Galileo Open Service Navigation Message

31/01/2018

S. Binda - GNSS Interferentie en Authenticatie, Haarlem, NL

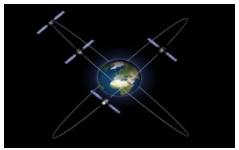
GALILEO System Current Status

Deployment / Exploitation Plan

Development
GIOVE A & B

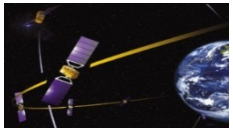
2005 & 2008

In-Orbit Validation



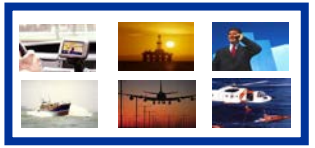
2011-2013

Initial Services



2014-2017

Enhanced Services



2018-2019

Full Services

2020

Galileo constellation Status

Navigation Payload (14 Operational)

22 satellites in orbit

- 4 under commissioning
- 2 in testing
- 1 spare
- 1 unavailable

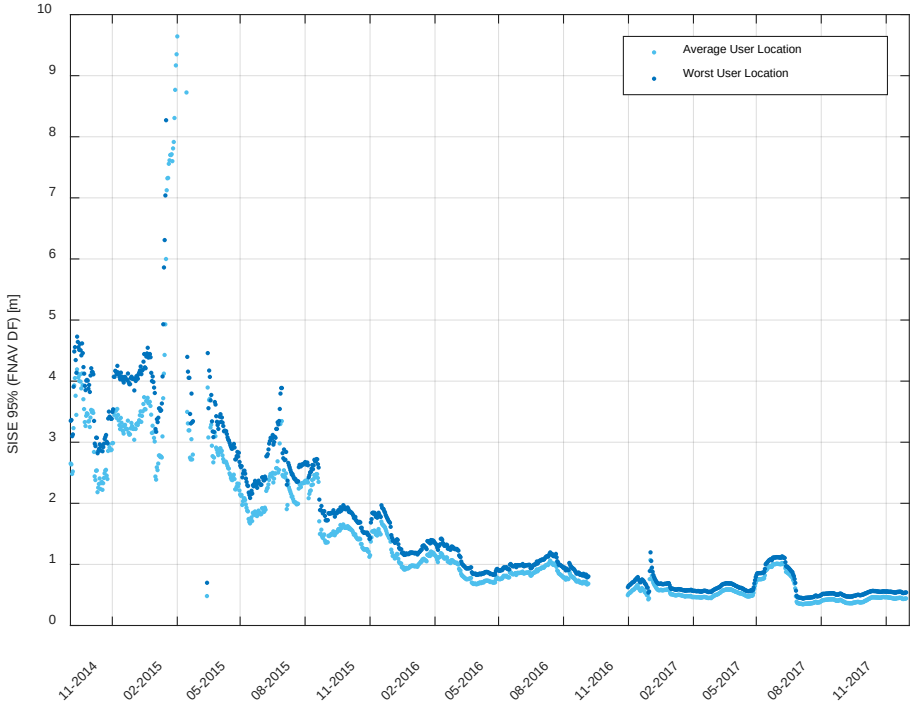
Search and Rescue Payload (15 Operational)

- 2 out of 22 satellites with no SAR Transponder (by design)
- 4 under commissioning
- 1 spare

4 unoccupied reference slots

Accuracy and Availability

As-observed Ranging Performance



- Decreasing Ranging Error trend due to increasing number of Satellites and G/S improvements
- Ranging accuracy (95%) 0.43m all satellites, 0.56m worst satellite in November 2017

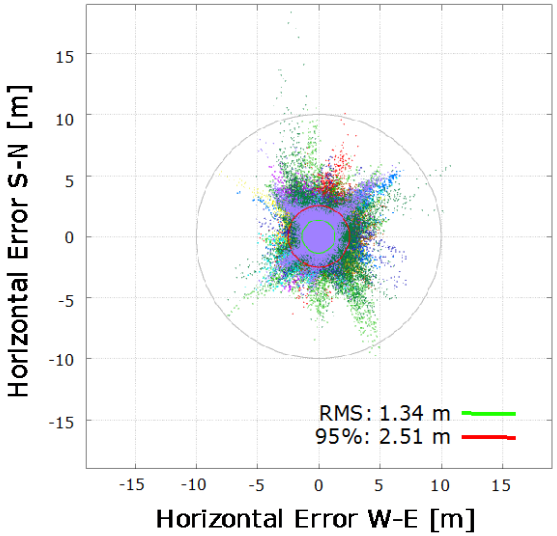
Galileo and GPS Scoreboards

Source: GPS Programme Update, UN ICG-12, December 2017

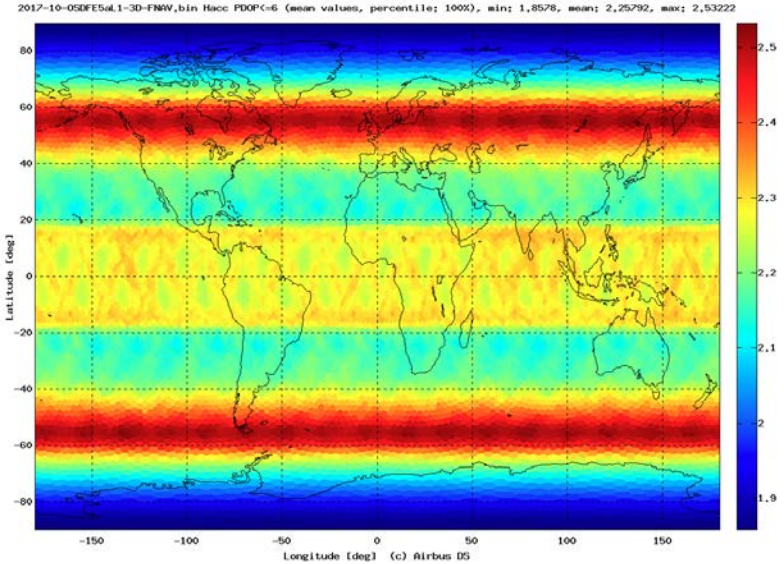
Source: Galileo OS KPI Monthly Report, December 2017

Positioning Performance & Availability

- 14 satellites usable
- 86% Availability of H Accuracy <10 m
- 72% Availability of Global PDOP <=6

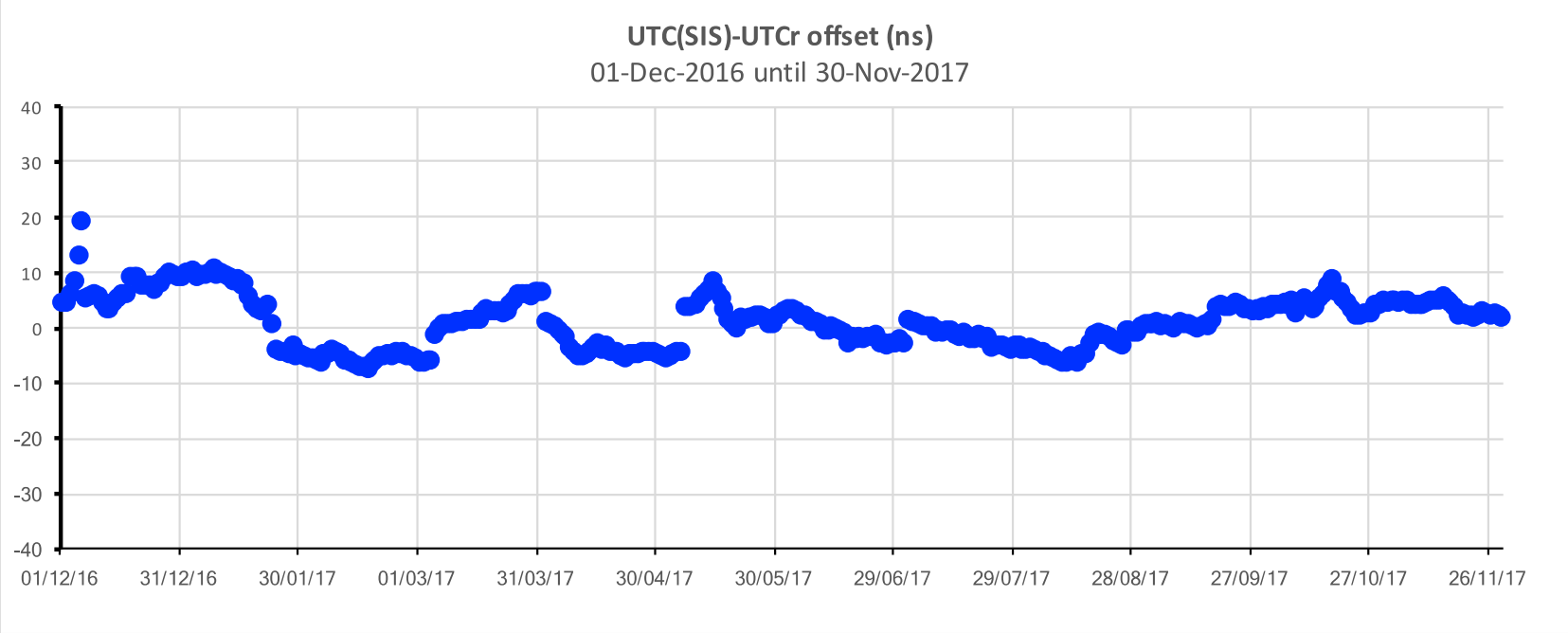


Dual Frequency Horizontal Accuracy measured by global Receiver Network (10 – 13 Dec. 2017)



Global Dual Frequency Horizontal Accuracy (when PDOP <= 6)

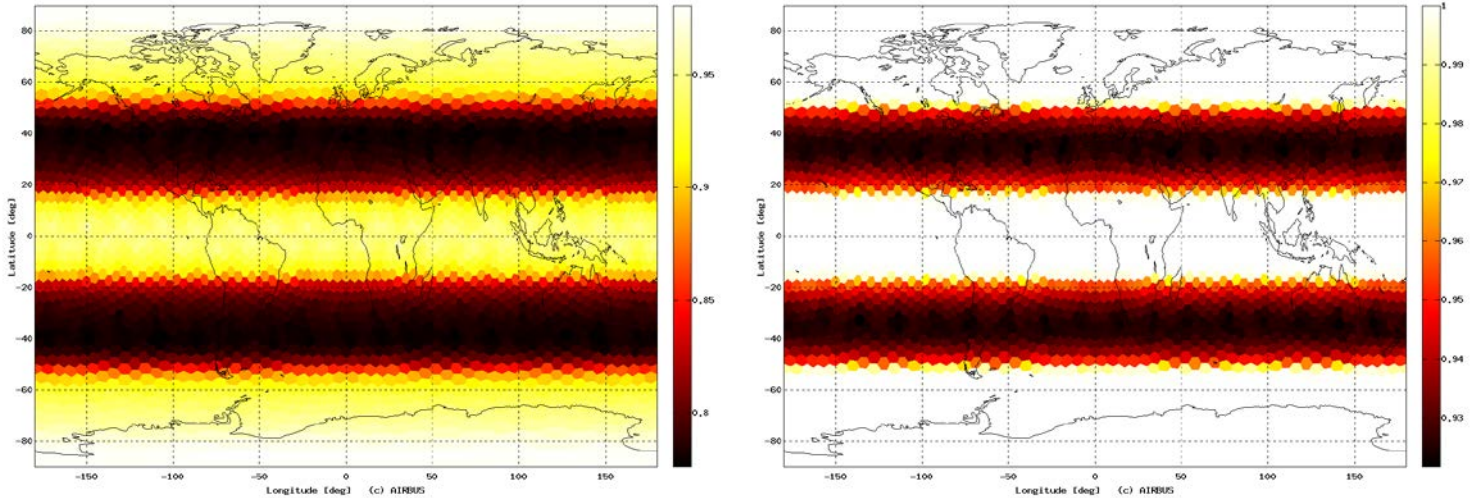
Timing Accuracy and Availability



- Overall very good performance of 8.9 ns (95%)
- Initial Services target: 30 ns (95%)

Predicted Positioning Performance & Availability with L9

- 4 more satellites operational in Q3 2018
- Satellites in operational constellation: 14 → 18
- Availability of H Accuracy <10 m 86% → 96% (Average User Location)
- Global PDOP <=6 availability 72% → 95% (Average User Location)



Availability of Horizontal Position Accuracy < 10 m for 14 satellites (left) and 18 satellites (right)

Satellite Metadata for High Accuracy Services

Requested by

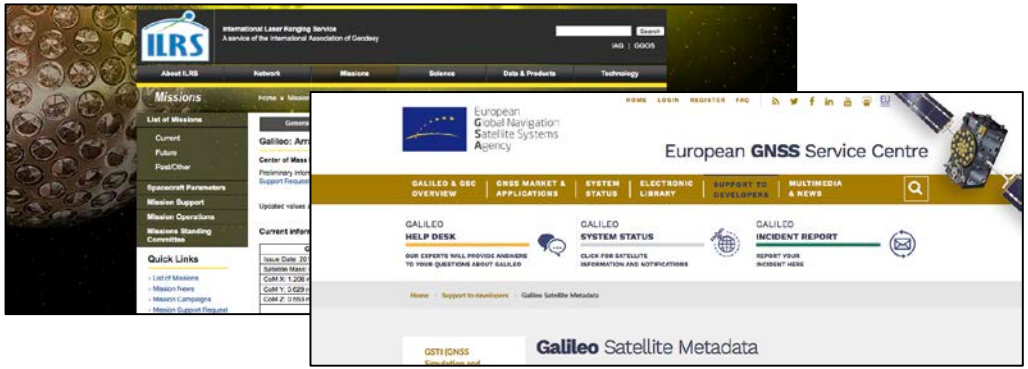
- Galileo scientific advisory committee (GSAC)
- International GNSS Service (IGS)

Status

- Galileo IOV Satellite Metadata released during Initial Service Declaration (Dec-2016)
- Galileo FOC metadata released (Oct-2017)
- Galileo FOC metadata update for L9 and 10 (planned 2018)

Content

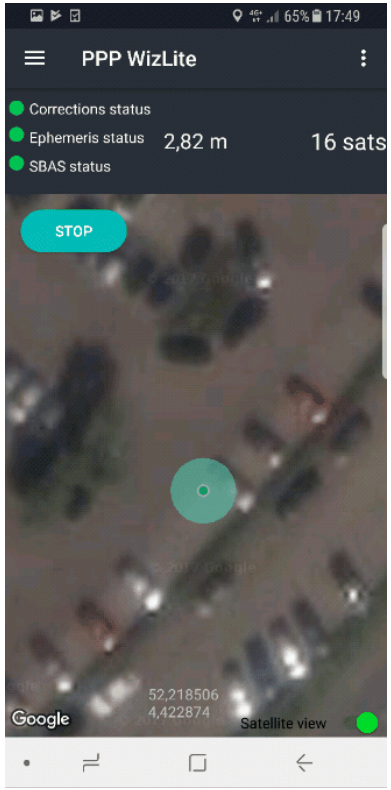
- Attitude Law
- Mass and Centre Of Mass evolution
- Navigation Antenna Phase Centre Corrections
- Geometry and optical properties
- Laser Retro Reflector Location
- Satellite Group Delay



https://www.gsc-europa.eu/support-to-developers/galileo-iov-satellite-metadata#2

https://ilrs.cddis.eosdis.nasa.gov/missions/satellite_missions/current_missions/ga01_com.html

CNES PPP WizLite an example of high accuracy GNSS app based on the Android 7.0 (Nougat) raw measurements



Samsung S8 test in ESTEC car parking

CNES Precise Point Positioning WizLite engine implemented on Android devices exploiting multi constellation raw measurements.

- **From conventional smartphone accuracy of about 10m (95%) to sub-meter positioning for static user and meter level for dynamic mode. Convergence time is below 10 minutes.**

- PPP enabled using precise orbit, clock and ionosphere corrections (VTEC) from the IGS Real Time Service (RTCM format).

- GPS, GLONASS and GALILEO supported (E1 only). SBAS enabled.

- Only code and Doppler measurements processed in this demonstration. Carrier phase not yet exploited due to limitations associated to power duty cycle in smartphones.

https://play.google.com/store/apps/details?id=jocs.fr.gnss_ppp&hl=nl
Based on raw GNSS measurements, the app combines RTK library and very high level algorithms developed by the French Space Agency (CNES PPP-Wizard)

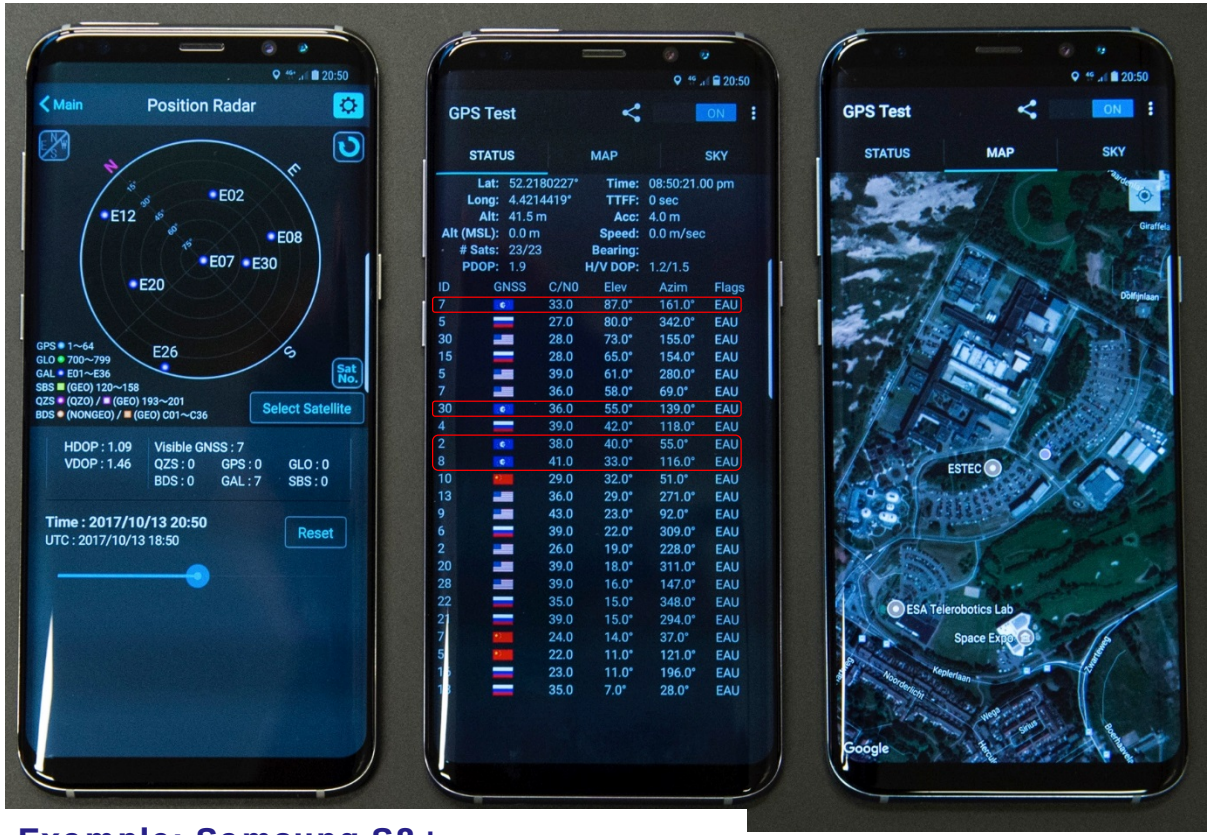
GALILEO In Use

Multi-GNSS Single Frequency interoperability

Number of Galileo-enabled smartphones growing…

Brand	Type
Apple	iPhone 8 Plus
Apple	iPhone 10/X
Apple	iPhone 8
bq	Aquaris V Plus
bq	Aquaris V
BQ	Aquaris X5 Plus
BQ	Aquaris X
BQ	Aquaris X Pro
Google	Pixel 2
Google	Google Pixel 2 XL
Huawei	P10 plus
Huawei	Mate 9 pro

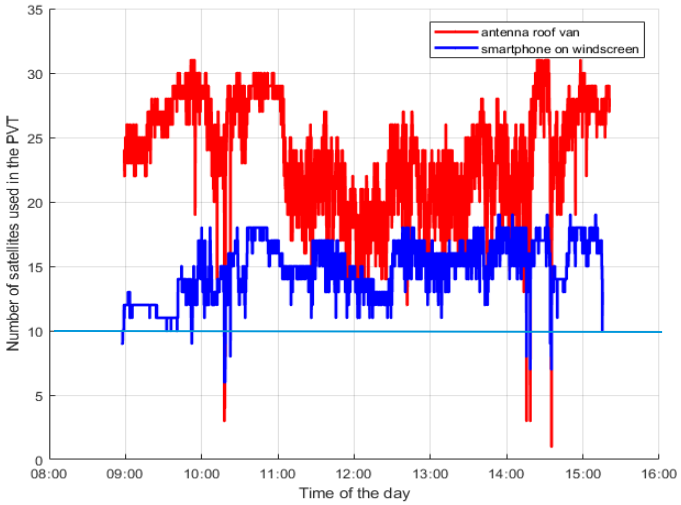
Brand	Type
Huawei	P10
Huawei	Mate 10 Pro
Huawei	Mate 9
LG	V30
Mediatek	Meizu Pro 7 Plus
Mediatek	Meizu Pro 7
Motorola	Moto X4
Oneplus	Oneplus5
Samsung	S8+
Samsung	S8
Sony	Xperia XZ Premium
Vernee	Apollo 2

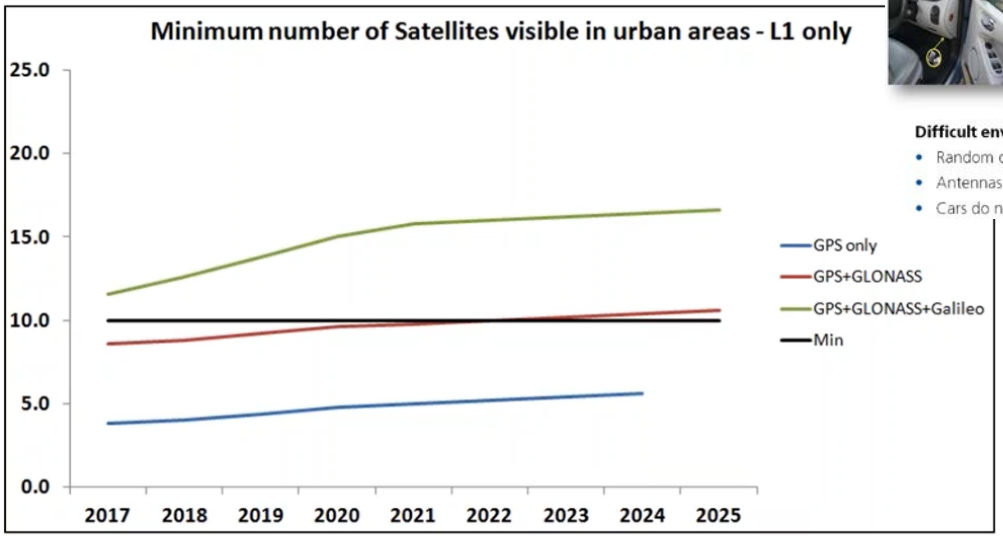


Example: Samsung S8+

Multi-GNSS Single Frequency availability

- Multi-constellation needed for target availability of satellites (10 measurements)
- Results from smartphones used as after-market in car navigator or in urban environments
- Triple constellation GPS + GAL + GLO already now allows good reception in urban environments (further improvement with constellation completion)





Difficult environment

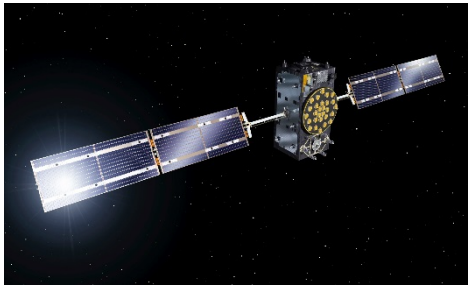
- Random device placement
- Antennas are miniaturized
- Cars do not stay on highways only

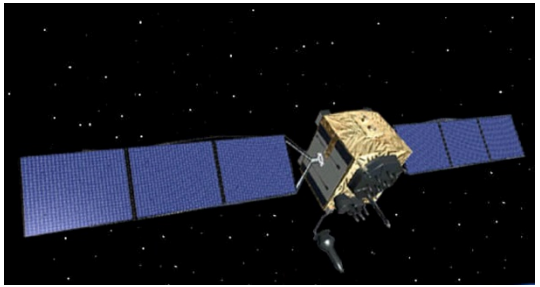
A min. of 10 Satellites visible is constantly required to achieve reliable positioning

First mass-market dual frequency GNSS receiver

- World's first mass-market, dual frequency GNSS receiver device for smartphones
- Usage of E1/L1 and E5/L5 frequencies benefit from better accuracy, ionosphere error cancellation, improved code tracking pseudorange estimates and faster transition from code tracking to phase tracking
- Provides lane-level accuracy with minimal power consumption and footprint enabling high-precision LBS applications, including lane-level vehicle navigation and mobile augmented reality (AR)

15 operational Galileo satellites (E1/E5) + **12 operational GPS Block IIF satellites (L1/L5)**





Future GNSS/RNSS common frequencies, showing the potential of E5a/L5 and of E1/L1 combination

	L5 / L5OC / E5a / B2a	L2 / L2C / L2OC	E6 / LEX	L1 / L1OC / E1 / B1
GPS	30	30		30
GLONASS	24	24		24
Galileo	30		30	30
BeiDou	35		35	35
QZSS	3	3	3	3
IRNSS	7			
	129	← ARNS* Bands →		122

Frequency band used by the system, with N = number of satellites

Frequency band not used by the system

* ARNS = Aeronautical Radio Navigation Service: Frequency bands allocated worldwide to GNSS on a primary basis, granting a better protection against interference

AUTHENTICATION

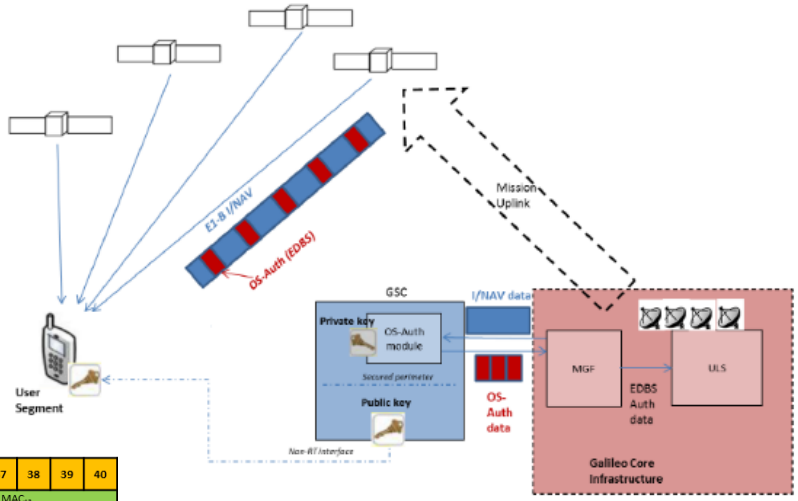
Towards Robust PNT

Issue	System requirements	Receiver requirements
Signal generators, non authentic Navigation data	Navigation Message Authentication (NMA)	NMA software module User based protection (industry choice)
Signal based replay attacks	Code Based Authentication (CBA)	CBA module User based protection (industry choice)

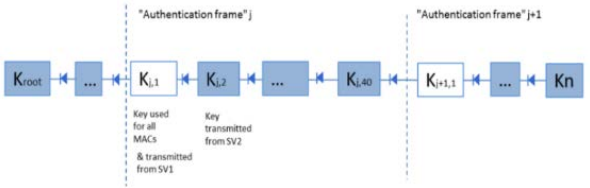
- → **Galileo aims to compete** in the robust PNT market
- → Stepwise introduction of the authentication services, to align with user needs and receive feedback:
  - **Short-term**: **NMA** is the target for Galileo, low system impact and easy integration in receivers
  - **Long-term**: **CBA** is currently under design for next generation satellites, for enhanced robustness and capability to provide ranging authentication. Impact at ground, space and user segment.
- → Difficulty to adapt modern ICT security life cycle (security patches in computer and networks performed in hours) to GNSS space systems (**life cycle of 20 years**).

OS Navigation Message Authentication

- E1B External Data Broadcast Service (page changing every 2s) to provide authentication data to the user
- Reuse of 40bits of previous External Region Integrity Status (ERIS)
- Protocol based on an adaptation of TESLA protocol [IETF RFC 4082]
- Asymmetry provided by delayed key
- It offers unpredictability features but does not provide a ranging authentication service



Pag	1	...	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
1	NMA Head			MAC_{11}										MAC_{11} info field																MAC_{12}					
2	DSM Head			MAC_{12}										MAC_{12} info field																MAC_{13}					
3	DSM block(i)			MAC_{13} info field																										Key_1					
4				Key_1																															
5				Key_1																															
6				MAC_{21}										MAC_{21} info field																MAC_{22}					
7				MAC_{22}										MAC_{22} info field																MAC_{23}					
8				MAC_{23} info field																											Key_2					
9				Key_2																															
10				Key_2																															
11				MAC_{31}										MAC_{31} info field																MAC_{32}					
12				MAC_{32}										MAC_{32} info field																MAC_{33}					
13				MAC_{33} info field																											Key_3					
14				Key_3																															
15				Key_3																															



MAC: Message Authentication Code DSM: Digital Signature Message

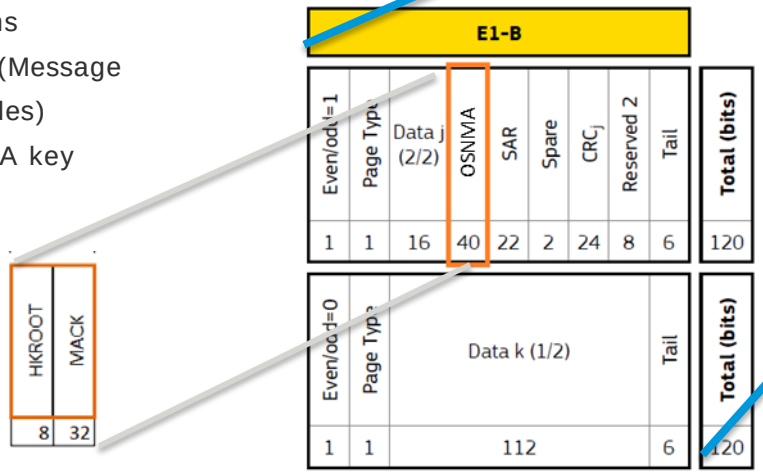
OS NMA Format

Specification

https://www.gsa.europa.eu/development-supply-and-testing-galileo-open-service-authentication-user-terminal-os-nma-gsa

Format

- HKROOT (Headers and KROOT) section: 120 bits per subframe
  - NMA and DSM (Digital Signature Message) Header (8+8 bits)
  - DSM block (104 bits)
- MACK section: 480 bits per subframe
  - 1 to 3 MACKEY sections
    - n truncated MACs (Message Authentication Codes)
    - time-delayed TESLA key



T_0 (GST_0 sync.)	E1-B content					E1-B page	E1-B sub frame ID
0 s	Spare Word (2/2)	ERIS	SAR	CRC	Region status	Odd	N-1
1 s	Word 2 (1/2)					Even	N
2 s	Word 2 (2/2)	ERIS	SAR	CRC	Region status	Odd	N
3 s	Word 4 (1/2)					Even	N
4 s	Word 4 (2/2)	ERIS	SAR	CRC	Region status	Odd	N
5 s	Word 6 (1/2)					Even	N
6 s	Word 6 (2/2)	ERIS	SAR	CRC	Region status	Odd	N

[…]

23 s	Word 3 (1/2)					Even	N
24 s	Word 3 (2/2)	ERIS	SAR	CRC	Region status	Odd	N
25 s	Word 5 (1/2)					Even	N
26 s	Word 5 (2/2)	ERIS	SAR	CRC	Region status	Odd	N
27 s	Spare Word (1/2)					Even	N
28 s	Spare Word (2/2)	ERIS	SAR	CRC	Region status	Odd	N
29 s	Spare Word (1/2)					Even	N
30 s	Spare Word (2/2)	ERIS	SAR	CRC	Region status	Odd	N

OS NMA Operations

Authenticated Data

- Eph, Clk & Health
- Galileo Subframe
- Almanac
- GST-UTC & GST-GPS
- Other NAV Msg elements

Algorithm

- Verification of TESLA key
  - chain starts with root key K_0 (public), and ends with K_n (secret – known to provider only)
  - $K_m = F(K_{m+1})$ backward until K_0
  - K_0 validated through the DSM-KROOT and Public Key
- Computation/Verification local MAC vs broadcast MAC
- Public Key Renewal:
  - installation in receiver from public internet server
  - over the air

PARAMETER	DESCRIPTION	VALUE
DSF	Digital Signature Function	ECDSA P256
NB	Number of DS blocks	7
NMACK	Number of MACK sections	2
HF	Hash Function	SHA-256
MF	MAC Function	SHA-256
KS	Key Size	128 bits
MS	MAC Size	12
MO	MACK Offset	Off

MACK index	MACK #1				MACK #2			
MAC index	MAC #1	MAC #2	MAC #3	MAC #4	MAC #1	MAC #2	MAC #3	MAC #4
SV index	6	5	4	SELF	3	2	1	SELF

Actual config from “Implementation and Testing of OSNMA for Galileo”, C.Sarto, 29 September 2017, ION GNSS+ 2017

OS-NMA Authentication Intended Applications

- **Smart Digital Tachograph:** improving the reliability of truck driver resting time monitoring by means of secure and free of charge GNSS signals
  [REGULATION (EU) 2016/799 of 18 March 2016]
- **Maritime in restricted waters and fisheries:** to establish fishing zones without territorial inclusion.
  [REGULATION (EC) 2244/2003 of 18 December 2003]
- **Other applications:** Multimodal transportation and transportation of valuable and dangerous goods handover, Vehicle tracking and Fleet Management Services (FMS), Authenticated time-stamping, etc.

OS authentication user terminal, by means of a valid key, continuously process the navigation data and inform users about the received data authenticity:

- GNSS chipset/receiver,
- interface to receive the public key
- authentication management software tailored for target application

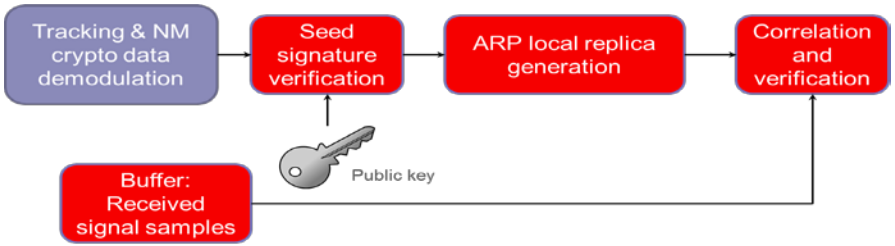
→ Note: **112-based eCall in-vehicle systems:** [REGULATION (EC) 2015/758] requires Galileo but not authentication explicitly

Availability

- **First live test end 2018**
- **Initial Service 2019**

OS Range Level Authentication

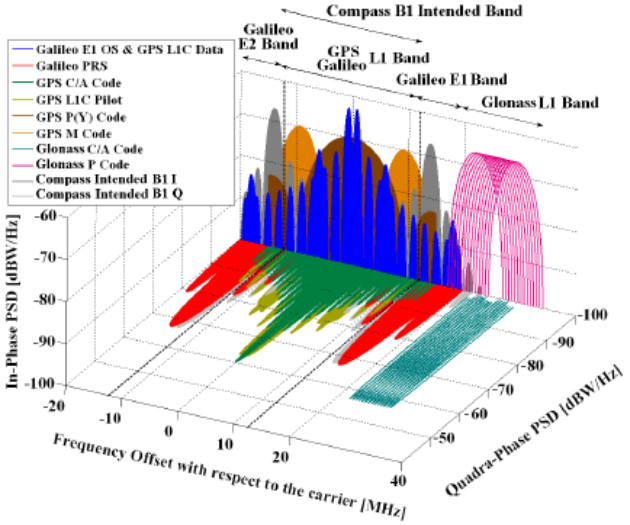
- **User and Operational Targets** identified for Code Based Authentication
  - Enable the user to detect a number of signal based replay attacks that introduce a ranging bias into one or more range measurements within few seconds
  - Participation to Code Based Authentication scheme shall
    - ✓ Not require costly and complex tamper resistant user equipment
    - ✓ Support all user operational modes (incl. cold start)
    - ✓ Cover all ranges of receiver equipment (incl. low end IoT devices)
    - ✓ Be possible also in challenging user local environments (e.g. urban)
- **Possible Implementation:** dedicated Galileo Anti-Replay Protection (**ARP**) SIS component in E1
- **User concept:**



1. Tracking of Standard OS
2. Sampling of the incoming signal and sample storage
3. Crypto data demodulation from SIS and seed signature verification
4. ARP local replica re-generation
5. Acquisition and tracking of ARP SIS component (available in stored samples) with the locally generated ARP
6. Correlation and verification of the ARP range measurement with Standard OS range measurement

Possible OS Signal Evolutions under study

- **Anti-replay (ARP) signal**
  - ✓ Protection against anti-replay attacks using Code Based Authentication
  - ✓ Low energy encrypted signal and/or watermarking (partial encryption)
- **Fast Acquisition (pilot) component**
  - ✓ Low complexity acquisition to support low-end Mass Market Rx (Lesson Learned from Galileo chipset testing)
  - ✓ Improved robustness against interference/jamming events
- **Fast TTFF (data) component**
  - ✓ Very low TTFF (e.g. below 18sec@GPS L1C)
  - ✓ Improved Data demodulation sensitivity (improvement in urban compared to GPS L1C)
  - ✓ Built-in flexibility for new content in nav msg
  - ✓ Anti-replay supporting data



OS Signal evolutions still under study at this stage.

Conclusions

- **Galileo in use** since **Initial Services Declaration on 15th December 2016** followed by **handover** to GSA and Galileo Service Operator **in 2017**
- **22 satellites in orbit**
  - In the field-proven **accuracy**
  - Galileo has entered the **Single Frequency mass-market**
  - Galileo is the **de facto standard for Dual Frequency** applications
- 4 additional SVs to be launched in **2018** and Procurement of additional **3rd Batch of 8+4 satellites** initiated (38 in total)
- **Authentication** is a desirable **differentiator** for Galileo to ensure that these capabilities are protected from counterfeiting attempts
  - **Navigation Message** Authentication under implementation and **Code Based** Authentication under definition