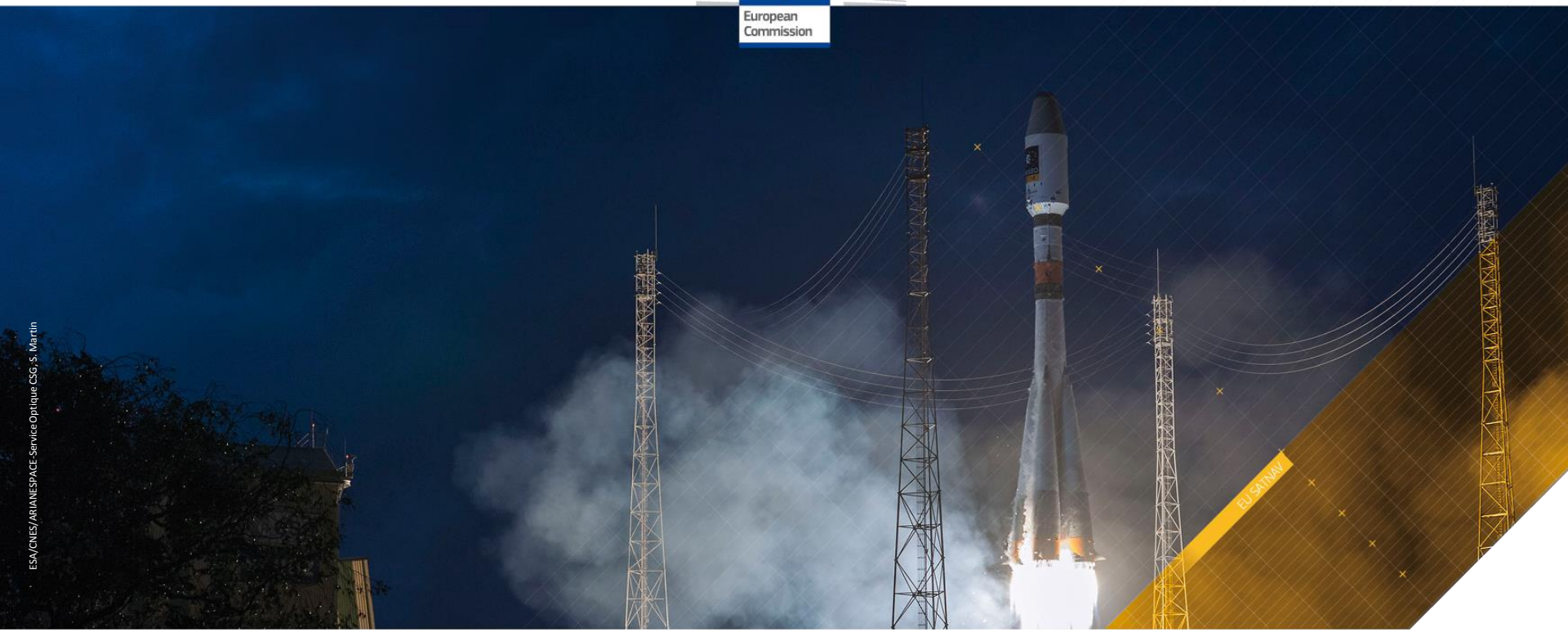
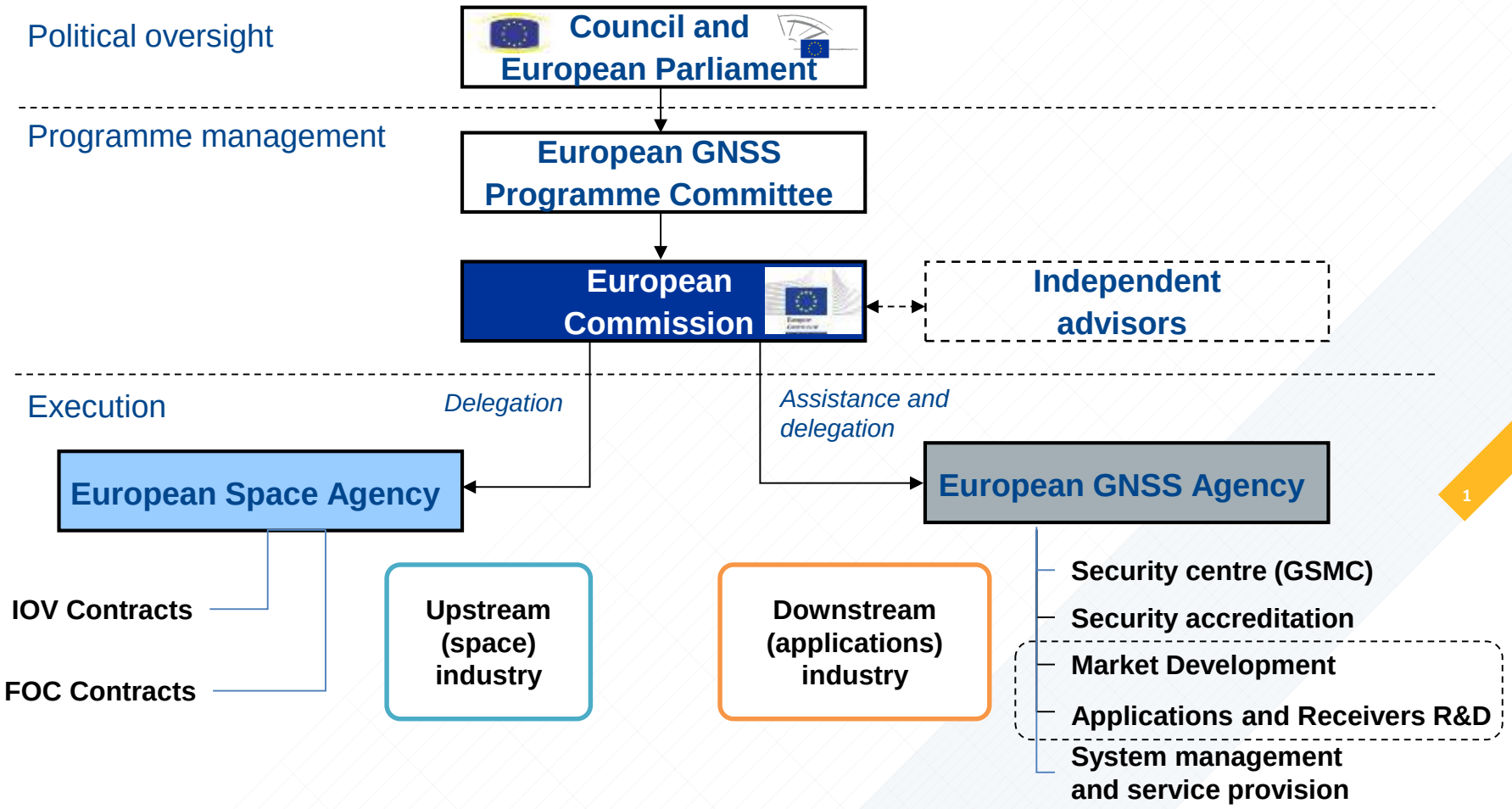



# European satellite-based navigation (GNSS) for Smart Tachographs: *Galileo Open Service authentication*

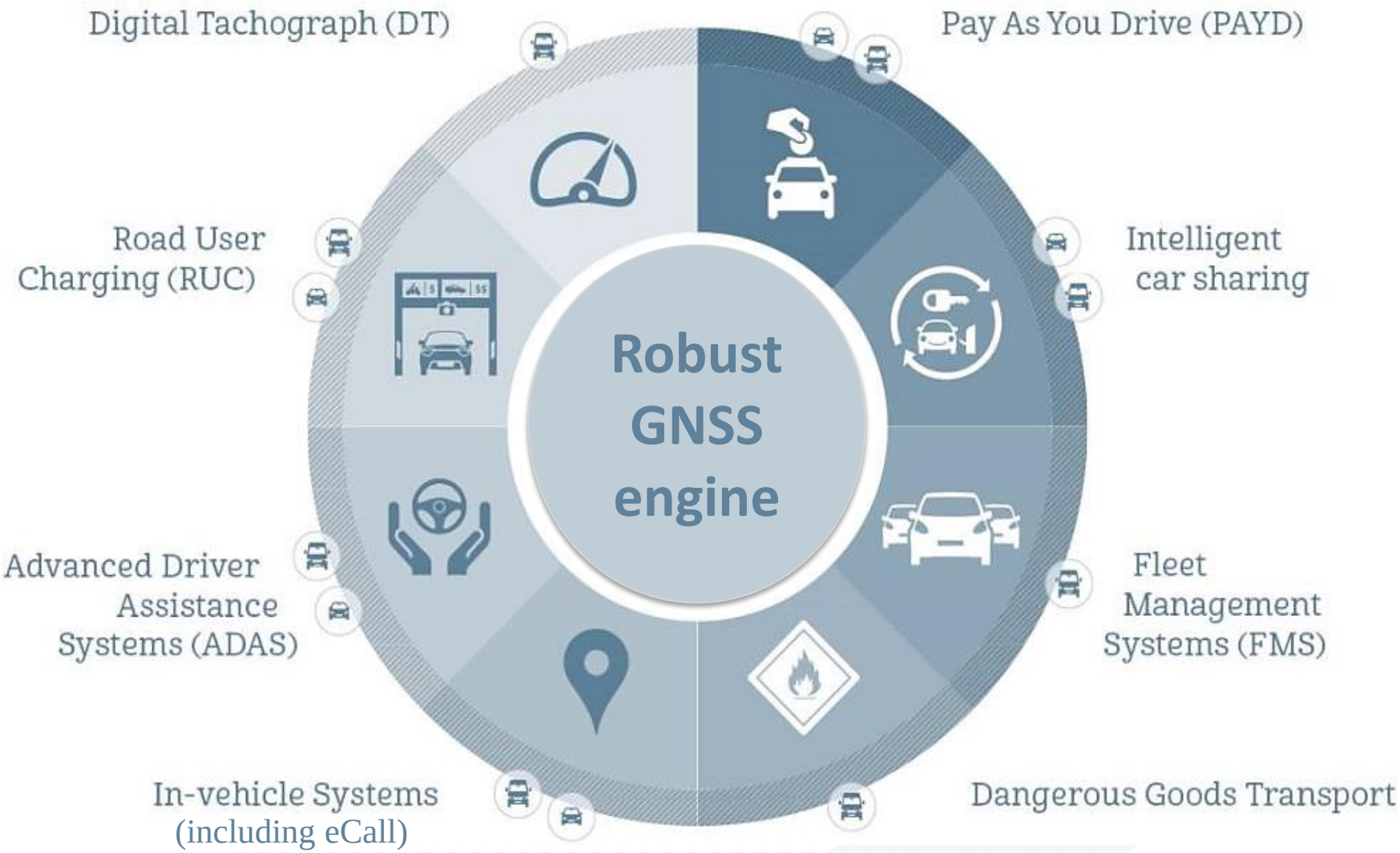
Ignacio Fernández Hernández - European Commission
Alberto Fernández Wyttenbach - European GNSS Agency

**Tachograph Forum, 28 November 2016**

# THE EU GNSS PROGRAMMES

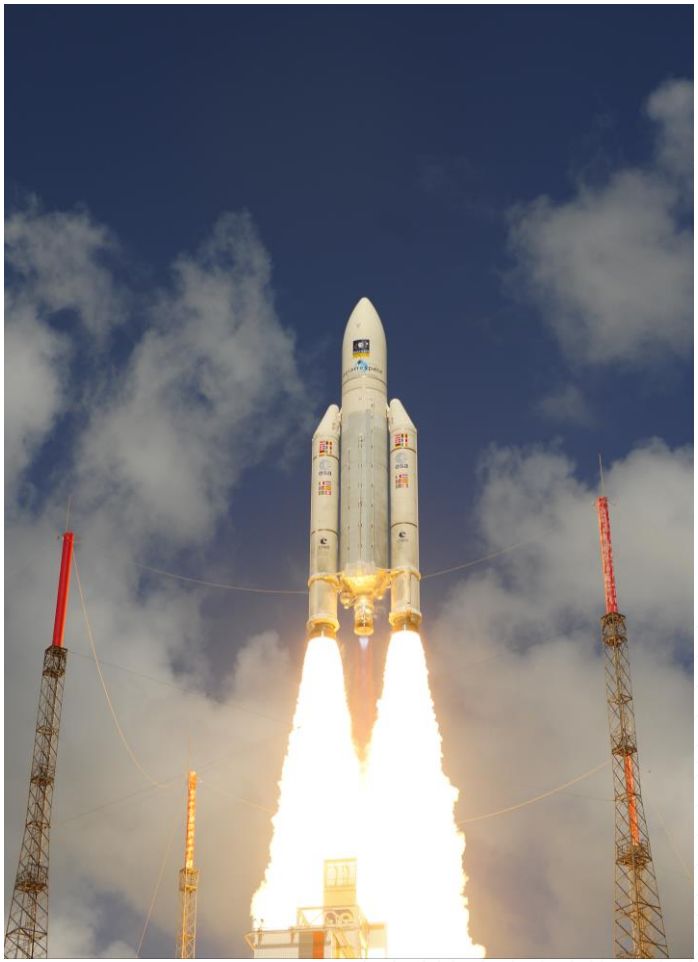


# OUR VISION: A ROBUST GNSS CAN ACT AS A SINGLE LOCATION "ENGINE" FOR MULTIPLE ROAD APPLICATIONS




*Source: FOSTER ITS project, 2016*

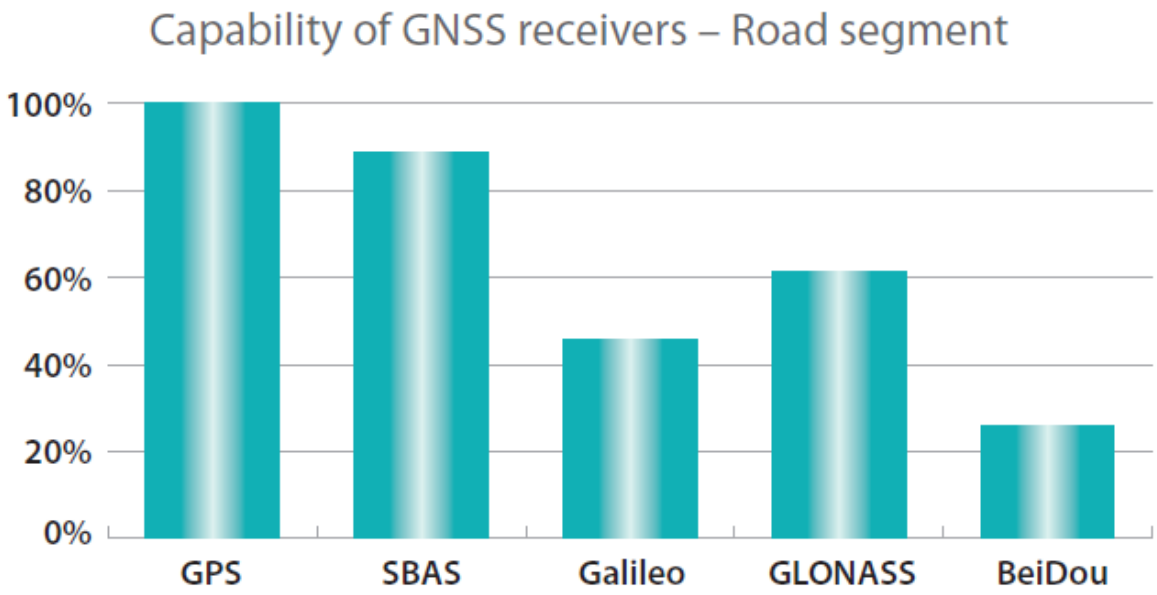
# GALILEO IS IMPLEMENTED IN A STEP-WISE APPROACH



*Source: ESA, 2016*

- **Global coverage**
- **Fully compatible with GPS**
- **Open service free-of-charge and delivering dual frequencies** (better performances)
- **18 satellites have been launched**, till now:
  - ✓ 4 satellites launched together in Nov 17
- **12 additional** satellites already in production
  - ✓ 4 satellites per year until 2020
- **Initial operational services** declaration at the end 2016

# ANALYSIS OF THE RECEIVERS' CAPABILITIES SHOWS GALILEO ENCOURAGING POSITION WITHIN MULTI-CONSTELLATION



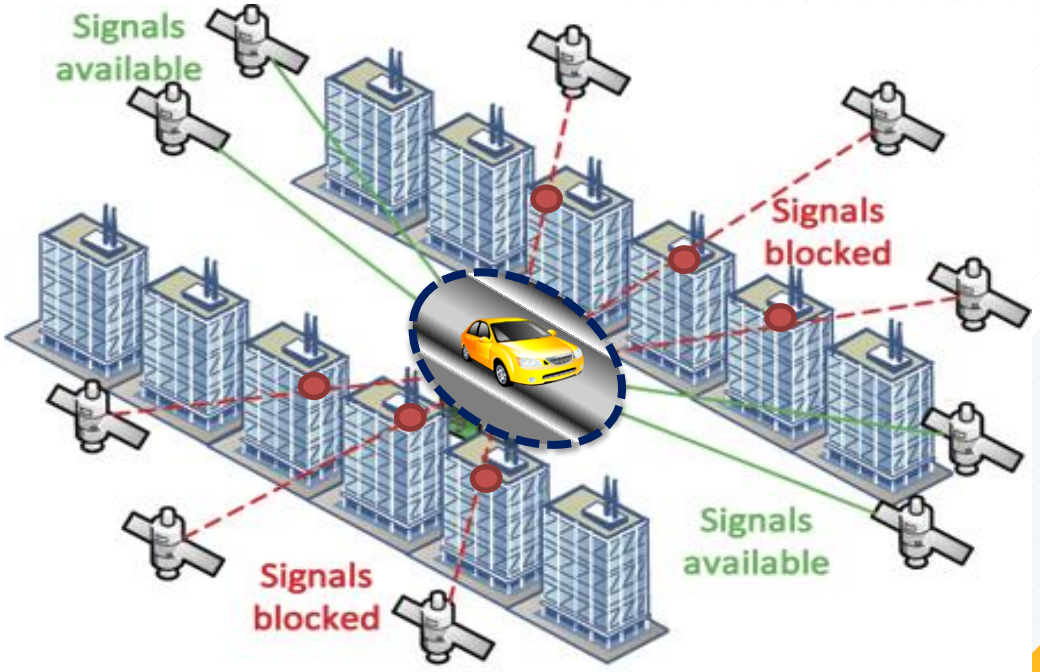

Automotive chipset suppliers leaders support Galileo

GNSS MARKET REPORT
ISSUE 4

Source: http://www.gsa.europa.eu/system/files/reports/GNSS-Market-Report-2015-issue4_0.pdf

# MULTI-CONSTELLATION AND MULTI-FREQUENCY CONCEPTS

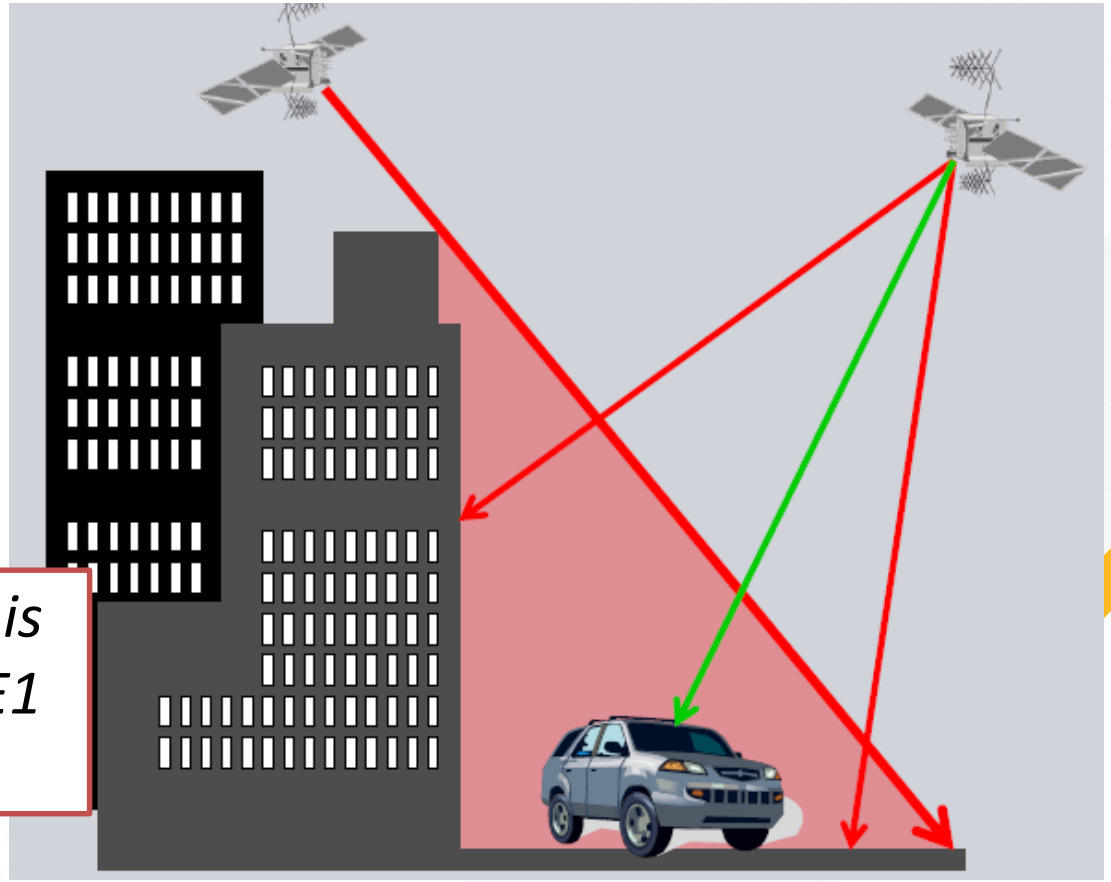
✓ *Multi-constellation*:
When buildings block the signal and reduce the number of visible satellites, the availability of more constellations ensures a **much more accurate final position**




✓ *Multi-frequency:*
Galileo, as well as GPS, is providing a **second frequency on the Open Service, the E5/L5**: increased accuracy (elimination of ionospheric errors and quick transition form code phase to carrier phase navigation) and increased resistance to multipath (also respect to L2C, the other second frequency of GPS…)

# GALILEO CONTRIBUTION TO THE MULTIPATH PROBLEM

The strength of Galileo signal, together with an **advanced code modulation**, makes Galileo better mitigating multipath effects (especially in E5, but also E1)

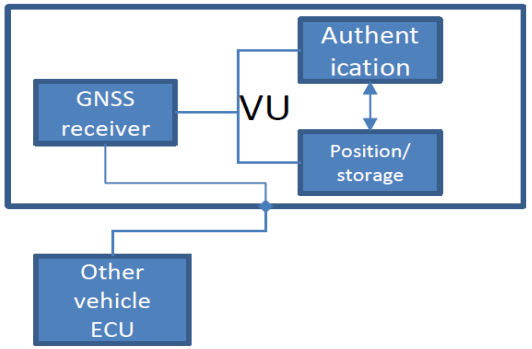


*"The effect of multipath is **2x smaller** with Galileo E1 compared to GPS L1"*

BROADCOM

# GALILEO UNIQUE DIFFERENTIATOR: SIGNAL AUTHENTICATION

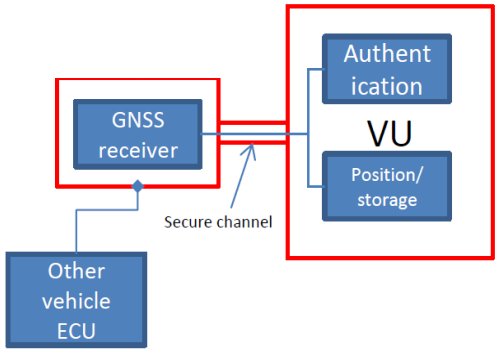
- **Security** is a **major concern** in the Smart Tachograph
- Galileo provides an **efficient**, **resilient** and **low-cost solution** against jamming or spoofing attacks




**Authentication**

- Ability of the system to guarantee to the users that they are utilizing signals from the Galileo satellites and not from any other source

vs.




Authentication of Galileo signals in the Open Service looks **more convenient for the industry** than the signal encryption between GNSS receiver and VU

# INTENTIONAL AND NON-INTENTIONAL THREATS

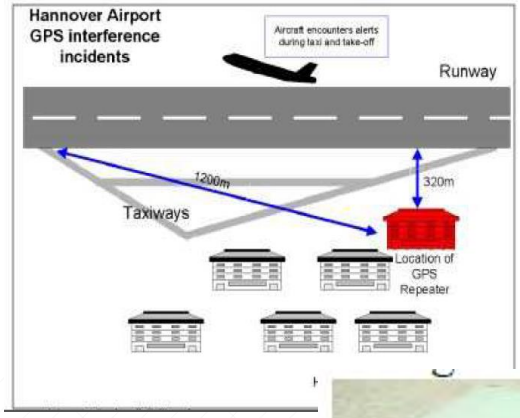
- Hannover Airport, 2010: GPS repeater at higher-than expected power. Hangar door open. Planes took off with wrong GPS position.

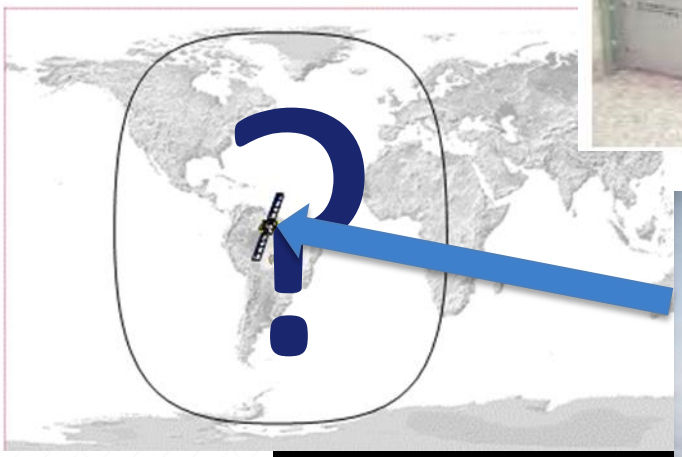
- Careless GNSS-like signal transmission for testing purposes.

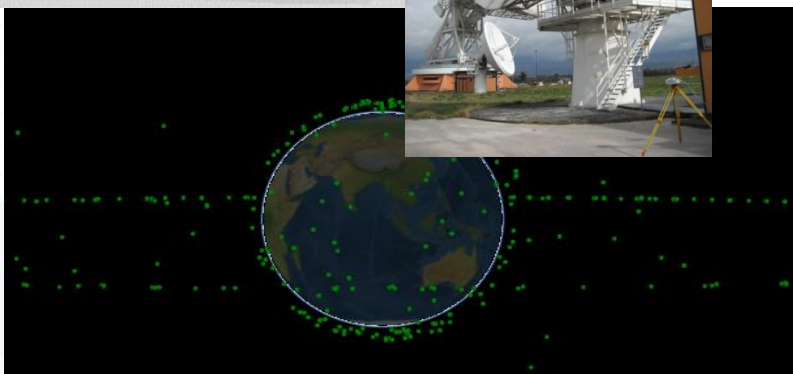
- RF regulation under each Sovereing State (repeaters, pseudolites…)

- Many academic (Texas Austin), and non-academic spoofing attacks demonstrated.

- **What about non-publicised GNSS spoofing?**





# INTENTIONAL AND NON-INTENTIONAL THREATS

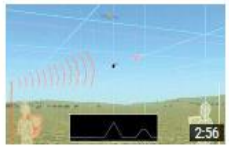
GALILEO EGNOS
NAVIGATION SOLUTIONS POWERED BY EUROPE

YouTube BE

GPS spoofing

Filters

**JUNE 2016 ->** About 5,350 results




Demonstration of a Remote Unmanned Aerial Vehicle Hijacking via GPS Spoofing
CockrellSchool
3 years ago • 14,291 views
Military Global Positioning System (GPS) signals have long been encrypted to prevent counterfeiting and unauthorized use.


DEF CON 23 - Lin Huang and Qing Yang - Low cost GPS simulator: GPS spoofing by SDR
DEFCONConference
6 months ago • 2,262 views
It is known that GPS L1 signal is unencrypted so that someone can produce or replay the fake GPS signal to make GPS receivers ...
CC


Simple GPS Spoofing Attack
Noone Known
8 months ago • 645 views
N/A.


Spoofing GPS Signal
MobileMap
1 year ago • 3,466 views
Showa how to make GPS, QZSS SPOOF Signal.


Fake Your GPS Location to Anywhere in the World - Android [How-To]
GadgetHacks
1 year ago • 32,527 views
How to Spoof Your Location for Improved Security Full Tutorial: ...

GPS spoofing

Filters

**NOVEMBER 2016 ->** About 40,000 results


Pokemon Go Hack - How to Not Get Banned While Using GPS Spoofing!
Max Lee
4 months ago • 559,221 views
Here's a tutorial on how to not get banned while using Pokemon Go hacks/cheats that use **GPS spoofing**. VPN app is available for ...


POKEMON GO ++ GPS TELEPORT HACK (WORKING) UPDATED!! GPS SPOOFING HACK 1.3.1
str0bots GAMING
3 months ago • 243,003 views
SUBSCRIBE: http://bit.ly/str0botsgaming Hey guys! Since the usual teleport pokemon go app is down on iosemus, i decided to ...


Pokemon GO Moving GPS Spoof | Best Farming Hack
SMHax Nizlmmk
4 months ago • 238,786 views
Showing off the best method to farm pokemon and pokecenters using GPS Location hack. THIS ISNT A TUTORIAL, DON'T BE ...


Pokemon Go GPS Location Spoofing on iOS without jailbreak
Tommy Callaway
4 months ago • 458,278 views
Learn how to change the iPhone GPS location using some pretty standard developer tools provided by Apple, and a little bit of ...

# EU COMMITMENT TO GALILEO AUTHENTICATION

- ***European Parliament resolution (June'16):***

*"Recalls that Galileo will have 'differentiators', that is, certain advantages not provided by other GNSS constellations, such as* ***open service authentication*** *and the very high precision and* ***reliability of the commercial service****; stresses that it is essential for these differentiators to be made available as soon as possible to help ensure that Galileo becomes a reference constellation and that advantages over its competitors can be promoted; "*

**European Parliament**
2014-2019

**TEXTS ADOPTED**
*Provisional edition*

**P8_TA-PROV(2016)0268**

**Space market uptake**

**European Parliament resolution of 8 June 2016 on space market uptake (2016/2731(RSP))**

# EU COMMITMENT TO GALILEO AUTHENTICATION

***European Commission and European Member States:***

- The majority of EU member states explicitly support the introduction of OS NMA and CS Authentication for Galileo between 2018-2020.
- Implementing Act approval process in its final stage, including OS NMA and CS Authentication (in addition to already foreseen PRS).
- ESA/GSA estimation of development and operation cost introduced in internal Cost-Benefit Analysis exercise with positive results. Estimated cost of implementation and 10-year operation of NMA of ~10M€.

(...)

(6) The authentication capacity should increase the degree of safety and prevent risks of falsification and fraud in particular. Additional features must therefore be incorporated into satellite signals in order to assure users that the information which they receive does come from the system under the Galileo programme and not from an unrecognised source. The authentication capacity of the commercial service would be based on that developed by the open service, which already comprises the identification of data linked to geolocation contained in the signals. However, with a view to improved protection, it would also incorporate the recognition of encrypted codes also contained in the signals.

(7) Technical and operational specifications should therefore be established to allow the commercial service offered by the system under the Galileo programme to fulfil the function referred to in Article 2(4)(c) of Regulation (EU) No 1285/2013.

(8) The measures referred to in this decision are in line with the opinion of the Committee set up pursuant to Article 36(1) of Regulation (EU) No 1285/2013,

HAS ADOPTED THIS DECISION:

*Article 1*

The technical and operational specifications allowing the commercial service offered by the system under the Galileo programme to fulfil the function referred to in Article 2(4)(c) of Regulation (EU) No 1285/2013 are set out in the Annex.

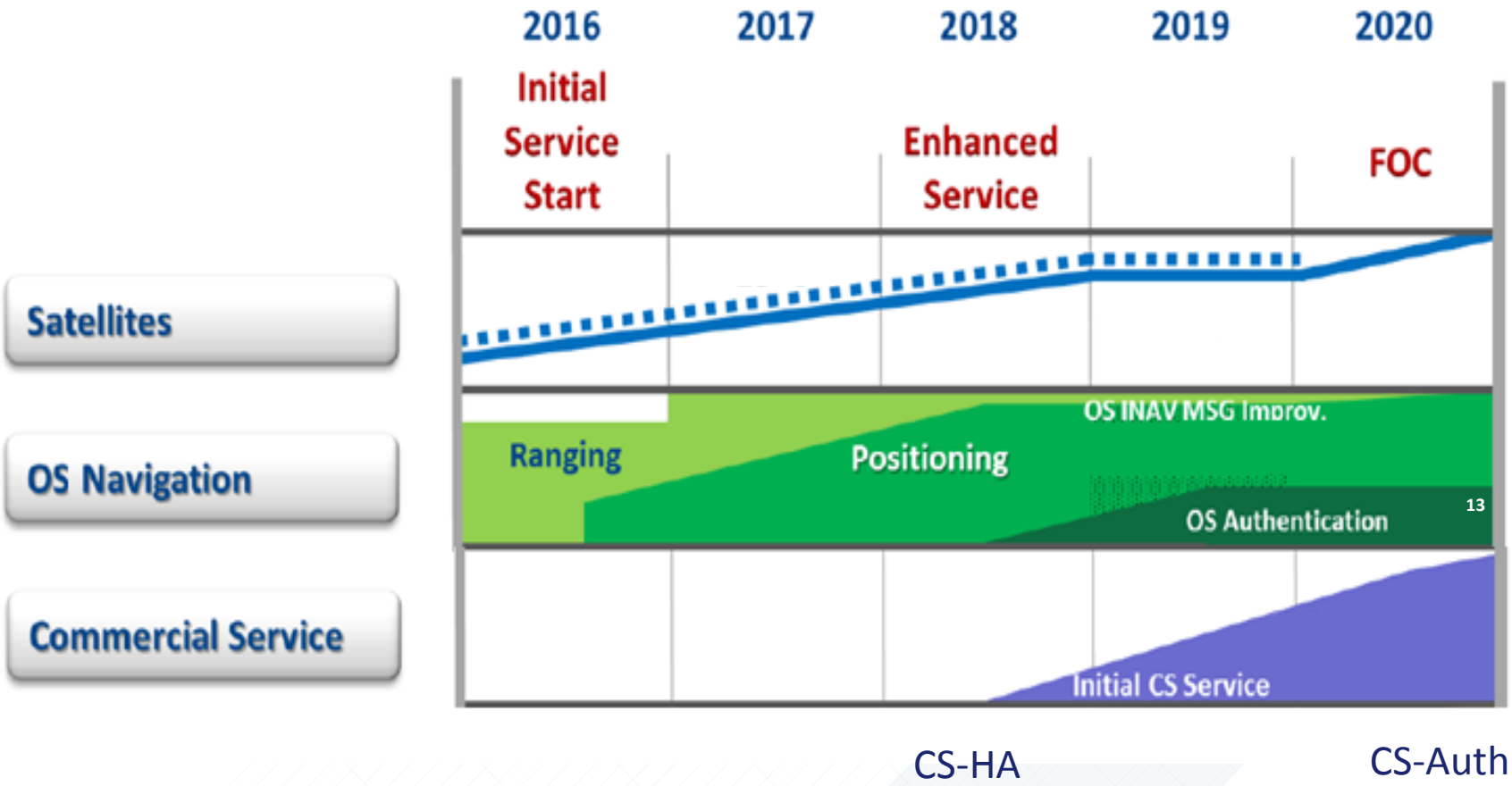
*Article 2*

This Decision shall enter into force on the twentieth day following its publication in the *Official Journal of the European Union*.

Done at Brussels,

*By the Commission*
*President*
*Jean-Claude JUNCKER*

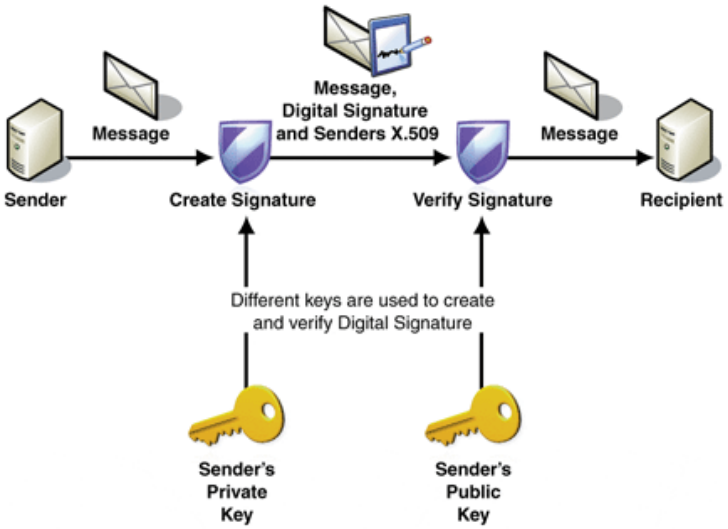
# GALILEO AUTHENTICATION SERVICES PROPOSED (non-PRS)




*(Subject to confirmation at SDCDR)*

# SERVICE DEFINITION DRIVERS

- **Open access**: asymmetric cryptography.
- **One-to-many, one way** communication.
- **Noisy, low bandwidth** channel
- Long-term **cryptographically secure**.
- **Backward compatible**. Does not affect users not interested.
- Commensurate **receiver requirements**: CPU, memory, connectivity,  protection.



# OSNMA SUMMARY

| Indicator | Result | Comments |
|---|---|---|
| **Availability** | No degradation | Same performance as standard navigation with Galileo I/NAV |
| **Accuracy** | No degradation | Same performance as standard navigation with Galileo I/NAV |
| **TTFAF** | No degradation | Except in "cold start, no K-root" or "slow MAC" cases |
| **TBA** | 10-15 sec | |
| **Signal unpredictability (symbol level)** | ~every 1.6 sec | ~10 unpredictable sps transmitted. Improves protection against signal replay attacks. |
| **Receiver Implementation Effort** | low | Only firmware update to process OSNMA.<br><br>Can be combined with other measures (clock, sensors, power monitoring) to further enhance protection against replay attacks. |

# CONCLUSIONS

- GNSS is at the center of road applications
- GNSS receiver trends are toward multiconstellation, including Galileo
- Galileo constellation is deploying very fast and follows the expected schedule
- SIS authentication is desirable (SCA, NMA) for future satnav services.
- EU is committed to adding authentication as a differentiator of Galileo, for OS, CS and PRS (different user types): CS E6 signals with SCA by 2020 and OS E1B with OSNMA starting 2018 and FOC at 2020, at very low cost.
- Current OSNMA proposed in "Reserved 1" field (20bps) of E1-B through TESLA protocol. Analyses and simulations incl. Degraded environments show no performance degradation wrt. Standard PNT.
- OSNMA receiver implementation efforts/HW are low.

# THANK YOU

# Q&A?

Ignacio Fernández Hernández - European Commission
Alberto Fernández Wyttenbach - European GNSS Agency