EU SPACE

# Galileo Signal Authentication Service (SAS)

12 September 2024

*Tom Willems, Senior Consultant at CGI Belgium*
*Advisor to the European Commission DG DEFIS*
*(Ref. GSA/OP/05/20/Lot6/SC5)*

*Thanks to Ignacio Fernandez-Hernandez (EC DG DEFIS) for the slides upon which this presentation is based*

# Agenda

- Background
  - OSNMA
- Galileo Signal Authentication Service (SAS)
  - History
  - How it works
  - Status and future
- Conclusion

# Background

- GNSS spoofing threat is steadily growing
- Galileo has implemented **OSNMA** (Open Service Navigation Message Authentication) to provide authentication of **navigation data**
- Navigation data is modulated onto code sequences *(ranging codes, spreading codes).* The resulting signal is used for ranging.
- Galileo **SAS** (Signal Authentication Service) will provide authentication of **code sequences**, assisted by OSNMA
- Authenticated signal (SAS/OSNMA) + authenticated data (OSNMA) = strongly authenticated position

# Open Service Navigation Message Authentication

- OSNMA authenticates Galileo **OS I/NAV data**; in the future also GPS navigation data
- OSNMA combines symmetric and asymmetric cryptography
- The navigation data is **signed** using a cryptographic key
  - The data + signature is transmitted
- The key is transmitted with a **delay** with respect to the data + signature
  - Once the key is received, the receiver can check that data and signature are consistent. If so, the data is authentic.
- The receiver must also check that the received key itself is authentic
  - Check that it belongs to an authentic "key chain" → *beyond scope here*

✓A spoofer cannot generate correctly signed navigation data

# History of Galileo Signal Authentication Service

- Originally conceived as part of “Commercial Service”, as **CS Authentication**. Based on private keys, fee-based (2017). Then renamed as **“Commercial Authentication Service” (CAS)**.
- 2017-2023: “Semi-assisted” concept designed and developed, not requiring receiver private keys. Renamed as “**Assisted Commercial Authentication Service” (ACAS)**.
- July 2024: EU decision to provide signal authentication for free, based on a semi-assisted concept, in G1G. ACAS considered as a first step of Galileo Signal Authentication Service, and renamed as **Galileo SAS**.

# Commission Implementing Decision (EU) 2024/1882 […] as regards the **free provision of a signal authentication service**

EN

[…] The Annex to Implementing Decision (EU) 2017/224 is amended as follows:

- in the row 'Components of the signals used', subcolumn 'Specifications specific to the CS: authentication using encrypted codes', the text is replaced by the following: **'E6, E6-C component encrypted (pilot)';**
- in the row 'Specifications of the user segment', subcolumn 'Specifications specific to the CS: authentication using encrypted codes', the text is replaced by the following: **'Verification of the authenticity of the signals by decrypting E6 codes re-encrypted with an OS data authentication key';**
- in the row 'System architecture', subcolumn 'Specifications specific to the CS: authentication using encrypted codes', the text is replaced by the following: **'Encryption of the E6 signal codes by the Galileo satellites, transmission of the private keys generated by the ground segment to the GNSS Service Centre (GSC), and publication of re-encrypted portions of the E6 signal codes with a future OS data authentication key';**
- in the row 'Access to the service', column 'CS authentication', the text is replaced by the following: **'Free access'**;
- in the row 'Deployment of the service', subcolumn 'Specifications specific to the CS: authentication using encrypted codes', the two indents are replaced by the following:
  - **Initial signals supply phase by 2024,**
  - **Service supply phase from 2026';**
- in the row 'Use of EU classified information', subcolumn 'Specifications specific to the CS: authentication using encrypted codes', the text is replaced by the following: **'No use of EUCI by the end user'.** […]

# Commission Implementing Decision (EU) 2024/1882 […] as regards the **free provision of a signal authentication service**

[…] De bijlage bij Uitvoeringsbesluit (EU) 2017/224 wordt als volgt gewijzigd:

- In de rij “Gebruikte signaalelementen”, subkolom “Specificaties die alleen voor de CS gelden: authenticatie met versleutelde codes” wordt de tekst vervangen door: **“E6, element E6-C versleuteld (pilot)”**.
- In de rij “Specificaties van het gebruikerssegment”, subkolom “Specificaties die alleen voor de CS gelden: authenticatie met versleutelde codes” wordt de tekst vervangen door: **“Verificatie van de authenticiteit van de signalen door ontcijfering van E6-codes die opnieuw zijn versleuteld met een OS-gegevensauthenticatiesleutel”.**
- In de rij “Architectuur van het systeem”, subkolom “Specificaties die alleen voor de CS gelden: authenticatie met versleutelde codes” wordt de tekst vervangen door: **“Encryptie van codes van de E6-signalen door Galileosatellieten, doorgifte van door het grondsegment gegenereerde niet-publieke sleutels aan het GNSS-dienstencentrum (GSC) en publicatie van opnieuw versleutelde delen van codes van de E6-signalen met een toekomstige OS-gegevensauthenticatiesleutel”.**
- In de rij “Toegang tot de dienst”, kolom “CS authenticatie”, wordt de tekst vervangen door: **“Gratis toegang”.**
- In de rij “Invoering van de dienst”, subkolom “Specificaties die alleen voor de CS gelden: authenticatie met versleutelde codes” worden de twee streepjes vervangen door:
  - **“Eerste verstrekking signalen uiterlijk vanaf 2024**
  - **Volledige dienstverlening uiterlijk vanaf 2026”.**
- In de rij “Gebruik van gerubriceerde EU-informatie (EUCI)”, subkolom “Specificaties die alleen voor de CS gelden: authenticatie met versleutelde codes” wordt de tekst vervangen door: **“Geen gebruik van EUCI door de eindgebruiker”.** […]

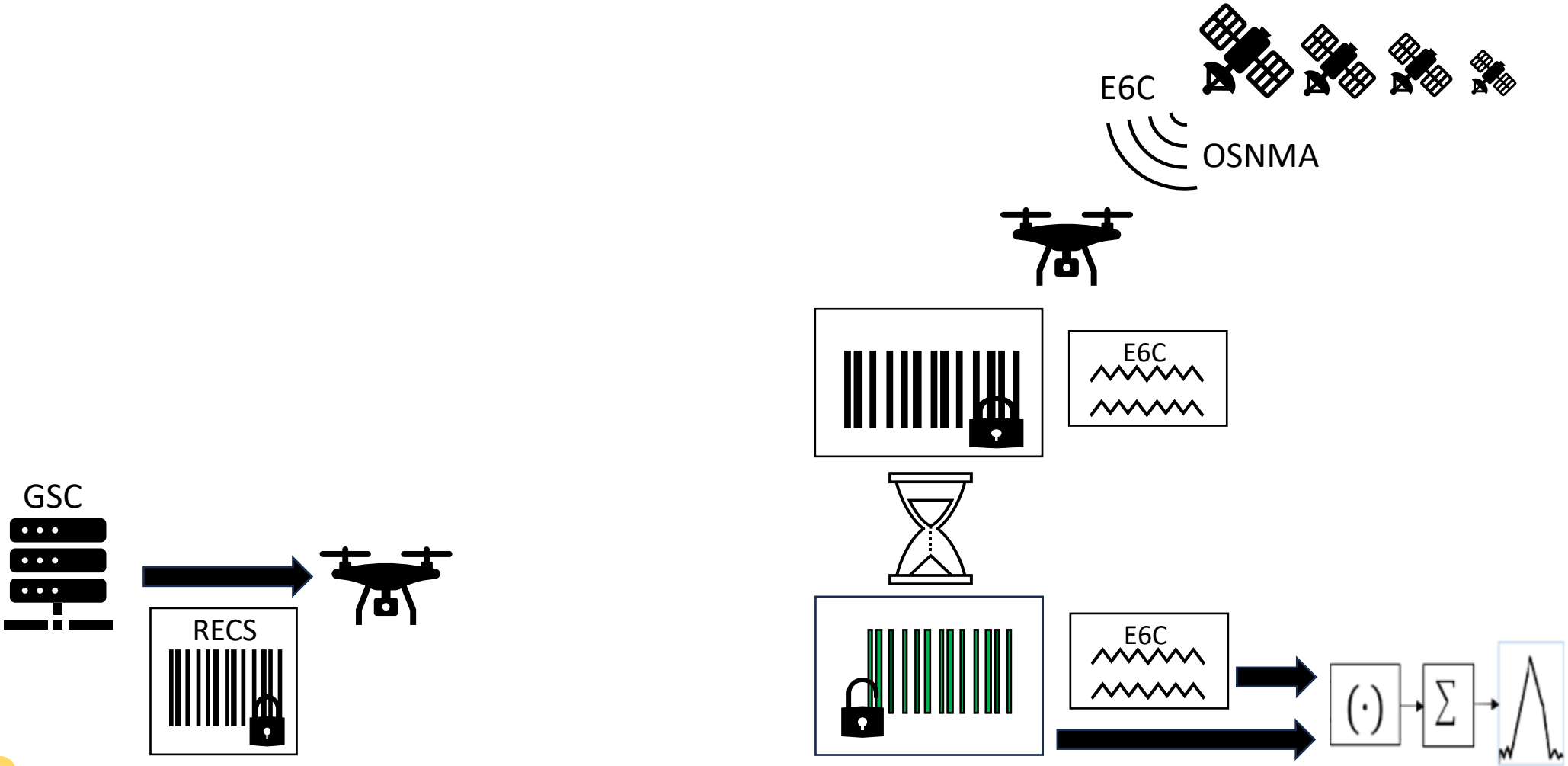
# Galileo Signal Authentication Service

- Objective: Provide signal authentication “as easy as possible” for users and system
  - No or minor change to Galileo system
  - Avoid private keys in receiver
  - Avoid need for real-time connection to an assistance channel in receiver
- However, existing Galileo OS/CS was not designed to provide signal authentication
  - OSNMA was already added, providing regular unpredictable and authenticatable elements
- Galileo E6 signal consists of two components:
  - E6B data signal: unencrypted; used to transmit High Accuracy Service (HAS) data
  - E6C pilot signal: currently unencrypted → capability is there to encrypt E6C

# How Galileo SAS Works

- **Galileo SAS is based on encrypted E6C signals and an internet service providing future fragments (snippets) of the encrypted code sequences. The fragments provided by the server are re-encrypted using a future OSNMA key.**
- Receiver downloads some Re-Encrypted Code Sequences (RECS) from the SAS server before autonomous operation
- For every position authentication:
  - Store an E6C signal snapshot of some tens of ms
  - Wait for OSNMA key
  - Decrypt RECS with OSNMA(-based) key → Encrypted Code Sequences (ECS)
  - **Correlate ECS with snapshot**
  - If correlation, the E6C pseudorange measurement is considered authentic (under some assumptions). We can then use authentic E6C measurements + OSNMA authenticated data for PVT.

# How Galileo SAS Works



# Commission Implementing Decision […]
## *Now we understand what this means:*

[…] De bijlage bij Uitvoeringsbesluit (EU) 2017/224 wordt als volgt gewijzigd:

- In de rij “Gebruikte signaalelementen”, subkolom “Specificaties die alleen voor de CS gelden: authenticatie met versleutelde codes” wordt de tekst vervangen door: **“E6, element E6-C versleuteld (pilot)”**.
- In de rij “Specificaties van het gebruikerssegment”, subkolom “Specificaties die alleen voor de CS gelden: authenticatie met versleutelde codes” wordt de tekst vervangen door: **“Verificatie van de authenticiteit van de signalen door ontcijfering van E6-codes die opnieuw zijn versleuteld met een OS-gegevensauthenticatiesleutel”.**
- In de rij “Architectuur van het systeem”, subkolom “Specificaties die alleen voor de CS gelden: authenticatie met versleutelde codes” wordt de tekst vervangen door: **“Encryptie van codes van de E6-signalen door Galileosatellieten, doorgifte van door het grondsegment gegenereerde niet-publieke sleutels aan het GNSS-dienstencentrum (GSC) en publicatie van opnieuw versleutelde delen van codes van de E6-signalen met een toekomstige OS-gegevensauthenticatiesleutel”.**
- In de rij “Toegang tot de dienst”, kolom “CS authenticatie”, wordt de tekst vervangen door: **“Gratis toegang”.**
- In de rij “Invoering van de dienst”, subkolom “Specificaties die alleen voor de CS gelden: authenticatie met versleutelde codes” worden de twee streepjes vervangen door:
  - **“Eerste verstrekking signalen uiterlijk vanaf 2024**
  - **Volledige dienstverlening uiterlijk vanaf 2026”.**
- In de rij “Gebruik van gerubriceerde EU-informatie (EUCI)”, subkolom “Specificaties die alleen voor de CS gelden: authenticatie met versleutelde codes” wordt de tekst vervangen door: **“Geen gebruik van EUCI door de eindgebruiker”.** […]

# Status and Future

- To be published: specification of GSC (Galileo Service Centre) SAS server and time server interface:
  - Retrieving RECS to perform a-posteriori E6C correlation
  - Retrieving BGD values and status information → *beyond scope here*
  - Performing secure time synchronisation
  - Containing details on required cryptographic operations
- Prototyping has been performed in multiple projects. Implementation of prototype real-time receiver and server is ongoing in another project.
- Testing with live signals as of end 2024 / beginning 2025
- Initial operational service in 2026
- To be evolved in G2G with new signals and better performance (2030+)

# Conclusion

- Today, Galileo OSNMA already provides authentication of navigation data
- In the near future, Galileo SAS will allow authentication of E6C signals, assisted by OSNMA
- Receivers will need to connect to a server, after which autonomous (offline) operation is possible
- By combining authenticated data (using OSNMA) and authenticated signals (using SAS and OSNMA), we can be assured of a highly “spoof-proof” authenticated position
- Further evolutions planned in G2G

EU SPACE

# Questions?

**Thanks to the Galileo SAS Team:**

*Ignacio Fernandez-Hernandez, Jon Winkel, Cillian O'Driscoll, Gianluca Caparra, Rafael Terris-Gallego, José A. López-Salcedo, Gonzalo Seco-Granados, Beatrice Motella, Daniel Blonski, Javier de Blas, and many others*