Authentication and other new services on Galileo

Ignacio Fernández Hernández
European Commission
13 Oct 2022
Table of contents

• Galileo

• Galileo Open Service Navigation Message Authentication (OSNMA)

• Gailleo High Accuracy Service (HAS)
Table of contents

• Galileo

• Galileo Open Service Navigation Message Authentication (OSNMA)

• Galileo High Accuracy Service (HAS)
Galileo

• Galileo is the EU satellite navigation system

• Initial service since 2016

• Some data:
  • Space segment: 3 orbital planes, 8 + spare SV per plane. SV altitude: 23,222 km
  • Ground segment: 2 control centers (IT, DE), 14 monitoring stations worldwide, 5 uplink stations, 6 TTC stations
  • 4 carriers: E1 (1575.42 MHz), E5a (1176.45 MHz), E5b(1207.14 MHz), E6 (1278.75 MHz), BOC and BPSK signals
Galileo satellites

Weight: ~ 730 kg
Power consumption: ~ 2000 W
Transmitted power per signal: ~ 30 W
Galileo satellites

Weight: ~ 730 kg
Power consumption: ~ 2000 W
Transmitted power per signal: ~ 30 W
Galileo availability

For more information:
https://gsc-europa.eu
Table of contents

• Galileo

• Galileo Open Service Navigation Message Authentication (OSNMA)

• Galileo High Accuracy Service (HAS)
What is Galileo OSNMA?

- What is Galileo OSNMA?
  - Stands for Open Service Navigation Message Authentication
  - Mechanism to authenticate the Galileo data used to calculate a position: satellite orbits and clock corrections, satellite status flags, time...
  - Equivalent to a Galileo “digital signature”
  - Transmitted in 40 bits every other second in the Galileo I/NAV message, E1B component, 1575.42 MHz
  - Makes the signal unpredictable

- Why OSNMA?
Why OSNMA
Why OSNMA
Why OSNMA
The OSNMA protocol

OSNMA server at GNSS Service Centre (GSC)

Galileo Satellite
OSNMA signal
OSNMA enabled user receiver

CRYPTOGRAPHIC FUNCTION
is navigation data authentic?

- No
  - Navigation data not authenticated
- Yes
  - Navigation data authenticated
    - Trusted use for positioning
OSNMA Receiver processing logic

Signal in space

- NAV message
- TESLA chain key
- Tag
- TESLA root key

OSNMA enabled receiver

- Received NAV message
- TESLA chain key verification
- Received Tag
- TESLA root key verification

Tag computation

Computed Tag

Public key

=?
OSNMA Receiver processing logic

Signal in space

- NAV message
- TESLA chain key
- Tag

OSNMA enabled receiver

- Received NAV message
- TESLA chain key verification
- Received Tag
- Tag computation
- Computed Tag

- TESLA root key verification
- Public key

= ?
OSNMA Receiver processing logic

Signal in space

- NAV message
- TESLA chain key
- Tag
- TESLA root key

OSNMA enabled receiver

- Received NAV message
- TESLA chain key verification
- Received Tag
- TESLA root key verification

- Tag computation
- Computed Tag

Public key

=?
OSNMA Receiver processing logic
OSNMA Receiver processing logic
OSNMA Receiver processing logic

Signal in space

NAV message

TESLA chain key

Tag

TESLA root key

Received NAV message

TESLA chain key verification

Received Tag

Public key

Tag computation

Computed Tag

OSNMA enabled receiver
OSNMA current status

- **2014-2020: Studies, design, devpt**
- **2021-2022: Public testing**
- **2023: Service declaration (OSNMA status switch from 'test' to 'operational')**

- SIS ICD (test phase), "Info note" and guidelines published*

- SIS reliably transmitted worldwide for almost two years, 1+ year publicly

Examples of OSNMA applications

**Safety-Critical Applications**: OSNMA-secured GNSS positioning to support safety-critical applications, such as in the automotive sector
→ OSNMA included in the EU Digital Tachograph regulation

**Telecom**: to allow telecom operators to have accurate and consistent time and frequency at distant points of network.
→ Clear interest on GNSS authentication

**Insurance telematics**: use of GNSS data to increase the fairness of motor insurance for both insurers and subscribers in the frame of usage-based insurance.
→ Liability critical application

More applications can be found in ‘*Galileo Open Service Navigation Message Authentication (OSNMA) Info Note*’, European Union Agency for the Space Programme (EUSPA), 2021.
Some EU projects exploiting OSNMA

**PATROL:** Development, supply and testing of an **OSNMA user terminal** for smart tachographs.

**GIANO**

**Galileo-based timing platform** (TRL7), using OSNMA and EGNOS corrections.

**ASGARD**

Design, integration and V&V of a shipborne receiver **dual-frequency multi-constellation Galileo OS enabled including OSNMA** and IEC GNSS approval.

**ROOT**

Assessment of the benefits introduced by **Galileo authenticated signals (OSNMA)** in the specific context of **synchronisation of 5G telecommunication networks**.

Open-source OSNMA library: [https://github.com/Algafix/OSNMA](https://github.com/Algafix/OSNMA)
OSNMA availability

Availability of Tags for Galileo I/NAV orbit & clock data (ADKO), for target security level and for at least 4 SV in view (120 [s] 80-bit accumulation window)

August 2022

Source: ADS/EUSPA
OSNMA accuracy

Average difference between legacy and OSNMA vertical and horizontal position accuracy (95%) measured at each TGVFx GESS from 1st May until 30th June 2022
Next Steps

- Continue public testing
- Publication of Service ICD (Q4’22/Q1’23). Mostly compatible with current (test) ICD
- Publication of operational cryptographic data to be installed in receivers for the operational phase
- Operational service declaration: 2023 (date TBC EUSPA)
- To be complemented by signal authentication (ACAS) and HAS data authentication in Galileo 1st Generation, then ranging authentication in all frequencies in Galileo 2nd Generation
Table of contents

• Galileo

• Galileo Open Service Navigation Message Authentication (OSNMA)

• Galileo High Accuracy Service (HAS)
Overview of Galileo HAS

• Galileo HAS provides precise corrections, allowing PPP positioning worldwide and for free

• Corrections provided for orbits, clocks, code biases and phase biases: Galileo I/NAV, E1, E5a,E5b, E6B/C; GPS CNAV, L1C/A, L2C, L2P

• SIS dissemination through E6B (1278.75 MHz) and ground dissemination channel through a real-time connection in RTCM-like format

HAS infrastructure

Galileo HAS Phase 1 architecture. The 14 GSS (Galileo Sensor Stations) are depicted with a single antenna, and the five ULS (Up-Link stations) are depicted with four antennas.
HAS current status

- Three phases:
  - Phase 0 (testing)
  - Phase 1 (initial service)
  - Phase 2 (full service)

- Current status: Finishing Phase 0
  - HAS SIS ICD available since May 22*
  - SIS readily available worldwide (HAS Status flag = ‘test’ mode)

- Initial Service declaration by end2022/early2023

# Galileo HAS phases and performance targets

<table>
<thead>
<tr>
<th></th>
<th>Phase 0 SIS Testing</th>
<th>Phase 1 Initial Service</th>
<th>Phase 2 Full Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Coverage</strong></td>
<td>EU+</td>
<td>EU+</td>
<td>Global</td>
</tr>
<tr>
<td><strong>Clock biases</strong></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Phase biases</strong></td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Galileo corrected signals</strong></td>
<td>E1, E5a, E5b, E6</td>
<td>E1, E5a, E5b, E6</td>
<td>E1, E5a, E5b, E5, E6</td>
</tr>
<tr>
<td><strong>GPS corrected signals</strong></td>
<td>L1, L2P</td>
<td>L1, L2P, L2C</td>
<td>L1, L2C, L5</td>
</tr>
<tr>
<td><strong>Horizontal accuracy requirement 95%</strong></td>
<td>N/A</td>
<td>&lt;20 cm TBC</td>
<td>&lt;20 cm</td>
</tr>
<tr>
<td><strong>Vertical accuracy requirement 95%</strong></td>
<td>N/A</td>
<td>&lt;40 cm TBC</td>
<td>&lt;40 cm</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>N/A</td>
<td>99% TBC</td>
<td>99%</td>
</tr>
<tr>
<td><strong>Convergence time requirement Global, no ionosphere (SL1)</strong></td>
<td>N/A</td>
<td>&lt;300 s TBC</td>
<td>&lt;300 s</td>
</tr>
<tr>
<td><strong>EU, Ionosphere corrections (SL2)</strong></td>
<td>N/A</td>
<td>N/A</td>
<td>&lt;100 s</td>
</tr>
<tr>
<td><strong>Ground channel</strong></td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Start</strong></td>
<td>2020</td>
<td>2022-23</td>
<td>2024+</td>
</tr>
</tbody>
</table>
HAS message

- Current sequence every 10s:
  - 7 “slow” message pages: mask, orbit, CB, PB
  - 2 “fast” message pages: clock
  - 1 dummy message


- Total: around 8000 bits
HAS message reception performance

<table>
<thead>
<tr>
<th></th>
<th>Mean [s]</th>
<th>Mode [s]</th>
<th>Median [s]</th>
<th>95% Quantile [s]</th>
<th>Max [s]</th>
<th>Min [s]</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEB 27A</td>
<td>8.46</td>
<td>7</td>
<td>8</td>
<td>13</td>
<td>33</td>
<td>6</td>
</tr>
<tr>
<td>FEB 27B</td>
<td>8.71</td>
<td>7</td>
<td>7</td>
<td>17</td>
<td>65</td>
<td>4</td>
</tr>
<tr>
<td>FEB 28A</td>
<td>11.16</td>
<td>7</td>
<td>8</td>
<td>32</td>
<td>152</td>
<td>4</td>
</tr>
<tr>
<td>FEB 28B</td>
<td>7.61</td>
<td>6</td>
<td>6</td>
<td>14</td>
<td>36</td>
<td>5</td>
</tr>
</tbody>
</table>

HAS orbit & clock correction accuracy

- HAS orbit and clock with live signals between May 2021 and June 2022
- Septentrio PolaRx5S rx with Trimble Zephyr 2 antenna @JRC EC (Italy)
- HAS broadcast test signals and performance might not be representative of final service ones

HAS orbit & clock correction accuracy

- HAS orbit and clock with live signals between May 2021 and June 2022
- Septentrio PolaRx5S rx with Trimble Zephyr 2 antenna @JRC EC (Italy)
- HAS broadcast test signals and performance might not be representative of final service ones
HAS PPP user performance

- User PPP accuracy from HAS signal tested worldwide
- Conditions: static, open sky (GMV’s monitoring network)
- Performance measured in stationary mode after convergence
- RMS and 95th percentile of errors from 6 days: 31/8-6/9
- PPP configuration used:
  - Multiconstellation GAL+GPS
  - Double frequency E1-E5a and L1C/A-L2CL (Iono-free + ionospheric estimation)
  - PPP float
### HAS PPP user performance

<table>
<thead>
<tr>
<th>Region</th>
<th>Errors RMS (cm)</th>
<th>Errors p95 (cm)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>North</strong></td>
<td><strong>East</strong></td>
<td><strong>Height</strong></td>
</tr>
<tr>
<td>Europe &amp; Africa</td>
<td>SPTR</td>
<td>4.5</td>
</tr>
<tr>
<td></td>
<td>ROBU</td>
<td>5.7</td>
</tr>
<tr>
<td></td>
<td>SWOJ</td>
<td>6.5</td>
</tr>
<tr>
<td></td>
<td>NAWI</td>
<td>4.0</td>
</tr>
<tr>
<td><strong>America</strong></td>
<td><strong>USNA</strong></td>
<td>6.0</td>
</tr>
<tr>
<td></td>
<td>CABU</td>
<td>6.1</td>
</tr>
<tr>
<td></td>
<td>CHSA</td>
<td>8.8</td>
</tr>
<tr>
<td></td>
<td>FRTA</td>
<td>9.1</td>
</tr>
<tr>
<td><strong>Asia</strong></td>
<td><strong>INKO</strong></td>
<td>5.8</td>
</tr>
<tr>
<td></td>
<td>TATA</td>
<td>8.6</td>
</tr>
</tbody>
</table>

HAS user PPP, Sweden
HAS user PPP, US
HAS and fault detection (not integrity!)

- If the HAS correction value grows and shows a degradation of the orbit and/or clock error, the user excludes the satellite to avoid impact on the position performance.

- In addition, the HAS message informs the user that the satellite shall not be used.

I. Martini et al. "Satellite Anomaly Detection with PPP Corrections: A Case Study with Galileo’s High Accuracy Service" ION ITM January 2022
Summary

• Galileo, the European GNSS, is providing global coverage with very good performance for the last years

• In addition, OSNMA and HAS already transmitted freely and worldwide, and to be officially declared next year

• OSNMA offers data authentication and signal unpredictability for Galileo. It is a pioneering, long awaited feature to protect against spoofing

• HAS is a PPP corrections service for GPS/Galileo. Aiming at 20/40cm 95% accuracy

• Next step: spreading code authentication in E6
12 October 1492
Authentication and other new services on Galileo

Ignacio Fernández Hernández
European Commission

Thank you for your attention

Acknowledgements: Galileo OSNMA/HAS teams (EC, EUSPA, ESA, PAULA, HADG, GSC...)