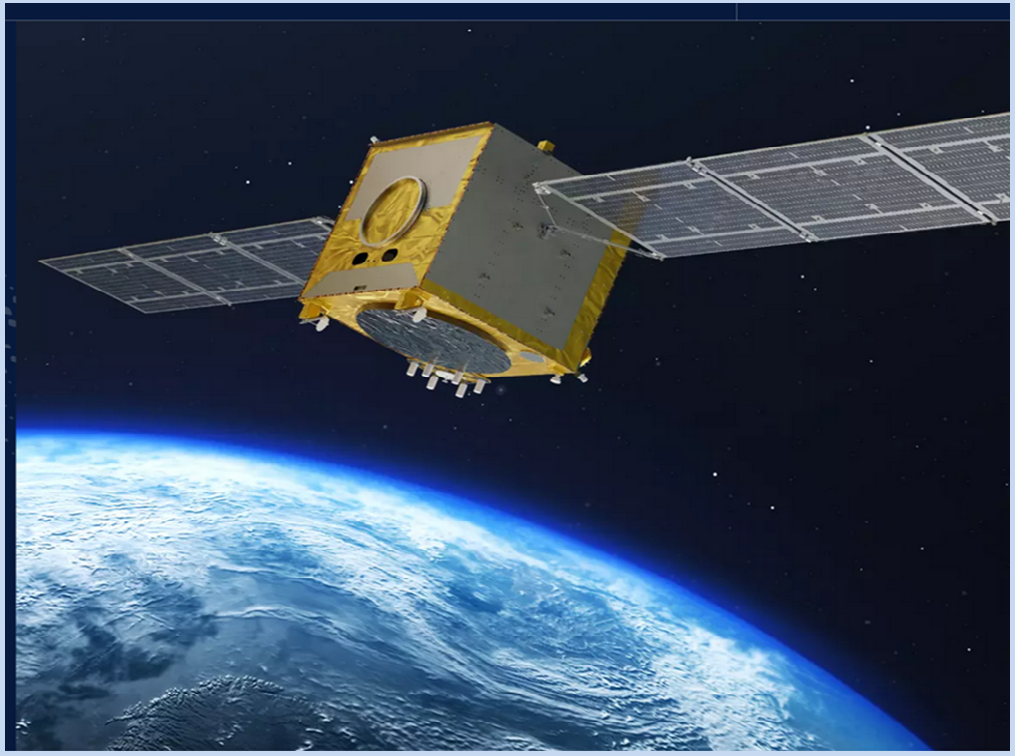
Galileo Authentication Services



Source: Airbus G2G Satellite

Robert Weber

AHORN 2025 (3/4.Dec 2025)

GNSS - Signals2Trust?

1985 – 2000 **Availability ?**

2000 - 2020 **Accuracy ?**

2015 - …….. **Resilience, Integrity, Authentication ?**

Why: **Counteracting Spoofing Activities = Control Signals used for Positioning and Timing e.g. Approach Airport, Train Integrity, (autonomous) LKW/ PKW-driving, financial transactions,…**

Requires: **Authenticated Signals, Concepts for Integrity for various application fields,…**

GNSS signals processing involves more and more fields of encryption techniques and statistics

Background

The EC Galileo Working Group for Authentication and High Accuracy (A-HA WG) has evolved from the previous Galileo Commercial WG. This WG reports to the higher-level NEXT WG (which deals with topics like G2G, LEO-PNT, IRIS2,..).

The membership of the A-HA WG is composed of EC, ESA, EUSPA, JRC representatives and last-but not least of representatives of the EU MS.

Topics to be discussed are the specification and ongoing development of the Galileo HA- and Authentication Services.

This presentation is **just a brief high-level introduction** to the currently operating and planned Galieo Authentication services **OSNMA and SAS .**

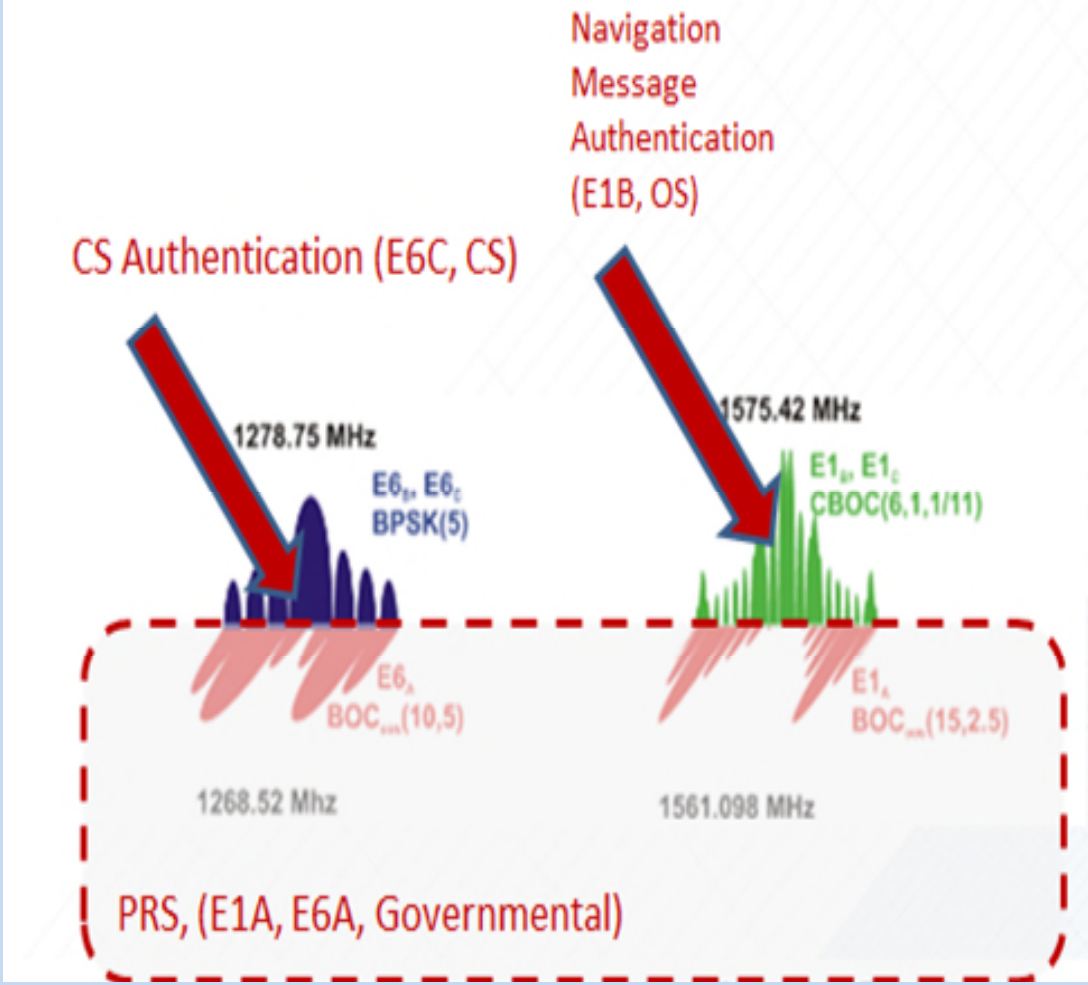
Galileo Leads the Way in GNSS Spoofing Protection with OSNMA (EC article, July 22nd,2025)

In response to this growing challenge, Galileo, the European Global Navigation Satellite System (GNSS), developed and is now launching a pioneering capability: Open Service Navigation Message Authentication (OSNMA). **This new feature will officially become operational on Thursday, 24 July 2025.**

What is OSNMA?

OSNMA enables Galileo satellites to transmit a “digital signature” along with their standard Open Service navigation data. This signature allows receivers to verify that the signal they are receiving genuinely originates from Galileo and not from a malicious or spoofed source. Receivers equipped to fully exploit OSNMA will enjoy significantly improved protection against spoofing attacks.

Signals used by Galileo Authentication Services (OSNMA, SAS)



Source: Galileo Authentication – A Programme and Police Perspective, I. Fernandez-Hernandez et al. , 69. Astr. Congress Bremen , 2018

E1B (OSNMA)	… not encrypted
E6B (HAS)	… not encrypted
E1A,E6A (PRS)	… encrypted
E6C (SAS)	… encrypted

Galileo G1G Authentication Services

Galileo OS – NMA Tesla	Galileo CAS/SAS Nav + Spreading Codes	GPS Nav + spreading codes Chimera	Galileo PRS Governmental
E1-B	E6-C (E6-B,E1-B)	L1C	E1-A, E6-A
I/NAV	I/NAV, TOW	C/NAV , TOW	
open	encrypted		encrypted
needs: E1 receiver,special OSNMA capacity	needs E1,E6 receiver, special data storage + OSNMA capacity	needs L1C receiver	needs special receiver module
In operation	Initial Service Q4/2026?	?	FOC 2025+

Galileo Authentication Services

(G1G Satellite Generation,

G2G Satellite Generation)

- OSNMA (Open Service Navigation Message Authentication)
- OS-A (Open Service –Authentication), Authenticating Galileo Open signals+data
- CAS (Commercial Service Authentication), Originally developed as fee-based -> now SAS = Signal Authentication Service
- PRS (Public Regulated Service)

Options - Authentication

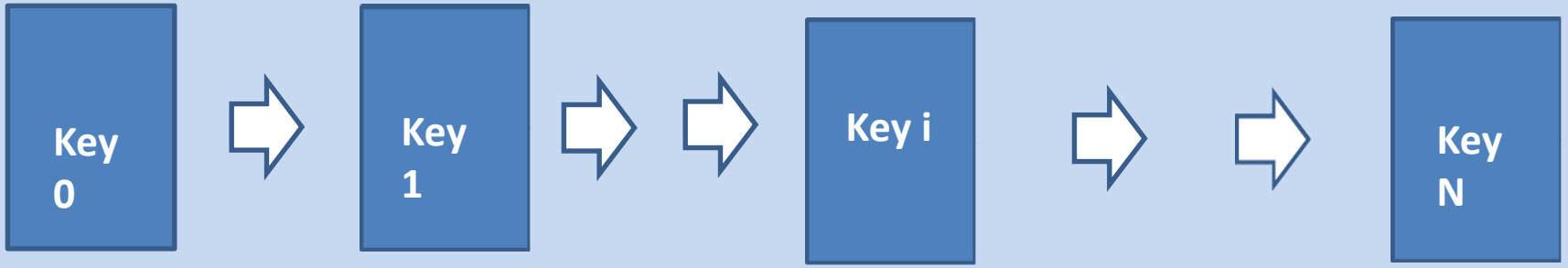
- Authentication of Navigation Message (NMA)
  or
  Authentication of Spreading Codes (Ranging Signals)
  or
  both

- Options : symmetric versus asymmetric key techniques
  symmetric -> satellite uses secret key to encode data
  and user requires same secret key to decode
  (problem: how to secure secret key at user level ?)
  asymmetric -> secret key is split in private key
  (secret, just known to Galileo System)
  and public key (User)

- **Galileo** -> ‚TESLA chain‘ makes use of a mixture
  asymmetric/symmetric to offer OS-NMA
  TESLA=Timed Efficient Streamed Loss-Tolerant
  Authentication

- **GPS** -> ‚Chimera‘ uses
  asymmetric key for C/Nav Authentication
- and most likely symmetric key for Spreading Codes

Chain of Keys
One way function f



Seed key secret, System

Root key, Known to user receiver

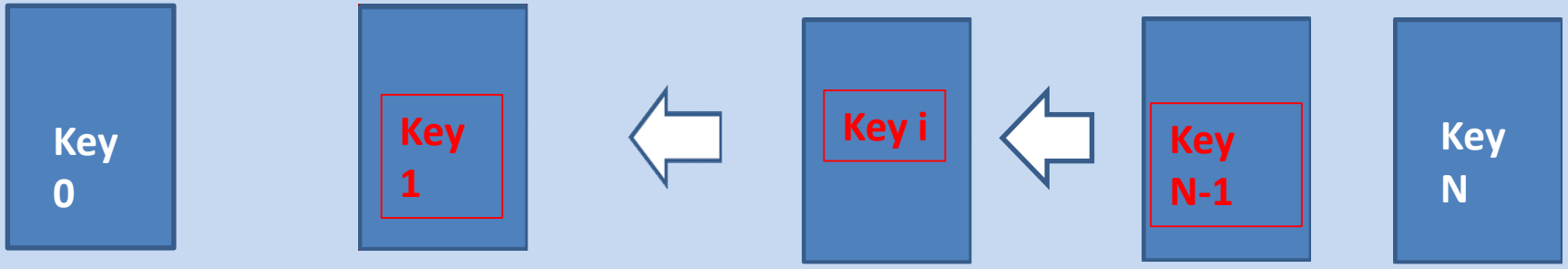
Key 1 $= f^{1}$ (key 0) , Key i $= f^{i}$ (key 0), Key N $= f^{N}$ (key 0)

Each key of Ki – chain is calculated from previous key K_{i-1} via funktion f $K_{i+1} = f(K_i)$. This function f can be easily evaluated ,

but cannot be inverted.

Therefore the user is not able to reproduce key K_{i-1}.

Timeline of key usage by Galileo



Seed key secret, System

Root key, has to be known by user receiver

Satellites use the keys in a sequence starting with K_{N-1} towards key K_1.

User Receiver downloads Root Key N beforehand via terrestrial networks (or similar distribution means)

Galileo OS-NMA Approach (TESLA)

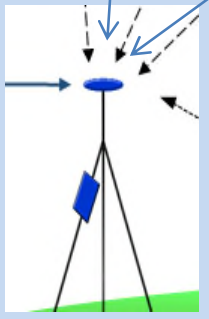
key 0 = seed key
key N = root key
key i = f (key 0)
key N = f (key 0)

MAC generated via key i ;
MAC = f(key i) +f(I/NAV);
Satellites broadcast I/NAV and MAC

key i will be broadcasted slightly delayed

key i = f(key0)

1. Generate Position and store MAC
2. Receiver checks if key i is part of TESLA chain
3. Use key i to check if Nav. Message and MAC are from the same source



I/NAV = E1 Navigation Message

MAC = Message Authentication Code

TESLA=Timed Efficient Streamed Loss-Tolerant Authentication

Process Sequence

- Satellite generates by means of key i and I/NAV a MAC
- Satellite broadcasts I/NAV and MAC
- **Receiver stores I/NAV and MAC**
- **Receiver calculates position**
- Satellite broadcasts time-delayed key i
- Receiver authenticates key i via funktion f and root key N
- Receiver generates MAC via key i, I/NAV and Funktion f
- If correct -> I/NAV = authenticated

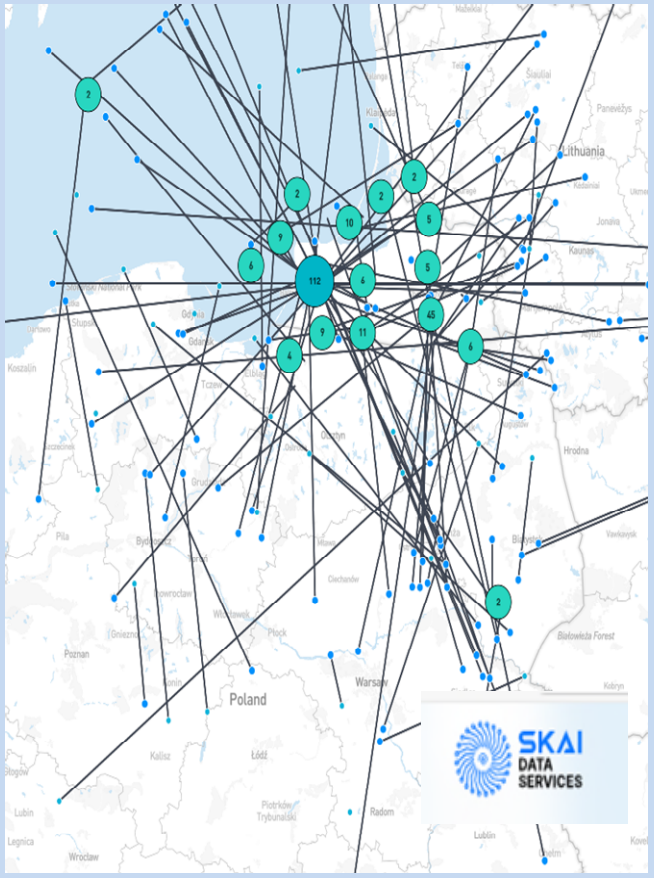
- **After some time this process starts at satellite level with key i-1**

Preconditions:
Satellite and Receiver have to be almost time-synchronized.
Key i is delayed by at least the signal travel time to prohibit spoofing.

Problems:
Same key or different keys used by different satellites at same epoch.
Simultaneous broadcasted signals arrive at different instants at receiver.

Galileo SAS (Signal Authentication Service)

- Galileo is testing Signal Authentication Service, or SAS, for signal authentication
- SAS Background:
  - 2017: Originally conceived as part of Galileo "Commercial Service", based on private keys, fee-based (2017)
  - 2017-2023: "semi-assisted" concept designed and developed, not requiring receiver private keys
  - 2024: EU Decision on the "free provision of a signal authentication service", based on semi-assisted concept, already in Galileo 1st Generation, **renamed as Galileo SAS**



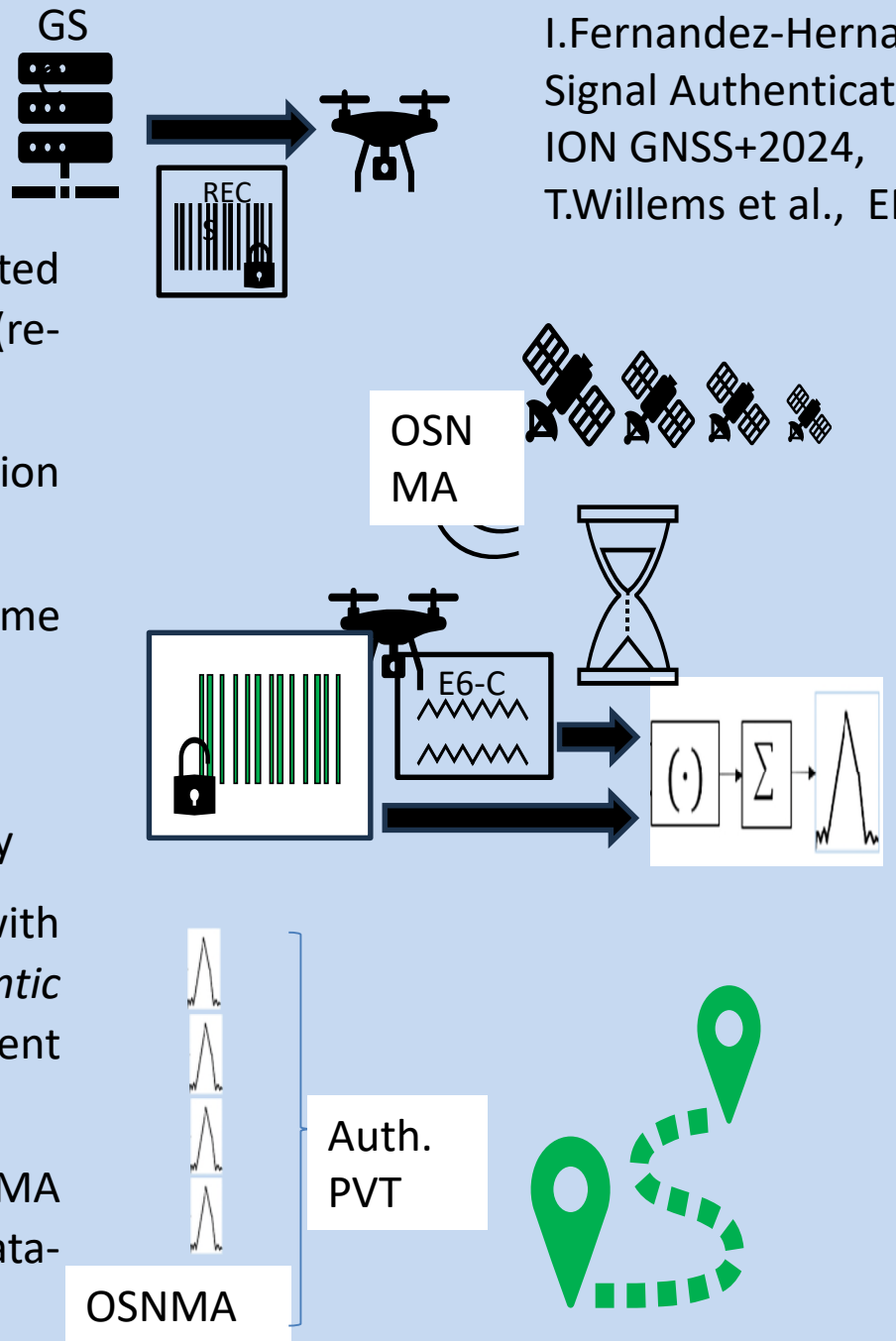
Spoofing cases reported from ADS-B, 19/5 10:00 to 21/5 10:00 CET

Source: T. Willems et al., ENC 2025

Technical Definition of SAS

Main concept (receiver side)

- Before operation, download Re-Encrypted Code Sequences (RECS) from GSC server (re-encrypted with future OSNMA keys)
- During operation, for every position authentication:
  - Record E6-C signal snapshot of some tens of ms
  - Wait for OSNMA key
  - Decrypt RECS with OSNMA-based key
  - Correlate decrypted RECS (or ECS) with snapshot. If correlation, *authentic* pseudorange E6-C measurement (under some assumptions)
  - Use E6-C measurements + OSNMA authentic data for a signal- and data-authenticated PVT



References:
I.Fernandez-Hernandez et al., Galileo Signal Authentication Service , ION GNSS+2024,
T.Willems et al., ENC 2025

Technical Definition of SAS

- **RECS** (Re-Encrypted Code Sequence) Files
  - They are the core of Galileo SAS

- **SAS concept** also includes:
  - **BGD** (Broadcast Group Delay) files: contain the estimations of the BGDs allowing E1-B I/NAV message use on E6-C measurements
  - **SLOG** (System and Log) files: Reports SAS status and related events
  - Cryptographic operations to decrypt RECS and determine optional delay randomization

References:
I.Fernandez-Hernandez et al., Galileo Signal Authentication Service , ION GNSS+2024,
T.Willems et al., ENC 2025

SAS full definition available in IONGNSS+ 2024 publication: *Galileo Signal Authentication Service (SAS),* Fernandez-Hernandez, I., et al. Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2024) (pp. 3292-3307)

Advantages of this concept

- Receiver needs no private key management or assistance channel
- System makes use of existing G1G capabilities (OSNMA, pilot E6C)

Disadvantages of this concept

- Authentication latency (at least a couple of seconds)
- Receiver needs to store RECS (some Mbytes)
- Encryption of the E6C pilot (problematic for robust recovery of E6C phase measurements)

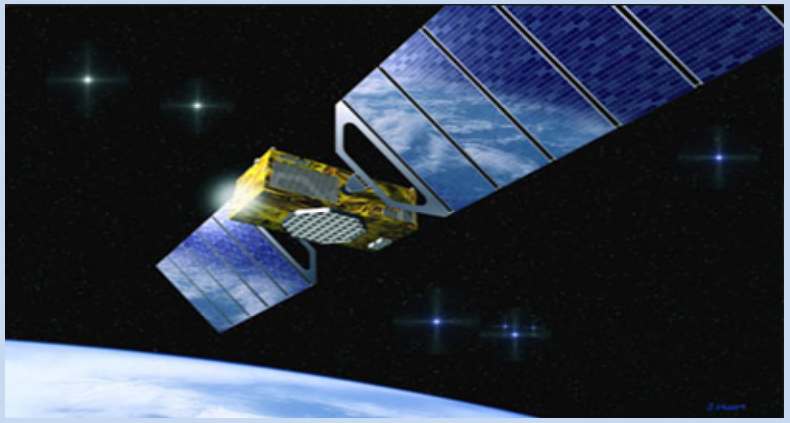
Most likely in G2G the encryption of E6C will make use of OSNMA dependent keys, thus receivers do not need to pre-store RECS

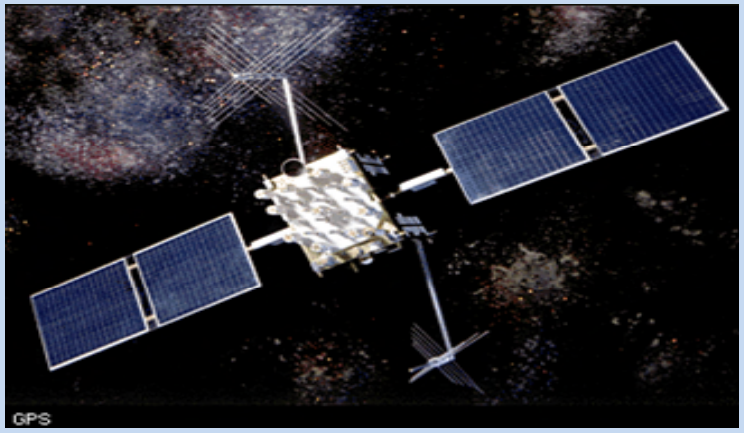
Initial Capability and Plans

- Initial Capability (Phase 0):
  - Early June 2025: L3 (GSAT202/E14) satellite E6-C encryption temporary activation for testing
  - End July 2025: permanent E6-C encryption in L3 (both GSAT202/E14 and GSAT201/E18)
  - Q3 2025: Prototype Server accessible (access policy and process under definition)
  - Q4 2025 (TBC): E6-C encryption in full constellation
- Initial Service (Phase 1):
  - Q4 2026 (TBC): Initial Service Declaration, allowing global and free use of SAS
- Full Service (Phase 2) and Evolutions:
  - Full Service Declaration (date TBD), introducing improvements with respect to Phase 1
  - Evolutions for integration of SAS with G2G Authentication (2030+)

Radio Technical Commision for Maritime Services – SC 134 Committee RTCM SC-134

- Established in 2018
- Goal: definition of a Standard Message Format for GNSS Integrity Augmentation at User and Service Level
- Special Sub Working Groups in various application fields (Automotive, Rail, Maritime , Open Satellite Correction Services,…)
- Main goal: to provide sufficient information for Protection Level calculation for all the noted application fields (not only for air traffic)
- SC-134 messages provide integrity bounds
- Version 1 format to be issued soon
- Covers a) Service Area, b) Minimum Integrity Messages (Satellite Health Status, Constellation Health Status, Frequency Integrity Flags, Augmentation Service Level) and c) Extended Integrity Messages (Pconst, Psat, Overbounding parameters (Phase and Code biases) for Protection Level calculation).





ENC 2026 - 28 - 30 April 2026 -
Call for Abstracts

ENC EUROPEAN NAVIGATION CONFERENCE 2026

Thank you for your attention