EUROPEAN COMMISSION
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

EU Satellite Navigation Programmes
Galileo and EGNOS - Programme Management and GNSS Policy

Ref. Ares(2016)6620281 - 25/11/2016

GROW/J1/IFH/kp/ARES(2016)6611263

Galileo Navigation Message Authentication Specification for Signal-In-Space Testing – v1.0

	Name	Date	Signature
Prepared by	I. Fernández, V. Rijmen, T. Ashur, P. Walker, G. Seco, J. Simón, C. Sarto, D. Burkey, O. Pozzobon.	18/11/16	
Checked by	I. Fernández J. Simón (GSA)	18/11/16 18/11/16	
Approved by	E. CHAMLE A. HOZO (GSA) J. GODET	21/11/16 21/11/16 21/11/16	
Authorised by	P. Flament	24/11/16	

Contents

CHANGE RECORD

V1.0, 11/11 /2016	First version.

1 INTRODUCTION AND PURPOSE

This document provides the bit-level specification of Galileo OSNMA service based on the TESLA protocol used for SIS testing in 2018. The TESLA protocol [1] is based on the transmission of message authentication codes generated with a key that is broadcast with some delay, and is part of a pre-generated one-way chain whose root is public, and which is transmitted in reverse order with respect to its generation. This document is organised as follows:

- Section 2 provides the overall OSNMA message structure
- Section 3 provides the HKROOT structure and fields.
- Section 4 provides the MACK structure and fields.
- Section 5 defines the cryptographic operations.
- Section 6 presents some general, non-exhaustive receiver guidelines for OSNMA implementation and testing.

2 OSNMA MESSAGE STRUCTURE

The OSNMA implementation here described is based on the TESLA protocol [1] fitted in the Galileo I/NAV navigation message transmitted in the E1-B Galileo Open Service signal. It uses the same key chain from all satellites and authenticates data transmitted by other satellites from a given satellite. It uses the field highlighted in Figure 1. This field is called "Reserved 1" in the ICD [2], or EDBS field in other Galileo documentation.

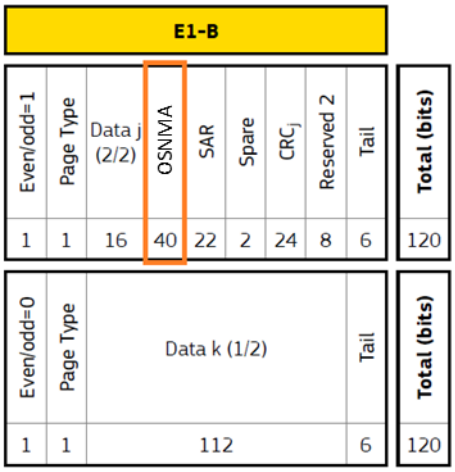

Figure 1 – OSNMA field in each I/NAV Word

Figure 2 left presents the Galileo E1-B I/NAV message structure and highlights the position of the OSNMA field (named as "Res") within a 30-second subframe. Figure 2 right presents the two sections that compose the OSNMA message, the HKROOT section (first 8 bits) and the MACK section (next 32 bits).

The HKROOT section includes the global headers and the Digital Signature Message (DSM). The MACK sections contain the MACs and associated keys, delivered later. They are described in the following sections.

T_0 (GST_0 sync.) (s)	E5b Sub frame ID	E1-B Content						E1-B Page	E1B Sub frame ID
6	N	Word 6 (2/2)	Res	SAR	Spare	CRC	Res	Odd	N
7	N	Word 7 or 9 (1/2)						Even	N
8	N	Word 7 or 9 (2/2)	Res	SAR	Spare	CRC	Res	Odd	N
9	N	Word 8 or 10 (1/2)						Even	N
10	N	Word 8 or 10 (2/2)	Res	SAR	Spare	CRC	Res	Odd	N
11	N	Reserved (1/2)						Even	N
12	N	Reserved (2/2)		SAR	Spare	CRC	Res	Odd	N
13	N	Reserved (1/2)						Even	N
14	N	Reserved (2/2)		SAR	Spare	CRC	Res	Odd	N
15	N	Reserved (1/2)						Even	N
16	N	Reserved (2/2)		SAR	Spare	CRC	Res	Odd	N
17	N	Reserved (1/2)						Even	N
18	N	Reserved (2/2)		SAR	Spare	CRC	Res	Odd	N
19	N	Reserved (1/2)						Even	N
20	N	Reserved (2/2)		SAR	Spare	CRC	Res	Odd	N
21	N	Word 1 (1/2)						Even	N
22	N	Word 1 (2/2)	Res	SAR	Spare	CRC	Res	Odd	N
23	N	Word 3 (1/2)						Even	N
24	N	Word 3 (2/2)	Res	SAR	Spare	CRC	Res	Odd	N
25	N	Word 5 (1/2)						Even	N
26	N	Word 5 (2/2)	Res	SAR	Spare	CRC	Res	Odd	N
27	N	Spare Word (1/2)						Even	N
28	N	Spare Word (2/2)	Res	SAR	Spare	CRC	Res	Odd	N
29	N	Spare Word (1/2)						Even	N
30	N+1	Spare Word (2/2)	Res	SAR	Spare	CRC	Res	Odd	N

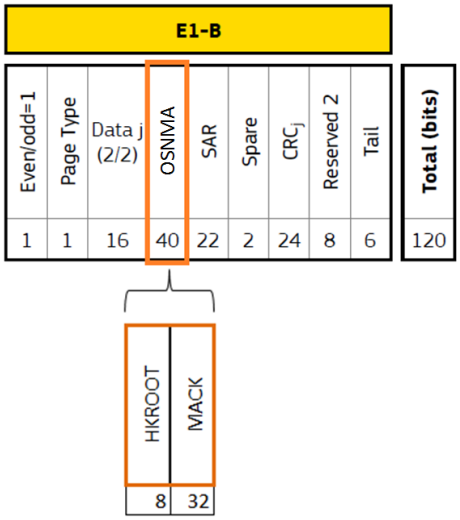

Figure 2 – Galileo E1B I/NAV message structure

3 HKROOT SECTION

The HKROOT (Headers and KROOT) section occupies 120 bits per subframe and contains three fields: the NMA Header (8 bits), the DSM (Digital Signature Message) Header (8 bits) and a DSM block (104 bits). The message signed in the DSM usually is a TESLA root key, or KROOT, but it can also be a new public key. Figure 3 shows the distribution of HKROOT fields in a full I/NAV 15-page subframe. A DSM is composed of various blocks, and therefore is transmitted through various subframes. Its total length is variable, depending on the message and the cryptographic parameters used. Satellites can transmit different blocks of the same DSM at a given subframe, or different blocks for different DSMs.

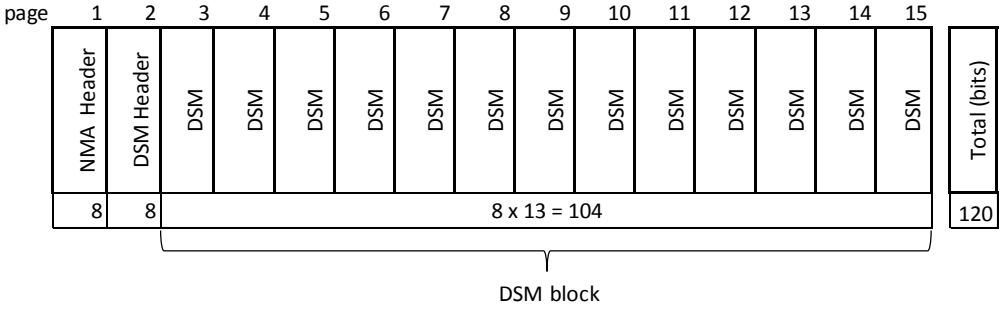

Figure 3- NMA Header and DSM fields as transmitted in the HKROOT in one I/NAV subframe (15 pages)

3.1 NMA Header

The NMA Header defines the status of the NMA service. Its fields are described below.

NMA Status	Chain Status	Chain ID	Reserved	Total (bits)
2	2	2	2	8

Table 1 – NMA Header

3.1.1 NMA Status

This field presents the overall status of the NMA service, according to the values in the following table.

0	1	2	3
Reserved	Test	Operational	Don't Use

Table 2 –NMA Status values

The modes are described as follows:

- "Reserved": this value is not used at the moment[1]
- "Test" indicates that NMA is provided without any operational guarantees. The receiver may use authenticated navigation data at its own risk.
- "Operational" mode indicates that NMA is provided according to the specifications.
- "Don't Use" mode warns the receiver not to navigate using NMA data. The receiver can continue reading the HKROOT and MACK sections for further information about the issue triggering the "Don't Use" status.

3.1.2 Chain Status

This field presents the status of the chain, according to the values in the following table.

0	1	2	3
Reserved	Nominal	EOC	CREV

Table 3 –Chain Status values

- "Reserved": this value is reserved for future use.
- "Nominal": this value indicates that chain is in force and nominally available. The receiver can continue using the current chain without processing the DSM, even if does not have the KROOT of the future chain.

[1] By not using the value '0', a correctly received NMA message cannot be confused with an EDBS dummy message of 40 zero-bits.

- "EOC" (End Of Chain): This mode notifies the receiver that the current chain, associated to *Chain ID* in the NMA Header, is coming to an end. The receiver must start processing the DSM in order to get the KROOT of the next Chain ID. See section 6 for more details.
- "CREV" (Chain Revoked) This mode reports that a chain is or has been revoked. It is interpreted in combination with the NMA Status field, as follows:
  - Chain Status = "CREV" and NMA Status = "Don't Use" implies that the *current* chain, associated to *Chain ID*, has been revoked.
  - Chain Status = "CREV" and NMA Status = "Operational" implies that a *past* chain, not the one associated to Chain ID, has been revoked in the past.

3.1.3 Chain ID (CID)

This 2-bit field represents the ID of the chain in force, i.e. the chain to which the keys in the MACK section in the current subframe belong.

3.1.4 Reserved

The last two bits of the OSNMA Header reserved for future use.

3.2 DSM Header

This header informs about the Digital Signature Message and block being transmitted. Its fields are described below.

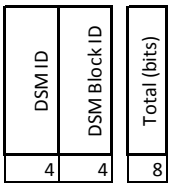

Table 4 – DSM Header

3.2.1 DSM ID

DSM ID is a 4-bit identifier of the DSM. As a DSM is transmitted in several blocks (1 block per subframe), DSM ID will serve to identify the DSM associated to the current block. There are two types of DSM:

- DSM-KROOT: A DSM that provides a digitally signed KROOT. This is the most frequently transmitted DSM type.
- DSM-PKR: A DSM for public key renewal. This type of DSM will only be transmitted when a public key renewal is required, which is expected to happen very seldom, if at all.

DSM IDs of values 0 to 11 are allocated to DSM-KROOT, while DSM IDs of values 12 to 15 are allocated to DSM-PKR, as shown in the below table.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
DSM-KROOT IDs												DSM-PKR IDs			

Table 5 – DSM-ID values

3.2.2 DSM Block ID (BID)

This field represents the ID of the DSM 104-bit block transmitted in the subframe. The blocks will in general be transmitted sequentially, but the current definition allows for scattered blocks, in case e.g. there is a problem in the EDBS transmission from the system and a block is rebroadcast. The DSM Block ID identifies the position of the block in the sequence, i.e. the first block is identified by BID = 0, the second block by BID = 1, etc., up to a maximum of 16 blocks, where the last block is BID = 15.In order to decode a full DSM, the receiver must be able to receive all the blocks and sort them in sequential order. The total number of blocks of a DSM is defined within Block 0 of the DSM, as described later.

3.3 DSM-KROOT

A DSM-KROOT authenticates a KROOT of the chain in force or the next chain with a trusted public key known by the receiver. It also defines and authenticates the chain cryptographic functions used, the key and MAC sizes, and other chain parameters. It is the DSM type that will be transmitted most of the time and the reason why its parent section is called HKROOT, even if new public keys can be transmitted in the HKROOT as well. The DSM-KROOT structure for a digitally signed KROOT is shown in Table 6 and described below.

Nb. of Blocks	Public Key ID	Chain ID KROOT	Nb of MACKs	Hash Function	MAC Function	Key Size	MAC Size	MACK Offset	KROOT WN	KROOT DOW	α	Digital Signature	KROOT	Padding	Total (bits)
4	4	2	2	2	2	4	4	1	12	3	48	v	v	v	v

DSM parameters

chain parameters

KROOT parameters

Table 6 –DSM-KROOT fields. 'v' in the bit size stands for 'variable'

The Digital Signature and Padding parameters are described in section 5.1. The remaining parameters are described below.

3.3.1 Nb. of Blocks (NB)

This field represents the number of blocks of the DSM. A DSM block corresponds to the 104 bits of DSM that are transmitted in a given I/NAV subframe, as per Figure 3 above. The 4-bit NB value does not express directly the number of blocks and needs to be converted as per the table below.

NB value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Nb. of Blocks	6	7	8	9	10	11	12	13	14	15	16	rsvd	rsvd	rsvd	rsvd	rsvd
DSM length (bits)	624	728	832	936	1040	1144	1248	1352	1456	1560	1664	n/a	n/a	n/a	n/a	n/a

Table 7 – Nb. Of Blocks field, including DSM total length (bits)

3.3.2 Public Key ID (PKID)

This field represents the ID of the public key to be used to verify the signature of the DSM. It is assumed that the receiver already has in its possession a trusted public key associated to the Public Key ID, either because it is installed from factory in the receiver, or because it has been transmitted through a DSM-PKR message.

The receiver also knows the DS algorithm related to the public key, as this information is provided from factory or from a trusted server. This information is statically associated with each public key. The cryptographic operations to be performed by the receiver are described in Section 5.

One or several trusted public keys, together with their IDs, will be published by the OSNMA provider in a trusted server, together with any information required to process the DSM-PKR message.

3.3.3 Chain ID of KROOT (CIDKR)

This field identifies the chain to which the signed KROOT belongs. Notice that *CIDKR* may not be the same as the *Chain ID* (*CID*) in the NMA Header (section 3.1.2).

3.3.4 Nb. of MACKs (NMACK)

This field identifies the number of MACK sections within a subframe. The below table shows the MACK sections associated to each NMACK value.

NMACK value	0	1	2	3
Number of MACK Sections per Subframe	rsvd	1	2	3
MACK Section length (bits)	n/a	480	240	160

Table 8 – Nb. of MACK sections per subframe, and MACK section length

3.3.5 Hash Function (HF)

This field identifies the hash function used for the chain. It is interpreted as follows:

HF value	0	1	2	3
Hash Function	SHA-256	SHA3-224	SHA3-256	rsvd

Table 9 – Hash Function field

3.3.6 MAC Function (MF)

This field identifies the MAC function used with the keys of the chain. It is interpreted as follows:

HF value	0	1	2	3
Hash Function	HMAC-SHA-256	CMAC-AES	rsvd	rsvd

Table 10 – MAC Function field

3.3.7 Key Size (KS)

This field identifies the size of the keys of the chain. It is interpreted as follows:

KS value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Key Size (bits)	80	82	84	86	88	90	92	94	96	98	100	112	128	256	rsvd	rsvd

Table 11 – Key Size field (size expressed in bits)

3.3.8 MAC Size (MS)

This field defines the degree of truncation of the MACs, according to the following definition:

MS value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
MAC Size (bits)	10	11	12	13	14	15	16	17	18	19	20	30	32	rsvd	rsvd	rsvd

Table 12 – MAC Size field (size expressed in bits)

3.3.9 MACK Offset

This field defines the time offset between MACK sections for different satellite groups.

MACK Offset value	0	1
Meaning	No Offset	Offset

Table 13 – Offsetting field

When set to '0', it means that no offset is configured, i.e. all MACK sections are distributed the same for all satellites. When set to '1', it means that MACK offsetting is configured as per section 5.5.

3.3.10 KROOT WN

This parameter refers to the time associated to the KROOT, referred to Galileo System Time (GST). It provides the Week Number of the time associated to KROOT (T-KROOT). WN is represented in 12 bits as in the Galileo SIS ICD [2].

3.3.11 KROOT DOW

Day of week associated to KROOT. DOW=0 corresponds to Sunday, DOW=1 corresponds to Monday… and DOW=6 corresponds to Saturday. WN and DOW are relative to the GST start epoch which is 0h UTC on Sunday, 22 August 1999 (midnight between 21 and 22 August), as per [2]. The combination of WN-KROOT and DOW-KROOT gives an unambiguous time reference associated to KROOT in the following way: KROOT is the key immediately preceding the first key of the chain whose application time corresponds to the subframe starting at WN, start of DOW (00:00:00). The KROOT is therefore derivable from the first key applicable at this time in just one step. KROOT-WN and KROOT-DOW compose the time associated to KROOT, or KROOT Time. It is provided with 1 day of resolution.

3.3.12 α

This field includes the random pattern to be included in the hashing process of the chain, as per section 5.3.

3.3.13 Digital Signature (DS)

This field includes the digital signature of the DSM-KROOT, as per section 5.1. The DS verification is performed according to the function statically associated by PKID and known by the receiver.

3.3.14 KROOT

Root key associated to KROOT Time, and signed, with the chain information, in the DSM-KROOT. Notice that several KROOTs of the same chain associated to different times can be transmitted by the system during the time the chain is in force, to facilitate the authentication of a TESLA key.

3.3.15 Padding

This field includes padding bits to be added to the DSM in order to fit to a total length multiple of one DSM block. The padding is explained in detail in section 5.1.

3.4 DSM-PKR

The DMS-PKR definition will be provided at a later version of the specification. For the moment, the receiver can assume that it has authentic public keys associated to a known digital signature algorithm and to a given PKID.

4 MACK SECTION

The other section to be transmitted in parallel to the HKROOT will contain the truncated MACs and time-delayed keys. As the HKROOT section consumes 120 bits per subframe, the remaining 480 bits are available for the MACK section. The number of MACK sections in a subframe is provided in the DSM-KROOT (NMACK parameter). 1 to 4 keys are theoretically possible every subframe, although only 1 to 3 are represented in the NMACK field and the most likely values are 2 or 3. MACK sections are identical in format. Each one is composed of several MACs, or tags, each with a 'MAC-Info' field, providing information about the data authenticated. Figure 4 summarises the structure of the MACK section. The different fields are grouped by type: all MAC and MAC-Info sections of a given MACK section are put in a column, the associated key is put in the next column, and so on. The order in which the information is received is given by reading each row from left to right, and then from top to bottom.

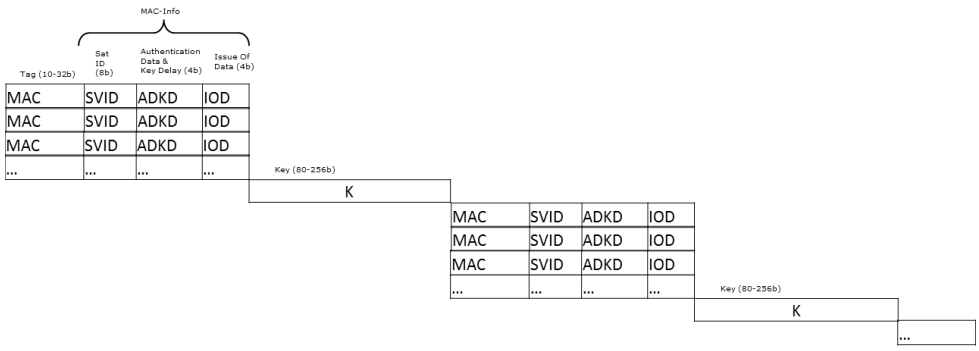

Figure 4 – MACK section structure

By knowing the number of MACK sections per subframe, and the lengths of the MACs and keys also from the DSM-KROOT, the number of MACs per MACK section can be calculated as:

$$n_M = floor\left(\frac{l_{MK} - l_K}{l_M + l_{MI}}\right)$$

Where n_M is the number of MACs per MACK section, l_{MK} is the MACK section length, l_K is the key size, l_M is the MAC size, and l_{MI} is the MAC-Info size. l_{MK}, l_K and l_M are defined in the DSM-KROOT. *floor(A)* is the largest integer no greater than *A*. If the sum of MAC sections, MAC-Info sections and key does not equal the maximum MACK length (120, 160, 240, 480 bits) the spare bits are set to '0' at the end of each MACK section.

The MAC and MAC-Info fields are described in the following subsections

4.1.1 MAC

Truncated MAC (from the MSB), or tag, with the length as defined in the MAC Size field of the DSM-KROOT. Section 5.4 describes the generation and verification of the tag.

4.1.2 MAC-Info

This section contains the fields PRN, Authentication Data & Key Delay (ADKD) and Issue Of Data (IOD), as shown in Table **14**. They identify the data authenticated by the tag.

field	PRN	ADKD	IOD	*total length*
length	8	4	4	*16*

Table 14 – MAC-Info

4.1.2.1 PRN (8 bits)

PRN of the satellite transmitting navigation data which is authenticated. By using 8 bits, up to 255 satellites could be authenticated, which allows for the authentication of satellite data from Galileo and other constellations (mainly GPS but also, GLONASS, Beidou or others) and regional systems as SBAS. The convention proposed for the PRN field is:

- PRN = 0: Do not use the MAC authentication. Check HKROOT for further information.
- PRNs ∈ [1,36]: Galileo PRNs as per Galileo signal specification [2], SV_{ID} field.
- PRNs ∈ [37,72]: GPS PRNs as per GPS signal specification [3], minus 36 (e.g. PRN 37 is GPS PRN 1)
- PRN ∈ [73,108]: GLONASS authentication, reserved for future implementation, (GLONASS satellite numbers as per GLONASS ICD [4], minus 72. E.g. PRN 73 is GLONASS PRN 1).
- PRN ∈ [109,144]: BDS authentication, reserved for future implementation (MEO PRNs as per Beidou ICD [5], minus 108. E.g. PRN 109 is Beidou PRN 1).

- PRN ∈ [144,162]: SBAS authentication, reserved for future implementation TBC (SBAS GEO PRNs, as per SBAS MOPS [6], minus 24. E.g. PRN 144 is SBAS MOPS PRN 120).
- PRN ∈ [163,251]: reserved.
- PRN = 252: Reserved for future implementation (general BEIDOU constellation information that does not relate specifically to a satellite).
- PRN = 253: Reserved for future implementation (general GLONASS constellation information that does not relate specifically to a satellite).
- PRN = 254: General GPS constellation information that does not relate specifically to a satellite.
- PRN = 255: General Galileo constellation information that does not relate specifically to a satellite.

4.1.2.2 Authentication Data & Key Delay (4 bits)

This field describes the signed navigation data, as per the below table. It also describes, in the case of the *SLMAC* ("Slow MAC") values, the time between the MAC and the associated key transmission.

ADKD	Definition
0	Eph, Clk & Health
1	SAR / GPS LNAV Iono
2	Galileo Subframe
3	Almanac
4	GST-UTC & GST-GPS
5	Other NAV Msg
6	Rsvd
7	Rsvd
8	Rsvd
9	Rsvd
10	Rsvd
11	SLMAC, Eph, Clk & Health, 1-subframe delay (30s)
12	SLMAC, Eph, Clk & Health, 6-subframes delay (5 min)
13	Rsvd
14	Rsvd
15	Rsvd

Table 15 – ADKD parameter proposed definition

Table 16 below interprets ADKD values for Galileo and GPS. ADKDs for other global or regional systems are left for future implementation at the moment.

ADKD	Galileo (PRN 1-36)	GPS (PRN 37-72)
'0'	Words 1-5 of [2]: the MAC authenticates the bits of the fields related to the Ephemeris (1/4), (2/4), (3/4), SIS, Ephemeris (4/4), Clock Correction, Ionospheric Correction, BGD(E1,E5a),BGD(E1,E5b), $E5b_{HS}$, $E1B_{HS}$, $E5b_{DVS}$, $E1B_{DVB}$, of the given satellite	Eph, Clk & Health: In case of a GPS satellite, it refers to the bits transmitted in the GPS L1 C/A signal (LNAV) for SV accuracy (URA Index), SV health, clock corrections and ephemeris parameters [9]. This data is included in 6-seconds subframes 1, 2 and 3 of a GPS L1 C/A

	(PRN/SV_{ID}) and IODnav. Reserved/Spare bits and GST are not included[2].	30-second frame. It does not include the TLM/HOW words (words 1-2) but only words 3 to 10 of subframes 1 to 3 (including parity bits).
'1'	*For future implementation.* SAR. This MAC authenticates the 22-bit SAR fields transmitted in the E1-B I/NAV pages of the previous subframe. It is meant to be transmitted only when the RLSP carries information.	For GPS, the MAC authenticates the most recent ionospheric model information as transmitted in Subframe 4, page 18 (α_{0-3}, β_{0-3}).
'2'	Subframe: the MAC authenticates the bits of the 128-bit word data of the 15 pages of the last full subframe. It does not include fields outside the word data, as 'page type', SAR, CRC, 'Reserved 1', 'Reserved 2' or spare.	Frame: the MAC authenticates the bits of the last full GPS 30-s frame (subframes 1 to 5, all words per subframe). It authenticates the 150 bits of the five 10-Word subframes of the GPS LNAV, as per [3].
'3'	Almanac: the MAC authenticates the full almanac identified by IODa. It includes WN_a and t_{0a} bits before the remaining parameters as transmitted in WT7. Associated PRN value is 255.	*For future implementation.*
'4'	GST-UTC conversion parameters (WT6), TOW (WT6) and GST-GPS (WT10) authenticated as per the last WT6 and WT10 transmitted in the E1-B I/NAV. Associated PRN value is 255.	*For future implementation.*
'5'	Gal F/NAV: the MAC authenticates the F/NAV page 1 to 4, excluding GST, spare, CRC and tail bits.	*For future implementation.* (GPS CNAV)
'11' to '12'	To relax the synchronization requirement in the receiver, MACs validated with a key transmitted some time later, or "slow MACs", can be transmitted. For example, if ADKD field is 12, the receiver will get the key associated to that MAC exactly with 6 subframes (5 minutes) delay in addition to the delay with which it would have received it in normal conditions.	N/A

Table 16 – ADKD interpretation for Galileo and GPS

4.1.2.3 Issue-Of-Data (4 bits)

Identification of the Issue Of Data of the authenticated information. It is interpreted in Table 17 as follows, for different ADKDs:

[2] Note that the GST in WT5, which should be common to all satellites, is authenticated by authenticating any TESLA key, as a TESLA key used to authenticate the navigation must be related to the correct GST. The same occurs with GPS Time in GPS navigation authentication, which holds a constant and deterministic relationship (aside from GGTO, which can be estimated or authenticated from ADKD='4'.

ADKD	Galileo (PRN 1-36)	GPS (PRN 37-72)
'0'	The first bit is '1' when the data authenticated is new, and '0' otherwise. This can happen because there is a new IODnav, or because the WT5 authenticated information has changed. The WT5 authenticated corresponds to the last one transmitted in the I/NAV E1-B. The following 3 bits are the LSB-truncated IODnav bits. Note that GST (WN, TOW) changes on every page, but this is not considered new data and thus not triggering the flag, as it is not part of the signed plain text.	The first bit is '1' when the data authenticated is new, and '0' otherwise. The following 3 bits are the LSB-truncated IODe bits. The IODC of the authenticated clock corrections is that of the clock corrections transmitted with the last IODE.
'1'	For future implementation.	N/A. Set to zero.
'2'	N/A. Set to zero.	N/A. Set to zero.
'3'	The first bit is '1' when the data authenticated is new, and '0' otherwise. The following 3 bits are the LSB-truncated IODa bits.	For future implementation.
'4'	N/A. Set to zero.	N/A. Set to zero.
'5'	The first bit is '1' when the data authenticated is new, and '0' otherwise. This can happen because there is a new IODnav, or because the GST-UTC or GST-GPS information has changed, or the SIS flags have changed. The following 3 bits are the LSB-truncated IODnav bits. Note that TOW changes on every page, but this is not considered new data and thus not triggering the flag.	For future implementation.
'11' to '12'	Same as ADKD='0'.	N/A. Not transmitted.

Table 17 – IOD interpretation as per ADKD and PRN (Gal/GPS)

4.1.3 Key

This field contains the TESLA chain key. The position in the chain depends on the satellite PRN and time as defined in section 5.3.

5 RECEIVER CRYPTOGRAPHIC OPERATIONS

This section describes the cryptographic operations to be implemented for OSNMA. Cryptographic operations are divided in the following categories:

- DSM-KROOT, comprising the reception and verification of a root key.
- DSM-PKR, comprising the reception and verification of a new public key.
- Key verification, comprising the verification of a TESLA key with a root key.

- MAC verification, comprising the navigation data authentication.

5.1 DSM-KROOT

The signature is produced by concatenating the fields described below where MSB is represented to the left, and verifying a digital signature with the public key in the possession of the receiver. The public key to be used is identified by the *Public Key ID* field. The message *M* to be signed is:

$$M = (NMA\_Header \,||\, CIDKR \,||\, NMACK \,||\, HF \,||\, MF \,||\, KS \,||\, MS \,||\, MO \,||\, KROOT\ WN \,||\, KROOT\ DOW \,||\, \alpha \,||\, KROOT)$$

Where

- (X || Y) concatenates bitset X to bitset Y bits, with X at the MSB
- *NMA_Header* correspond to the 8-bit NMA Header as per 3.1 (I/NAV Word 1), transmitted in parallel to the DSM-KROOT;
- The rest of the fields are described in section 3.3.

Note that the message is composed by the bit values as received in the OSNMA message fields, and not by their meaning (e.g. the *KS* bits to be authenticated for an 80-bit key will be "0000").

Following the KROOT parameters, the digital signature S is transmitted.

$$S = signature(M)$$

The algorithm proposed for the digital signature is ECDSA [7], supporting the following signature lengths: 448, 512, 768 or 1042 (key lengths 224, 256, 384 and 521 respectively) and the curves P-224, P-256, P-384, and P-521. These parameters are statically and univocally associated to the *Public Key ID*. In addition to the signature S, the Padding field (*T*) is added as follows:

$$T = trunc_L\,(hash(M \,||\, S))$$

$$L = (104 \cdot B) - M - S$$

Where T is the Padding field as per 3.3; the function $trunc_L$ retains the L MSBs of the input; *hash* is SHA-256 irrespective of the signature scheme or length; and B is the *Nb. of Blocks* as defined by 3.3.1. Note that B is the smallest value such that L>=0, i.e. the NMA message will use the minimum number of blocks to transmit a given DSM.

5.2 DSM-PKR

The DMS-PKR definition will be provided at a later version of the specification. For the moment, the receiver can assume that it has authentic public keys associated to a known digital signature algorithm and to a given PKID.

5.3 TESLA Key generation and verification

The TESLA chain starts with a random seed key K_n, which is secret and only known by the OSNMA provider, and ends with a root key K_0 that is public and certified through the DSM-KROOT. K_n and K_0 relate as follows:

$$K_0 = F^n(K_n)$$

Where F^n means recursively applying n times the function F, so each element of the chain can be constructed by applying F to the previous element. The key K_n is a 256-bit random number truncated by removing the LSBs to the Key Size (l_k below) as defined in 3.3.5. The function F is applied for iteration m as follows:

$$K_m = F(K_{m+1}) = trunc(l_k, hash(K_{m+1} \,||\, GST_{SF} \,||\, \alpha))$$

where K_m is the key to be generated from K_{m+1}, the previous key in the chain; *trunc(n,p)* is the truncation function whereby the message p is truncated to the n MSB; l_k is the chain key size as per 3.3.5; *hash* is the selected hash function as per HF field in 3.3.5; and α is the unpredictable chain pattern defined in 3.3.12. GST_{SF} is the Galileo System Time of the start of the 30 second interval from GST 00:00:00 in which the sub-frame in which the key will be applied begins transmission. For E1, this is the sub-frame start time minus 1 second. It is a 32-bit number with the number of seconds since GST start epoch. The start epoch is defined in [2]. The format is not the standard GST format used in [2], but an integer number of seconds. Figure 5 presents how the TESLA keys are assigned in time and transmitter and how they relate to each other.

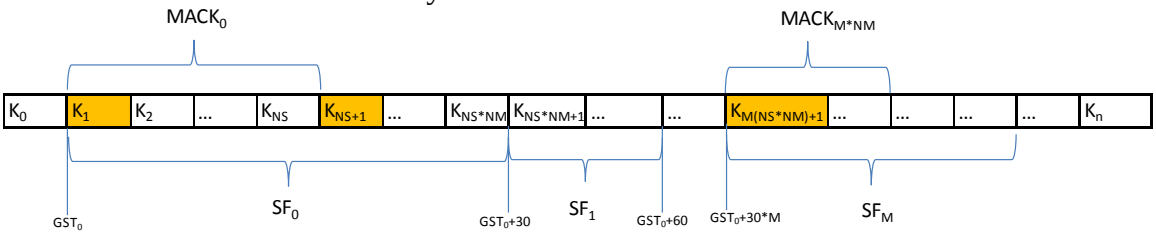

Figure 5 –TESLA one-way chain with different keys from different senders

The key generator must produce NS·NMACK keys per subframe (NMACK is referred to as NM in the figure), where NS stands for the number of satellites. The first key of a MACK section (e.g. K_1, K_{NS+1}, $K_{M(NS*NM)+1}$) is the key used to generate all the MACs transmitted in that MACK section, except for the SLMAC case, and the case when MACK Offset = 1, detailed below. It will also be transmitted by PRN 1, while the following (K_2, K_{NS+2}, $K_{M(NS*NM)+2}$…) by PRN2, and so on. NS = 36 although for testing purposes it should be configurable, as per section 6.11. The GST_{SF} used in F can be computed as follows:

$$GST_{SF} = GST_0 + 30 \cdot floor(\frac{m}{NS \cdot NMACK})$$

Where GST_0 is the start time of the chain, m is the chain link position, NS is the number of keys per MACK section, $NMACK$ is the total number of MACK Sections per subframe, and *floor(A)* is the largest integer no greater than A. Note that the key index decrements from the seed value down to 1, which is the first key that will be used. To provide a trusted root for the entire chain, the key chain must be continued to K_0, as this is the key that is signed when a new chain is disseminated. Note for evaluating K_0, $GST_{SF} = GST_0 - 30$ seconds, where GST_0 is the start time associated with the chain.

Note that when a new chain root is disseminated prior to the entry into force of that chain from GST_0 a signed root must be sent that will never be used for MAC production. It is nominally the last key from the preceding time-slice ($GST_0 - 30$), though it would never

have been used then as that is before the applicability of the chain. For simplicity, all intermediate roots that are signed and transmitted via a DSM-KROOT (after their applicability has passed) will conform to the same model, so the time of applicability associated with the intermediate key will be the time of applicability of the first key after the one that is sent. This means that a receiver can use the exact same algorithm to validate a key against a signature irrespective of whether it is a root key of a new chain.

Several hash functions are defined in HF field. SHA-2 family hashes (SHA-256) are defined in the latest FIPS publication (FIPS PUB 180-4) [8]. SHA-3 family is implemented according to the Keccak algorithm [9]. This field provides some reserved values for future standard hash functions that may be standardised.

5.4 Tag verification

Tags are generated and verified in the following way.

$$m = (PRN\_N \,||\, PRN\_A \,||\, GST_{SF} \,||\, CTR \,||\, NMA\_Status\_Header \,||\, navdata)$$

$$tag = trunc(n, mac(K,m))$$

Where

- *m* is the message to be authenticated
- *PRN_N* is the satellite ID *being authenticated* as defined in the MAC-info section, PRN field.
- *PRN_A* is the satellite ID *providing authentication* as defined in the MAC-info section, PRN field (it can only be a Galileo satellite).
- GST_{SF} is the Galileo system time (seconds), as per [2], of the start of the thirty second cycle in which the subframe starts in which the MAC is due to be transmitted, not accounting for offsetting delays. For transmission in E1 this is the sub-frame start time minus 1 second.
- *CTR* is an 8-bit unsigned integer identifying position of the MAC within a single MAC-K Section; it has a value of '1' for the MAC at the MSB, incrementing by one for each subsequent MAC towards the LSB of that section
- *NMA_Status_Header* is the NMA Status field in the NMA Header transmitted in the current subframe.
- *navdata* is the navigation data authenticated as defined in the MAC-info section, ADKD field.
- *tag* is the truncated message authentication code transmitted in the signal.
- *trunc(n,p)* is the truncation function whereby the message p is truncated to the n MSB.
- *n* is the truncated MAC length for the chain in force, as defined in the DSM.
- *mac* is the MAC function used for the chain in force, as defined in the DSM.
- *K* is the key from the one-way chain used for the MAC.

Note that the combination of *PRN_A*, *CTR* and *K* are unique for each MAC generated during the system lifetime. An attacker cannot replace a valid MAC by a previously

transmitted valid MAC, without being noticed. Note also that the signal transmission time is authenticated just by ensuring the authenticity of a key vs the KROOT: if a key of a certain subframe is authenticated using the TOW of that subframe, the TOW must be authentic too as otherwise the key verification process would not lead to the KROOT.

Concerning the MAC types, HMAC-SHA-256 is standardized in [10] and in [11]. CMAC-AES is standardized as Algorithm 5 in [12], and in [13].

In order to perform the message authentication, a tag has to be stored and compared with the one re-generated according to the MAC-Info section once a valid key is received and the data is available.

5.5 MACK Offsetting

The key allocation described above corresponds to the case with no MACK Offsetting (i.e. Offsetting = '0' in DSM-KROOT). However, when configured, satellites can have an offset to relate its 30 second MACK cycle to the E1-B 30 second sub-frame.

The offset values per PRN are defined in the Offsetting parameter, section 3.3.9. When the field is set to '1', PRNs 1 to 15 will have a zero offset and will use the key transmitted by PRN=1 for the MACs, and setting PRNs 16 and above to use *the key transmitted by PRN=16 for the MACs,* and have an offset defined as follows:

$$\Delta = round(\frac{15}{2 \cdot NMACK})$$

Where Δ is the offset, in number of I/NAV pages (1 page = 2 seconds), *round(A)* is the closest integer to *A* (the lowest in case two integers are the same close), and *NMACK* is the number of MACK sections in a subframe. For example, if *NMACK* = 2, Δ = 4 (8 seconds), and if *NMACK* = 3, Δ = 2 (4 seconds).

6 GUIDELINES FOR IMPLEMENTATION AND TESTING

This section provides some guidelines for OSNMA implementation and testing, including some details on how the OSNMA information is transmitted, to complement the previous sections. These guidelines are not-exhaustive.

6.1 DSM reception

This section provides some guidelines for the reception and processing of the DSM:

- DSM blocks are transmitted by the connected Galileo satellites, and blocks of the same DSM ID are scattered across different satellites. The receiver must be able to store DSM blocks non-sequentially, and from different satellites, until the full DSM is received.
- Two DSM IDs can be transmitted in parallel, e.g. when the Chain Status is set to EOC and a new chain will enter into force soon. Therefore the receiver must be able to store and build several DSMs in parallel.
- If the transmission of a DSM is interrupted, the receiver must delete DSM blocks associated to incomplete DSM IDs after a maximum of 1 hour.

- During the transmission of a DSM, the NMA Header shall not change. If the NMA Header changes, a new DSM will start to be transmitted.

6.2 Use of floating KROOTs

During the time a chain is in force, the distance between the root key K_0 and the transmitted keys K_m can increase to a point where the CPU consumption in the receiver may be too high. To avoid that, the receiver should replace the root key K_0 by an already authenticated key K_m in the chain from the MACK section, and use K_m to authenticate the subsequent keys.

DSM-KROOTs associated to past, but more recent keys than the initial K_0, or *floating KROOTs*, will be regularly transmitted in the HKROOT section, to facilitate the key authentication process for receivers that switch on in the middle of a TESLA chain.

6.3 Chain renewal

This section presents the TESLA key chain renewal process. It is depicted in Figure 6 and comprised by the following steps:

- **Step 1**: The Chain Status goes from Nominal to EOC, reporting that the chain in force (CID = i) is coming to an end. Receivers can process a new DSM-KROOT for the new chain (CID = i+1); note that, in general, CIDs will follow a sequential order, (mod 4, as per section 3.1.3). During this step, the DSM transmission alternates a new DSM-KROOT of the chain currently in force (as the NMA header, which is authenticated, changes), with another new DSM-KROOT with the root key of the next chain. The time associated to the KROOT sets the new chain start time.
- **Step 2**: At the transition time, the receiver switches to the new chain. The Chain Status goes from EOC back to Nominal, the CID is updated in the NMA Header to reflect the new chain, and the DSM transmits only KROOTs for the new chain. Once the CID is updated in the NMA Header, the previous chain (CID=i) can be considered as expired.

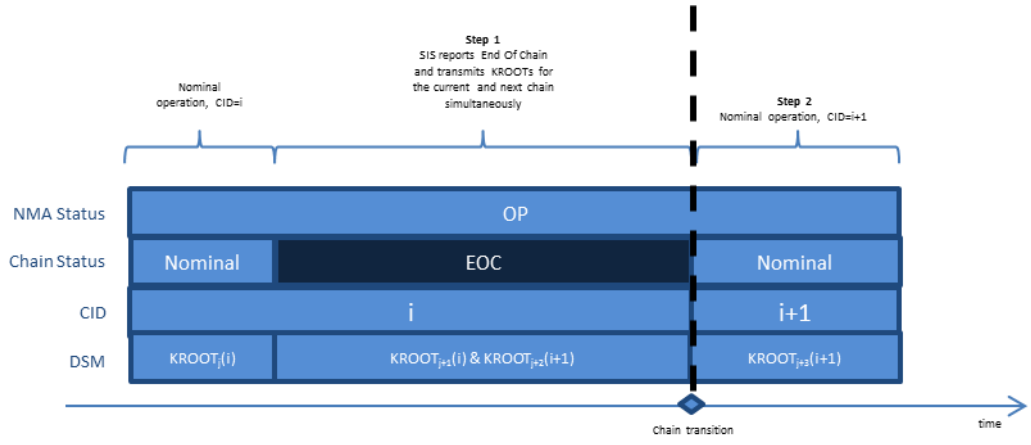

Figure 6 – OSNMA Chain Renewal

6.4 Chain revocation

This section presents the TESLA key chain revocation process. It is depicted in Figure 7 and comprised by the following steps:

- **Step 1**: The OSNMA Header reports that the chain in use (CID=i) is revoked. The system starts transmitting a DSM-KROOT with the KROOT of a new chain (CID=i+1). During this time, the OSNMA Status is set to "Don't Use" and the Chain Status is set to "CREV".
- **Step 2**: After the KROOT for a new chain (CID=i+1) is transmitted and the new chain enters into force, the NMA Status is back to "Operational". Due to the change in header, a new DSM-KROOT is required. During step, the Chain Status field is still set to "CREV", to report (in combination with NMA Status = "Operational") that a previous chain has been revoked.
- **Step 3**: The Chain status is back to nominal.

Note that chain revocation process is expected to occur very seldom, if at all. Note also that, in all cases, the applicability of a new chain is defined by the CID field in the NMA Header. In the case of chain revocation, the KROOT may relate to a time before the chain becomes applicable (notice that the KROOT time currently has a 1-day resolution). While the CID change and KROOT time are foreseen to coincide in the case of a nominal key transition, this may not be the case in the key revocation process. In this case, the KROOT of a new chain may be associated to a time in the past, in which case the receiver must perform the required number of chain steps as soon as the new chain is in force.

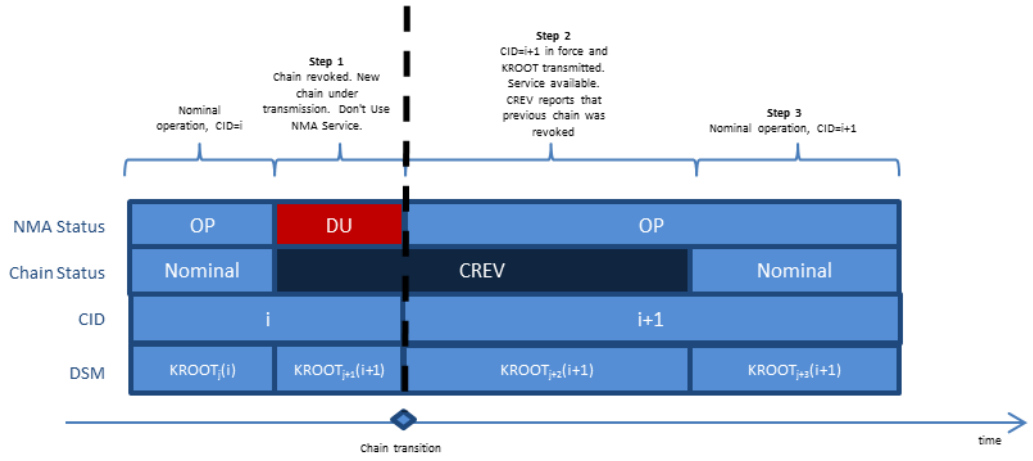

Figure 7 – OSNMA Chain Revocation

6.5 Public Key renewal and revocation

The DMS-PKR definition will be provided at a later version of the specification. For the moment, the receiver can assume that it has authentic public keys associated to a known digital signature algorithm and to a given PKID.

6.6 Chain cryptoperiods and lengths

The crypto periods of the proposed scheme must protect against two attack models: online and offline. The online adversary tries to find a value that can be hashed in L steps to last released key. Finding such a value is sufficient to feed the user with false navigation data for L/NS MACK sections. The offline adversary wishes to feed the user with false navigation data during L/NS MACK sections starting in a future yet predetermined MACK section. The adversary then precomputes some chains, hoping that when the time comes, the endpoint of one of them will match the released key.

Taking these attack models into account, the proposed chain key sizes provide sufficient security margins against both types of adversaries. It is recommended that the chain be replaced after releasing 2^{25} to 2^{26} keys, thus further thwarting the offline attack. For example, using 82-bit keys, NS=36 and 3 MACK sections per subframe, a chain crypto period of around 4 months can be allowed.

The crypto algorithms, their parameters, and the cryptoperiods should be reevaluated once a year, taking into account changes in standards, improvement of cryptanalytic techniques, and decrease in hardware costs. As future changes in those are indeed foreseeable, it is recommended to include tests for different parameters in the test period.

6.7 Processing the OSNMA field

The OSNMA 40-bit field is filled in only for satellites connected to the Galileo ground segment. The maximum current system capacity for ground connection is 20, so out of the 24 satellites nominally composing the Galileo constellation, only a maximum of 20 will be transmitting OSNMA. As the uplink antennas will switch between satellites, the transmission of OSNMA information may be interrupted at any time. When a satellite is not connected to ground and therefore not transmitting OSNMA, the OSNMA field will be set to 40-zeros. As the NMA Status flag cannot have a "0" value, a receiver decoding a NMA Status of "0" (00b) shall interpret that the satellite is not connected and not transmitting NMA.

6.8 Use of I/NAV Page CRC and tag accumulation

Using OSNMA information only from words with a correct CRC result may lead to discarding correct OSNMA information and therefore decrease availability. A receiver can replace the use of the CRC by the OSNMA, as long as it discriminates between bad reception conditions and spoofing alerts. Different strategies may be implemented in the receiver depending on the use case and OSNMA information:

- Regarding the reception of the keys in the MACK section, the I/NAV CRC verification of the pages including the key can be replaced by the key verification with a previous key of the chain.
- Regarding the MAC & MAC-Info section, which will always be transmitted in 1 or 2 pages, the receiver can use the CRC verification of the related pages or replace it by the authentication verification.
- Regarding the navigation data, the receiver can follow the standard navigation reception process, including the I/NAV CRC verification, or use the authentication check.
- Regarding the HKROOT, the receiver may use the I/NAV CRC to ensure that an HKROOT byte in an I/NAV page is properly received. For example, once DSM ID and BID are properly obtained from the DSM Header (I/NAV page 2), a receiver can accumulate 1-byte sub-blocks from CRC-valid pages, of the same DSM ID and Block ID, as it does with the I/NAV message, if reception conditions prevent continuously receive a Block ID from the same transmitter.

If a given chain is transmitting highly truncated tags (down to 10-bits) and the receiver application requires to reduce the probability that a false tag and/or false key and/or false navigation lead to a successful verification beyond that provided by a single tag, the

receiver can accumulate more than one tag for the same satellite. This may not have a high impact in the time to authenticate, as several tens of tags can be received in a subframe, and the tags will mostly authenticate satellites visible by the receiver.

6.9 Management of different IODnav between I/NAV Words and OSNMA

Even if the OSNMA information will be generated with a latency of some seconds, the IODnav transmitted in the I/NAV message in E1-B (Words 1,2,3,4), once completed, will correspond, in nominal operation, with the IODnav authenticated by the tags transmitted at the same time, even when a new IODnav is transmitted. However, in some cases, the receiver may dispose of different IODnavs for navigation and OSNMA. For example, a receiver may be switched on in cold/warm start, receive the authentication of a new IODnav, but take some more subframes to decode the WT-1-4. In these cases, the NMA-PVT must be based on the last authenticated IODnav, as long as it is still valid according to [2].

6.10 Protection against replay attacks

This specification covers NMA only. Protection against replay attacks is subject to receiver implementations and therefore out of the scope of this specification. Nevertheless, it can use the unpredictable symbols encoding the NMA message.

6.11 Configurable parameters and guidelines for SIS testing

Many parameters are configurable as part of the operational specification, in order to cope with changes over the lifetime of the service. In addition, there are some parameters that should be fixed in the operational specification but must be configurable in both the OSNMA data generator and the OSNMA test receivers during the SIS OSNMA transmissions, and others which can be configurable in the final specification but can be fixed for testing purposes:

- NS (Number of Satellites), described in section 5.3, must be set by default to 36, but it must be configurable between 1 and 36. When NS is lower than the number of satellites in the test, keys will be repeated as necessary (e.g. if NS=4, the keys will be repeated as follows: [PRN=1 -> K_1; PRN=2 -> K_2… PRN=4 -> K_4; PRN=5->K_1…].
- The MACK sections between a tag and its associated key (do not confound with the MACK offset) must be configurable between 1 and 0 and set to '0' by default (i.e. the tag and associated key are transmitted in the same MACK). A value of '1' implies that a tag will be authenticated with a key broadcast in the *next* MACK section.
- The crypto functions implemented can be reduced to those allowing the proof of concept, provided that the non-implemented functions will provide similar results.
- The mask of authenticated bits for each ADKD should be configurable in the receiver implementation, allowing to modify it if needed.
- MACK offsetting (as per section 5.5) is recommended to be configurable on a per-satellite basis, (i.e. each satellite must have an offset in transmitting the MACK section, allowing the configuration described in section 5.5, which is the one by default when MACK Offset is '1', but also other configurations.

ANNEX A – LIST OF ACRONYMS

ADKD	Authentication Data & Key Delay
AGC	Automatic Gain Control
α_S	αSize
BGD	Broadcast Group Delay
C/N_0	Carrier to Noise ratio
CID	Chain ID
CRC	Cyclic Redundancy Check
CREV	Chain Revocation
CTR	Counter
DS	Digital Signature
DSID	Digital Signature ID
DSM	Digital Signature Message
DSMH	Digital Signature Message Header
DVS	Data Validity Status
DSM BID	Digital Signature Message - Block ID
EDBS	External Data Broadcast Service
EOC	End of Chain
GPS	Global Positioning System
GST	Galileo System Time
HF	Hash Function
HKROOT	Header and KROOT
HS	Health Status
ICD	Interface Control Document
IOD	Issue Of Data
IODC	Issue Of Data - Clock
IODE	Issue Of Data – Ephemeris
IRNSS	Indian Radio Navigation Satellite System
KROOT	Root key
KS	Key Size
LSB	Least Significant Bit
MAC	Message Authentication Code
MACK	MAC & Key (section)
MF	MAC Function
MS	MAC Size
MSB	Most Significant Bit
n/a	Not Applicable
NB	Number of Blocks
NS	Number of Satellites
MOPS	Minimum Operational Performance Standards
NMACK	Number of MACK Sections
OS	Open Service
OSNMA	Open Service Navigation Message Authentication
PK	Public Key
PKID	Public Key ID
PKR	Public Key Renewal
PRN	Pseudo Random Noise
RFI	Radio Frequency Interference

RLSP	Return Link Service Provider
rsvd	Reserved
SAR	Search and Rescue
SBAS	Satellite-Based Augmentation Systems
SHA	Secure Hash Algorithm
SIS	Signal In Space
SISA	Signal-In-Space Accuracy
SVID	Space Vehicle ID
TLM/HOW	Telemetry/Handover Word
TOW	Time Of Week
TS	Trusted Server
URA	User Range Accuracy
WN	Week Number

ANNEX B – BIBLIOGRAPHY

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

[2] European Union, "OSSISICD: Open Service Signal In Space Interface Control Document, Issue 1.2," 2015.

[3] The US Government, "GPS Interface Specification IS-GPS-200," 2014.

[4] Russian Institute of Space Device Engineering, "Glonass Interface Control Document - Navigational Radiosignal In Bands L1, L2 (Edition 5.1)," 2008.

[5] China Satellite Navigation Office, "BeiDou Navigation Satellite System Signal In Space - Interface Control Document - Open Service Signal B1I (Version 1.0)," 2012.

[6] RTCA SC-159, "MINIMUM OPERATIONAL PERFORMANCE STANDARDS FOR GLOBAL POSITIONING SYSTEMIWIDE AREA AUGMENTATION SYSTEM AIRBORNE EQUIPMENT - DO229D (with Change 1, Feb 2013)," 2006.

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

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

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

[10] H. Krawczyk, M. Bellare and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," *Network Working Group*, 1997.

[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 for Authentication," 2004.

End of the Document

Corrigendum for Galileo Navigation Message Authentication Specification for Signal-In-Space Testing – v1.0

- page 10, sect. 3.3.3, replace *"(section 3.1.2)"* with *"(section 3.1.3)"*.

- page 12, Figure 4, replace *"SVID"* with *"PRN"*.

- pages 14-15, Tables 15 and 16, replace *"6 subframes"* with *"10 subframes"*.

- page 14, Table 16, second row, second column. Replace *"SIS"* with *"SISA"* and *"$E1B_{DVB}$"* by *"$E1B_{DVS}$"*.

- page 14, Table 16, second row, third column, replace *"[9]"* with *"[3]"*.

- page 15, Table 16, fourth row, second column, replace description of ADKD '2' for Galileo with *"Subframe: the MAC authenticates the bits* ***of the 'Page Type' and the*** *128-bit word data* ***of the I/NAV nominal page (or the 192-bit word data in case I/NAV Dummy Page)*** *of the 15 pages of the last full subframe. It does not include the fields SAR, CRC, 'Reserved 1', 'Reserved 2' or spare"*.

- page 15, Table 16, fourth row, third column, replace description of ADKD '2' for GPS with *"Frame: the MAC authenticates the bits of the last full GPS 30-s frame (subframes 1 to 5, all words per subframe) LNAV, as per [3].* ***Parity bits are excluded.*** *All other bits are included"*.

- page 17, sect. 5.1, replace *"M"* with *"length(M)"* and *"S"* with *"length(S)"* in the formula *"$L = (104 \cdot B) – M – S$"*.

- page 18, sect. 5.3, replace *"as defined in 3.3.5"* and *"as per 3.3.5"* with *"as defined in 3.3.7"* and *"as per 3.3.7"*, respectively.

- page 19, sect. 5.4, replace *"PRN_A is the satellite ID providing authentication as defined in the MAC-info section"* by *" PRN_A is the satellite ID providing authentication"*.

- page 23, sect. 6.7. The following sentence: *"As the NMA Status flag (…) not transmitting NMA."* is removed.

- page 24, sect. 6.11. The following paragraph: *"MACK offsetting (…) but also other configurations."* is removed.