#EUSpace

Linking space to user needs

Galileo Open Service Navigation Message Authentication (OSNMA)

Sept 16 2024 - CGSIC - Baltimore, Maryland, USA

Ignacio Fernandez-Hernandez, European Commission DG DEFIS

Javier Simón, EUSPA

What is Galileo OSNMA

- “Navigation Message Authentication” is the ability of the Galileo system to guarantee to the users that they are utilizing navigation data that has not been modified and comes from the Galileo satellites and not from any other source.
- Resulting signal characteristics potentially exploited at receiver to increase signal protection level.

Galileo 1st generation contribution to increase the robustness of the OS user position

Fully **backward compatible (use of reserved bits from OS SIS ICD)**

Disseminated on the first Galileo frequency (**E1B**)

Same performance as for standard OS user: accuracy, availability

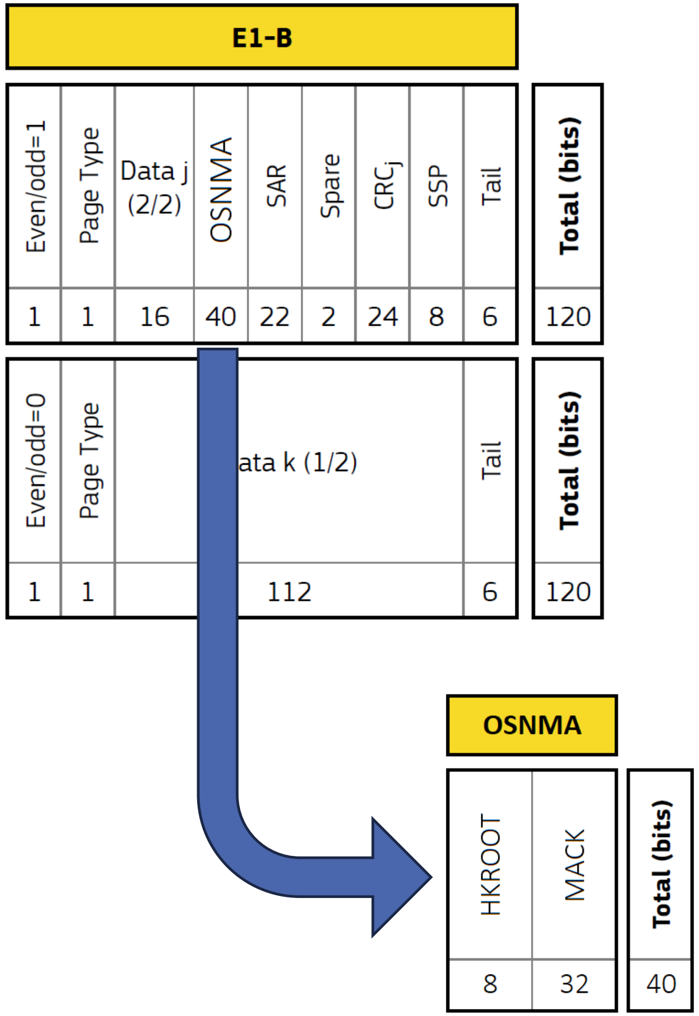
No need to store secret keys in Rx, just public key. Need to guarantee integrity of stored material in Rx. Additional user synchronization requirements.

Follows crypto standards and recommendations to be secure over the next decades

OSNMA Service Design – signal in space

OSNMA Signal in the Galileo E1-B I/NAV:

- HROOT section:
  - Digital signature
- MACK section:
  - TESLA chain keys
  - Message Authentication Code (MAC or Tag)



E1-B

Even/odd=1	Page Type	Data j (2/2)	OSNMA	SAR	Spare	CRC$_j$	SSP	Tail	**Total (bits)**
1	1	16	40	22	2	24	8	6	120

Even/odd=0	Page Type	ata k (1/2)	Tail	**Total (bits)**
1	1	112	6	120

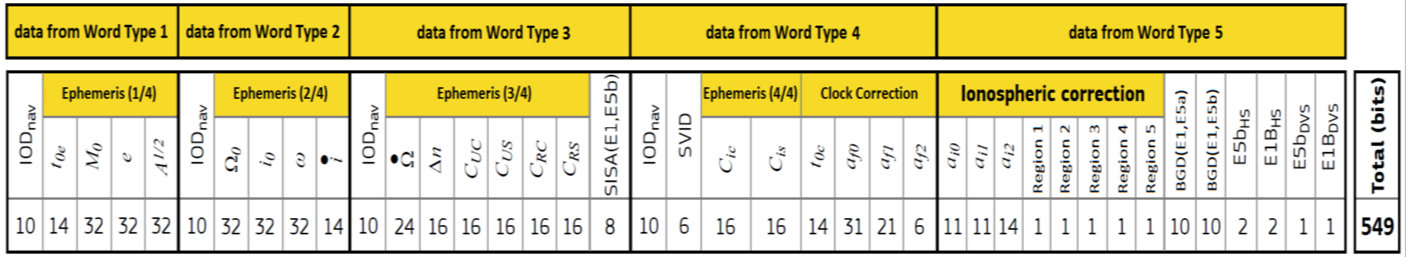
OSNMA

HKROOT	MACK	**Total (bits)**
8	32	40

OSNMA Service Design – signal in space

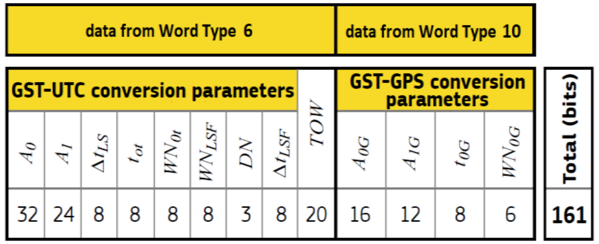
Authenticated navigation data (ADKD tags types as per OSNMA SIS ICD)

1. Galileo I/NAV Ephemeris, Clock and Status (ADKD#0 and ADKD#12)



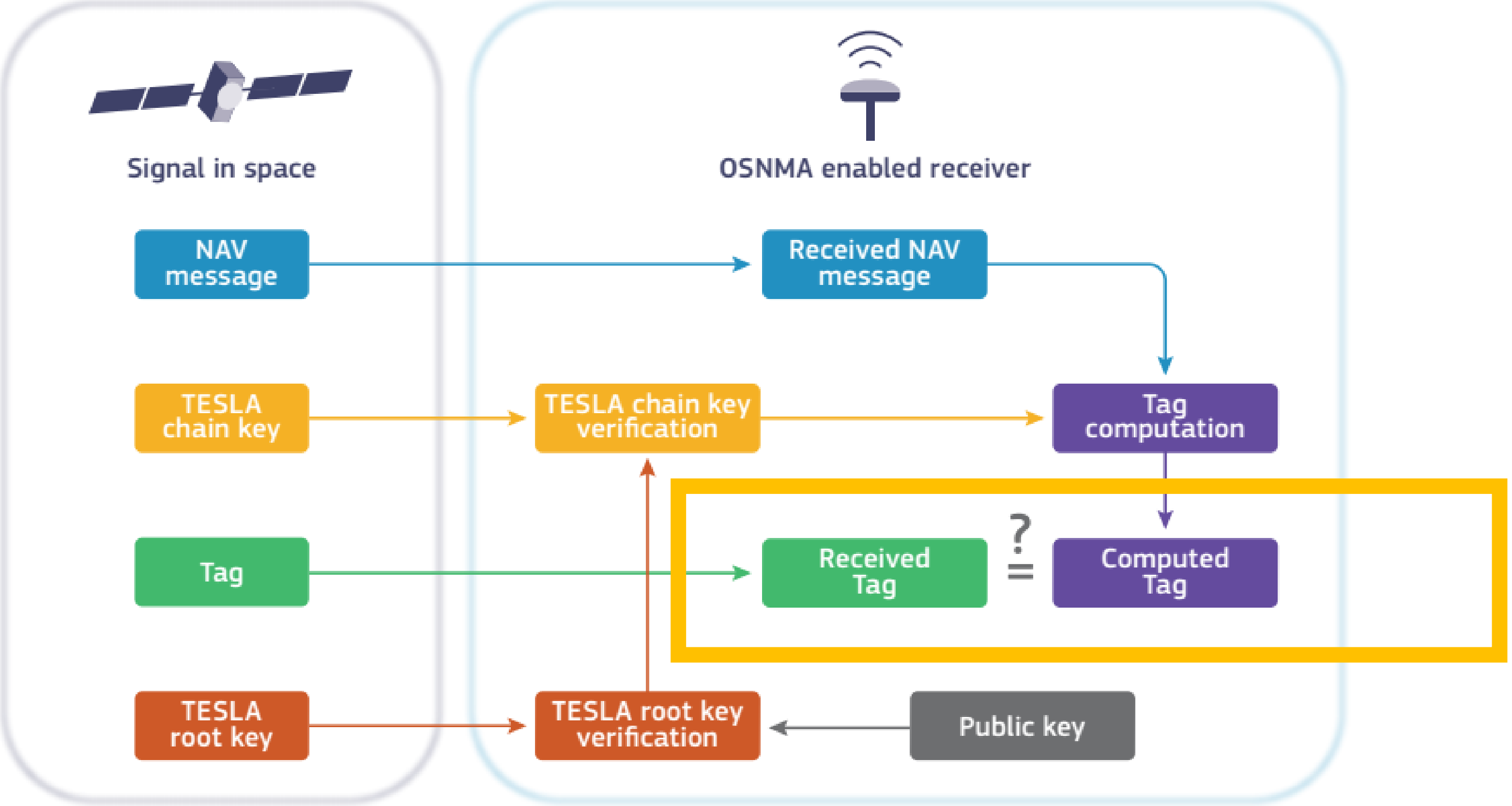
data from Word Type 1					data from Word Type 2					data from Word Type 3								data from Word Type 4								data from Word Type 5														
	Ephemeris (1/4)					Ephemeris (2/4)					Ephemeris (3/4)									Ephemeris (4/4)		Clock Correction				Ionospheric correction														
IOD_{nav}	t_{0e}	M_0	e	$A^{1/2}$	IOD_{nav}	Ω_0	i_0	ω	$\dot{i}$	IOD_{nav}	$\dot{\Omega}$	Δn	C_{UC}	C_{US}	C_{RC}	C_{RS}	SISA(E1,E5b)	IOD_{nav}	SVID	C_{ic}	C_{is}	t_{0c}	a_{f0}	a_{f1}	a_{f2}	a_{i0}	a_{i1}	a_{i2}	Region 1	Region 2	Region 3	Region 4	Region 5	BGD(E1,E5a)	BGD(E1,E5b)	$E5b_{HS}$	$E1B_{HS}$	$E5b_{DVS}$	$E1B_{DVS}$	**Total (bits)**
10	14	32	32	32	10	32	32	32	14	10	24	16	16	16	16	16	8	10	6	16	16	14	31	21	6	11	11	14	1	1	1	1	1	10	10	2	2	1	1	**549**

2. Galileo I/NAV Timing Parameters (ADKD#4)



data from Word Type 6									data from Word Type 10				
GST-UTC conversion parameters									GST-GPS conversion parameters				
A_0	A_1	Δt_{LS}	t_{ot}	WN_{0t}	WN_{LSF}	DN	Δt_{LSF}	TOW	A_{0G}	A_{1G}	t_{0G}	WN_{0G}	**Total (bits)**
32	24	8	8	8	8	3	8	20	16	12	8	6	**161**

OSNMA Service Design – User Logic



Service Specification

https://www.gsc-europa.eu/electronic-library/programme-reference-documents#OSNMA

- **OSNMA SIS ICD (v1.1, Oct 2023)**: Together with the OS SIS ICD, contains all information on the OSNMA SIS and specifies the interface between the Galileo Space and User Segments.
- **OSNMA Receiver Guidelines (v1.3, Jan 2024)**: Complements OSNMA SIS ICD with user implementation guidelines. Specifies user capabilities and steps to verify the authenticity of the Galileo navigation message.
- **OSNMA IDD ICD (v1.1, Jan 2024)**: Specifies how to retrieve the cryptographic data (Public Key and Merkle Tree) via the Internet. Supported by Public Key Infrastructure (PKI) certificates.

These document versions are the ones to be used for entry into operation.

Cryptographic material and certificates

The OSNMA applicable certificates and revocation lists are provided for RCA, SCA and ICA through the EUSPA and GSC web portals. In connection to that, the EUSPA certification policy and practices (CP/CPS) for issuing digital certificates for the three PKI levels (RCA, SCA and ICA) are provided

https://www.gsc-europa.eu/gsc-products/OSNMA/MT

- **OSNMA Merkle Tree (MT) applicable root and leaves**, since Jan 2024.
- OSNMA certificates and revocation lists of Merkle Tree (MT)

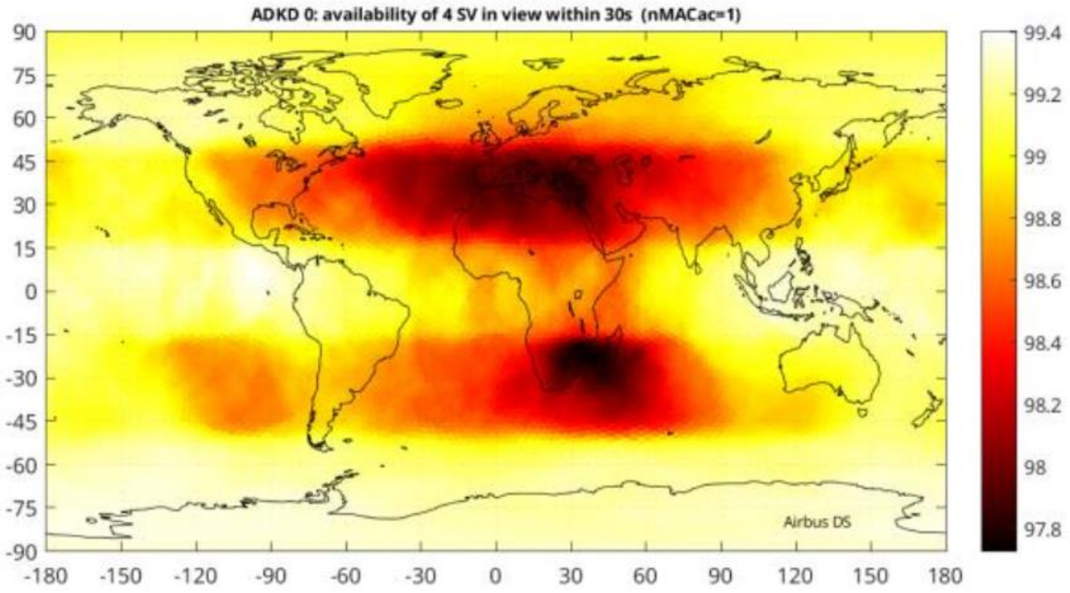
https://www.gsc-europa.eu/gsc-products/OSNMA/PKI

- **OSNMA Public Key (PK) applicable**, since Jan 2024.
- OSNMA certificates and revocation lists of OSNMA Public Key (PK)

OSNMA operational certificates, cryptographic material and associated documentation are the ones to be used for entry into operation.

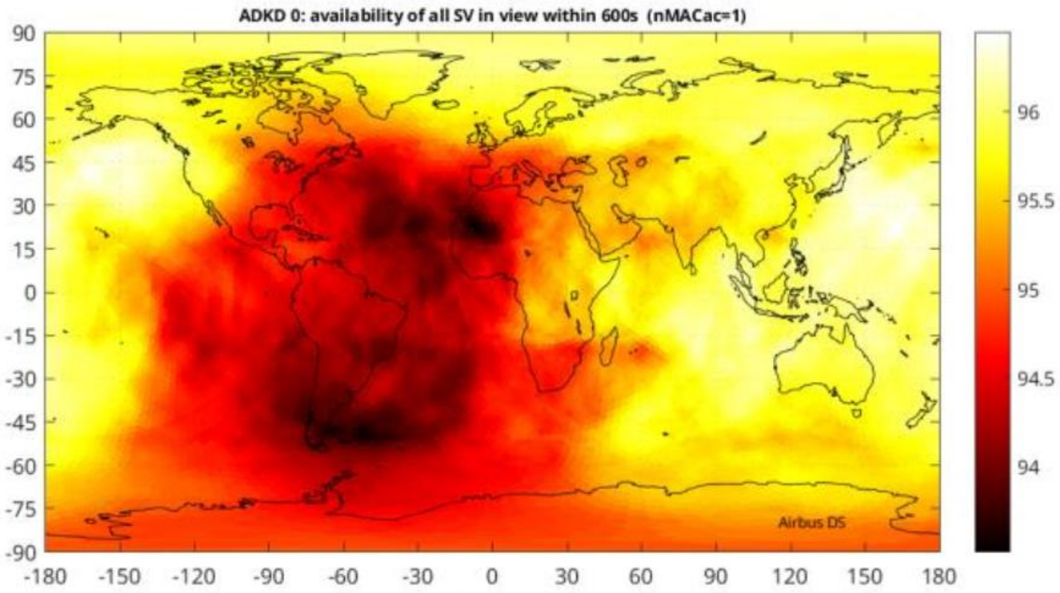
OSNMA Performance – Tag Availability (I)

Availability of ADKD0 (authentication for Galileo I/NAV orbit and clock data, Word Types 1 – 5) over 5° elevation, from 1st to 31st May 2024.



ADKD0 for 4 or more satellites in view within 30s

min: 97.73% | mean: 98.90% | max: 99.40%



ADKD0 for *all* satellites in view within 600s

min: 93.52% | mean: 95.27% | max: 96.45%

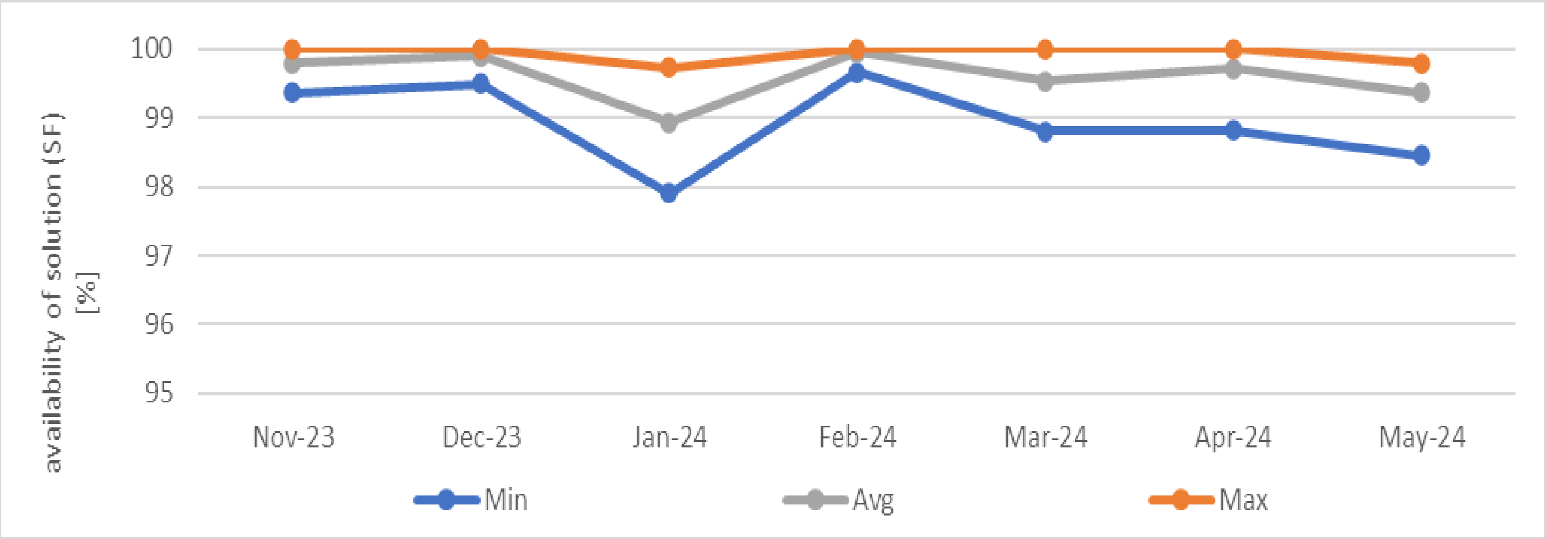
OSNMA Performance –Tag Availability (III)

Measured Tag	Average of Monthly Availabilities at WUL 1st January – 31st May 2024
ADKD0 - All SVs in view, 600s	96.3154%
ADKD0 – At least 4 SVs in view, 30s	98.7157%
ADKD 4 – At least 1 SV in view, 60s	99.2567%
ADKD12– At least 4 SVs in view, 240s	97.5368%

Similar or even higher tag availability is expected for entry into operation.

OSNMA Performance – Position Availability

Availability of OSNMA position solution (ADKD0) users versus Galileo OS users. Defined as percentage of time when OSNMA and Galileo OS position solutions use the same satellites.



Single Frequency

	Yearly Availability at WUL (January – May 2024)
Single Frequency Users	≥ 99.0233%
Dual Frequency Users	≥ 99.0233%

Similar or even higher position availability is expected for entry into operation.

Next Steps

- The OSNMA Public Observation Test phase is ongoing since November 2021. Users can subscribe: https://www.gsc-europa.eu/support-to-developers/osnmapublic-observation-test-phase/register
- The testing activities were concluded in early June 2024 with the execution of TESLA chain renewal and revocation processes
- The OSNMA signal will continue to be provided without interruptions and with the same performance experienced in the last months. The current behavior and performance of the OSNMA signal is nominal and representative of the service phase.
- Galileo is now preparing the forthcoming OSNMA Initial Service declaration. The OSNMA Initial Service Declaration will consist of a formal process including an EC communication, the publication of the OSNMA Service Definition Document (SDD), and the transition of the OSNMA Status Flag from ‘test’ to ‘operational’
- Further service evolutions are under development to:
  - Authenticate additional data types by means of OSNMA, including data from other GNSS (GPS)
  - Provide signal protection to complement OSNMA (Signal Authentication Service) .

More details here: https://www.gsc-europa.eu/news/galileo-is-getting-ready-for-the-upcoming-osnma-operational-declaration

Teamwork

J. Simon, T. Rodriguez, A. Scorzolini, P. da Silva, F. Sbardellati, *European Union Space Program Agency (EUSPA)*

- I. Fernandez-Hernandez, S. Damy, *European Commission (EC)*
- D. Ibanez, *European Space Agency (ESA)*

The authors would like to acknowledge the effort and commitment of all the EUSPA, EC and ESA teams and supporting contractors involved in the development of the Galileo OSNMA service.

#EUSpace

EUSPA
European Union Agency for the Space Programme

THANK YOU FOR YOUR ATTENTION

EU4Space

EUSPA

@EU4Space

@space4eu

EUSPA

@EUSPA@social.network.europa.eu

EUSPA is hiring!

Apply today and help shape the future of #EUSpace!

#EUSpace

EUSPA European Union Agency for the Space Programme

BACKUP SLIDES

Get in touch with us

www.euspa.europa.eu

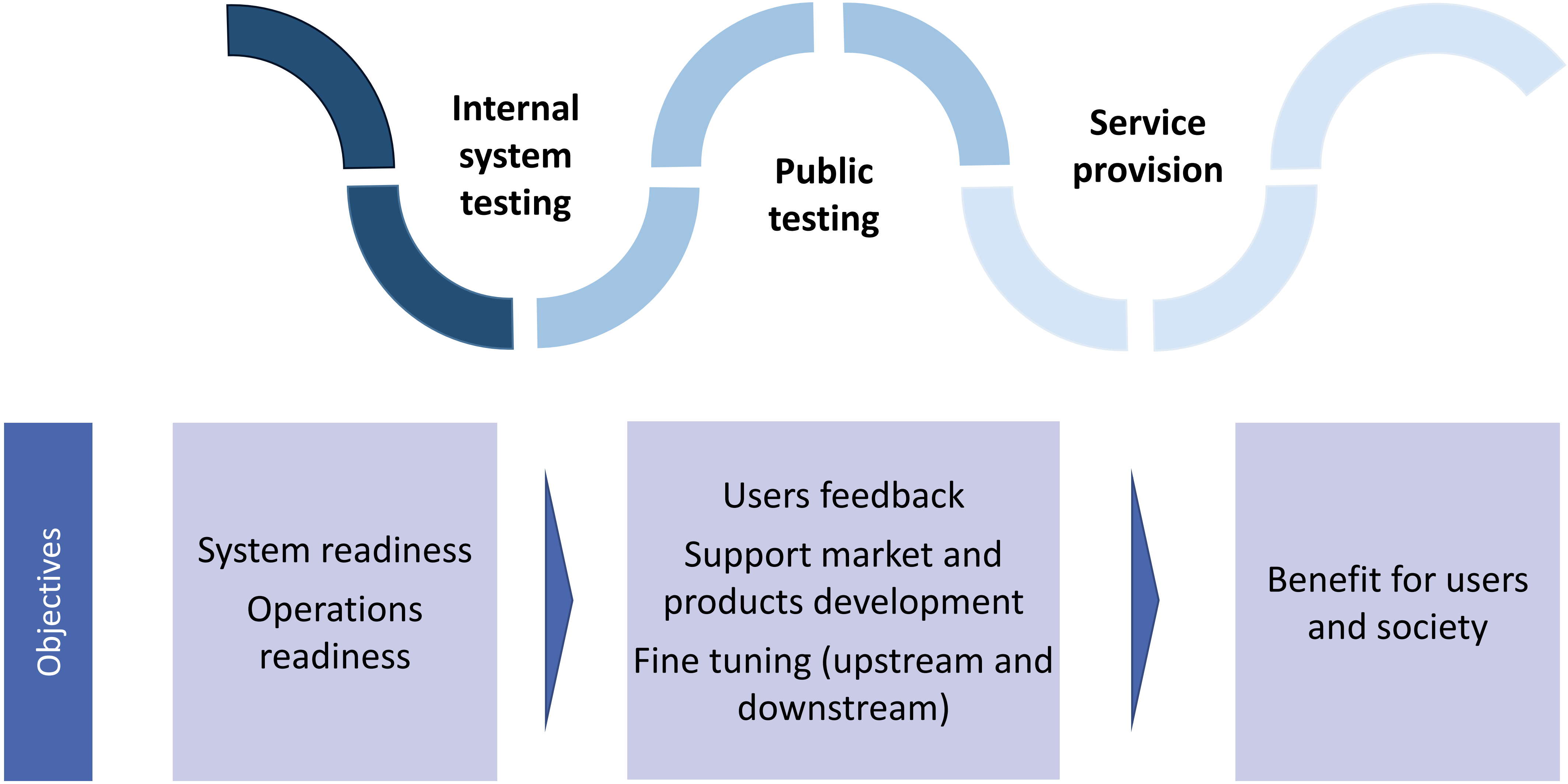
EU4Space EUSPA @EU4Space @space4eu EUSPA @EUSPA@social.network.europa.eu

EUSPA is hiring!

Apply today and help shape the future of #EUSpace!

Roadmap

1st authentication signal provided by a GNSS ever enabled by Galileo worldwide



Internal system testing

Public testing

Service provision

Objectives

System readiness

Operations readiness

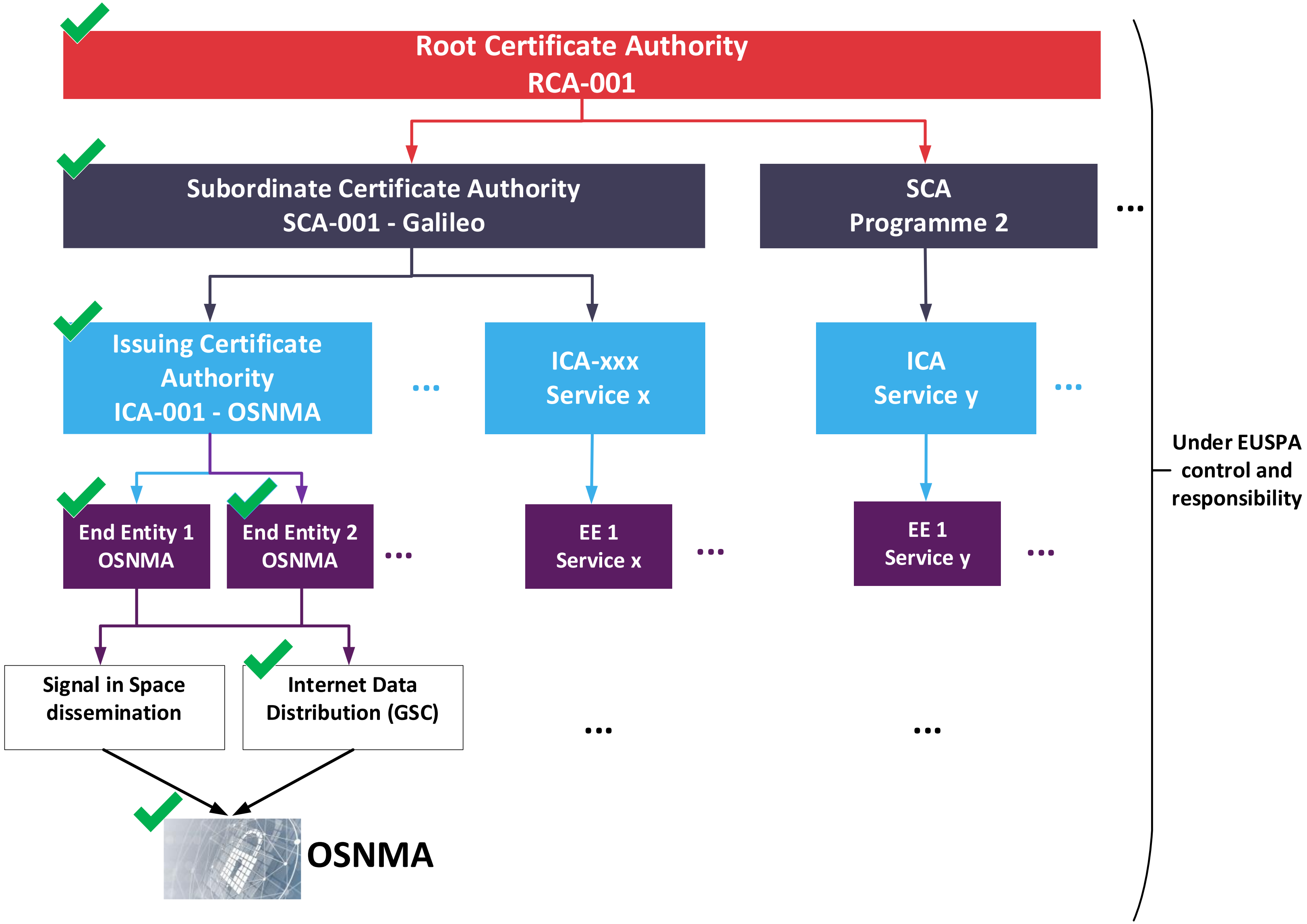
Users feedback

Support market and products development

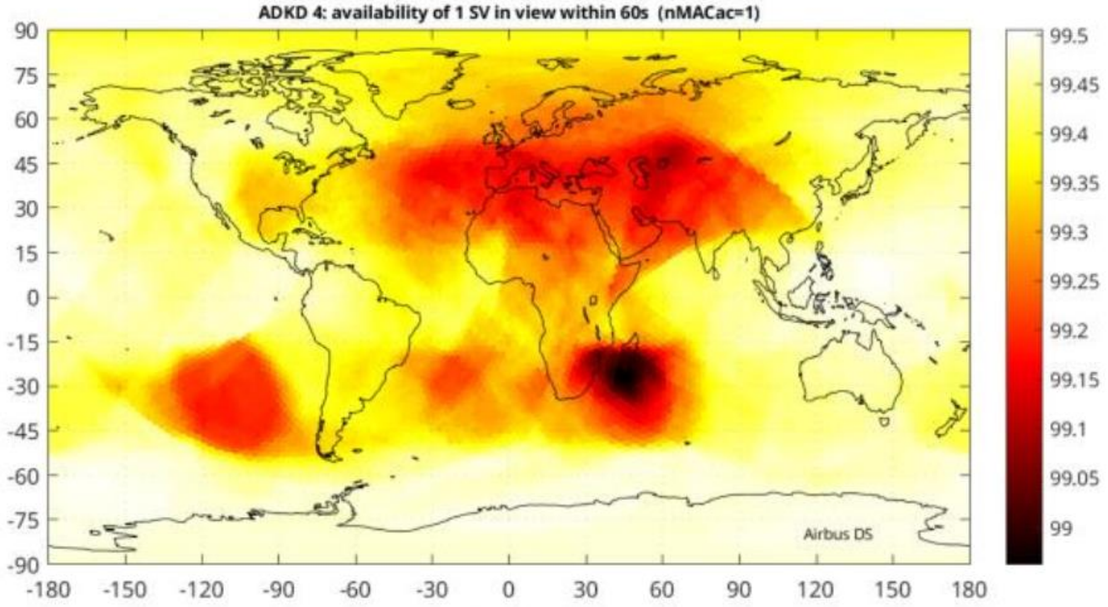
Fine tuning (upstream and downstream)

Benefit for users and society

OSNMA Design – Public key infrastructure

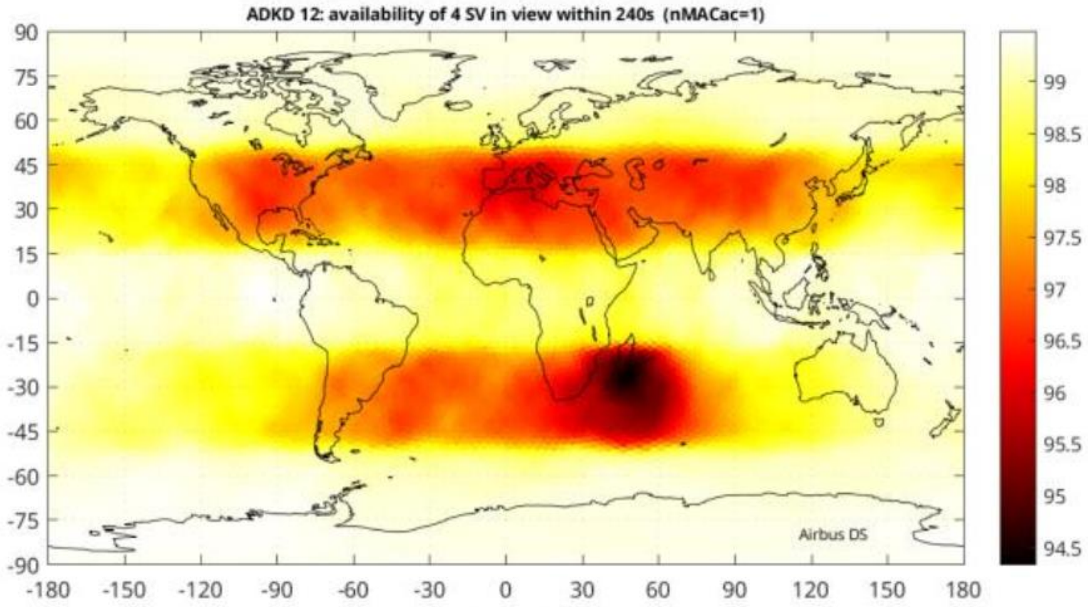

Root Certificate Authority
RCA-001
Subordinate Certificate Authority
SCA-001 - Galileo
SCA
Programme 2
…
Issuing Certificate Authority
ICA-001 - OSNMA
…
ICA-xxx
Service x
ICA
Service y
…
End Entity 1
OSNMA
End Entity 2
OSNMA
…
EE 1
Service x
…
EE 1
Service y
…
Signal in Space dissemination
Internet Data Distribution (GSC)
…
…
OSNMA
Under EUSPA control and responsibility

OSNMA Performance –Tag Availability (II)



Availability of ADKD4 (authentication of Galileo I/NAV timing data, Word Types 6 and 10) over 5° elevation, from 1st to 31st May 2024, within 60s from 1+ satellites

min: 98.96% | mean: 99.38% | max: 99.50%



Availability ADKD12 (authentication of Galileo I/NAV orbit/clock data, Word Types 1-5, with a 5-min delayed key wrt. ADKD0 for loose time sync.) over 5° elevation, from 1st to 31st May 2024, within 240 s from 4+ satellites

min: 94.34% | mean: 98.38% | max: 99.48%