Open Service
Navigation Message Authentication

User Consultation Platform 2020

Flavio SBARDELLATI, European GNSS Agency

Organised by:

Under the auspices of:

EU Space Programme:
Why is Authentication needed?

GNSS is known to be vulnerable to jamming and spoofing

➢ Service disruption or denial incidents are more and more frequently observed

➢ Potentially severe consequences, especially for safety or liability critical applications

The role of authentication is to detect spoofing events

➢ Thus to avoid or mitigate their consequences

Source: GPS World
Chinese GPS spoofing circles could hide Iran oil shipments
GNSS Authentication

GNSS authentication is one important contributor to the overall trustworthiness of PVT based applications. ➔ Not the only one!

GNSS authentication can be done at two complementary levels:

➢ **Data level**, to authenticate the broadcast navigation messages;

➢ **Range level**, to authenticate the measured ranges to the satellites;

Combining the 2 allows authentication of the GNSS solution.
What is OS-NMA and how does it work?

OS-NMA is a **data authentication** function

- Worldwide, Free of charge, with no impact on OS performance or on existing receivers (backward compatible).

Based on transmission of cryptographic material in previously reserved fields on the I/NAV message on the E1B signal component

- Only OS-NMA ready receivers can decode these fields and authenticate the Galileo navigation data

**Technical requirements**

(i) Continuous E1B tracking

(ii) Availability of a trustable knowledge of time

(iii) Capability to store and ensure the integrity of a public key
### OS-NMA characteristics

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>OS-NMA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GNSS receiver minimal capabilities</strong></td>
<td>Single frequency E1</td>
</tr>
<tr>
<td><strong>Object of authentication</strong></td>
<td>Nav Data (E1B I/Nav and E5b I/Nav, capability for E5a F/Nav if required)</td>
</tr>
<tr>
<td><strong>Required components</strong></td>
<td>E1B</td>
</tr>
<tr>
<td><strong>Need of a network connection</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Clock &amp; Ephemeris Data (CED), Delayed</td>
</tr>
<tr>
<td><strong>Time to first Authentication</strong></td>
<td>One to several minutes</td>
</tr>
<tr>
<td><strong>Anti-tampering characteristic for receiver</strong></td>
<td>Not needed: the receiver only stores a public key</td>
</tr>
<tr>
<td><strong>Other requirements</strong></td>
<td>Loose time synchronisation</td>
</tr>
</tbody>
</table>
You are all invited!

**OS-NMA Roadmap**

<table>
<thead>
<tr>
<th>PUBLIC NOTE</th>
<th>OS-NMA INFO NOTE v1.0</th>
<th>OS-NMA INFO NOTE v1.1</th>
<th>OS-NMA INFO NOTE v2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>TECHNICAL BASELINE</td>
<td>USER ICD, RX GUIDELINES FOR PUBLIC TESTING — AS DESIGNED</td>
<td>USER ICD, RX GUIDELINES FOR PUBLIC TESTING PUBLISHED</td>
<td>OS-NMA USER ICD, Rx GUIDELINES, SERVICE DEFINITION PUBLISHED</td>
</tr>
<tr>
<td>OBJECTIVE</td>
<td>SYSTEM READINESS OPERATIONS READINESS</td>
<td>(i) USERS FEEDBACKS (ii) SUPPORT MARKET AND PRODUCTS DEVELOPMENT (iii) FINE TUNING (UPSTREAM AND DOWNSTREAM)</td>
<td>BENEFIT FOR USERS AND SOCIETY</td>
</tr>
</tbody>
</table>
Any questions?

For service related information  www.gsc-europa.eu

For market related aspects  MARKET@gsa.europa.eu
Linking space to user needs

How to get in touch:

www.GSA.europa.eu

EGNOS-portal.eu

GSC-europa.eu

UseGalileo.eu

The European GNSS Agency is hiring!

Apply today and help shape the future of satellite navigation!