
Teseo VI and Teseo APP2–OSNMA interface and testing procedures

Introduction

This document describes some testing procedures to simulate the OSNMA interface.

The open service navigation message authentication (OSNMA) is a data authentication function for the Galileo satellite service. Thanks to OSNMA, the Teseo VI and Teseo APP2 receivers can ensure that the Galileo navigation message coming from the Galileo system has not been modified or altered, thus ensuring its authenticity.

OSNMA is authenticating data for geolocation information from the open service through the navigation message (I/NAV) broadcast on the E1-B signal component. This is realized by transmitting authentication-specific data in previously reserved fields of the E1 I/NAV message.

The GNSS software with OSNMA capability implements a command interface at the NMEA/RTCM level to allow the usage and configuration of the system. It supports commands to enable/disable the OSNMA functionality or to store/delete up to two public keys into the NVM. Most of implemented commands could be used for testing the OSNMA performance in different working scenarios.



1 Preface

Teseo VI and Teseo APP2 devices embed the Arm® Cortex®-M7.

For information on the Arm® Cortex®-M7, refer to the technical reference manuals, available from the www.arm.com website.

Note: Arm, Cortex, and the Arm logo are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.



2 CDB configuration

The script configuration uses the following settings:

```
# Antispoofing 4 pools (bit 13)
16.2 : 2000,2000
# Integrity check (position, time)
16.5 : 00000003
# PPS sat mask (Galileo only)
20.4 : 00000008
# Enable NMA least square only (bit 18)
37.8 : 40000,40000
# OSNMA enable (bit 8) and PK verification enable (bit 9)
37.10 : 100,300
```

3 NMEA commands and message for OSNMA testing

The [Table 1](#) and [Table 2](#) report NMEA commands and message for OSNMA testing. Refer to [UM3407](#) for a detailed description.

Table 1. NMEA commands for OSNMA testing

NMEA commands	Description
\$PSTMNMASETMTR	Uploads the Merkle tree root into the OSNMA database.
\$PSTMNMAGETMTR	Displays the Merkle tree root stored in the OSNMA database
\$PSTMNMACLRMTTR	Removes the Merkle tree root stored in the OSNMA database
\$PSTMNMASETITN	Uploads the intermediate node into the OSNMA database.
\$PSTMNMAGETITN	Displays the intermediate node stored in the OSNMA database
\$PSTMNMACLRITN	Removes the intermediate node stored in the OSNMA database
\$PSTMNMAPK	Uploads the key into the OSNMA database.
\$PSTMNMACLRAM	Clears the alert message flag preventing the OSNMA from running
\$PSTMNMA	Turns ON/OFF the service and enables different working modes.
\$PSTMNMACLRPK	Clear PK in OSNMA database
\$PSTMNMAGETPK	Get PK stored in OSNMA database
\$PSTMNMACLRKROOT	Clear KROOT stored in OSNMA database
\$PSTMNMAGETDSM	Get DSM blocks already downloaded
\$PSTMNMASETDSM	Add DSM blocks among already downloaded blocks

Table 2. NMEA message for OSNMA testing

NMEA message	Description
\$GPAMC	Authenticated minimum specific message
\$GAASA	Authenticated active satellites message
\$PSTMNMAACV	OSNMA output event MACV message
\$PSTMNMA DSMV	OSNMA output event DSMV message
\$PSTMNMA PKRV	OSNMA output event PKRV message
\$PSTMNMA STATUS	OSNMA status message
\$PSTMNMAAM	Alert message

4 RTCM commands and message for OSNMA testing

This input message allows the user to configure OSNMA.

Table 3. Proprietary RTCM3 STNMA Messages

Msg number	Sub type ID	STNMA type ID	Description	Direction
4050 (or 999 for backward compatibility)	14	0	NVM invalidate	In
		1	Status on/off	In/Out
		4	TSL	In
		5	MACSEQ Flags	In
		6	Set PK	In
		11	Get PK	In
		12	Clear PK	In
		13	Set MTR	In
		14	Get MTR	In
		15	Clear MTR	In
		16	Set ITN	In
		17	Get ITN	In
		18	Clear ITN	In
		19	Clear Alert message flag	In
		20	Clear KROOT	In
		22	Get DSM	In
		23	Set DSM	In

Table 4. GNSS OSNMA (STNMA) message header

Data field	DF	Bit pos	Bits	Notes
Message number	DF002	0	12	ST proprietary ID (4050, or 999 for backward compatibility)
Sub type ID	DF02P	12	8	14 for STNMA
Response ID	DF53P	20	10	For output is always 0x0000
STNMA type ID	DF116P	30	6	See Table 3. Proprietary RTCM3 STNMA Messages

This output message sends OSNMA event information (refer to the [Section 5: OSNMA testing procedure](#) for details).

Table 5. Proprietary RTCM3 STNMAEVT messages

Msg number	Sub type ID	STNMAEVT type ID	Description	Direction
4050 (or 999 for backward compatibility)	36	7	MACV event	Out
		8	DSMV event	Out
		9	PKRV event	Out
		10	Alarm event	Out
		21	NMA status event	Out

Table 6. GNSS OSNMA (STNMAEVT) message header

Data field	DF	Bit pos	Bits	Notes
Message number	DF002	0	12	ST proprietary ID (4050, or 999 for backward compatibility)
Sub type ID	DF02P	12	8	36 for STNMA event
STNMA type ID	DF116P	20	6	See Table 5. Proprietary RTCM3 STNMAEVT messages

5 OSNMA testing procedure

The following section illustrates the procedure required to test the system and obtain an authenticated position with OSNMA. The user should obtain the public key and its related key ID (refer to <https://www.gsc-europa.eu/> and OSNMA ICD 1.0 for further details).

For this test the following NMEA commands shall be used:

1. `$PSTMNMASETMTR,0,[sha_type],[current_MTR]`
`$PSTMNMASETMTR,1,[sha_type],[future_MTR] (optional)`
2. `$PSTMNMASETITN,0,[ITN_level_0]`
`$PSTMNMASETITN,1,[ITN_level_1]`
`$PSTMNMASETITN,2,[ITN_level_2]`
`$PSTMNMASETITN,3,[ITN_level_3]`
3. `# To inject the public key`
`$PSTMNMAPK,[msg_id],[key_idx],[p_key]`

Step 2 is required to verify the public key received from the sky in DSM-PKR message and to verify the injected public key if PK verification is enabled in firmware configuration.

When verifying the public key, the current MTR is used. If verification fails, a second attempt is made using the future MTR. The MTR successfully used is reported in the PKR event message in case of public key received from the sky or in \$PSTMNMAPKOK message if PK verification is enabled in firmware configuration (currently not reported in RTCM3).

Step 3 is required only if the PK verification is enabled in the firmware configuration.

After performing the procedure at least 5 minutes are required to let the system calculate the key. By checking the \$GAASA message the user can ensure that the authenticated position fix is reached when the status field changes to "A".

The injected keys are saved in NVM, thus, after a reset or a power cycle, the system will perform the authenticated fix again. The user can manually invalidate the saved keys using the command \$PSTMNMA, 0. After the invalidation command, a system reset is advised for the change to take effect.

Since the injected public key is saved in NVM, every time the user issues a startup command (Hot/Warm/Cold) the system performs an authenticated warm start.

Here after an example in NMEA with a dummy public key and key ID.

NMEA example

```
$PSTMNMASETMTR,0,2,832E15EDE55655EAC6E399A539477B7C034CCE24C3C93FFC904ACD9BF842F04E
$PSTMNMASETMTR,1,2,832E15EDE55655EAC6E399A539477B7C034CCE24C3C93FFC904ACD9BF842F04E
$PSTMNMASETITN,0,941BD34EA7DF668B6FC5BE75C1D93464D109BC615CB52C8124847FAFB09CBB2B
$PSTMNMASETITN,1,6AAFDE28017BF0744D42819CE40E3A0CDA1ECA3F7A4EA67E134E7AA714C1E843
$PSTMNMASETITN,2,DE73D209E4C5BCDC34CD117F2FE40FD08B110009997AD2B3291D3A2CF29943F9
$PSTMNMASETITN,3,84DE3669E6DA551292979E5B8D045787FA967C57CC23638A30237614EDD9171A
$PSTMNMAPK,0,1,0397EB43789AA0F6D052A638468ECF5278E6F6DF8465ECB8D8B84B8C7A3501F73B
```

Here after an example in RTCM with a dummy public key and key ID.

RTCM example

```
# SEND CURRENT MTR
SENDRTCM "[12]0XFD2,[8]0XE,[10]0X0,[6]0XD,[1]0X0,[1]0X0,[32]0X832E15ED,[32]0XE55655EA,[32]0XC6E399A5,[32]0X39477B7C,[32]0X034CCE24,[32]0XC3C93FFC,[32]0X904ACD9B,[32]0XF842F04E"
# SEND FUTURE MTR
SENDRTCM "[12]0XFD2,[8]0XE,[10]0X0,[6]0XD,[1]0X1,[1]0X0,[32]0X832E15ED,[32]0XE55655EA,[32]0XC6E399A5,[32]0X39477B7C,[32]0X034CCE24,[32]0XC3C93FFC,[32]0X904ACD9B,[32]0XF842F04E"

# SEND ITN 0,1,2,3
SENDRTCM "[12]0XFD2,[8]0XE,[10]0X0,[6]0X10,[32]0X941BD34E,[32]0XA7DF668B,[32]0X6FC5BE75,[32]0XC1D93464,[32]0XD109BC61,[32]0X5CB52C81,[32]0X24847FAF,[32]0XB09CBB2B,[32]0X6AAFDE28,[32]0X017BF074,[32]0X4D42819C,[32]0XE40E3A0C,[32]0XDA1ECA3F,[32]0X7A4EA67E,[32]0X134E7AA7,[32]0X14C1E843,[32]0XDE73D209,[32]0XE4C5BCDC,[32]0X34CD117F,[32]0X2FE40FD0,[32]0X8B110009,[32]0X997AD2B3,[32]0X291D3A2C,[32]0XF29943F9,[32]0X84DE3669,[32]0XE6DA5512,[32]0X92979E5B,[32]0X8D045787,[32]0XFA967C57,[32]0XCC23638A,[32]0X30237614,[32]0XEDD9171A"
```

```
# SEND PK  
SENDRTCM "[12]0XFD2,[8]0XE,[10]0X0,[6]0X6,[4]0X0,[4]0X1,[4]0X0,[32]0X0397EB43,[32]0X789AA0F6  
,[32]0XD052A638,[32]0X468ECF52,[32]0X78E6F6DF,[32]0X8465ECB8,[32]0XD8B84B8C,[32]0X7A3501F7,[8  
]0X3B"
```

Appendix A Acronyms and reference documents

Table 7. Acronyms

Keyword	Definition
AM	Alert message
Checksum	Calculated from the transmitted characters of a message by XORing the 8-bit character values excluding delimiters \$ and *
Galileo	Europe's global navigation satellite system
GDOP	Geometric dilution of position–Quality value representing all geometry based error factors in a system.
GNSS	Global navigation satellite system–Satellite based system to calculate the position of the receiver on the earth surface.
HDOP	Horizontal dilution of precision–Quality value representing all 2D plane geometry based error factors in a system.
ITN	Merkle Tree intermediate node
Lat	Latitude–Angular difference of a given position to the equator. Values include 0°–90° either North or South
Long	Longitude–Angular difference to a “reference” Longitude indicated as “000”. Values include 0° ... 180° either West or East.
MTR	Merkle Tree Root
NMEA	National marine electronics association–United States standards organization for marine equipment
NVM	Nonvolatile memory
OSNMA	Open service navigation message authentication
PK	Public Key
PRN	Pseudorandom number–Satellite specific 1023-bit number used for spread spectrum modulation

Table 8. Reference documents

Document name	Document title
UM3407	Teseo VI and Teseo APP2–NMEA specifications and commands
Galileo OSNMA SIS ICD	Galileo open service navigation message authentication (OSNMA) signal-in space interface control document (SIS ICD) https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OSNMA_SIS_ICD_v1.1.pdf

Revision history

Table 9. Document revision history

Date	Revision	Changes
16-Apr-2025	1	Initial release.
26-Nov-2025	2	Added Section 1: Preface. Updated Table 1. NMEA commands for OSNMA testing. Updated Table 3. Proprietary RTCM3 STNMA Messages and Table 5. Proprietary RTCM3 STNMAEVT messages. Updated Section 5: OSNMA testing procedure.

Contents

1	Preface	2
2	CDB configuration	3
3	NMEA commands and message for OSNMA testing	4
4	RTCM commands and message for OSNMA testing	5
5	OSNMA testing procedure	7
Appendix A	Acronyms and reference documents	9
	Revision history	10

List of tables

Table 1.	NMEA commands for OSNMA testing	4
Table 2.	NMEA message for OSNMA testing	4
Table 3.	Proprietary RTCM3 STNMA Messages	5
Table 4.	GNSS OSNMA (STNMA) message header	5
Table 5.	Proprietary RTCM3 STNMAEVT messages	5
Table 6.	GNSS OSNMA (STNMAEVT) message header	6
Table 7.	Acronyms	9
Table 8.	Reference documents	9
Table 9.	Document revision history	10

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST's terms and conditions of sale in place at the time of order acknowledgment.

The purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of the purchasers' products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

If the purchasers identify an ST product that meets their functional and performance requirements but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2025 STMicroelectronics – All rights reserved