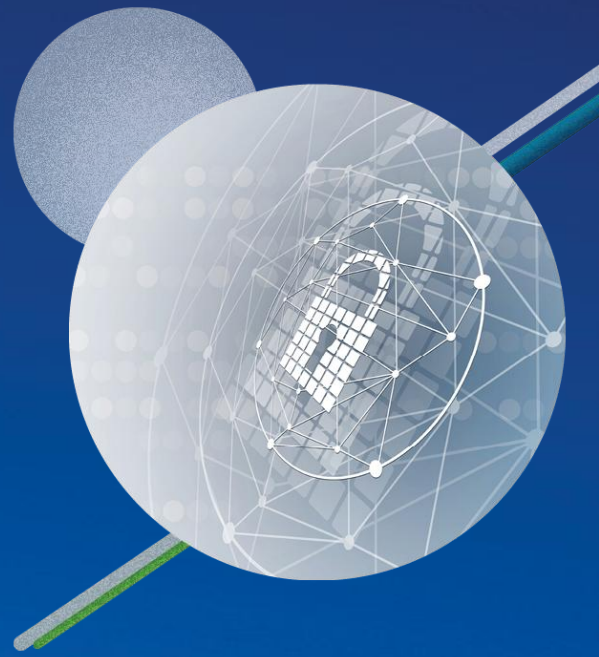
#EUSpace



Beyond OSNMA: Signal Authentication Service

EUSPA OSNMA Day 2026

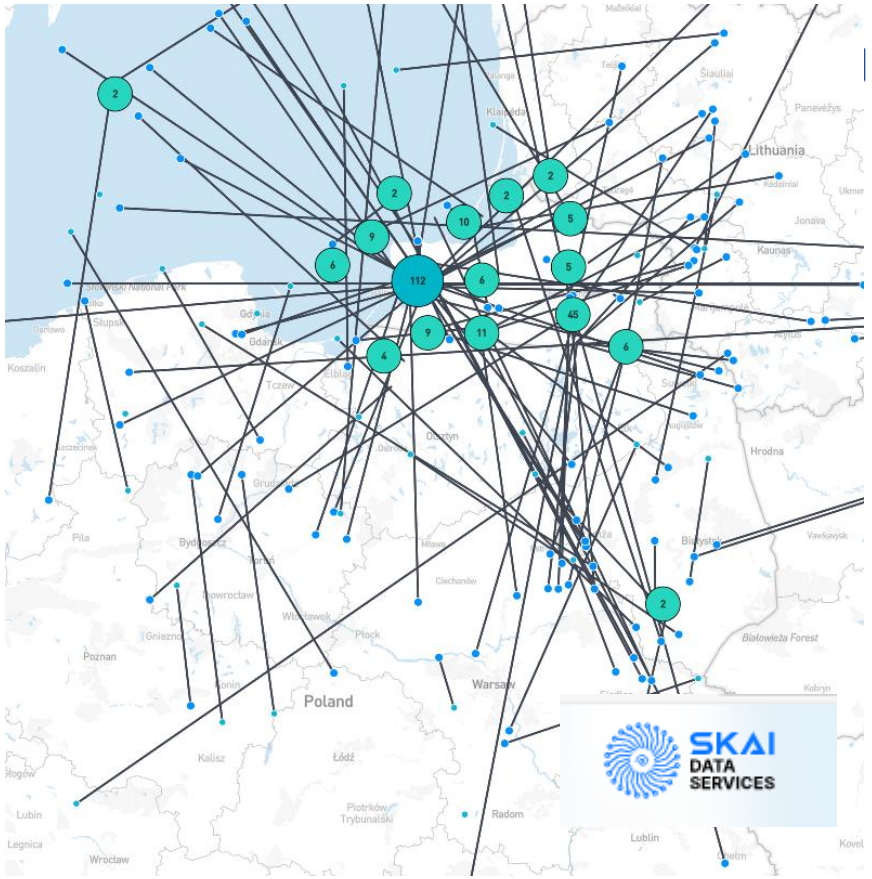
Ignacio Fernandez-Hernandez

European Commission DG DEFIS D2

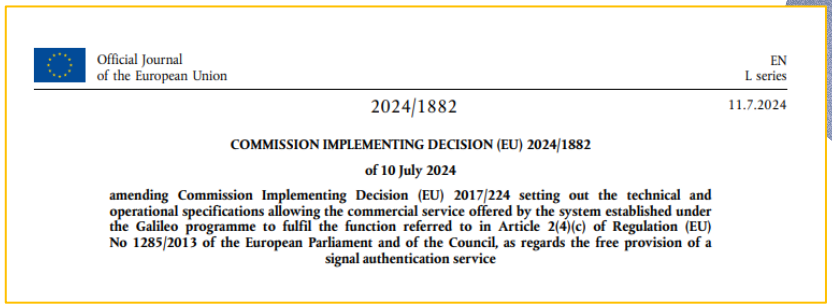
EUSPA
European Union Agency for the Space Programme

Introduction

- The GNSS spoofing threat has moved from the lab (2000s) to the field (2020s)
- Galileo has developed OSNMA for data authentication: ensures navigation data is authentic and makes signal replays more difficult, if signal unpredictability is verified
- Galileo is testing Signal Authentication Service, or SAS, for signal authentication by protection of the GNSS spreading code, used for ranging
- 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



Official Journal of the European Union — EN L series

2024/1882 — 11.7.2024

COMMISSION IMPLEMENTING DECISION (EU) 2024/1882

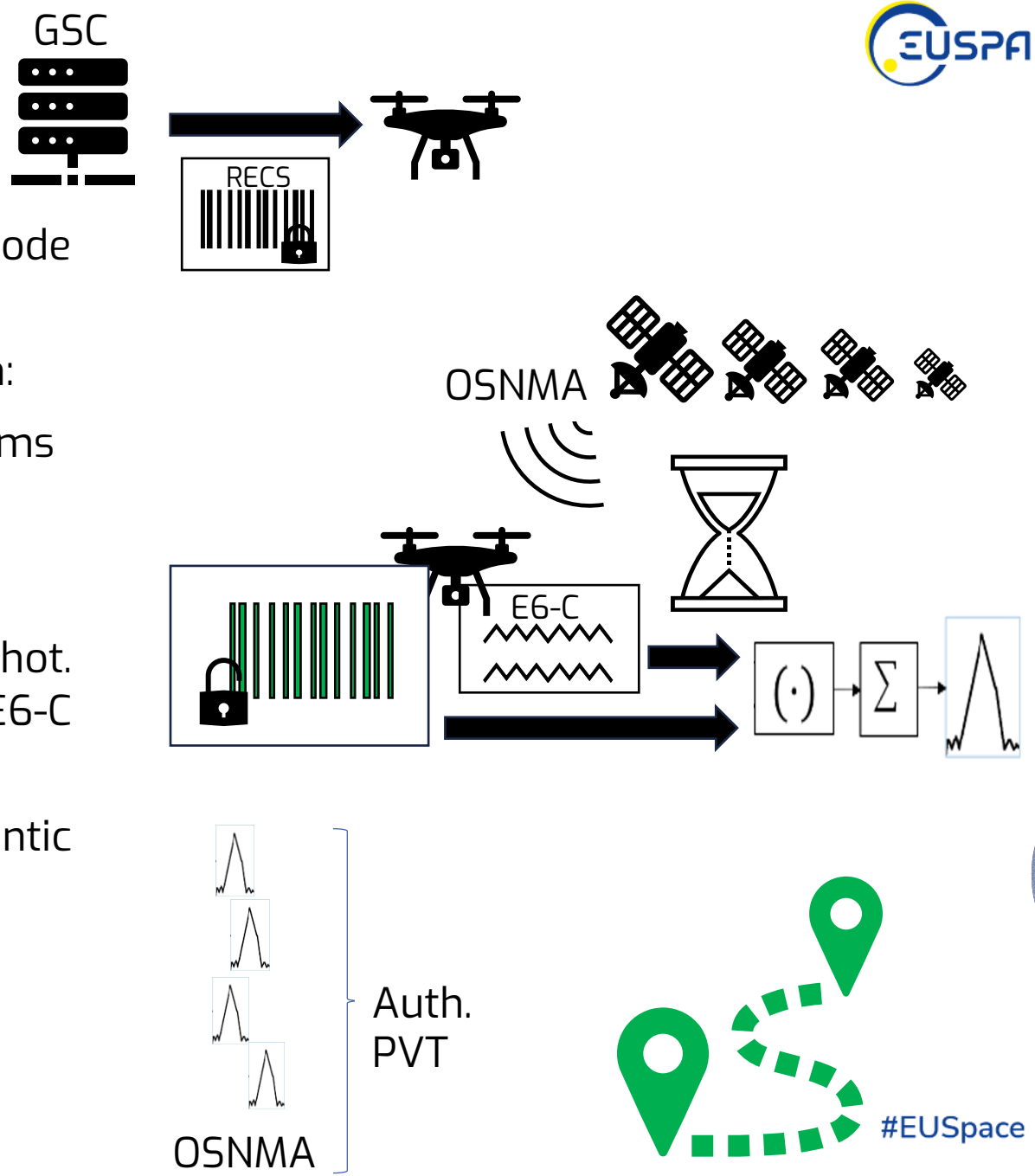
of 10 July 2024

amending Commission Implementing Decision (EU) 2017/224 setting out the technical and operational specifications allowing the commercial service offered by the system established under the Galileo programme to fulfil the function referred to in Article 2(4)(c) of Regulation (EU) No 1285/2013 of the European Parliament and of the Council, as regards the free provision of a signal authentication service

Technical Definition of SAS

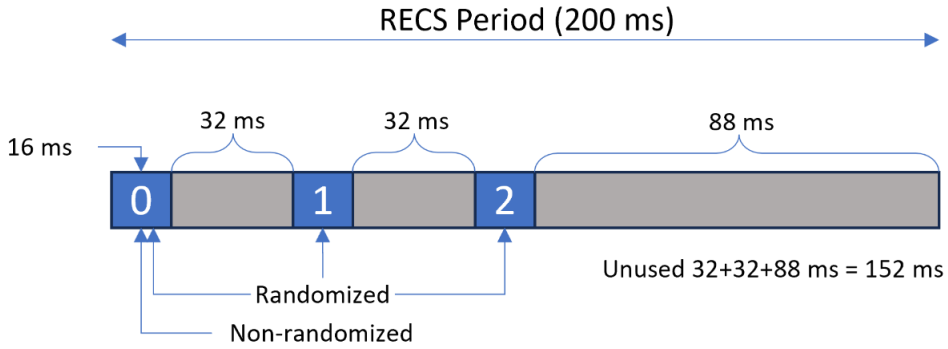
Main concept (receiver side)

- Before operation, download Re-Encrypted Code Sequences (RECS) from GSC server
- During operation, for every position authentication:
  - Record E6-C signal snaphsot 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



Technical Definition of SAS

- **RECS** (Re-Encrypted Code Sequence) Files
  - They are the core of Galileo SAS
  - Contain up to 16 ms correlation per sat. per 200ms
- 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



SAS latest public 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)

Technical Definition of SAS

- RECS Cryptographic Operations
  - Generate OSNMA-derived key
  - Generate ECS (decrypt RECS)
  - If RAND = 1, use K'_j to determine position (0,1,2)
- RECS/BGD/SLOG files are digitally signed, and verified with a public key provided by the Galileo PKI

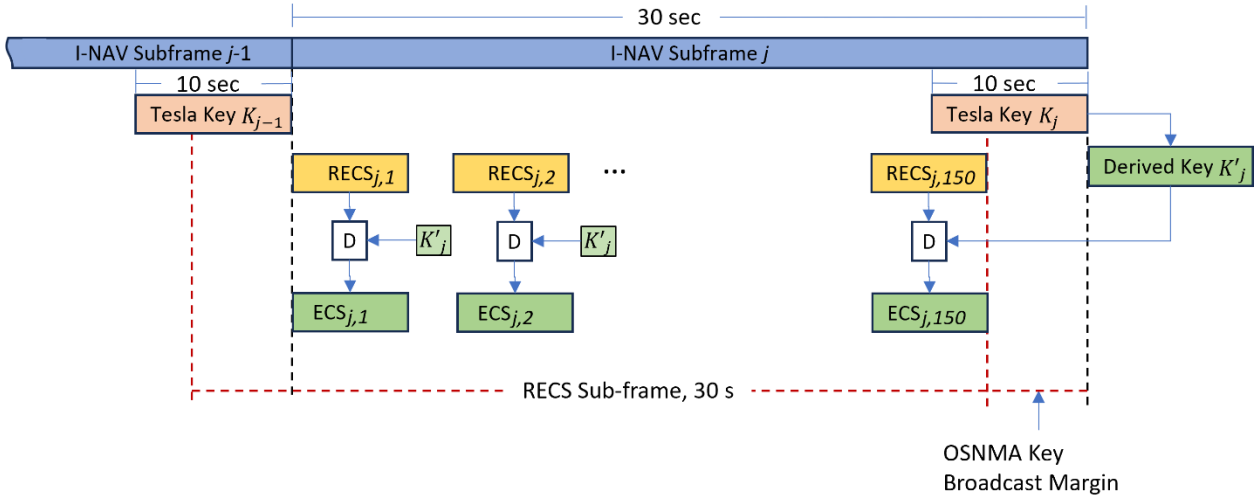
$$K'_j = SHA256(K_j)$$

$$ECS_{j,i} = AES256^{-1}_{CBC}(K'_j, RECS_{j,i}, IV)$$

$$IV = trunc(128, SHA256(P_j))$$

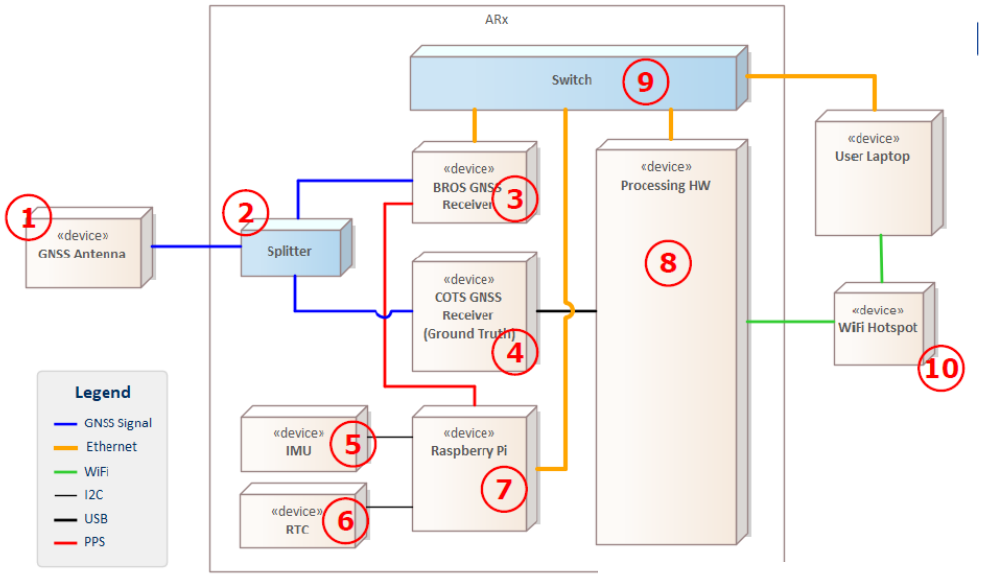
$$P_j = (GST_{SF,j} \,||\, RAND \,||\, p1)$$

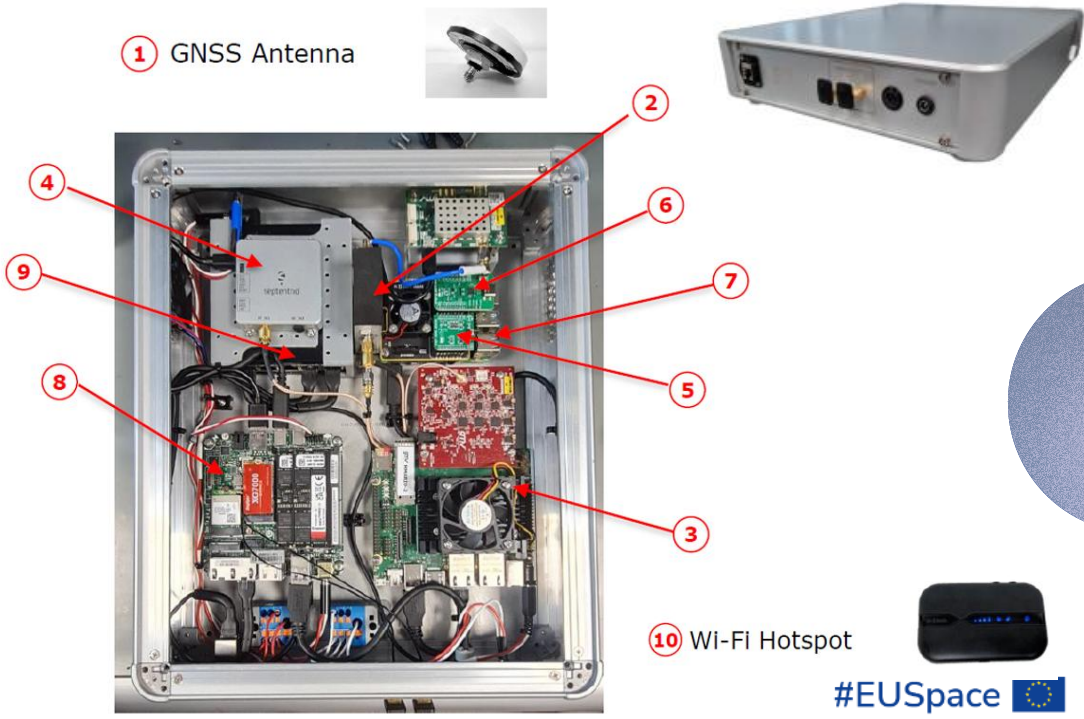
$$p1 = 00000000000$$



Receiver and Testing Prototypes: SAS Receiver

- A SAS Receiver, SAS Prototype Server and the Testing Platform have been developed in EC's MMARIO (Message and Measurement Authentication Receiver for Initial Operations) project with GMV, ADS, UAB and Qascom. Already qualified and under experimentation
- SAS Receiver:
  - Allows SAS testing in multiple RECS configurations and combinations with other checks
  - E1/E5/E6 antenna and Front End (BROS receiver)
  - Signal processing engine (BROS receiver) allowing pre-calibrated and synchronized E6 snapshot recording and standard tracking (E1, E6)
  - PVT engine allowing OSNMA and multiple position solutions (SF, DF, HAS…) and E1-E6 verifications
  - Additional checks: vestigial signal search, CN_0/AGC, measurement consistency, E1 OSNMA-based anti-replay
  - Others: ground truth (Mosaic 5 with RTK), IMU, NTP/NTS, Wifi





#EUSpace

Receiver and Testing Prototypes: SAS Prototype Server

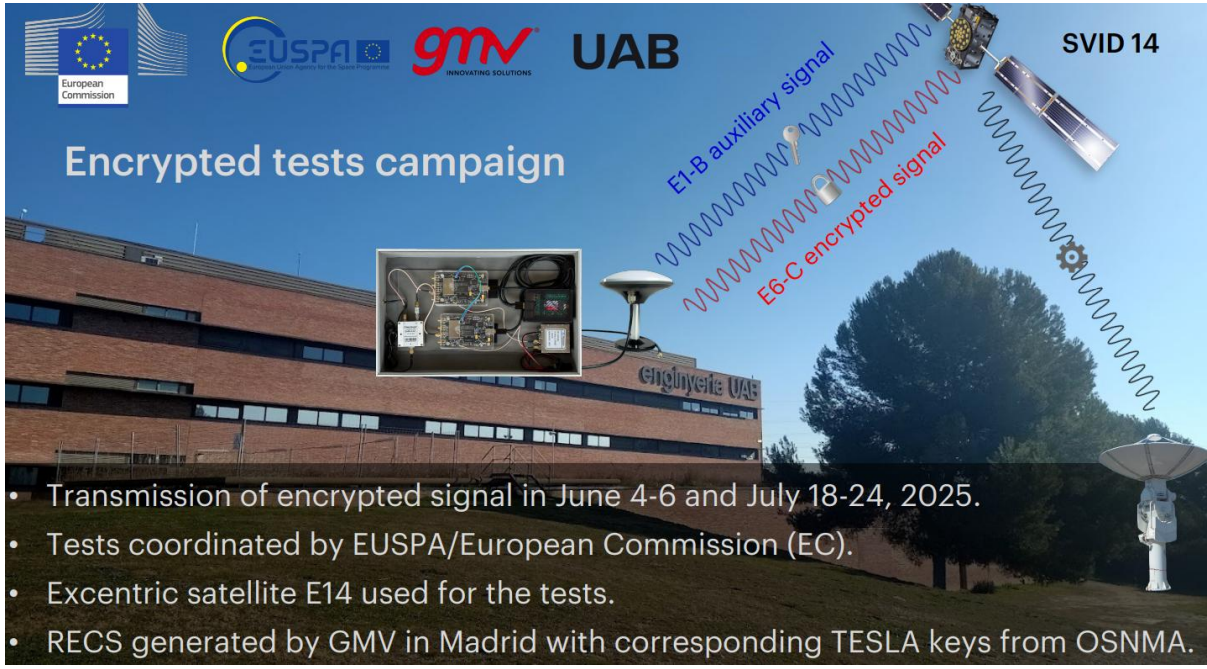
- Generates and stores RECS files from OSNMA-derived keys (not yet released) and E6-C encryption key (NAVSEC)
- Generates BGD and SLOG files
- Answers SAS receiver queries and provides RECS/BGD/SLOG files
- Provides NTP/NTS synchronization (±50 ns accuracy at the server end)
- Example of RECS https query:

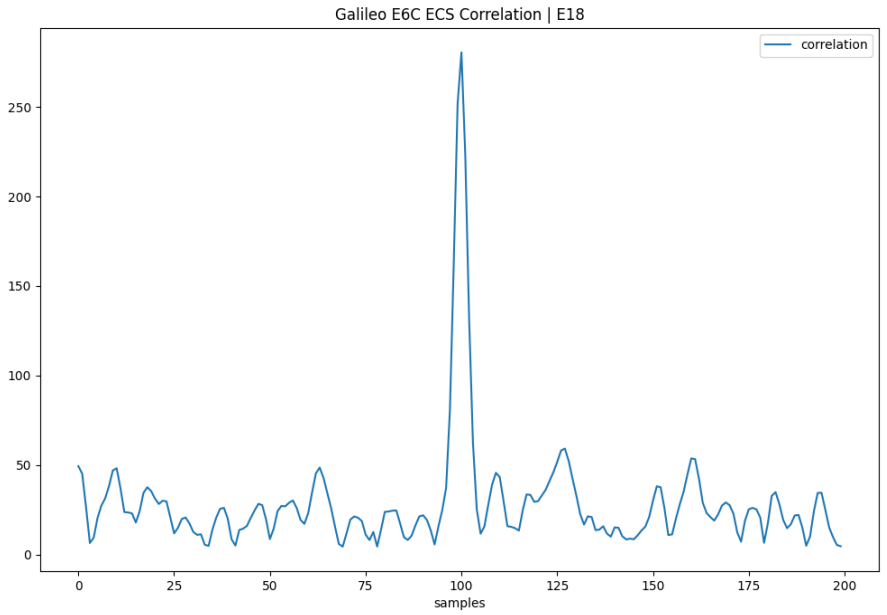
```
https://[TBD]/sas/recs?intv=01&tstart=25101080000&tdur=007200&rtba=00300&svids=01+02+05+24&kdi=0&rand=1&nchip=3
```

- `intv=01:` RECS interface version. Allows interface changes;
- `tstart=25101080000:` Start time of autonomy period in YYDDDHHMMSSS format (2025, DOY=101, 08:00:00)
- `tdur=007200:` Duration [s] of period (7200s)
- `rtba=00300:` Autonomy RECS Time Between Authentications [s/10] (30s)
- `svids=01+02+05+24:` SVIDs for which RECS are provided (SVIDs 01, 02, 05, 24)
- `kdi=0:` Key Delay Indicator (fixed to 0 => OSNMA key in *current* subframe - offset)
- `rand=1:` Randomization: position ‘0’ or ‘1’ or ‘2’ in the stream
- `nchip=3`: 8.008 ms RECS length

SAS Testing and Next Steps

- In June-July 2025, L3 satellites (GSAT202/E14 and and GSAT201/E18) E6-C encryption temporary activated for testing
- Since December 2025:
  - L3 satellites (GSAT202/E14 and and GSAT201/E18) *permanently* encrypted
  - SAS Prototype Server available for internal testing, including RECS/BGD/SLOG download from EU Member States
- Next steps foreseen:
  - 2nd half of 2026: E6-C encryption of all Galileo constellation
  - Early 2027: SAS Initial Service Declaration

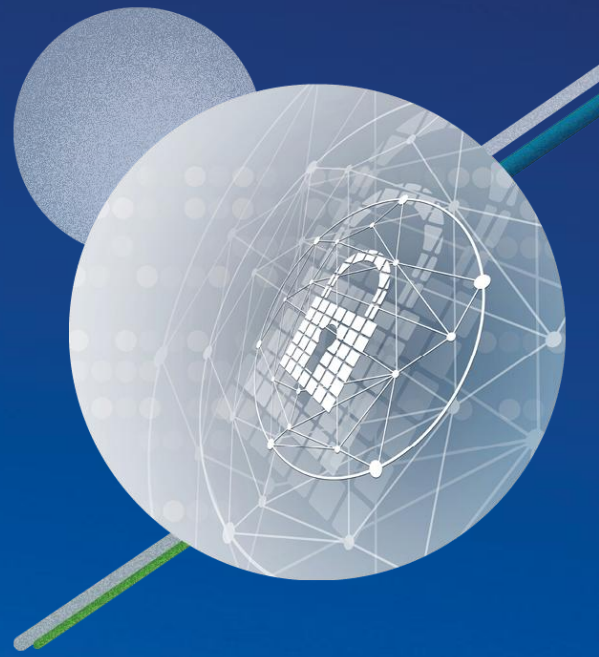




Conclusions

- Galileo SAS is the first global GNSS signal authentication service, offered freely and openly
- SAS receiver, prototype server and testing platform already qualified
- Initial SAS capability started permanently in December 2025 with L3 satellites
- Next steps:
  - Publication of SAS ICD and Guidelines: 2026
  - Initial SAS capability in full constellation foreseen by 2nd half of 2026
  - SAS Initial Service Declaration foreseen in early 2027

#EUSpace



Thank you for your attention

EUSPA OSNMA Day 2026

Ignacio Fernandez-Hernandez

European Commission DG DEFIS D2

EUSPA
European Union Agency for the Space Programme

#EUSpace

EUSPA
European Union Agency for the Space Programme

Linking space to user needs

Get in touch with us

www.euspa.europa.eu

EUSPA | EU4Space | EUSPA | space4eu | EUSPA

EUSPA OSNMA Day 2026