



European Global Navigation Satellite Systems Agency



Galileo authentication and market opportunities

Swedish Radio Navigation Board

Flavio SBARDELLATI, European GNSS Agency (GSA)

11 May 2021, online

Agenda



- Role of authentication
- Galileo authentication (OS-NMA, CAS and PRS)
- Galileo Navigation Message Authentication
- OS-NMA market opportunities
- OS-NMA roadmap



Why is Authentication needed?

Any 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 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



GNSS authentication is one important contributor to the overall trustworthiness of PVT based applications,

 \rightarrow Not the only one!

Credit: INLANE project, funded by the GSA (H2020)

Galileo services contribute to mitigate the spoofing risk of GNSS-based solutions





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 (TESLA protocol – asymmetric)

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 main 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) and timing parameters (GGTO and UTC), delayed	
Time to first Authentication	One to few minutes	
Anti-tampering characteristic for	Light: the receiver only stores a public key.	
receiver	To be considered depending on the specific application threats.	
Other requirements	Loose time synchronisation.	
	(In the order of 18 s under nominal conditions)	

A clear differentiator set to make the difference in several markets

















The GSA has been funding the integration of OS-NMA capability across various market segments

🗾 Fraunhofer

IK4O

- Galileo based positioning solution for **connected automated** driving applications
- Exploiting the distinguished features of Galileo signals as well as combining it with other positioning and sensor technologies. \rightarrow OS-NMA

Da

....





ASTAZERO

Trustable Galileo-based timing receiver for critical infrastructures



GIAN

deimos

GSA is funding two projects (GIANO and GEARS) aiming to increase robustness and resilience of timing and synchronization (T&S) services for energy, finance and communication networks but also for transport and other governmental applications.



GNSS resilience to spoofing and jamming achieved through:

PIK TIME SYSTEMS

- **GNSS** Authentication (OS-NMA)
- Multi-frequency

halesAlenia

- Multi-constellation
- RF Interference detection and mitigation techniques



Also addressing regulated applications: Smart Tachograph





OSNMA Roadmap





PUBLIC NOTE	OS-NMA INFO NOTE	-	-
TECHNICAL BASELINE	-	OSNMA ICD, RX guidelines for Public Testing	OSNMA ICD, Rx Guidelines, Service Definition Document
OBJECTIVE	System readiness Operations Readiness	(1) User feedback (11) Support market and product development (111) Fine tuning (upstream and downstream)	Benefit for users and society

Any questions?





13

Thank you!

Linking space to user needs



European **G**lobal Navigation How to get in touch: **S**atellite Systems www.GSA.europa.eu Agency EGNOS-portal.eu UseGalileo.eu GSC-europa.eu G - œ GALILEO The European GNSS Agency is hiring! Apply today and help shape the future of satellite navigation!