EUROPEAN SPACE WEEK

ONLINE EDITION

#EUSpaceWeek

Open Service Navigation Message Authentication

User Consultation Platform 2020

Organised by:

European GNSS Agency

European Commission

Under the auspices of:

eu2020.de

EU Space Programme:

Copernicus

EGNOS

GALILEO

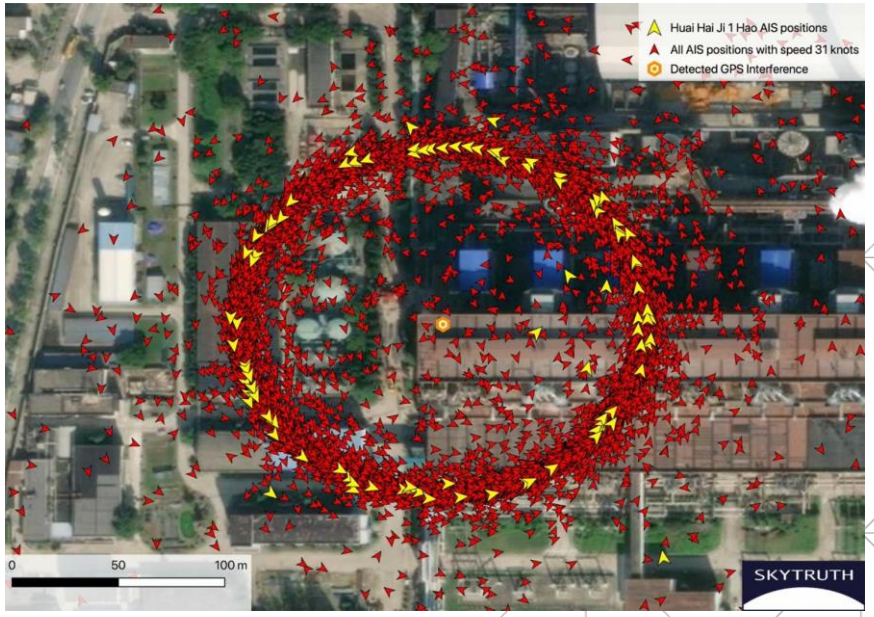
Why is Authentication needed?

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



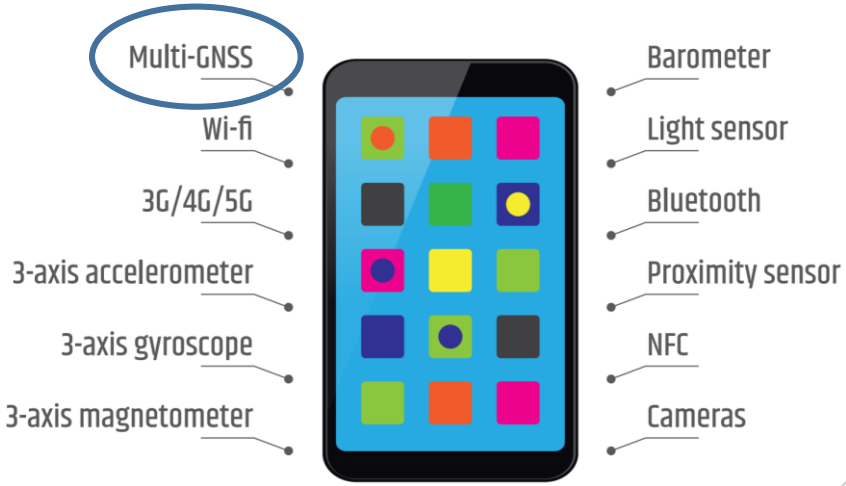
Source: GPS World
[Chinese GPS spoofing circles could hide Iran oil shipments]

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

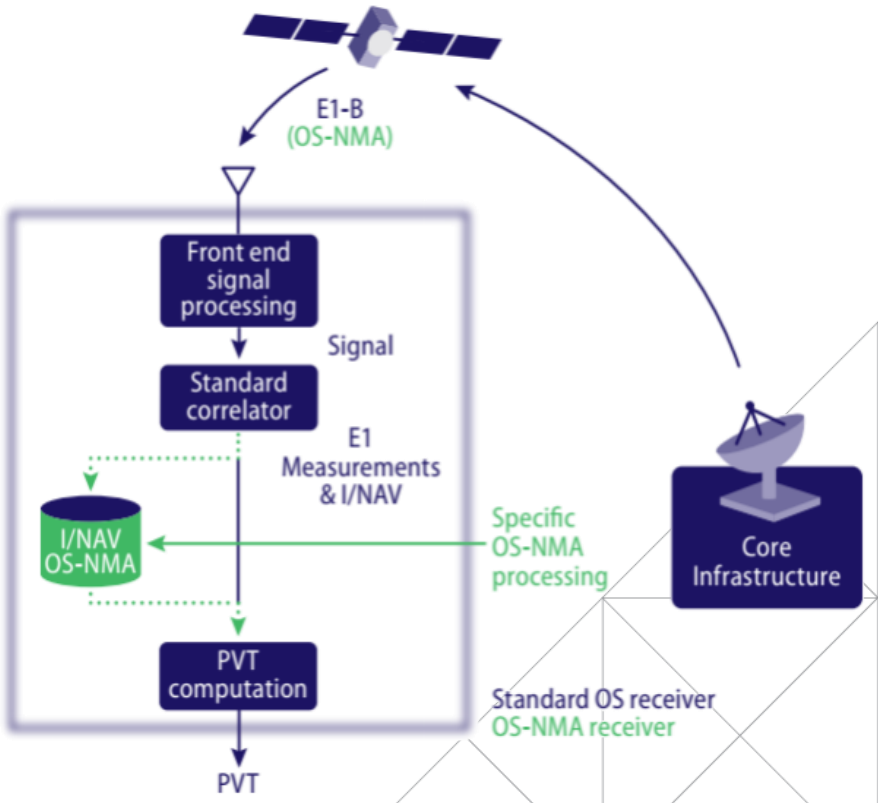
What is OS-NMA and how does it work?

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



<u>Technical requirements</u>

(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

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

OS-NMA Roadmap

You are all invited!

PUBLIC NOTE	OS-NMA INFO NOTE V1.0	OS-NMA INFO NOTE V1.1	OS-NMA INFO NOTE V2.0
TECHNICAL BASELINE	USER ICD, RX GUIDELINES FOR PUBLIC TESTING –AS DESIGNED	USER ICD, RX GUIDELINES FOR PUBLIC TESTING PUBLISHED	OS-NMA USER ICD, RX GUIDELINES, SERVICE DEFINITION PUBLISHED
OBJECTIVE	SYSTEM READINESS OPERATIONS READINESS	(I) USERS FEEDBACKS (II) SUPPORT MARKET AND PRODUCTS DEVELOPMENT (III) FINE TUNING (UPSTREAM AND DOWNSTREAM)	BENEFIT FOR USERS AND SOCIETY

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:

European GNSS Agency

www.GSA.europa.eu

EGNOS-portal.eu

GSC-europa.eu

UseGalileo.eu