Configuring and verifying OSNMA using u-center

OSNMA configuration and verification for generation-9 receivers

Application note

Abstract

This document explains how to configure the u-blox receiver to verify the OSNMA feature for GALILEO constellation.

Document information

Title	Configuring and verifying OSNMA using u-center	
Subtitle	OSNMA configuration and verification for generation-9 receivers	
Document type	Application note	
Document number	UBXDOC-963802114-12194	
Revision and date	R03	10-Mar-2025
Disclosure restriction	C1-Public	

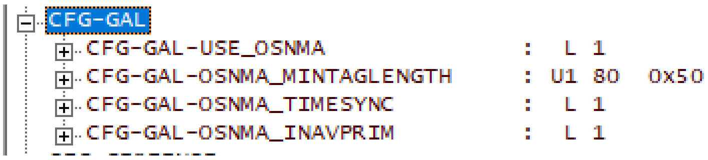
Contents

1 Overview

Selected u-blox receivers support the evaluation of the new GALILEO Open Service Navigation Message Authentication (OSNMA) feature. OSNMA is a data authentication function for Galileo Open Service that provides receivers with the assurance that the received Galileo navigation message comes from the system itself and has not been modified. This application note provides information on providing OSNMA assistance to the receiver and verifying the OSNMA feature using u-center v24.02 and greater.

2 Configuring OSNMA feature

The Galileo OSNMA protocol is configured using the CFG-GAL configuration items as shown in Figure 1. For more information about the configuration items, refer to the applicable Interface description.



```
CFG-GAL
   CFG-GAL-USE_OSNMA                : L 1
   CFG-GAL-OSNMA_MINTAGLENGTH       : U1 80  0x50
   CFG-GAL-OSNMA_TIMESYNC           : L 1
   CFG-GAL-OSNMA_INAVPRIM           : L 1
```

Figure 1: CFG-GAL configuration items for OSNMA protocol.

Table 1 lists the UBX-MGA assistance messages which can be used to provide key and time information to the firmware. Table 1 also includes the CFG-NAVSPG configuration items for additional OSNMA configuration.

Input assistance message	Description
UBX-MGA-GAL-OSNMA_MERKLE	Allows to provide Merkle tree root assistance for OSNMA service
UBX-MGA-GAL-OSNMA_PUBKEY	Allows to provide public key assistance for OSNMA service
UBX-MGA-INI-TIME_UTC	Allows to provide time trusted flag to the UTC time assistance
UBX-MGA-INI-TIME_GNSS	Allows to provide time trusted flag to the GNSS time assistance
CFG-NAVSPG-ONLY_AUTHDATA	When enabled, use signals with authenticated navigation data only
CFG-NAVSPG-MAX_TIMETRUSTED_ACC	Configure max. trusted time accuracy value to perform time authentication

Table 1: Configuration messages for OSNMA service.

2.1 Providing OSNMA assistance

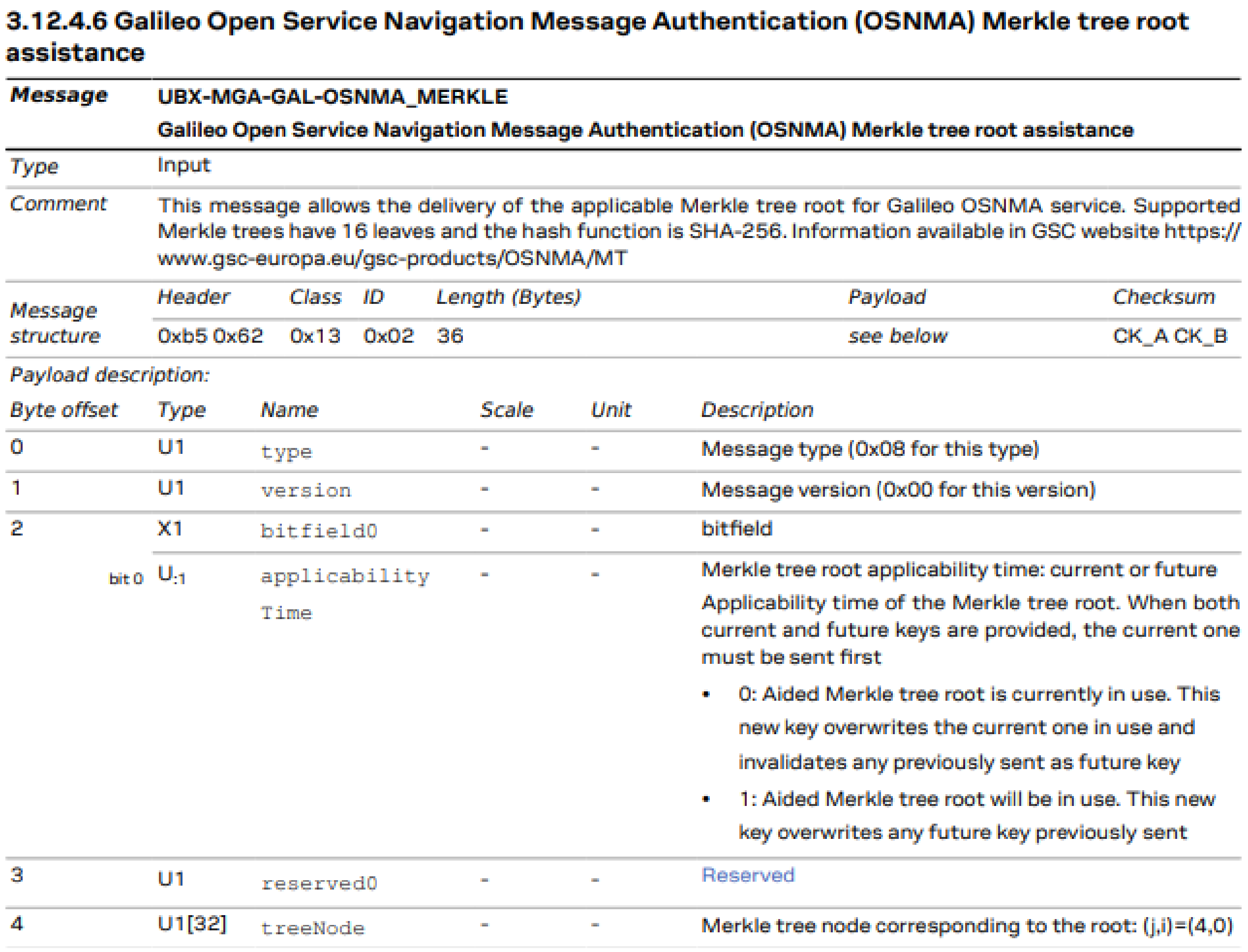
The UBX-MGA OSNMA assistance messages can be sent to the receiver from the UBX message window in the u-center messages view. To send the OSNMA assistance messages, you need the following information.

To download the Public Key and Merkle tree root, register at the European GNSS Service Center (GSC) web portal. Subscribe to the OSNMA products and after that has been confirmed, download the Public Key and Merkle tree xml files from the GSC PRODUCTS menu.

For detailed information, refer to the GSC OSNMA Internet data distribution interface control document [1].

2.1.1 UBX-MGA-GAL-OSNMA_MERKLE

The UBX-MGA-GAL-OSNMA_MERKLE message is explained in Figure 2. For further information, refer to the applicable Interface description.



3.12.4.6 Galileo Open Service Navigation Message Authentication (OSNMA) Merkle tree root assistance

Message	**UBX-MGA-GAL-OSNMA_MERKLE** **Galileo Open Service Navigation Message Authentication (OSNMA) Merkle tree root assistance**
Type	Input
Comment	This message allows the delivery of the applicable Merkle tree root for Galileo OSNMA service. Supported Merkle trees have 16 leaves and the hash function is SHA-256. Information available in GSC website https://www.gsc-europa.eu/gsc-products/OSNMA/MT

Message structure	*Header*	*Class*	*ID*	*Length (Bytes)*	*Payload*	*Checksum*
	0xb5 0x62	0x13	0x02	36	*see below*	CK_A CK_B

Payload description:

Byte offset	*Type*	*Name*	*Scale*	*Unit*	*Description*
0	U1	`type`	-	-	Message type (0x08 for this type)
1	U1	`version`	-	-	Message version (0x00 for this version)
2	X1	`bitfield0`	-	-	bitfield
bit 0	U:1	`applicability Time`	-	-	Merkle tree root applicability time: current or future Applicability time of the Merkle tree root. When both current and future keys are provided, the current one must be sent first • 0: Aided Merkle tree root is currently in use. This new key overwrites the current one in use and invalidates any previously sent as future key • 1: Aided Merkle tree root will be in use. This new key overwrites any future key previously sent
3	U1	`reserved0`	-	-	Reserved
4	U1[32]	`treeNode`	-	-	Merkle tree node corresponding to the root: (j,i)=(4,0)

Figure 2: OSNMA_MERKLE message.

The 32-byte Merkle tree node is available in the Merkle tree xml file downloaded from the GSC OSNMA server. Use the HEX string with tag <x_ji>, corresponding to the Tree node j= 4, i=0

Example:

The Merkle tree node from Merkle tree xml at the time of writing (April 2024) is:

```
<TreeNode>
        <j>4</j>
        <i>0</i>
        <lengthInBits>256</lengthInBits>
        <x_ji>832E15EDE55655EAC6E399A539477B7C034CCE24C3C93FFC904ACD9BF842F04E</x_ji>
</TreeNode>
```

Merkle tree to be provided in the UBX-MGA-GAL-OSNMA MERKLE message window is: *83 2E 15 ED E5 56 55 EA C6 E3 99 A5 39 47 7B 7C 03 4C CE 24 C3 C9 3F FC 90 4A CD 9B F8 42 F0 4E*

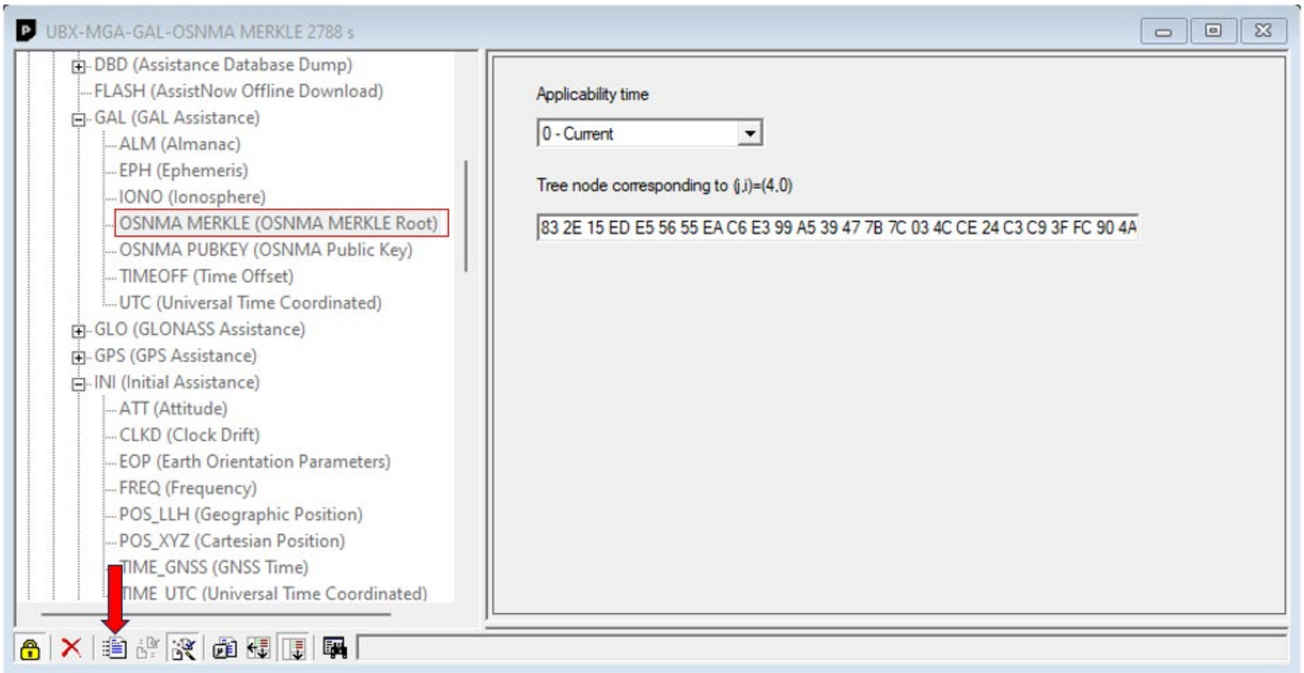
For sending the Merkle tree hex string using the UBX-MGA-GAL-OSNMA MERKLE message window in u-center, see Figure 3

The applicability time of Merkle tree has two options, current and future:

- The future Merkle tree is used only during the Merkle tree renewal process.

- The new Merkle tree will be published in the GSC OSNMA server at least two years before the planned renewal.

For more information, refer to the Merkle tree renewal process section in GSC Signal-in-Space interface control document [1].


UBX-MGA-GAL-OSNMA MERKLE 2788 s
DBD (Assistance Database Dump)
FLASH (AssistNow Offline Download)
GAL (GAL Assistance)
ALM (Almanac)
EPH (Ephemeris)
IONO (Ionosphere)
OSNMA MERKLE (OSNMA MERKLE Root)
OSNMA PUBKEY (OSNMA Public Key)
TIMEOFF (Time Offset)
UTC (Universal Time Coordinated)
GLO (GLONASS Assistance)
GPS (GPS Assistance)
INI (Initial Assistance)
ATT (Attitude)
CLKD (Clock Drift)
EOP (Earth Orientation Parameters)
FREQ (Frequency)
POS_LLH (Geographic Position)
POS_XYZ (Cartesian Position)
TIME_GNSS (GNSS Time)
TIME_UTC (Universal Time Coordinated)

Applicability time

0 - Current

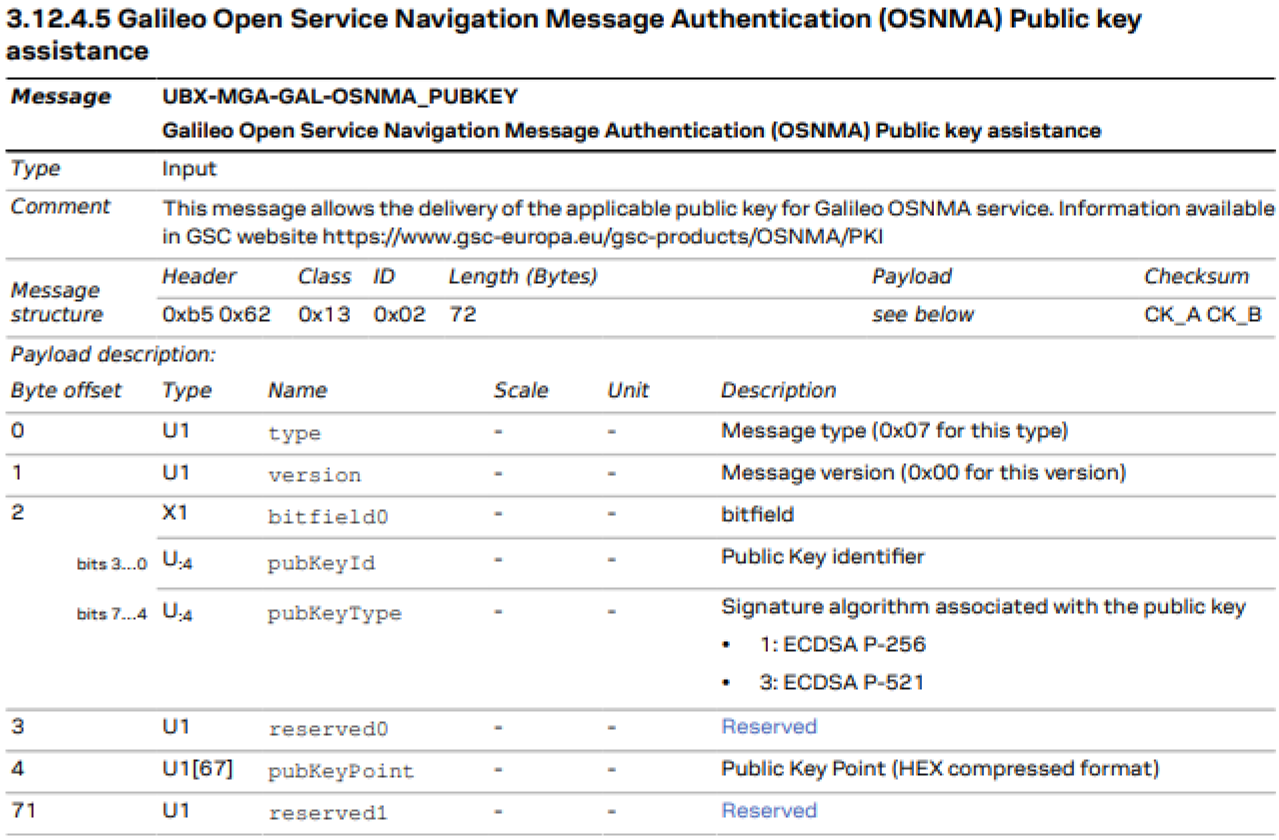
Tree node corresponding to (j,i)=(4,0)

83 2E 15 ED E5 56 55 EA C6 E3 99 A5 39 47 7B 7C 03 4C CE 24 C3 C9 3F FC 90 4A

Figure 3: Sending Merkle tree assistance using UBX-MGA-GAL-OSNMA MERKLE message window in u-center.

2.1.2 UBX-MGA-GAL-OSNMA_PUBKEY

The UBX-MGA-GAL-OSNMA_PUBKEY message is explained in Figure 4. For further information, refer to the applicable Interface description.



3.12.4.5 Galileo Open Service Navigation Message Authentication (OSNMA) Public key assistance

Message	**UBX-MGA-GAL-OSNMA_PUBKEY** **Galileo Open Service Navigation Message Authentication (OSNMA) Public key assistance**						
Type	Input						
Comment	This message allows the delivery of the applicable public key for Galileo OSNMA service. Information available in GSC website https://www.gsc-europa.eu/gsc-products/OSNMA/PKI						
Message structure	*Header*	*Class*	*ID*	*Length (Bytes)*	*Payload*	*Checksum*	
	0xb5 0x62	0x13	0x02	72	*see below*	CK_A CK_B	

Payload description:

Byte offset	*Type*	*Name*	*Scale*	*Unit*	*Description*
0	U1	`type`	-	-	Message type (0x07 for this type)
1	U1	`version`	-	-	Message version (0x00 for this version)
2	X1	`bitfield0`	-	-	bitfield
bits 3...0	U:4	`pubKeyId`	-	-	Public Key identifier
bits 7...4	U:4	`pubKeyType`	-	-	Signature algorithm associated with the public key • 1: ECDSA P-256 • 3: ECDSA P-521
3	U1	`reserved0`	-	-	Reserved
4	U1[67]	`pubKeyPoint`	-	-	Public Key Point (HEX compressed format)
71	U1	`reserved1`	-	-	Reserved

Figure 4: OSNMA_PUBKEY message.

The OSNMA public key is available in the public key xml file downloaded from the GSC OSNMA server. The required fields are explained below:

- Public key ID is available with tag <PKID>
- Public key type is available with tag <PKType> (ECDSA P-256 / ECDSA P-512)
- Public key point is available with tag <point>

Example:

At the time of writing (April 2024), the OSNMA public key from the public key xml file is:

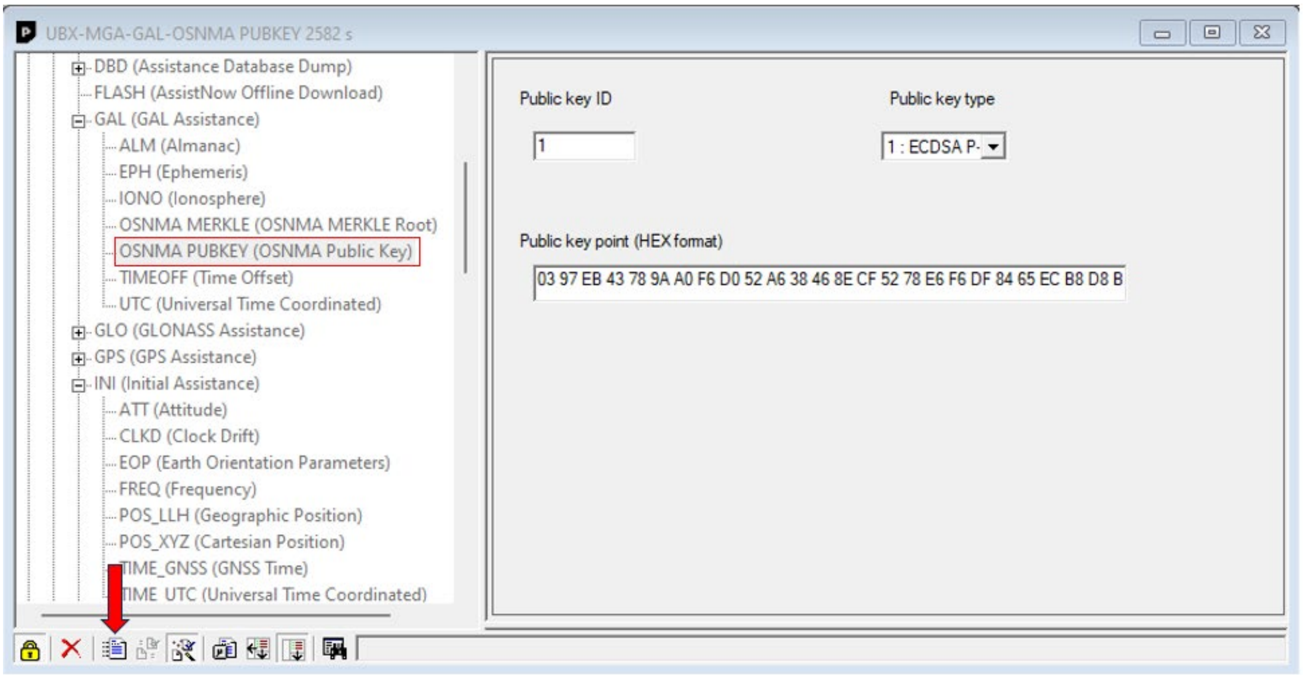
<PKID>1</PKID>

<point>0397EB43789AA0F6D052A638468ECF5278E6F6DF8465ECB8D8B84B8C7A3501F73B</point>

<PKType>ECDSA P-256/SHA-256</PKType>

Public key to be provided in UBX-MGA-GAL-OSNMA PUBKEY message window is: *03 97 EB 43 78 9A A0 F6 D0 52 A6 38 46 8E CF 52 78 E6 F6 DF 84 65 EC B8 D8 B8 4B 8C 7A 35 01 F7 3B*

For sending the public key assistance using the UBX-MGA-GAL-OSNMA PUBKEY message window in u-center, see Figure 5


UBX-MGA-GAL-OSNMA PUBKEY 2582 s
DBD (Assistance Database Dump)
FLASH (AssistNow Offline Download)
GAL (GAL Assistance)
ALM (Almanac)
EPH (Ephemeris)
IONO (Ionosphere)
OSNMA MERKLE (OSNMA MERKLE Root)
OSNMA PUBKEY (OSNMA Public Key)
TIMEOFF (Time Offset)
UTC (Universal Time Coordinated)
GLO (GLONASS Assistance)
GPS (GPS Assistance)
INI (Initial Assistance)
ATT (Attitude)
CLKD (Clock Drift)
EOP (Earth Orientation Parameters)
FREQ (Frequency)
POS_LLH (Geographic Position)
POS_XYZ (Cartesian Position)
TIME_GNSS (GNSS Time)
TIME_UTC (Universal Time Coordinated)

Public key ID: 1

Public key type: 1 : ECDSA P-

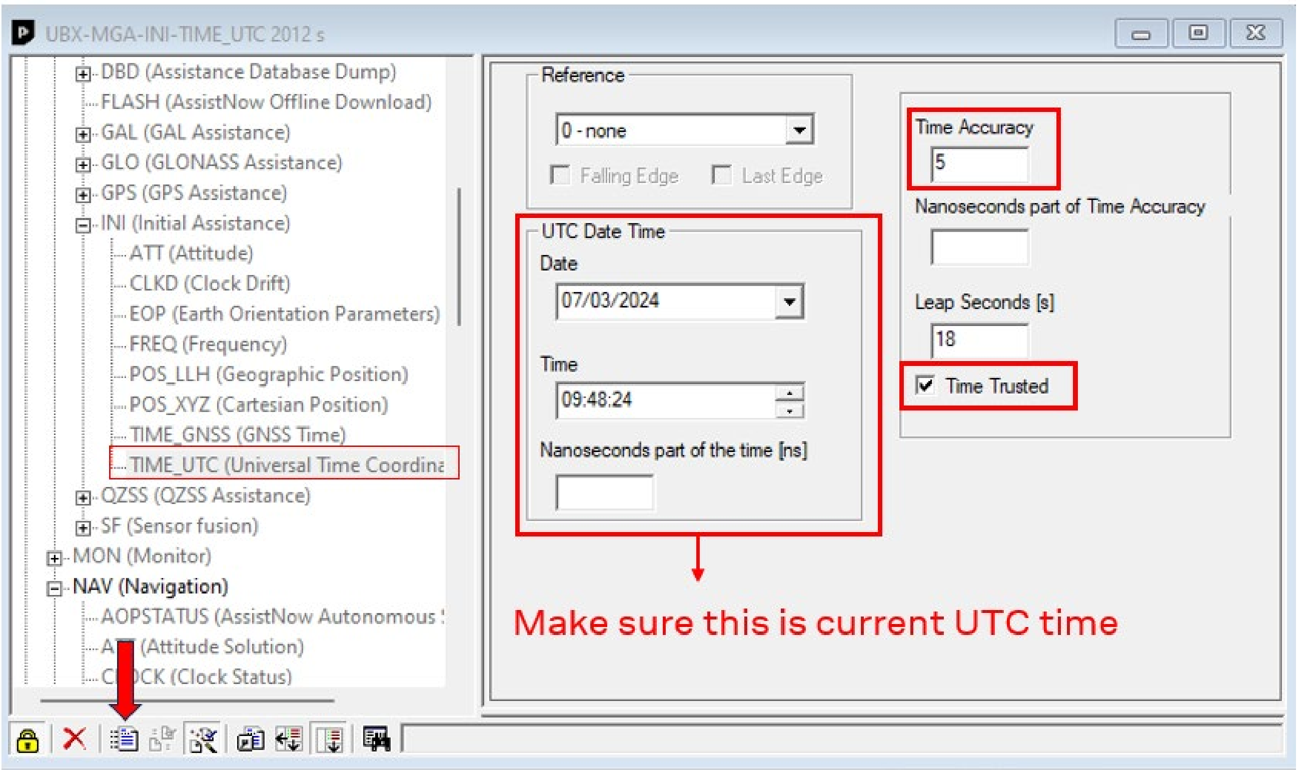
Public key point (HEX format): 03 97 EB 43 78 9A A0 F6 D0 52 A6 38 46 8E CF 52 78 E6 F6 DF 84 65 EC B8 D8 B

Figure 5: Sending public key assistance using UBX-MGA-GAL-OSNMA PUBKEY message window.

2.1.3 UBX-MGA-INI-TIME_UTC

UBX-MGA-INI-TIME_UTC message allows the user to send the trusted UTC time assistance to the receiver. For details about this message, refer to the applicable Interface description.

The u-center UBX-MGA-INI_TIME_UTC message window comes with pre-filled system date and time. Update the time to the **current UTC time** and specify the accuracy of the time provided. The accuracy should be better than 15 sec to allow normal OSNMA operation. Also, make sure that the "Time trusted" box is checked. For an example of sending the trusted time assistance, see Figure 6.



Reference: 0 - none

□ Falling Edge □ Last Edge

UTC Date Time

Date: 07/03/2024

Time: 09:48:24

Nanoseconds part of the time [ns]:

Time Accuracy: 5

Nanoseconds part of Time Accuracy:

Leap Seconds [s]: 18

☑ Time Trusted

Make sure this is current UTC time

Figure 6 : Sending trusted time assistance using UBX-MGA-INI-TIME_UTC message window.

For testing purposes, the trusted time check can be disabled using the CFG-GAL-OSNMA_TIMESYNC configuration item. In this case, the trusted time assistance is not necessary.

3 Verifying OSNMA feature

u-blox firmware offers multiple messages to verify the OSNMA feature, as listed in Table 2. The u-center application can be used to monitor these messages.

UBX message	Verification field
UBX-NAV-PVT	NMA and time authentication status
UBX-NAV-SIG	Galileo signal authentication status
UBX-SEC-OSNMA	OSNMA status information
UBX-NAV-TIMEUTC	UTC time authentication status
UBX-NAV-TIMETRUSTED	External trusted time information

Table 2: OSNMA verification messages

3.1.1 UBX-NAV-PVT

The UBX-NAV-PVT message has been modified to provide two extra fields to indicate if the OSNMA authentication data is used in the navigation solution.

NMA Fix status:

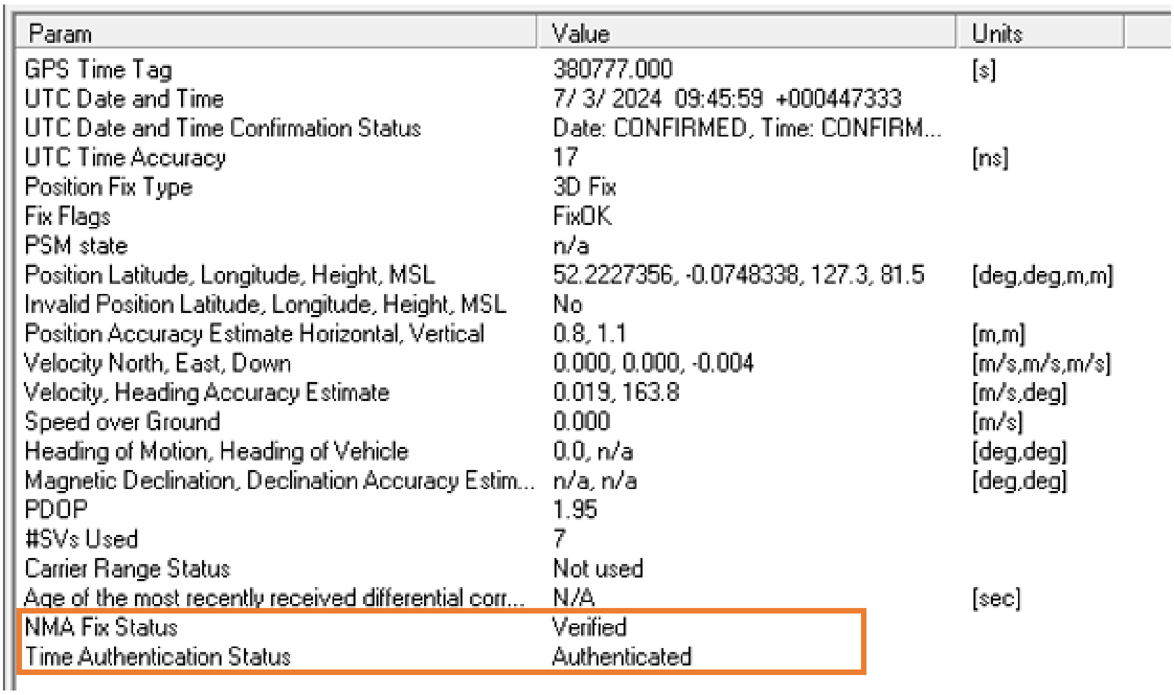
Unknown: It is not possible to perform the verification (does not imply spoofing).

Verified: The navigation solution uses enough signals with OSNMA authenticated data.

Time Authentication Status:

Not authenticated: Trusted time has not been provided, or its accuracy is not good enough to perform the authentication, or estimated time does not match trusted time.

Authenticated: Trusted time and estimated time match with required accuracy.

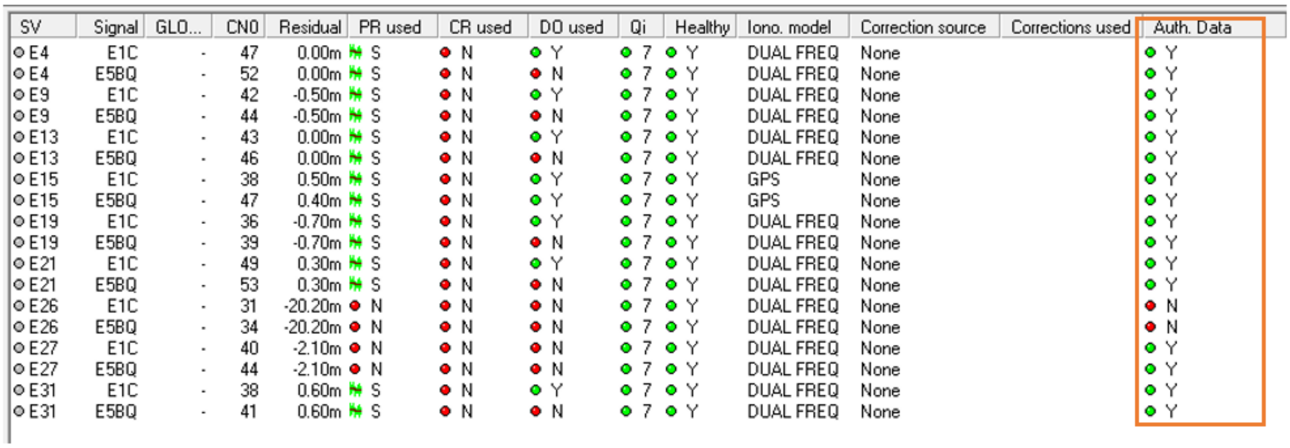


Param	Value	Units
GPS Time Tag	380777.000	[s]
UTC Date and Time	7/ 3/ 2024 09:45:59 +000447333	
UTC Date and Time Confirmation Status	Date: CONFIRMED, Time: CONFIRM...	
UTC Time Accuracy	17	[ns]
Position Fix Type	3D Fix	
Fix Flags	FixOK	
PSM state	n/a	
Position Latitude, Longitude, Height, MSL	52.2227356, -0.0748338, 127.3, 81.5	[deg,deg,m,m]
Invalid Position Latitude, Longitude, Height, MSL	No	
Position Accuracy Estimate Horizontal, Vertical	0.8, 1.1	[m,m]
Velocity North, East, Down	0.000, 0.000, -0.004	[m/s,m/s,m/s]
Velocity, Heading Accuracy Estimate	0.019, 163.8	[m/s,deg]
Speed over Ground	0.000	[m/s]
Heading of Motion, Heading of Vehicle	0.0, n/a	[deg,deg]
Magnetic Declination, Declination Accuracy Estim...	n/a, n/a	[deg,deg]
PDOP	1.95	
#SVs Used	7	
Carrier Range Status	Not used	
Age of the most recently received differential corr...	N/A	[sec]
NMA Fix Status	Verified	
Time Authentication Status	Authenticated	

Figure 7: UBX-NAV-PVT authentication information fields.

3.1.2 UBX-NAV-SIG

The UBX-NAV-SIG message indicates if the navigation data from Galileo INAV signal has been authenticated.

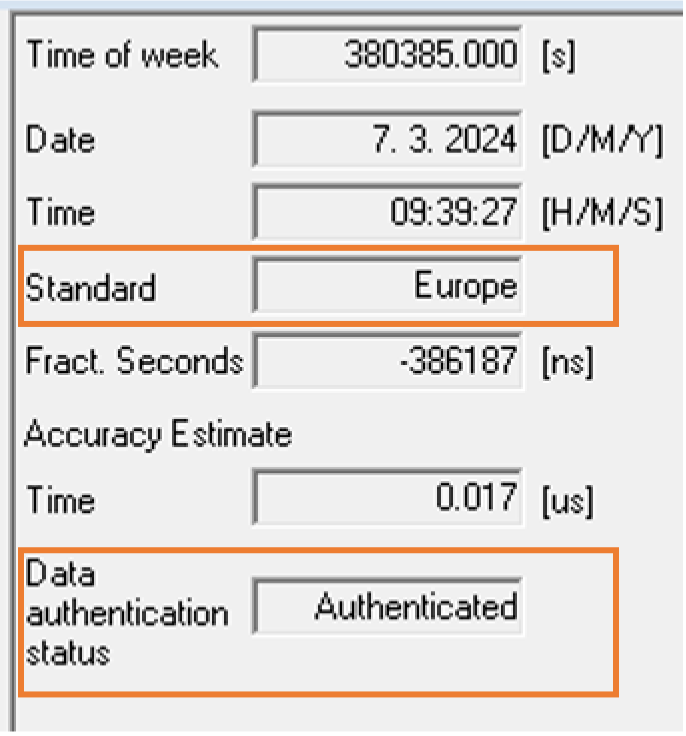


SV	Signal	GLO...	CNO	Residual	PR used	CR used	DO used	Qi	Healthy	Iono. model	Correction source	Corrections used	Auth. Data
E4	E1C	-	47	0.00m	S	N	Y	7	Y	DUAL FREQ	None		Y
E4	E5BQ	-	52	0.00m	S	N	N	7	Y	DUAL FREQ	None		Y
E9	E1C	-	42	-0.50m	S	N	Y	7	Y	DUAL FREQ	None		Y
E9	E5BQ	-	44	-0.50m	S	N	N	7	Y	DUAL FREQ	None		Y
E13	E1C	-	43	0.00m	S	N	Y	7	Y	DUAL FREQ	None		Y
E13	E5BQ	-	46	0.00m	S	N	N	7	Y	DUAL FREQ	None		Y
E15	E1C	-	38	0.50m	S	N	Y	7	Y	GPS	None		Y
E15	E5BQ	-	47	0.40m	S	N	Y	7	Y	GPS	None		Y
E19	E1C	-	36	-0.70m	S	N	Y	7	Y	DUAL FREQ	None		Y
E19	E5BQ	-	39	-0.70m	S	N	N	7	Y	DUAL FREQ	None		Y
E21	E1C	-	49	0.30m	S	N	Y	7	Y	DUAL FREQ	None		Y
E21	E5BQ	-	53	0.30m	S	N	N	7	Y	DUAL FREQ	None		Y
E26	E1C	-	31	-20.20m	N	N	N	7	Y	DUAL FREQ	None		N
E26	E5BQ	-	34	-20.20m	N	N	N	7	Y	DUAL FREQ	None		N
E27	E1C	-	40	-2.10m	N	N	N	7	Y	DUAL FREQ	None		Y
E27	E5BQ	-	44	-2.10m	N	N	N	7	Y	DUAL FREQ	None		Y
E31	E1C	-	38	0.60m	S	N	Y	7	Y	DUAL FREQ	None		Y
E31	E5BQ	-	41	0.60m	S	N	N	7	Y	DUAL FREQ	None		Y

Figure 8: UBX-NAV-SIG authentication data field.

3.1.3 UBX-NAV-TIMEUTC

The UBX-NAV-TIMEUTC has an extra field to indicate the UTC data authentication status. OSNMA authenticates the parameters to convert Galileo time to UTC time. To get the UTC time using authenticated data, change CFG-NAVSPG-UTCSTANDARD to the European standard.

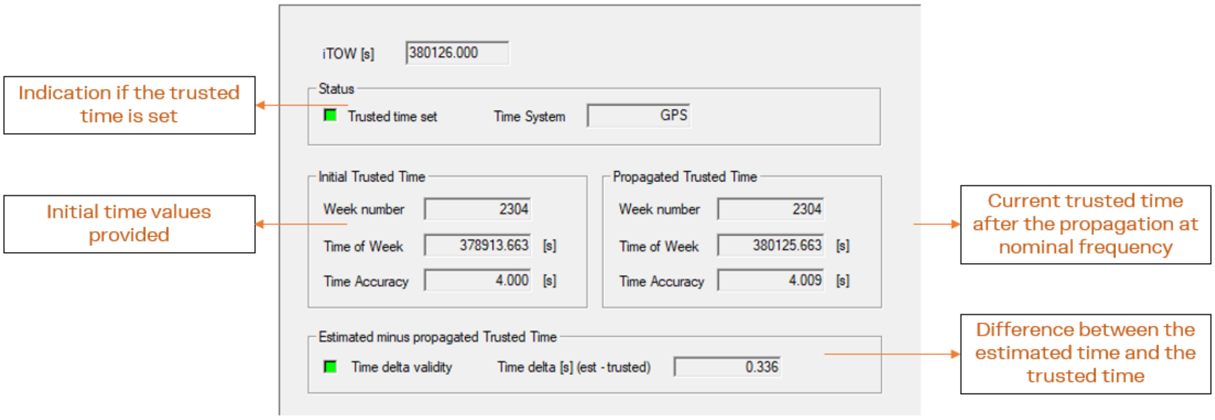


Time of week	380385.000	[s]
Date	7. 3. 2024	[D/M/Y]
Time	09:39:27	[H/M/S]
Standard	Europe	
Fract. Seconds	-386187	[ns]
Accuracy Estimate		
Time	0.017	[us]
Data authentication status	Authenticated	

Figure 9: UBX-NAV-TIMEUTC data authentication field.

3.1.4 UBX-NAV-TIMETRUSTED

The UBX-NAV-TIMETRUSTED message gives information about external trusted time. It displays the comparison between provided trusted time and the estimated time.



iTOW [s] 380126.000

Status

🟩 Trusted time set Time System GPS

Initial Trusted Time

Week number 2304

Time of Week 378913.663 [s]

Time Accuracy 4.000 [s]

Propagated Trusted Time

Week number 2304

Time of Week 380125.663 [s]

Time Accuracy 4.009 [s]

Estimated minus propagated Trusted Time

🟩 Time delta validity Time delta [s] (est - trusted) 0.336

Indication if the trusted time is set

Initial time values provided

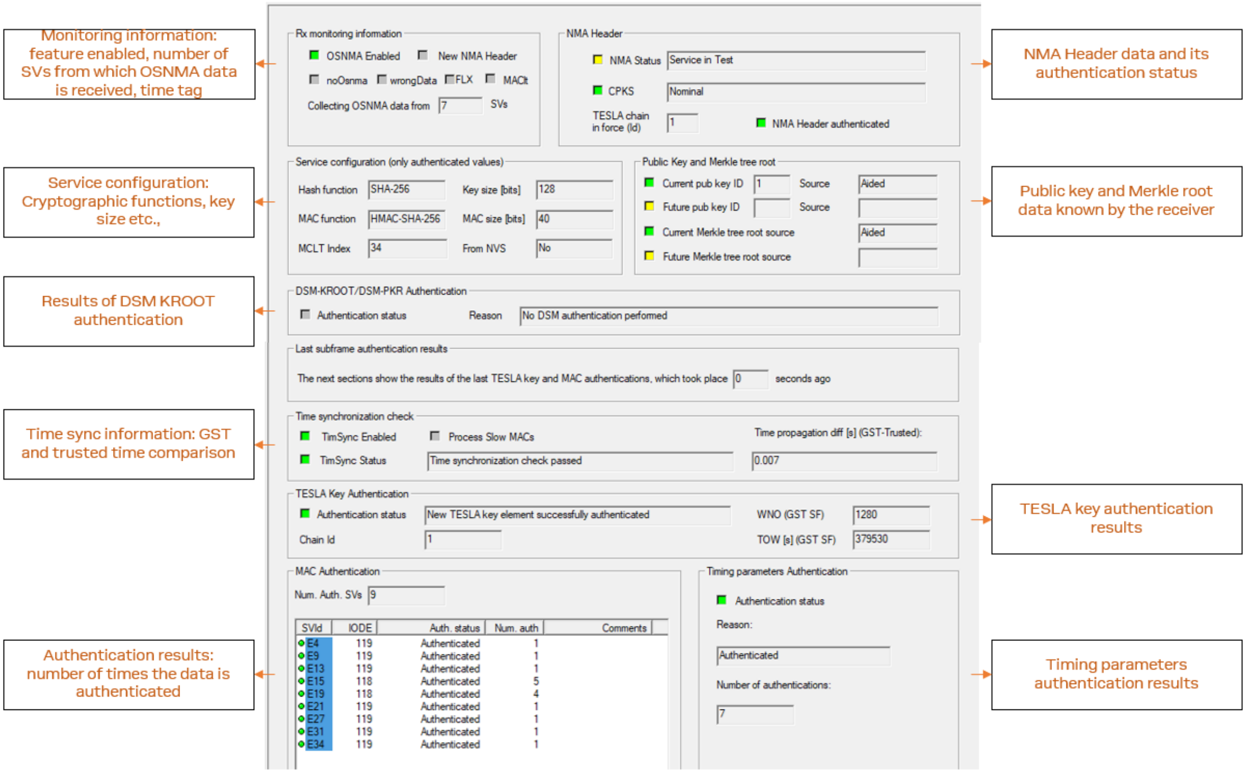
Current trusted time after the propagation at nominal frequency

Difference between the estimated time and the trusted time

Figure 10: UBX-NAV-TIMETRUSTED message information.

3.1.5 UBX-SEC-OSNMA

The new UBX-SEC-OSNMA message provides all the information about the OSNMA status.



Rx monitoring information

🟩 OSNMA Enabled □ New NMA Header

□ noOsnma □ wrongData □ FLX □ MACIt

Collecting OSNMA data from 7 SVs

NMA Header

🟨 NMA Status Service in Test

🟩 CPKS Nominal

TESLA chain in force (Id) 1 🟩 NMA Header authenticated

Service configuration (only authenticated values)

Hash function SHA-256 Key size [bits] 128

MAC function HMAC-SHA-256 MAC size [bits] 40

MCLT Index 34 From NVS No

Public Key and Merkle tree root

🟩 Current pub key ID 1 Source Aided

🟨 Future pub key ID Source

🟩 Current Merkle tree root source Aided

🟨 Future Merkle tree root source

DSM-KROOT/DSM-PKR Authentication

□ Authentication status Reason No DSM authentication performed

Last subframe authentication results

The next sections show the results of the last TESLA key and MAC authentications, which took place 0 seconds ago

Time synchronization check

🟩 TimSync Enabled □ Process Slow MACs Time propagation diff [s] (GST-Trusted):

🟩 TimSync Status Time synchronization check passed 0.007

TESLA Key Authentication

🟩 Authentication status New TESLA key element successfully authenticated WNO (GST SF) 1280

Chain Id 1 TOW [s] (GST SF) 379530

MAC Authentication

Num. Auth. SVs 9

SVId	IODE	Auth. status	Num. auth	Comments
● E4	119	Authenticated	1	
● E9	119	Authenticated	1	
● E13	119	Authenticated	1	
● E15	118	Authenticated	5	
● E19	118	Authenticated	4	
● E21	119	Authenticated	1	
● E27	119	Authenticated	1	
● E31	119	Authenticated	1	
● E34	119	Authenticated	1	

Timing parameters Authentication

🟩 Authentication status

Reason: Authenticated

Number of authentications: 7

Monitoring information: feature enabled, number of SVs from which OSNMA data is received, time tag

Service configuration: Cryptographic functions, key size etc.,

Results of DSM KROOT authentication

Time sync information: GST and trusted time comparison

Authentication results: number of times the data is authenticated

NMA Header data and its authentication status

Public key and Merkle root data known by the receiver

TESLA key authentication results

Timing parameters authentication results

Figure 11: UBX-SEC-OSNMA message information.

If the difference between GST (Galileo system time) and the trusted time provided is:

- <15 sec: OSNMA uses fast MACs. Normal OSNMA operation.
- 15 – 165 sec: OSNMA uses slow MACs. Time to authentication is longer than with fast MACs.

- >=165 sec: OSNMA will not be performed.

☞ The UBX-NAV-TIMETRUSTED message displays the difference between the estimated time and the trusted time assistance, whereas the UBX-SEC-OSNMA message displays the difference between the GST (time decoded from Galileo signals) and the trusted time assistance.

Related documentation

[1] GSC OSNMA Internet data distribution interface control document

☞ For product change notifications and regular updates of u-blox documentation, register on our website, www.u-blox.com.

Revision history

Revision	Date	Comments
R01	17-Aug-2023	Initial release
R02	02-Apr-2024	Updated firmware Updated Merkle tree and public key Changed OSNMA assistance providing procedure
R03	10-Mar-2025	Updated for all generation-9 u-blox receivers which support OSNMA

Contact

u-blox AG

Address: Zürcherstrasse 68
8800 Thalwil
Switzerland

For further support and contact information, visit us at www.u-blox.com/support.