursuant to the Authorisation, the EU's covenant not to assert covers the following activities of the Authorised Person:

a. the use of the Technical Data of the OSNMA User ICD for the Test Phase, including their integration and incorporation into any Products, by the Authorised Person or by third parties contractors used by the Authorised Person for manufacturing said Products;

b. the storage of the Technical Data of the OSNMA User ICD for the Test Phase, provided the source is acknowledged;

c. the reproduction of the OSNMA User ICD for the Test Phase, in whole or in part, its distribution and its publication for non-commercial not-for-profit purposes and scale without amending the document or adding any element;

d. providing links to the EU website where the document is published, provided the source is acknowledged, in accordance with the copyright notice in the OSNMA User ICD for the Test Phase.

This list is exhaustive. No other activity shall benefit from the Authorisation. The practice of any of the OSNMA User ICD for the Test Phase IPRs outside of the scope of the Authorisation shall be deemed in breach of the intellectual property rights of the EU.

Subject to the foregoing, the Authorised Person shall have the discretion to select distributors and otherwise determine the commercial strategy, including all channels of distribution, regarding the distribution and sale of the Products in the Territory.

The Authorised Person shall be solely responsible for (but failure to strictly abide bya) and

b) below shall not be in contradiction with the Authorisation):

a. exercising its activities hereunder strictly in compliance with all laws and regulations of each of the countries in which such activity takes place;

b. compliance with all Export Controls.

F.4. Additional Intellectual Property Rights and Maintenance of Patent Rights

The EU reserves the right, in the course of the Authorisation term, to acquire ownership or control of additional intellectual or industrial property rights related to the OSNMA Signal. In that case, the EU may update section G.12 accordingly. The EU however takes no obligation to communicate the acquisition of or licence to additional intellectual or industrial property rights related to the OSNMA Signal.

The Authorisation shall automatically cover any such additional intellectual or industrial property rights included in the updated section G.12, without the need to amend the Authorisation.

The EU shall have no obligation, duty or commitment whatsoever to:

a. maintain the OSNMA User ICD for the Test Phase IPRs in force, whether in full or partly, nor shall it be obliged to communicate any decision thereto to the Authorised Person;

b. furnish any assistance, technical information or know-how to the Authorised Person.

F.5. Duration and Termination

With respect to each of the OSNMA User ICD for the Test Phase IPRs, the Authorisation shall be valid for the whole duration of said OSNMA User ICD for the Test Phase IPRs insofar as the terms, conditions and limitations of the Authorisation are respected.

The Authorisation shall terminate automatically upon any act of the Authorised Person that violates any of the terms, conditions or limitation of the Authorisation, unless the European Union agrees to the remedial measures proposed by the Authorised Person and the latter are implemented in reasonable time set by the Union.

In the event of a termination of the Authorisation for whatever reason, the Authorised Person shall:

a. immediately discontinue the development or use of the Products or any other activity covered under the scope of the Authorisation as defined in Section 4 above; and

b. except in cases of termination for violation of this Authorisation by the Authorised Person, as a temporary exception to point a. above, have the right, during 6 (six) months after the termination of the Authorisation, to sell all remaining Products in stock or in process of being manufactured at that date, or within that term of 6 (six) months, have terminated, finished and/or fulfilled all agreements which have been entered into prior to the termination.

The Authorisation and its validity shall not be influenced by the fact that one or more of the OSNMA User ICD for the Test Phase IPRs whose practice, use or copy is authorised hereunder should finally be declared not granted or invalid.

F.6. Warranties and Liability

The Authorisation is issued under the OSNMA User ICD for the Test Phase IPRs as they are. The EU makes no representation and no express or implied warranty, and assumes no liabilities as to any matter whatsoever concerning the OSNMA User ICD for the Test Phase IPRs, including as to:

a. the condition, the patentability and/or validity and enforceability of the OSNMA User ICD for the Test Phase IPRs;

b. the freedom to practice, use or copy the OSNMA User ICD for the Test PhaseIPRs, to perform the activities that benefit from the Authorisation, or to develop, commercialise or exploit the Products;

c. any third party's prior rights to use the OSNMA User ICD for the Test Phase IPRs and/or to enjoin the activities that benefit from the Authorisation;

d. the dependency of the OSNMA User ICD for the Test Phase IPRs on third parties' intellectual or industrial property rights;

e. the merchantability or fitness for a particular purpose of the OSNMA User ICD for the Test Phase IPRs and/ or the Products.

To the full extent allowed by law, all warranties, whether expressed or implied, for any use of OSNMA User ICD for the Test Phase IPRs or related to the Products, including on product liability, are excluded, and the EU shall not be held liable for any claim or damage related thereto, being asserted by the Authorised Person or any third party with respect to the activities of the Authorised Person under the Authorisation.

F.7. Infringements by Third Parties

The EU shall have the discretionary right and faculty to decide whether or not to bring an

action for any infringements of the OSNMA User ICD for the Test Phase IPRs in the case where a third party does not benefit from the Authorisation, even where the EU has been duly informed about such alleged infringement by the Authorised Person. The EU shall have no obligation whatsoever to bring such an action nor to notify any decision thereto to the Authorised Person.

F.8. Action for Infringement Brought by Third Parties

The Authorised Person shall defend itself and at its own expenses, and bear all the consequences, including the payment of damages and attorney fees, against any claim, suit or proceeding made or brought against the Authorised Person and arising from its activities under the Authorisation, including any claim, suit or proceeding for infringement of third parties' rights as a result of the Authorised Person's practice, use or copy of the OSNMA User ICD for the Test Phase IPRs or commercialisation of Products. The Authorised Person shall notify the EU without undue delay about any such claim, suit or proceeding. The EU may, at its sole discretion, agree to provide the Authorised Person with any assistance which the EU considers to be appropriate, but the EU shall not in any way be obliged to do so. If the EU decides to defend either the Authorised Person or the OSNMA User ICD for the Test Phase IPRs, the Authorised Person shall collaborate with the EU and provide the EU with all the assistance necessary to such defence.

F.9. Permits

The necessary steps for obtaining all permits and licences required for the activities under the Authorisation, under the laws and regulations in force at the place where said activities of the Authorised Person are provided or to be provided, shall be the exclusive responsibility of the Authorised Person.

F.10. Applicable Law and Dispute Resolution

The Authorisation shall be governed by European Union law, complemented where necessary by the law of Belgium.

Except for the right of the EU and/or the Authorised Person to apply to a court of competent jurisdiction for a temporary restraining order or a preliminary injunction to prevent irreparable harm, any dispute, controversy or claim arising under, out of or relating to the Authorisation and any subsequent amendments thereof, including, without limitation, its validity, binding effect, interpretation, performance, breach or termination shall be submitted to mediation in accordance with the WIPO Mediation Rules. The place of mediation shall be Brussels. The language to be used in the mediation shall be English.

If, and to the extent that, any such dispute, controversy or claim has not been settled pursuant to the mediation within sixty (60) days of the commencement of the mediation, it shall, upon filing of a Request for Arbitration by either the EU or the Authorised Person, be referred to and finally determined by arbitration in accordance with the WIPO Expedited Arbitration Rules. Alternatively, if, before the expiration of said period of sixty (60) days, either the EU or the Authorised Person fails to participate or to continue to participate in the mediation, the dispute, controversy or claim shall, upon the filing of a Request for Arbitration by the participating EU or Authorised Person, be referred to and finally determined by arbitration in accordance with the WIPO Expedited Arbitration Rules. The arbitral tribunal shall consist of three arbitrators. The place of arbitration shall be Brussels. The language used in the arbitration proceedings shall be English.

In any action to enforce the Authorisation, the prevailing entity shall be entitled to recover its reasonable attorney's fees, court costs and related expenses from the other entity.

F.11. Miscellaneous

The provisions of the Authorisation are severable in the sense that the invalidity or unenforceability of any provision of the Authorisation that is not fundamental to its performance shall not affect the validity and/or enforceability of the remaining provisions hereof. Such invalidity or unenforceability of such non-fundamental provision shall not relieve the Authorised Person of its obligations under the remaining provisions of the Authorisation.

This Authorisation fully and exclusively states the scope of the authorisation concerning the OSNMA User ICD for the Test Phase IPRs that the EU wishes to issue.

The EU reserves the exclusive right to amend the Authorisation upon due public notice.

The fact that the Authorisation is self-executing and that the EU requires no signature of the Authorisation shall not be considered a waiver and shall have no effect on the binding character of the terms, conditions and limitations of the Authorisation upon the practice, use or copy of the OSNMA User ICD for the Test Phase IPRs by the Authorised Person.

F.12. List of IPRs

The IPRs listed in the following table are an integral part of the Authorisation.

	IPR	Name of IPR	Application Number	Date of filing	Applicant	Owner	Designated Countries
1	Patent	Multi-band antenna for satellite positioning system	PCT/ EP2006/ 064067	10/07/2006	EUSPA	EU	Australia Canada Norway USA S.Korea China India Japan Russia
2	Patent	Method for providing assistance data to a mobile station of a satellite positioning system	PCT/ EP2006/ 068177	07/11/2006	EUSPA	EU	Australia Canada Europe designated countries: (AT, BE, CH, CZ, DEDK, ES, FI, FR, GB, GR, HU, IE, IT, LU, NL, PL, PT, RO, SE, TR) USA S.Korea China India Japan Russia

	IPR	Name of IPR	Application Number	Date of filing	Applicant	Owner	Designated Countries
3	Patent	Method and generator for generating a spread-spectrum signal (initially referred to as Use of antiphase CBOC (6.1) modulation to improve ranging accuracy in satellite navigation signals)	11738006	20/04/2007	EUSPA	EU	USA
4	Patent	Method and generator for generating a spread-spectrum signal	12559874	15/09/2009	EUSPA	EU	USA
5	Patent	Chaotic spreading codes and their generation	PCT/ EP2007/ 063080	30/11/2007	EUSPA	EU	Australia Brazil Canada China Europe designated countries: (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR) India Japan S.Korea Russia USA
6	Copy right	OS SIS ICD	N/A	N/A	N/A	EU	Worldwide

	IPR	Name of IPR	Application Number	Date of filing	Applicant	Owner	Designated Countries
7	Patent	Spreading codes for a satellite navigation system (concerning memory codes)	PCT/ EP2004/ 014488	17/12/2004	ESA	EU	Canada Europe designated countries: (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR) USA Brazil China Japan
8	Patent	Spreading codes for a satellite navigation system (concerning secondary Codes)	PCT/ EP2005/ 007235	01/07/2005	ESA	EU	Canada Europe designated countries: (BE, CH, CZ, DE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, TR) USA Brazil China Japan
9	Patent	Method and device for generating a constant envelope navigation signal with four independent codes	PCT/ FR2003/ 003695	12/12/2003	CENTRE NAT ETD SPATIALES (CNES)	Control by the EU under licence from CNES	Europe designated countries (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LI, LU, MC, NL, PT, RO, SE, SI, SK, TR) USA

	IPR	Name of IPR	Application Number	Date of filing	Applicant	Owner	Designated Countries
10	Patent	Spread spectrum signal	PCT/ EP2006/ 050179	12/01/2006	CNES	Control by the EU under licence from CNES	Canada China Europe designated countries (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LI, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR) Japan Russia USA
11	Patent	GNSS radio signal with an improved navigation message	PCT/ EP2013/ 064477	09/07/2013	CNES	Control by the EU under licence from CNES	China Europe designated countries (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LI, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR) Japan South Korea USA

	IPR	Name of IPR	Application Number	Date of filing	Applicant	Owner	Designated Countries
12	Patent	GNSS radio signal for improved synch-ronisation	PCT/ EP2013/ 064573	10/07/2013	CNES	Control by the EU under licence from CNES	China Europe designated countries (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LI, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR) Japan South Korea USA
13	Patent	Modulation signals for a satellite navigation system	PCT/ GB2004/ 003745	01/09/2004	Secretary of State for Defence of the UK	Control by the EU under licence from the Secretary of State for Defence of the UK	Australia Canada China Europe designated countries (BE, DE, DK, ES, FI, FR, GB, IT, NL, SE) India Japan New Zealand Russia USA

	IPR	Name of IPR	Application Number	Date of filing	Applicant	Owner	Designated Countries
14	Patent	Signals, system, method and apparatus	PCT/ GB2007/ 002293	20/06/07	Secretary of State for Defence of the UK	Control by the EU under licence from the Secretary of State for Defence of the UK	Australia Brazil Canada China Europe designated countries (BE, CZ, DE, DK, ES, FI, FR, GB, HU, IT, NL, PT, SE, SK) Israel India Japan Republic of Korea Malaysia Norway New Zealand Russia Singapore USA
15	Patent Appli- cation	Techniques for Transmitting and Receiving GNSS Navigation Messages	16174636.7	15/06/16	Airbus Defence and Space GmbH	Control by the EU under licence from Airbus Defence and Space GmbH	EU (Pending)
16	Patent Appli- cation	Techniques for Transmitting and Receiving GNSS Navigation Messages	PCT/ EP2017/ 064120	09/06/17	Airbus Defence and Space GmbH	Control by the EU under licence from Airbus Defence and Space GmbH	USA, China, Japan (Pending)

	IPR	Name of IPR	Application Number	Date of filing	Applicant	Owner	Designated Countries
17	Patent Application	Digitally-signed satellite radio-navigation signals	PCT/EP2014/064285	04/07/2014	The European Union, represented by the European Commission	EU	Australia (AU) Brasil (BR) Canada (CA) China (CN) Europe designated countries (FR, IT, ES, DE) Great Britain (GB) India (IN) Japan (JP) South Korea (RU) Russia USA
18	Patent Application	Method and system to optimise the authentication of radio-navigation signals	PCT/EP2015/056120	23/03/2015	The European Union, represented by the European Commission	EU	Australia (AU) Brasil (BR) Canada (CA) China (CN) India (IN) Europe designated countries (FR, IT, ES, DE) Great Britain (GB) Japan (JP) South Korea Russia (RU), USA,

Annex G – Authorisation Concerning use of the Galileo Trade Marks

By using the Galileo Trade Marks in the Field of Use, YOU ACCEPT ALL TERMS AND CONDITIONS OF THIS AUTHORISATION including in particular the limitations on use, warranty and liability. If you are acting on behalf of a company or other legal entity, you represent and warrant that you have the legal authority to bind that company or legal entity to these terms and conditions.

The European Union (hereinafter "the EU") is the owner of the Galileo Trade Marks.

In the interest of facilitating and encouraging the market uptake of satellite navigation, as required by the Space Regulation, the EU represented by the European Commission hereby issues the Authorisation concerning the use of the Galileo Trade Marks in the Field of Use, towards natural or legal persons worldwide, subject to the terms, conditions and limitations described herein. The Authorisation is non- exclusive and royalty-free.

G.1. Definitions

The under mentioned terms printed with an initial capital letter shall have the meanings stated below. Any reference to the plural shall include the singular and any reference to the singular shall include the plural.

"Authorisation" – shall mean the EU's covenant that it shall not assert, seek to assert and / or enforce any of the rights and claims it has in relation to the Galileo Trade Marks against the use thereof, subject to the terms, conditions and limitations described herein.

"Authorised Person" – shall mean the natural or legal person that benefits from the Authorisation under the terms, conditions and limitations described herein.

"EU Stakeholders" – shall mean the European Space Agency (ESA), the European Union Agency for the Space Programme (EUSPA) and other international organisations with activities in GNSS, any of the EU, ESA or EUSPA contractors and subcontractors at any tier working in the Galileo programme, operator(s) of the Galileo satellite navigation system, EU Member States and their institutions and bodies, including national space agencies.

"Field of Use" – shall mean the use of one or more of the Galileo Trade Marks by the Authorised Person in order to signify that the respective Products make use of the GNSS Services provided by the EU and/or the EU Stakeholders. Reference to the Galileo Trade Marks may be made by any means associated with the marketing of the Products, including but not limited to packaging, instructional and promotional materials.

"Galileo Trade Marks" – shall mean any and all trade mark registrations and applications owned by EU and/or the EU Stakeholders, anywhere in the world consisting of or incorporating the word GALILEO, including without limitation the trade mark applications and registrations set out in section H.10.

"GNSS" – shall mean Global Navigation Satellite System.

"Space Regulation" – shall mean Regulation (EU) 2021/696 of the European Parliament and of the Council of 28th April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme. .

"GNSS Services " – shall mean the following activities contemplated by the Space Regulation:

a. open service (OS), which is free of charge to the user and provides positioning and

synchronisation information intended mainly for high-volume satellite navigation applications;

b. a high-accuracy service (HAS), which shall be free of charge for users and shall provide, through additional data disseminated in a supplementary frequency band, high-accuracy positioning and synchronisation information intended mainly for satellite navigation applications for professional or commercial use;;

c. a signal authentication service (SAS), based on the encrypted codes contained in the signals, intended mainly for satellite navigation applications for professional or commercial use;;

d. public regulated service (PRS),which shall be restricted to government-authorised users for sensitive applications which require a high level of service continuity, including in the area of security and defence, using strong, encrypted signals; it shall be free of charge for the Member States, the Council, the Commission, EEAS and, where appropriate, duly authorised Union agencies;

e. an emergency service (ES), which shall be free of charge for users and shall broadcast, through emitting signals, warnings regarding natural disasters or other emergencies in particular areas; where appropriate, it shall be provided in cooperation with Member States national civil protection authorities;

f. a timing service (TS), which shall be free of charge for users and shall provide an accurate and robust reference time, as well as realisation of the coordinated universal time, facilitating the development of timing applications based on Galileo and the use in critical applications.

g. contribution to the search and rescue support service (SAR) of the COSPAS-SARSAT system by detecting distress signals transmitted by beacons and relaying messages to them via a return link.

h. contribution to the integrity-monitoring services standardised at the Union or international level for use by safety-of-life services, on the basis the signals of Galileo open service and in combination with EGNOS and other satellite navigation systems;

i. contribution to the space weather information via the GNSS Service Centre and early warning services via the Galileo ground-based infrastructure, intended mainly to reduce the potential risks to users of the services provided by Galileo and other GNSSs related to space.

"Products" shall mean software, electronic devices (e.g., chipsets and receivers) and Value Added Services that are developed and marketed – directly or indirectly – by the Authorised Person.

"Value Added Services" shall mean any service delivering different or additional capabilities with respect to signals broadcasted by the infrastructure developed under the European GNSS Programmes.

G.2. Ownership of Rights

Ownership of the Galileo Trade Marks shall remain with the EU and therefore, no title of any intellectual property right on the Galileo Trade Marks under the Authorisation shall be acquired by the Authorised Person.

The Authorisation shall be withdrawn and shall not apply to any natural or legal person that challenges the validity or enforceability of any of the Galileo Trade Marks or participates in such a challenge, or encourages or supports any third parties in such a challenge.

G.3. Scope of the Authorisation

The scope of the Authorisation is limited to the Field of Use.

The Authorisation is non-transferable and non-licensable. The Authorised Person shall not assign, transfer or license any of the rights granted under the Authorisation.

The Authorised Person shall use the Galileo Trade Marks in the Field of Use under the Authorisation in a manner so as not to harm the security interests of the EU or its Member States as set forth in the Space Regulation .

The commercial exploitation of the Products in the Field of Use under the Authorisation shall be under the sole responsibility of the Authorised Person.

The Authorised Person shall not state or imply in any promotional material or elsewhere that the Products were developed by, are used by or for or have been approved or endorsed by the EU or the EU Stakeholders.

Pursuant to the Authorisation, the EU's covenant not to assert covers the use of the Galileo Trade Marks in the context of the development and marketing of any Products, including its use on the Products themselves and on their packaging, instructional and promotional materials, by the Authorised Person or by third party contractors used by the Authorised Person for manufacturing said Products, only in the Field of Use;

In addition to the limitations described above, the Authorised Person shall not:

a. Use the Galileo Trade Marks or any confusingly similar sign as, or as part of, the stand-alone brand name or sub-brand name of any of its Products, or as the stand-alone registered or trading name of any corporate entity or business. For the avoidance of doubt, this does not prevent the Authorised Person from affixing one or more Galileo Trade Marks to the packaging of their Products;

b. Apply for or obtain registration of any trade mark which consists of, comprises, or is confusingly similar to the Galileo Trade Marks;

c. Claim any interest or rights to the Galileo Trade Marks, other than the rights explicitly granted by the EU under the Authorisation;

By way of example, acceptable use of the Galileo Trade Marks under the Authorisation and in the Field of Use would include "the new [Product brand name] satnav powered by Galileo" or "the [Product brand name] Galileo receiver". "A Galileo receiver" or "Galileo receivers" shall also be considered acceptable as referential uses. Unacceptable uses would include "a new satna v by Galileo" and “the Galileo receiver”.

The Authorised Person shall be solely responsible for exercising its activities hereunder strictly in compliance with all laws and regulations of each of the countries in which such activity takes place.

G.4. Additional Intellectual Property Rights and Maintenance of Rights

The EU reserves the right, in the course of the Authorisation term, to acquire ownership or control of additional trade marks related with the sign Galileo. In that case, the EU may update section H.10 accordingly. The EU however takes no obligation to communicate the acquisition of additional trade mark rights to the Authorised Person.

The Authorisation shall automatically cover any such additional trade mark rights included in the updated section H.10, without the need to amend the Authorisation. The EU shall have no obligation, duty or commitment whatsoever to:

a. maintain the Galileo Trade Marks in force nor shall it be obliged to communicate any decision thereto to the Authorised Person;

b. provide any assistance, technical information or know-how to the Authorised Person.

G.5. Duration and Termination

The Authorisation shall be valid as long as the Galileo Trade Marks remain valid and in force, insofar as the terms, conditions and limitations of the Authorisation are respected.

The Authorisation shall terminate automatically upon any act of the Authorised Person that violates any of the terms, conditions or limitation of the Authorisation.

The Authorisation and its validity shall not be influenced by the fact that one or more of the Galileo Trade Marks whose use is authorised hereunder should finally be declared not granted or invalid.

G.6. Warranties and Liability

The Authorisation is issued under the Galileo Trade Marks as they are. The EU makes no representation and no express or implied warranty, and assumes no liabilities as to any matter whatsoever concerning the Galileo Trade Marks, including as to the validity and enforceability of the Galileo Trade Marks;

To the full extent allowed by law, all warranties, whether expressed or implied, for any use of the Galileo Trade Marks are excluded. The EU shall not be held liable for any claim or damage related thereto, being asserted by the Authorised Person or any third party with respect to the activities of the Authorised Person under the Authorisation.

G.7. Action for Infringement Brought by Third Parties

The Authorised Person shall defend itself and at its own expenses, and bear all the consequences, including the payment of damages and attorney fees, against any claim, suit or proceeding made or brought against the Authorised Person and arising from its activities under the Authorisation, including any claim, suit or proceeding for infringement of third parties' rights as a result of the Authorised Person's use of the Galileo Trade Marks or marketing of the Products. The Authorised Person shall notify the EU without undue delay about any such claim, suit or proceeding. The EU may, at its sole discretion, agree to provide the Authorised Person with any assistance which the EU considers to be appropriate, but the EU shall not in any way be obliged to do so. If the EU decides to defend either the Authorised Person or the Galileo Trade Marks, the Authorised Person shall collaborate with the EU and provide the EU with all the assistance necessary to such defence.

G.8. Applicable Law and Dispute Resolution

The Authorisation shall be governed by European Union law, complemented where necessary by the law of Belgium.

The courts of Brussels have exclusive jurisdiction over any dispute regarding the interpretation, application or validity of the Contract.

G.9. Miscellaneous

The provisions of the Authorisation are severable in the sense that the invalidity or unenforceability of any provision of the Authorisation that is not fundamental to its performance shall not affect the validity and/or enforceability of the remaining provisions hereof. Such invalidity or unenforceability of such non-fundamental provision shall not relieve the Authorised Person of its obligations under the remaining provisions of the Authorisation.

This Authorisation fully and exclusively states the scope of the authorisation concerning the Galileo Trade Marks.

The EU reserves the exclusive right to amend the Authorisation upon due public notice.

The fact that the Authorisation is self-executing and that the EU requires no signature of the Authorisation shall not be considered a waiver and shall have no effect on the binding character of the terms, conditions and limitations of the Authorisation upon the use of the Galileo Trade Marks by the Authorised Person.

G.10. Galileo Trade Marks

The trade marks listed in the following tables are an integral part of the Authorisation.

APPLICATIONS

Mark	Territory	Application number
GALILEO JOINT UNDERTAKING	EU	3710712
GALILEI	EU	4546561
GALILEO	EU	11517984

Mark	Territory	Registration number
GALILEO	EU	2742237