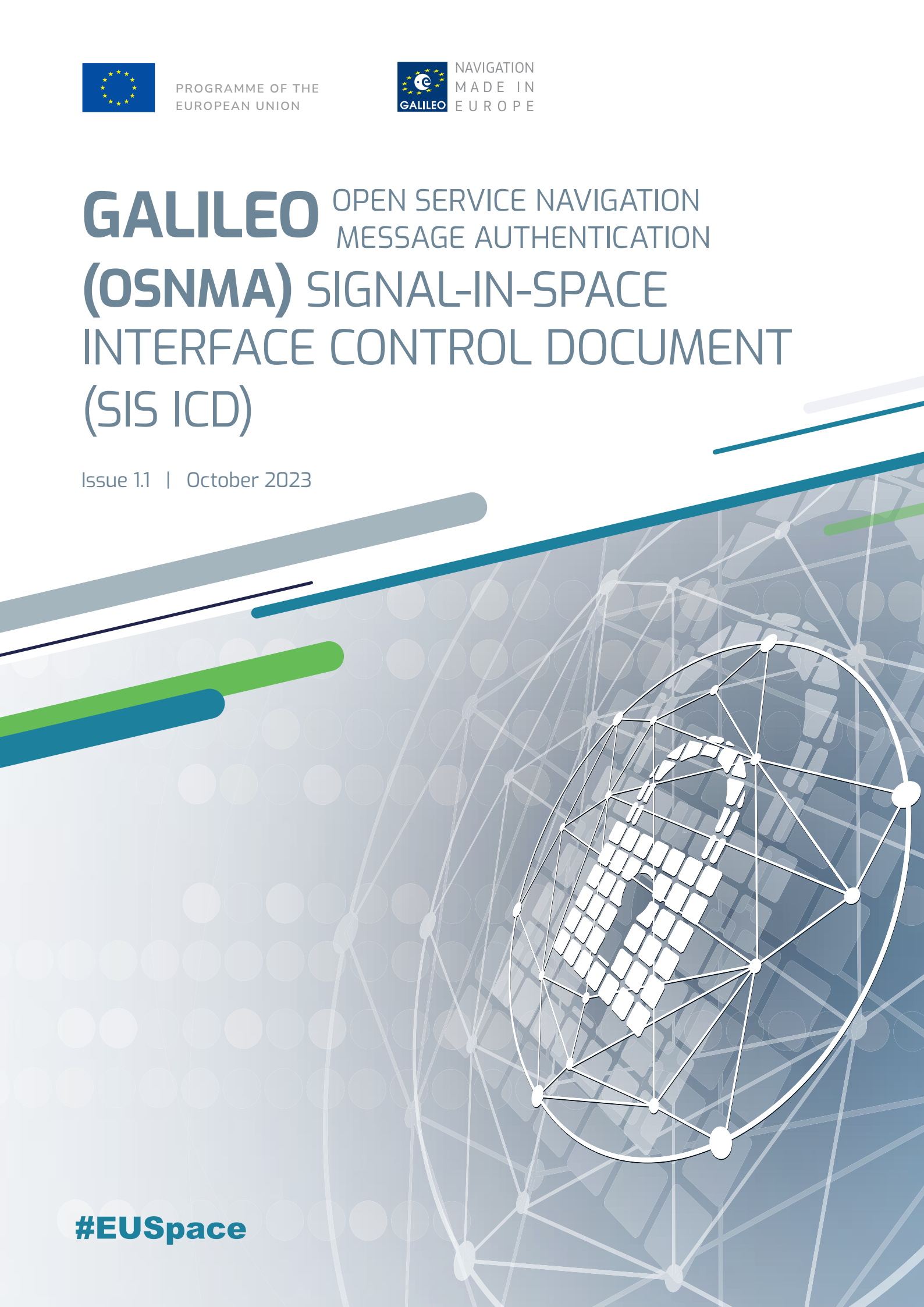
PROGRAMME OF THE EUROPEAN UNION

NAVIGATION MADE IN EUROPE

GALILEO OPEN SERVICE NAVIGATION MESSAGE AUTHENTICATION (OSNMA) SIGNAL-IN-SPACE INTERFACE CONTROL DOCUMENT (SIS ICD)

Issue 1.1 | October 2023



#EUSpace

TERMS OF USE AND DISCLAIMERS

Authorised Use and Scope of Use

The European GNSS (Galileo) Open Service Navigation Message Authentication (OSNMA) Signal-in-Space Interface Control Document Issue 1.1 (hereinafter referred to as OSNMA SIS ICD) and the information contained herein is made available to the public by the European Union (hereinafter referred to as Publishing Authority) 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.

General Disclaimer of Liability

With respect to the OSNMA SIS ICD and any information contained in the OSNMA SIS ICD, 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 SIS ICD or of the information contained herein. Liability is excluded as well for consequences of the use and / or abuse of the OSNMA SIS ICD or the information contained herein.

Intellectual Property Rights

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

Copyrights

The OSNMA SIS ICD is protected by copyright. Any alteration or translation in any language of the OSNMA SIS ICD as a whole or parts of it is prohibited unless the Publishing Authority provides a specific written prior permission. The OSNMA SIS ICD 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 E, are accepted, reproduced and transmitted entirely and unmodified together with the reproduced and/ or transmitted information;
- the copyright notice “© European Union 2023” is not removed from any page.

ISBN: 978-92-9206-067-1

DOI: 10.2878/594840

Industrial Property Rights

The use of the information contained in the OSNMA SIS ICD is authorised under the terms and conditions stated in ANNEX E. The use of the Galileo related trademarks that EU owns is authorised under the terms and conditions stated in ANNEX E.

Miscellaneous

No failure or delay in exercising any right in relation to the OSNMA SIS ICD 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.

Updates

The OSNMA SIS ICD could be subject to modification, update and variations.

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 SIS ICD, it does not assume any obligation to advise on further developments and updates of the OSNMA SIS ICD, nor to take into account any inputs, comments proposed by interested persons or entities, involved in the updating process.

DOCUMENT CHANGE RECORD

Reason for change	Issue	Revision	Date
First issue.	1	0	December 2022
Update of the document: • Correction of typos on the text. • Section 1.2 inclusion of a reference to the Galileo OSNMA IDD ICD and of cross-references in the document. • Section 6.6 inclusion of additional information about the verification of the FLX tags. • Annex C inclusion of new MAC sequences.	1	1	October 2023

Table of contents

List of Figures

List of Tables

1 Introduction

1.1 Document Scope

The present Galileo Open Service Navigation Message Authentication (OSNMA) Signal-in-Space (SIS) Interface Control Document (ICD), together with the Galileo Open Service Signal-In-Space Interface Control Document (OS SIS ICD) [AD.1] contain all information on the OSNMA SIS that is relevant for the user segment. The document is intended for the Galileo user community and specifies the interface between the Galileo Space Segment and the Galileo User Segment. The present OSNMA SIS ICD is intended to be used for the Galileo OSNMA Initial Service Phase.

The Galileo Service Centre (GSC) OSNMA Server provides Public Keys and Merkle tree roots, with their associated information and certificates. The interface between the Galileo User Segment and the Galileo Service Centre (GSC) OSNMA Server is specified in the Galileo Open Service Navigation Message Authentication (OSNMA) Internet Data Distribution (IDD) Interface Control Document (ICD) [AD.3].

1.2 Structure of the Document

The document is structured as follows:

- Chapter 2 describes the OSNMA Message Structure;
- Chapters 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 2.1, 2023.

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

[AD.3] European GNSS (Galileo) Open Service, Galileo OSNMA Internet Data Distribution Interface Control Document, Issue 1.0, 2023.

1.4 Galileo Open Service Navigation Message Authentication Overview

The Galileo programme will provide cryptographic data to authenticate its Open Service navigation messages [1] [2]. The authentication protocol described here 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 [8]. It is optimized for Galileo by using the same key chain for all satellites, 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, 20 at the time of publishing this document, out of the total constellation. The OS data of the remaining satellites will be cross-authenticated through the satellites transmitting OSNMA.

2 OSNMA Message Structure

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

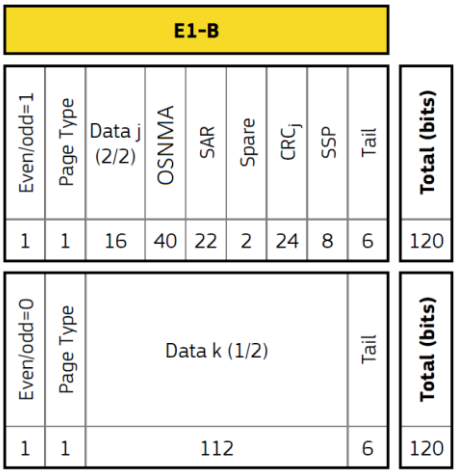


Figure 1. E1-B I/NAV Nominal Page with bits allocation, including OSNMA data

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. If a satellite is not part of the above mentioned subset, 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, including pages used to transmit the I/NAV Spare Word, an OSNMA message is transmitted. The OSNMA field has the following structure:

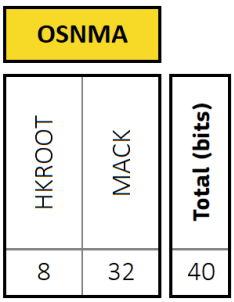


Figure 2. OSNMA data message

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. Therefore, a 120-bit HKROOT message and a 480-bit MACK message are 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 OSNMA Bit 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;
- Any zero padding is to be intended as right zero-padding (i.e. from the least significant bit).

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, consisting of a DSM Header, followed by 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
NMA Header	DSM Header	DSM Block *n*												
8	8	104												

Total (bits)
120

Figure 3. HKROOT Message

Several DSM blocks, transmitted through successive subframes, form a complete DSM 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 in 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
2	2	3	1

Total (bits)
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 defines the corresponding semantic for each value.

Table 1. NMAS values and corresponding semantic

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.

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 the following table defines the semantic of each possible status value.

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

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.

CPKS	Definition	Semantic
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	**New Merkle Tree (NMT)**	The Merkle tree is being renewed. The user shall obtain the new Merkle tree root from the GSC OSNMA Server.
7	**Alert Message (AM)**	OSNMA Alert Message is being provided.

Further details on TESLA chain renewal and revocation processes, Public Key renewal and revocation processes, Merkle tree renewal process and Alert Message provision are provided in sections 5.5.3, 5.4.1, 5.6 and 5.7, 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:

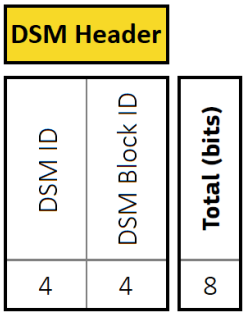


Figure 5. DSM Header

A DSM is identified 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: 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, for both 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).

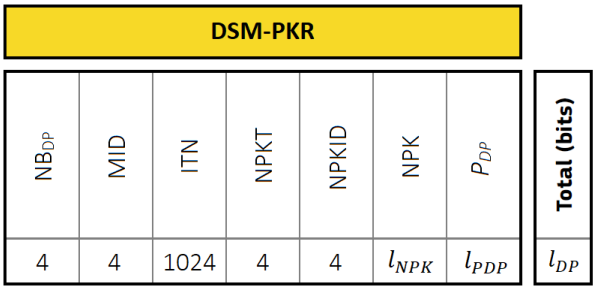


Figure 6. DSM-PKR Message

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:

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

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);
- $\lceil n \rceil$ is the ceiling operator, indicating the least integer greater than or equal to *n*.

Following the above, the total length of the DSM-PKR, 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 meaning 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_{DP} 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.

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

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

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.

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

MID value	Merkle Tree Leaf	Intermediate Tree 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	$x_{0,3}$	$x_{1,0}$	$x_{2,1}$	$x_{3,1}$

MID value	Merkle Tree Leaf	Intermediate Tree Nodes			
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_{11}	$x_{0,10}$	$x_{1,4}$	$x_{2,3}$	$x_{3,0}$
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}	$x_{0,14}$	$x_{1,6}$	$x_{2,2}$	$x_{3,0}$

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, as per the following table.

Table 5. NPKT field and corresponding message

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

As indicated in the previous table, NPKT=4 indicates that an OSNMA Alert Message (OAM) is being transmitted.

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 is provided in increasing order during service provision.

3.2.2.6. New Public Key (NPK)

This field provides the new OSNMA Public Key. Keys are provided as compressed Elliptic Curve Digital Signature Algorithm (ECDSA) keys, including sign field and rounded up to a whole number of bytes, as per [6] and [7].

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:

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

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

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 fits in the number of blocks indicated by the NB_{DP} field and therefore, following Table 3 and Eq. 1:

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

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:

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

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

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

Where:

- the operator $\text{trunc}(L, I)$ 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 [9].

3.2.3 DSM-KROOT

The DSM-KROOT provides the root key of the chain in force, or the one of the next chain, and the means to authenticate those keys using the Public Key in force. The DSM-KROOT provides the chain cryptographic functions, the key and tag sizes, as well as other parameters that are fixed for each given

chain. 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	Reserved2	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, l_{DK}, (expressed in bits) corresponds to:

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

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, Reserved2, 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 Reserved2 fields are reserved for future use.

Following the above, the total length of the DSM-KROOT, 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 meaning 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.

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

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

NB_{DK} value	Number of Blocks	DSM-KROOT total length, l_{DK} [bits]
5	11	1144
6	12	1248
7	13	1352
8	14	1456
9-15	*Reserved*	n/a

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:

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

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

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:

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

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

[1] SHA-2 family hashes (SHA-256) are defined in the latest FIPS publication [9]. SHA-3 family is implemented according to the Keccak algorithm [10].

[2] HMAC-SHA-256 is standardized in [11] and CMAC-AES is standardized [12] and [13].

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:

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

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*

3.2.3.7. Tag Size (TS)

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

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

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

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 4.2.1.3.

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 ADKD sequences.

3.2.3.9. KROOT Week Number and Time of Week (WN_K and $TOWH_K$)

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:

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

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

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

Where:

- the operator $\mathrm{trunc}(L, I)$ 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 specific information data associated (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.

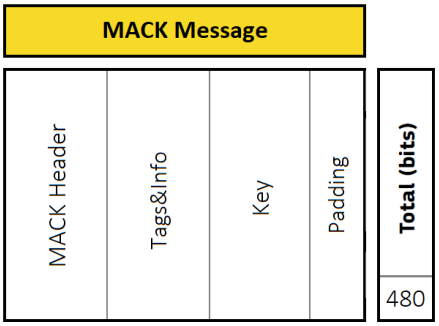


Figure 8. MACK Message

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 Tag_0, the MACSEQ and the corresponding COP are transmitted. The structure of the MACK Header is represented here below:

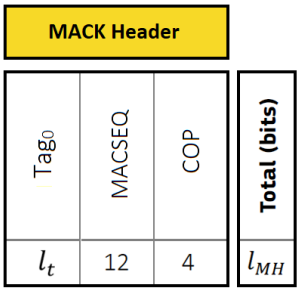


Figure 9. MACK Header

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.

4.1.3 Data Cut-Off Point (COP)

The COP is a 4-bit field that encodes the Data Cut-Off Point parameter. Details are provided in section 4.2.1.2.

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.

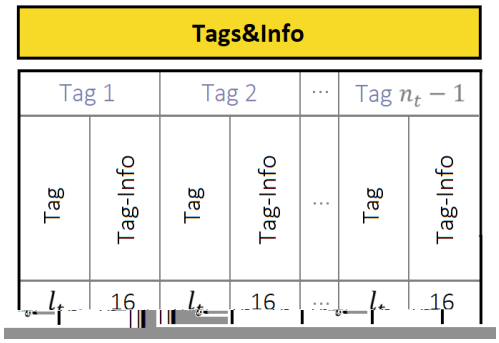


Figure 10. Tags&Info Message

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

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

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:

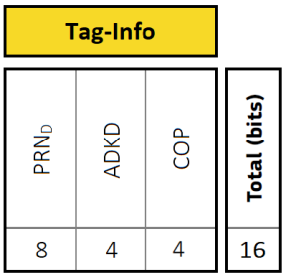


Figure 11. Tag-Info

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.

Table 12. Assignment for the PRN_D field

PRN_D 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)

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 SV_{ID} 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]

Table 13. PRN_D and PRN_A definition

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 SV_{ID} of the Galileo satellite transmitting the information	1-36

4.2.1.2. Data Cut-Off Point (COP)

The COP is a 4-bit field. The value COP = 0 is used to indicate the transmission of a dummy tag, verified with a dummy navigation data mask, as per section 6.7. The remaining 15 values are used to encode a parameter indicating the maximum time lag, T_{COP}, between the tag and the navigation data it authenticates. Within this time span, the navigation data authenticated by the tag has not changed. The time distance is defined as:

$$T_{COP} = \Delta_{COP} * \mathrm{COP}$$

Where Δ_{COP} is a fixed time interval, representing the duration of the logical data frame in which the specific set of data being authenticated is broadcast (e.g. the I/NAV sub-frame for ADKD0). The value of Δ_{COP} for the different ADKD types is defined in Table 14.

For example:

- A COP = 1 indicates that the tag is to be verified with the navigation data retrieved in the Δ_{COP} time interval specified in Table 14 for each ADKD (e.g. for ADKD0, data retrieved within the previous I/NAV sub-frame).
- A COP = 2 indicates that the data authenticated did not change in the two last Δ_{COP} intervals and that the data from either or both of these time intervals can be used to verify the tag (e.g. for ADKD0, data from the previous two I/NAV sub-frames).

Once the COP reaches its maximum (COP = 15), if the latest transmitted data is the same as the one transmitted in the previous 15 time intervals, the counter remains saturated at 15. It will be reset to 1 at the next change of data.

4.2.1.3. Authentication Data and Key Delay (ADKD)

The 4-bit ADKD field describes the authenticated navigation data, used to generate the associated tag. ADKD can assume values from 0 to 15, and for each of those values the corresponding authenticated data, Δ_{COP} time interval (see section 4.2.1.2) and PRN_D are provided in the following table for Galileo PRNs. Note that Δ_{COP} time intervals are defined in terms of Galileo message data structure terms, as per [AD.1]. The exact format of the authenticated data and their concatenation is shown in ANNEX B. New ADKD values might be added in future updates of this ICD.

Table 14. Galileo Authenticated Data with corresponding ADKD, PRN_D and Δ_{COP} Time Interval information.

ADKD	Galileo Authenticated Data[4]	PRN_D	Δ_{COP} Time Interval
0	**Galileo I/NAV Ephemeris, Clock and Status** The tag authenticates I/NAV data transmitted in the previous I/NAV sub-frame. The data authenticated are 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[5].	SV_{ID} of the Galileo satellite transmitting the data to be authenticated	I/NAV sub-frame
1-3	*Reserved*		
4	**Galileo I/NAV Timing Parameters** The tag authenticates the I/NAV data from the Word Type 6 transmitted one sub-frame earlier and the Word Type 10, transmitted one or two sub-frames earlier[6] (retrieved from E1-B only). The data authenticated includes: GST-UTC conversion parameters (Word Type 6) and GST-GPS conversion parameters (Word Type 10).	Same as ADKD=0	I/NAV sub-frame
5-11	*Reserved*		
12	**Slow MAC (additional 10 sub-frame delay, see section 5.8.2) - 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	Same as ADKD=0
13-15	*Reserved*		

[4] Note that the definition of specific time intervals identifying the data that each tag is authenticating for a certain ADKD (so called tag/data link) might evolve in future updates of this document.

[5] In rare cases the DVS value transmitted on E1 and E5b may differ within the same I/NAV sub-frame. This may lead to an ADKD0 tag verification failure for the affected satellite.

[6] WT10 is transmitted nominally every other I/NAV sub-frame, as per [AD.1].

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 Table 14.

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

As discussed in Chapter 2, OSNMA data are distributed only by a subset of Galileo satellites. If a satellite is not part of the above mentioned subset, the I/NAV OSNMA message transmitted 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 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 receiver 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, 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 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. Alternating DSM always have different DSM ID.

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 (see section 3.2.2) every 6 hours (starting at 00:00 GST, 06:00 GST, 12:00 GST and 18:00 GST) for a period of 30 minutes, alternated with broadcast DSM-KROOT and DSM-PKR, as described in the following sections, allowing the user to retrieve the applicable Public Key. This Public Key is published in the GSC OSNMA server as well, together with the relevant information required to verify it (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.

Public Keys can 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, the DSM alternates 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*). A DSM-PKR for the Public Key *p* will also be broadcast if the conditions outlined in section 5.4 are met (not represented in Figure 12).
- 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. CPKS is maintained as NPK for a maximum duration of 24 hours . 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 the DSMs of KROOT(*i*,*p’*) are transmitted. At this step, provision of a DSM-PKR for the Public Key *p’* takes place as explained in section 5.4.

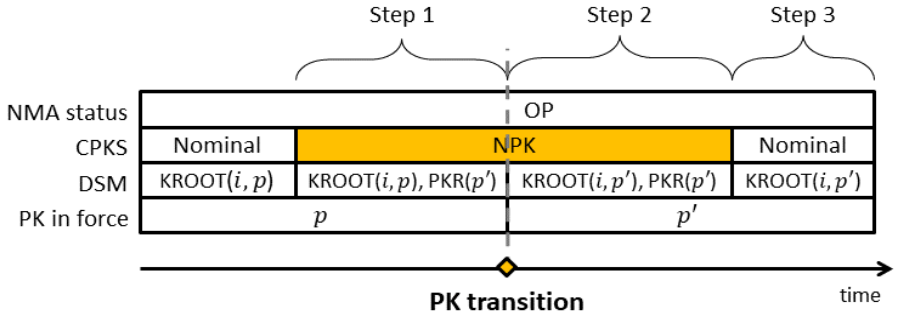


Figure 12. Public Key renewal

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 minimum duration of 2 hours, 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’*, starts 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 a minimum of 22 hours. The chain *i'* enters

into force at the same time. From this time, 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. At this step, provision of a DSM-PKR for the Public Key *p’* takes place as explained in section 5.4.

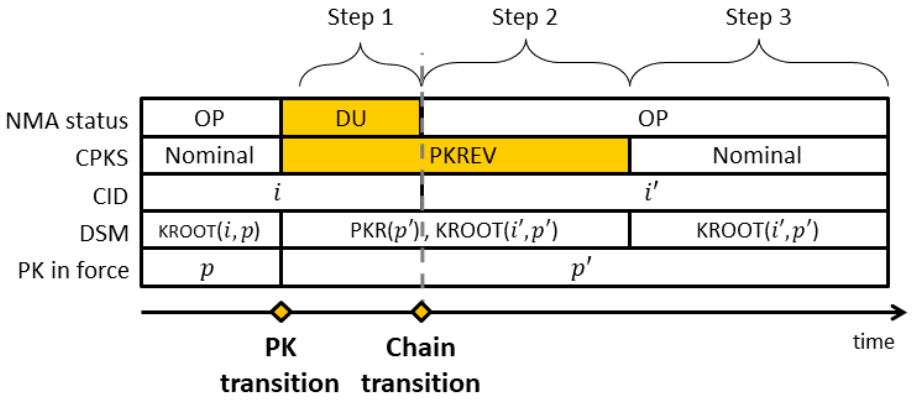


Figure 13. Public Key revocation

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 (see section 3.2.3). The time of applicability GST_0 is provided in the form of Week Number ($\mathrm{WN_K}$) and Time Of Week (expressed in Hours, $\mathrm{TOWH_K}$), as explained in section 3.2.3.9. These parameters are defined as follows:

- KROOT Week Number ($\mathrm{WN_K}$) 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, $\mathrm{TOWH_K}$) is defined as the number of hours that have elapsed since the transition from the previous to the current week. The $\mathrm{TOWH_K}$ covers an entire week from 0 to 167 hours and is reset to zero at the beginning of the week.

$\mathrm{WN_K}$ and $\mathrm{TOWH_K}$ 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 $\mathrm{GST}_0 - 30$ 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.

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 will be transmitted.

[7] During the test phase, floating KROOT will not be provided when a renewal or revocation process is taking place.

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 CPKS flag 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. A DSM-PKR for the current Public Key *p* will also be broadcast if the conditions outlined in section 5.4 are met (not represented in Figure 14).
- Step 2: At the transition time, the new chain *i'* comes into force. The CPKS is set to “Nominal”, the Chain ID (CID) 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. At this step, provision of a DSM-PKR for the Public Key *p* takes place, as explained in section 5.4.

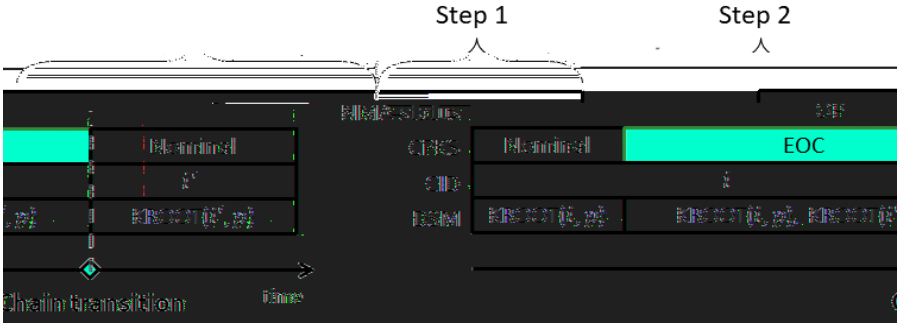


Figure 14. TESLA chain renewal

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 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 minimum duration of 2 hours. 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 been updated yet. 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*. A DSM-PKR for the Public Key *p* will also be broadcast if the conditions outlined in section 5.4 are met (not represented in Figure 15).
- 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 minimum duration of 22 hours, to report (in combination with the NMAS) 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. A DSM-PKR for the Public Key *p* will also be broadcast if the conditions outlined in section 5.4 are met (not represented in Figure 15).

- Step 3: The CPKS flag is set to “Nominal”. At this step, provision of a DSM-PKR for the Public Key *p* takes place, as explained in section 5.4.

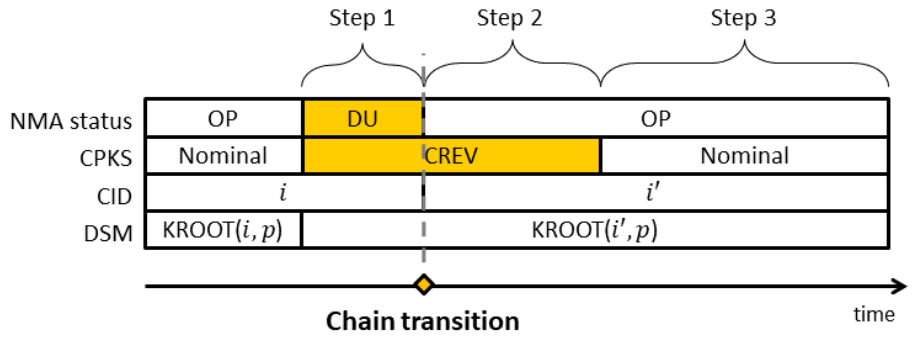


Figure 15. TESLA chain revocation

5.6 Merkle Tree Renewal Process

Within this section, various elements related with the renewal of the OSNMA Merkle tree are described.

Note that a renewal of the Merkle tree is expected to take place very rarely, typically after more than 10 years. The new Merkle tree root will be available on the GSC OSNMA server at least two years before the planned renewal. The Merkle tree renewal process is depicted in Figure 16 and comprises the following steps:

- Step 1: The CPKS flag is set to “New Merkle Tree” (NMT). A DSM-PKR for a new Public Key *p’* generated with the new Merkle tree and a DSM-KROOT using the applicable Public Key *p* (allowing to verify NMAS and CPKS flags) are broadcast. Once the reception of NMT status is verified, if the receiver does not have the new Merkle tree root in memory, it is requested to connect to the GSC OSNMA Server to retrieve it. Step 1 has a duration of 48 hours. A DSM-PKR for the Public Key *p* generated with the previous Merkle tree might be additionally broadcast depending on the duration and timing of execution of Step 1, as explained in section 5.4 (not shown in Figure 16).
- Step 2: *p’* enters into force by the transmission of a new KROOT(*i*,*p’*) transmitted in a new DSM-KROOT, and verified with *p’*. The DSM alternates the new DSM-KROOT with PKR(*p’*) from Step 1 generated with the new Merkle tree. The CPKS flag is maintained as NMT for a duration of 48 hours. The receiver shall discard any stored cryptographic material associated to the previous Merkle tree, including any previously stored Public Key. As the Merkle tree has been renewed, the PKID counter for Public Keys will be reset, i.e. only in this case the PKID of p' can have a lower value than that of p.
- Step 3: CPKS is set back to “Nominal” and the DSM-PKR stops being continuously transmitted. Provision of DSM-PKR for the Public Key *p’* takes place as explained in 5.4.

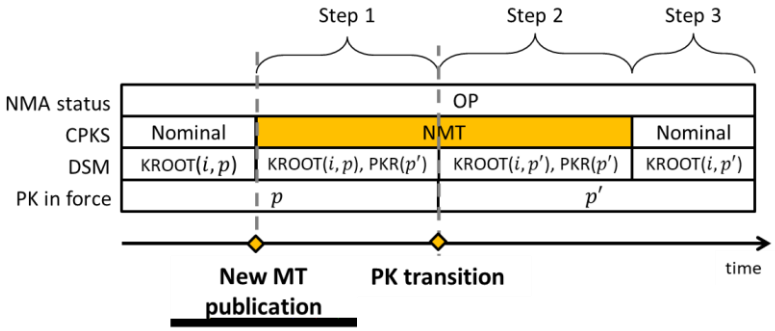


Figure 16. Merkle Tree renewal

5.7 OSNMA Alert Message Provision

The Alert Message is transmitted only for very specific situations that cannot be managed through different processes described in this document (TESLA chain renewal and revocation, Public Key renewal and revocation, Merkle tree renewal). Therefore, it is not expected to occur under nominal operations. The Alert Message process is depicted in Figure 17 and comprises the following steps:

- Step 1: The NMAS flag is set to “Don’t Use” (DU) and the CPKS flag is set to “Alert Message” (AM). A DSM-PKR notifying the provision of the Alert Message and a DSM-KROOT, allowing the verification of the NMAS and CPKS flags, are broadcast. Once the reception of the Alert Message is verified, the receiver is requested to stop processing OSNMA data and connect to the GSC OSNMA Server for further updates. The receiver shall discard any previously stored cryptographic material upon reception of Alert Message. Step 1 has no predefined duration.
- Step 2: During this step, no transmission of OSNMA takes place. Step 2 is optional and has no predefined duration. Recovery actions will take place and further updates will be provided on the GSC OSNMA Server.

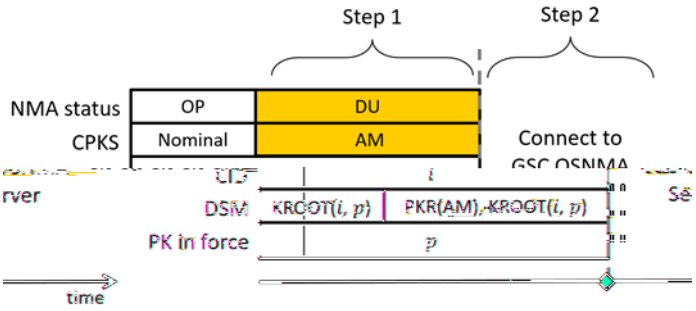


Figure 17. Alert Message

5.8 Tags Distribution

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

5.8.1 Tag Identification and Accumulation

Several tags (or Tag_0) can be retrieved and linked to a specific navigation data based on their Tag-Info field.

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

$$l_t \geq L_t^{min} \qquad \text{Eq. 9}$$

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

$$l_t \cdot N_t \geq L_t^{min} \qquad \text{Eq. 10}$$

Where N_t is the number of tags of length l_t, with the same PRN_D and ADKD fields, and relative to the same navigation data, as identified by the Δ_{COP} interval, to be accumulated in order to perform authentication.

The concept of tag accumulation is further discussed in [AD.2].

5.8.2 Applicable Keys for Tag 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-subframe delay. This is labelled also as “Slow MAC”. As a consequence, an additional delay of 10-subframe shall be taken into account when selecting the key to be used for a tag with an ADKD=12.

The relationship between the tags and the key is also applicable during the chain renewal and revocation processes. Tags transmitted before the transition can be verified with the keys transmitted after the transition. In the case of different tag lengths between the two chains, the tags before the transition are truncated according to the tag length applicable before the transition.

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:

- $\mathrm{hash}_{H256}(m)$ is the SHA-256[8] hash operation function applied to the input message m.
- $\mathrm{hash}_{\mathrm{chain}}(m)$ 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).
- $\mathrm{mac}(K, m)$ 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 zero-padded.

- $\mathrm{signature}(x, \mathrm{PK})$ is the specific digital signature algorithm chosen for the protocol, which is ECDSA [6], supporting different signature lengths and Public Key (PK) 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 and is also provided on the GSC OSNMA server in case the Public Key is retrieved there. The key to be used as an input to the signature algorithm is the ECDSA Public Key retrieved in the NPK field. The ECDSA signature length is given in Table 15.

Table 15. Supported ECDSA algorithm

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

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 [9]

[9] In the case of ECDSA P-521, the digital signature is composed of a pair of 66-bytes coordinate values, being transmitted consecutively over 528-bits each. The elliptic curve point coordinate is represented by the 521 least significant (rightmost) bits, as per [15].

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:

$$m_i = (\mathrm{NPKT} \| \mathrm{NPKID} \| \mathrm{NPK}) \quad \text{Eq. 11}$$

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 18. A Merkle tree leaf m_i is validated against the Merkle root, $x_{4,0}$, by means of the intermediate tree nodes $x_{j,i}$ (see section 3.2.2.3). Further details on the Merkle tree can be found in [AD.2].

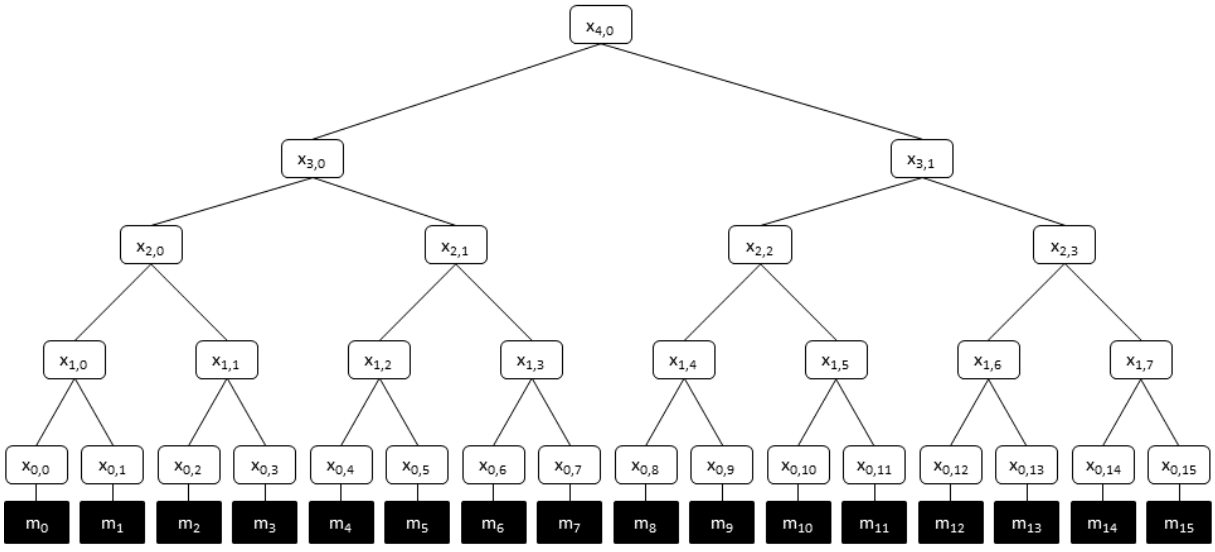


Figure 18. Galileo OSNMA Merkle tree

The base nodes of the tree $x_{0,i}$ can be computed as follows:

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

With $i = 0, \ldots, N-1$

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

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

With:

- $j = 1, \ldots, 4$ denotes the level in the tree;
- $i = 0, \ldots, 2^{4-j} - 1$, 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:

$$\mathrm{M} = \begin{pmatrix} \mathrm{NMA\ Header} \| \mathrm{CIDKR} \| \mathrm{Reserved1} \| \mathrm{HF} \| \mathrm{MF} \| \mathrm{KS} \| \mathrm{TS} \| \mathrm{MACLT} \| \ldots \\ \ldots \mathrm{Reserved2} \| \mathrm{WN_K} \| \mathrm{TOWH_K} \| \alpha \| \mathrm{KROOT} \end{pmatrix} \quad \text{Eq. 14}$$

Where:

- $\mathrm{NMA\ Header}$ 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 follows:

$$\mathrm{DS} = signature(M \| P, \mathrm{PK}) \quad \text{Eq. 15}$$

Where:

- P is a zero-padding sequence such that the length of the input for the signature algorithm fits an integer number of bytes;
- PK is the applicable Public Key to be used to verify the digital signature.

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:

$$K_0 = F^N(K_N) \quad \text{Eq. 16}$$

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:

$$K_I = F(K_{I+1}) = trunc\left(l_k, \mathrm{hash_{chain}}\left(K_{I+1} \| \mathrm{GST}_{SF,I} \| \alpha\right)\right) \quad \text{Eq. 17}$$

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;
- $\mathrm{GST}_{SF,I}$ 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:

$$\mathrm{GST}_{SF,I} = \mathrm{GST}_0 - 30 \text{ [seconds]} \quad \text{Eq. 18}$$

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.

$$I = \frac{\mathrm{GST}_{SF,I} - \mathrm{GST}_0}{30} + 1$$ Eq. 19

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 ADKD tag 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 ANNEX C). The MACSEQ is generated with the same key and MAC function as the rest of the tags 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:

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

Where K is the key from the TESLA chain used for the Tag generation (see section 5.8.2) and m is computed as follows:

$$m = (\mathrm{PRN_A} \| \mathrm{GST}_{SF} \| \mathrm{MFLEX}_1 \| \mathrm{MFLEX}_2 \| \ldots \| \mathrm{MFLEX_N})$$ Eq. 21

with

- $\mathrm{PRN_A}$ 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 $i = [1 \ldots N]$ 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. $\mathrm{MFLEX_N}$ 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:

$$m = (\mathrm{PRN_A} \| \mathrm{GST}_{SF})$$ Eq. 22

Note that the values currently defined as 'Reserved' for the PRND and ADKD fields (sections 4.2.1.1 and 4.2.1.3) may be transmitted in the MFLEX_i, e.g. for testing purposes. In case such values are retrieved, the user is expected to perform the MACLT verification as specified above, using the retrieved MFLEX_i, and to discard the tags associated to an PRND or ADKD defined as 'Reserved'.

6.7 Tag Verification

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

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

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 5.8.2;
- m is computed as follows:

$$m = (\mathrm{PRN_D} \| \mathrm{PRN_A} \| \mathrm{GST}_{SF} \| \mathrm{CTR} \| \mathrm{NMAS} \| navdata \| P) \quad \text{Eq. 24}$$

Where

- $\mathrm{PRN_D}$ 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);
- $\mathrm{PRN_A}$ 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) of the sub-frame in which the tag is transmitted;
- $navdata$ 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:

$$Tag_0 = trunc\big(l_t, mac(K, m_0)\big) \quad \text{Eq. 25}$$

$$m_0 = (\mathrm{PRN_A} \| \mathrm{GST}_{SF} \| \mathrm{CTR} \| \mathrm{NMAS} \| navdata \| P\ ) \quad \text{Eq. 26}$$

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.

As described in section 4.2.1.2, the system may transmit dummy tags, indicated by a COP field set to zero. Such tags are verified as per the previous equations, with the difference that the $navdata$ field is replaced by a sequence of zero bits. The length of this sequence is equal to the length of the data associated to the tag ADKD type, as indicated in ANNEX B.

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, PCT/EP2015/056120, 23/03/2015, European Union represented by European Commission

[5] Digitally-signed satellite radio-navigation signals, Patent 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] Standards for Efficient Cryptography Group (SECG), "SEC 1: Elliptic Curve Cryptography", Version 1.0, September 2000.

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

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

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

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

[12] 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.

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

[14] US Government, “GPS Interface Specification IS-GPS-200K”, 06.05.2019.

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

ANNEX A List of Acronyms

Acronym	Definition
ADKD	Authentication Data & Key Delay
AES	Advanced Encryption Standard
BID	Block ID
CID	Chain ID
CMAC	Cipher-based Message Authentication Code
COP	Cut-Off Point
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
NMT	New Merkle Tree
NPK	New Public Key
NPKID	New Public Key ID
NPKT	New Public Key Type
OAM	OSNMA Alert Message
OP	Operational
OS	Open Service
PK	Public Key
PKID	Public Key ID

Acronym	Definition
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							
	Ephemeris (1/4)					Ephemeris (2/4)					Ephemeris (3/4)						
IOD_{nav}	t_{0e}	M_0	e	$A^{1/2}$	IOD_{nav}	Ω_0	i_0	ω	$\dot{i}$	IOD_{nav}	$\dot{\Omega}$	Δn	C_{UC}	C_{US}	C_{RC}	C_{RS}	SISA(E1,E5b)
10	14	32	32	32	10	32	32	32	14	10	24	16	16	16	16	16	8

data from Word Type 4								data from Word Type 5																	
		Ephemeris (4/4)		Clock Correction				Ionospheric correction															
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	6	16	16	14	31	21	6	11	11	14	1	1	1	1	1	10	10	2	2	1	1	**549**

Figure 19. 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 encoding 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 and 10 (retrieved from E1-B only) are concatenated.

data from Word Type 6								data from Word Type 10				
GST-UTC conversion parameters								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}	**Total (bits)**
32	24	8	8	8	8	3	8	16	12	8	6	**141**

Figure 20. Concatenated Authenticated Data for ADKD=4

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. The receiver shall be configurable to implement new sequences that might be added in future updates of this OSNMA SIS ICD.

The first column (ID) 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 (n_t) 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, ‘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 Tag_0, as described in 4.1.1.

Table 16. MAC Look-up Table

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	2	6	00S, 00E, 04S, 00E, 12S, 00E	00S, 00E, 00E, 12S, 00E, 12E
34	2	6	00S, FLX, 04S, FLX, 12S, 00E	00S, FLX, 00E, 12S, 00E, 12E
35	2	6	00S, FLX, 04S, FLX, 12S, FLX	00S, FLX, FLX, 12S, FLX, FLX
36	2	5	00S, FLX, 04S, FLX, 12S	00S, FLX, 00E, 12S, 12E
37	2	5	00S, 00E, 04S, 00E, 12S	00S, 00E, 00E, 12S, 12E
38	2	5	00S, FLX, 04S, FLX, 12S	00S, FLX, FLX, 12S, FLX
39	2	4	00S, FLX, 04S, FLX	00S, FLX, 00E, 12S
40	2	4	00S, 00E, 04S, 12S	00S, 00E, 00E, 12E
41	2	4	00S, FLX, 04S, FLX	00S, FLX, FLX, 12S

ANNEX D Changes between this OSNMA SIS ICD and the OSNMA User ICD for the Test Phase[10]

This document supersedes the Galileo OSNMA User ICD for the Test Phase for what matters the definition and development of OSNMA receivers and processing. This annex is meant to support users in identifying the changes between the elements of the OSNMA User ICD for the Test Phase and those presented in this OSNMA SIS ICD.

OSNMA User ICD for the Test Phase, Issue 1.0	OSNMA SIS ICD, Issue 1.0	Description
3.1.3	3.1.3	Two new CPKS values are defined, corresponding to the Merkle tree renewal process and the OSNMA Alert Message provision.
4.1	4.1	The description of the MACK Header is updated to include the new COP parameter.
-	4.1.3	This new section introduces a new parameter, the Data Cut-Off Point (COP) is introduced.
4.2.1	4.2.1	The description of the Tag-Info section is updated to include the new COP parameter.
-	4.2.1.2	The definition of the COP parameter is provided in this new section. The value COP = 0 is used to indicate the transmission of a dummy tag by the system, which does not authenticate a specific part of the navigation message but can still be verified. The remaining values are used to define a time span over which the navigation data authenticated by the tag did not change.
4.1.4.2	4.2.1.3	The description of the ADKD in this section (formerly numbered 4.1.4.2) is updated to include considerations related to the COP. The definition of the data authenticated by ADKD 4 is also updated: The TOW parameter is removed and the PRND used for the verification is the SVID of the Galileo satellite transmitting the data to be authenticated, as for ADKD 0.
5.4	5.4	The provision of nominal DSM-PKR at fixed time intervals is specified.
5.4.1	5.4.1	The nominal provision of the DSM-PKR is reflected on the Public Key renewal and revocation processes.
5.5.3	5.5.3	The nominal provision of the DSM-PKR is reflected on the TESLA chain key renewal and revocation processes.
-	5.6	This new section describes in details the Merkle tree renewal process.
-	5.7	This new section describes in details the provision of an OSNMA Alert Message.
5.6	5.8	No change, formally numbered 5.6.
5.6.1	5.8.1	The tag accumulation principle is updated so that users can exploit the new COP parameter to identify tags that can be accumulated with each other in this section formally numbered 5.6.1..
5.6.2	5.8.2	The relationship between the tags and the applicable TESLA chain key is extended to the chain transition, under specific conditions described in this section formally numbered 5.6.2.

[10] European Commission, Galileo Open Service Navigation Authentication (OSNMA) User ICD for the Test Phase, Issue 1.0, November 2021

OSNMA User ICD for the Test Phase, Issue 1.0	OSNMA SIS ICD, Issue 1.0	Description
6.7	0	The tag verification is updated to include considerations about the verification of the dummy tags (as indicated by COP = 0).
Annex B.2	Annex B.2	The format of the authenticated data for the case ADKD = 4 is updated (TOW is removed).
Annex C	ANNEX C	The Annex incorporates the notice of updates in the MAC Lookup Table for service provision.
Annex D	-	The description of the interface with the European GNSS Service Centre (GSC) OSNMA Server is removed from the document (formally Annex D). This interface is specificed in the Galileo Open Service Navigation Message Authentication (OSNMA) Internet Data Distribution (IDD) Interface Control Document (ICD) [AD.3].

ANNEX E Authorisation Concerning the OSNMA SIS ICD IPRs

By practicing, using or copying the OSNMA SIS ICD 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 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 SIS ICD IPRs listed in section E.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 SIS ICD 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.

E.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 SIS ICD 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 SIS ICD 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 SIS ICD" – shall mean the Galileo Open Service Navigation Message Authentication (OSNMA) Signal-in-Space Interface Control Document 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 SIS ICD Copyright" – shall mean the copyright on and to the OSNMA SIS ICD document and/or its content.

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

"Patents" – shall mean any and all patents and/or patent applications mentioned in section E.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 SIS ICD" – 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 SIS ICD.

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

E.2 Ownership of Rights

Ownership and/or control of the OSNMA SIS ICD IPRs shall remain with the EU and therefore, no title of any intellectual property right on the OSNMA SIS ICD 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 SIS ICD IPRs or participates in such a challenge, or encourages or supports any third parties in such a challenge.

E.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 SIS ICD 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 SIS ICD, 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 SIS ICD, provided the source is acknowledged;

c. the reproduction of the OSNMA SIS ICD, 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 SIS ICD.

This list is exhaustive. No other activity shall benefit from the Authorisation. The practice of any of the OSNMA SIS ICD 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 by a) 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.

E.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 E.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 E.12, without the need to amend the Authorisation.

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

a. maintain the OSNMA SIS ICD 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.

E.5 Duration and Termination

With respect to each of the OSNMA SIS ICD IPRs, the Authorisation shall be valid for the whole duration of said OSNMA SIS ICD 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 SIS ICD IPRs whose practice, use or copy is authorised hereunder should finally be declared not granted or invalid.

E.6 Warranties and Liability

The Authorisation is issued under the OSNMA SIS ICD 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 SIS ICD IPRs, including as to:

a. the condition, the patentability and/or validity and enforceability of the OSNMA SIS ICD IPRs;

b. the freedom to practice, use or copy the OSNMA SIS ICD IPRs, 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 SIS ICD IPRs and/or to enjoin the activities that benefit from the Authorisation;

d. the dependency of the OSNMA SIS ICD IPRs on third parties' intellectual or industrial property rights;

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

To the full extent allowed by law, all warranties, whether expressed or implied, for any use of OSNMA SIS ICD 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.

E.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 SIS ICD 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.

E.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 SIS ICD 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 SIS ICD IPRs, the Authorised Person shall collaborate with the EU and provide the EU with all the assistance necessary to such defence.

E.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.

E.10 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 Authorisation.

E.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 SIS ICD 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 SIS ICD IPRs by the Authorised Person.

E.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 filling	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, 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, DE, DK, ES, FI, FR, GB, GR, HU, IE, IT, LU, NL, PL, PT, RO, SE, TR), USA, S. Korea, China, India, Japan, Russia
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	
4	Patent	Method and generator for generating a spread- spectrum signal	12559874	15/09/2009	EUSPA	EU	
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, CH, CZ, DE, DK, ES, FI, FR, GB, GR, HU, IE, IT, LT, LU, NL, PL, PT, RO, SE, TR), India, Japan, S.Korea, Russia, USA

	IPR	Name of IPR	Application Number	Date of filling	Applicant	Owner	Designated Countries
6	Copyright	OS SIS ICD	N/A	N/A	N/A	EU	Worldwide
7	Patent	Spreading codes for a satellite navigation system (concerning memory codes)	PCT/ EP2004/ 014488	17/12/2004	ESA	EU	Canada, Europe designated countries: (DE, ES, FR, GB, IT,) USA, Brazil, China, Japan, India, Russia, Hong Kong
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, IT, NL, PT, SE, TR) USA, Brazil, China, Japan, Russia, Hong Kong, India
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 licencefrom 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
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
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
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)

	IPR	Name of IPR	Application Number	Date of filling	Applicant	Owner	Designated Countries
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)
17	Patent	Digitally- signed satellite radio-navigation signals	PCT/ EP2014/ 064285	04/07/2014	The European Union, repre-sented by the European Commission	EU	Australia, Brasil, Canada, China, Europe designated countries (FR, IT, ES, DE), Great Britain , India, Japan, South Korea,Russia, USA
18	Patent	Method and system to optimise the authentication of radio- navigation signals	PCT/ EP2015/ 056120	23/03/2015	The European Union, repre-sented by the European Commission	EU	Australia, Brasil, Canada, China, India , Europe designated countries (FR, IT, ES, DE), Great Britain, Japan, South Korea, Russia, USA
19	Copyright	OSNMA SIS ICD	N/A	N/A	N/A	EU	Worldwide

TS-03-22-258-EN-N

EUSPA
European Union Agency for the Space Programme

LINKING SPACE TO USER NEEDS

www.euspa.europa.eu

@EU4Space

@EU4Space

EUSPA

@space4eu

EUSPA

#EUSpace