EUSPA
European Union Agency for the Space Programme

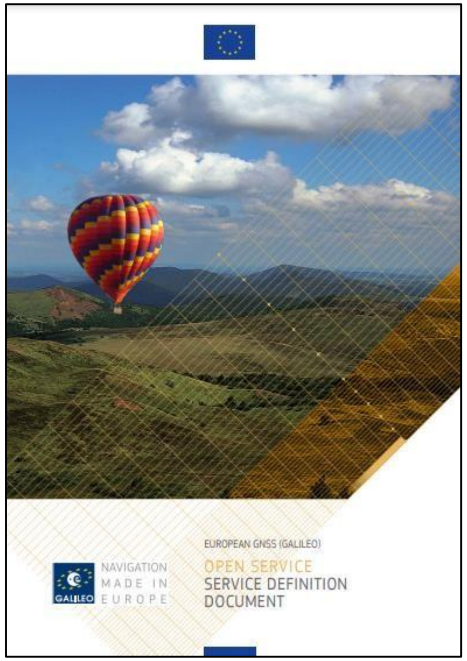
AIRBUS

OSNMA Typical Performance

6/9/2021

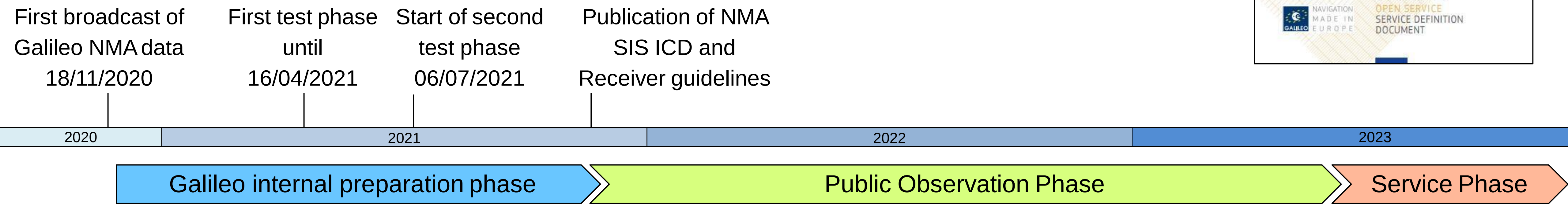
Introduction

- Galileo Open Service Navigation Message Authentication (OSNMA)
  - New service feature of the Galileo Open Service
    - to verify the authenticity of the navigation data source
    - globally available, free of charge
    - similar accuracy and availability as the OS Service



EUROPEAN GNSS (GALILEO)
OPEN SERVICE
SERVICE DEFINITION
DOCUMENT

- Timeline:



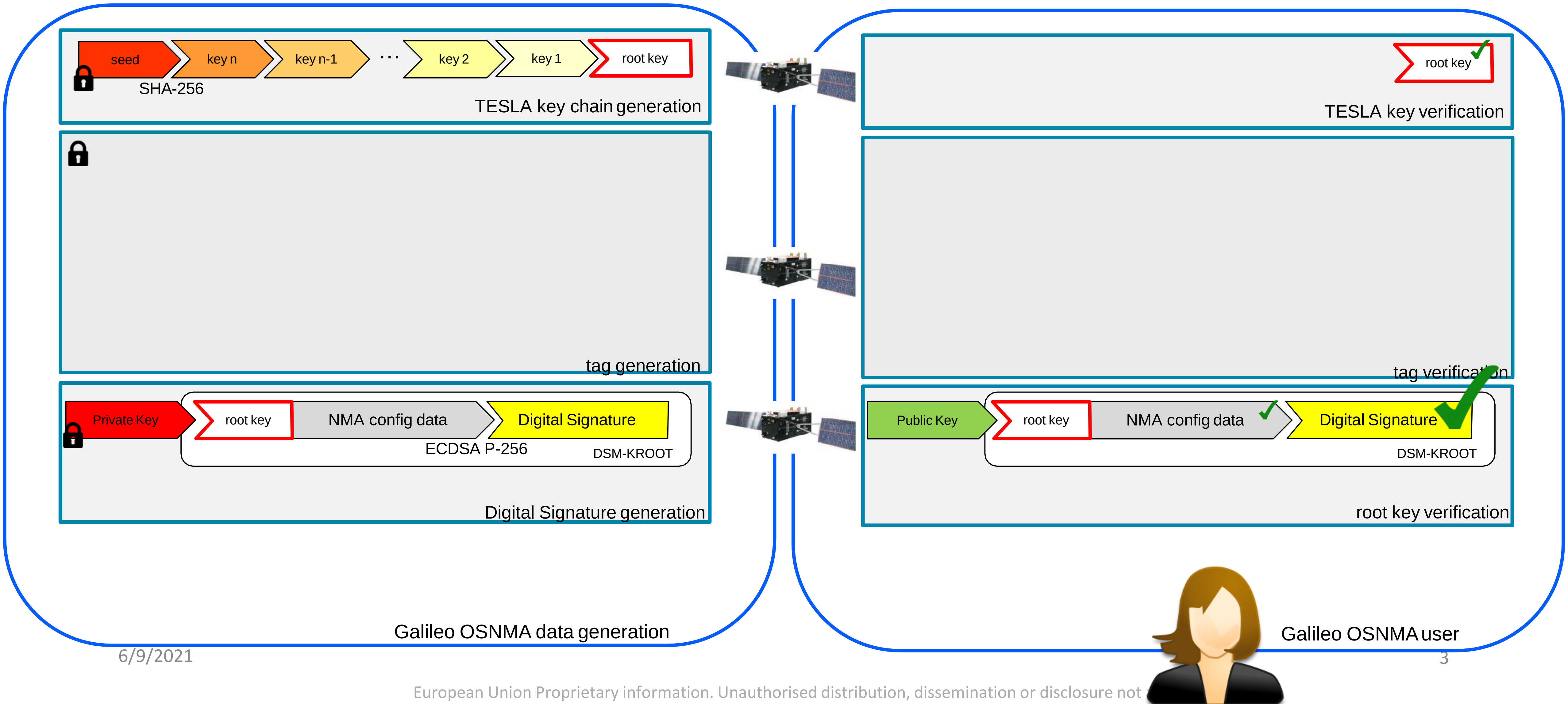
First broadcast of Galileo NMA data 18/11/2020

First test phase until 16/04/2021

Start of second test phase 06/07/2021

Publication of NMA SIS ICD and Receiver guidelines

Galileo Open Service Navigation Message Authentication



seed
key n
key n-1
…
key 2
key 1
root key
SHA-256
TESLA key chain generation

tag generation

Private Key
root key
NMA config data
Digital Signature
ECDSA P-256
DSM-KROOT
Digital Signature generation

Galileo OSNMA data generation

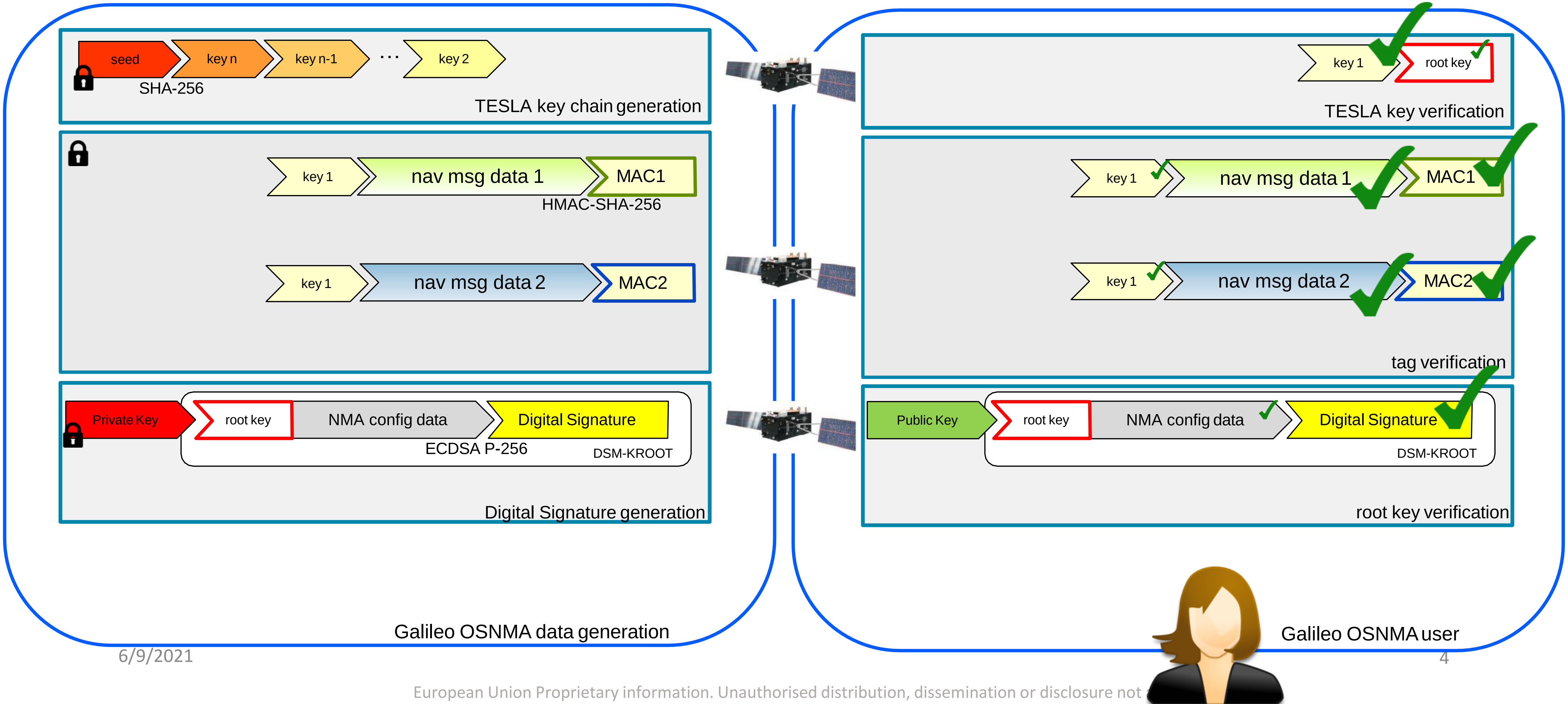
root key
TESLA key verification

tag verification

Public Key
root key
NMA config data
Digital Signature
DSM-KROOT
root key verification

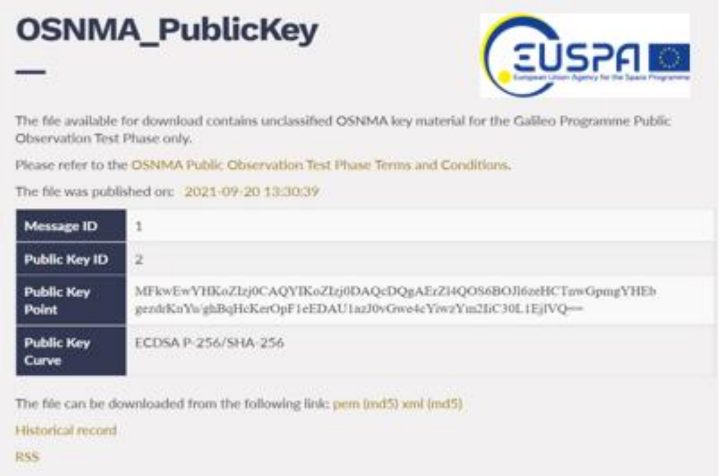
Galileo OSNMA user

Galileo Open Service Navigation Message Authentication



Galileo Open Service Navigation Message Authentication

- Public Key
  - Over-the-air-rekeying (verified by Merkle Tree)
  - Published on GSC website for registered users: https://gsc-europa.eu



OSNMA_PublicKey

The file available for download contains unclassified OSNMA key material for the Galileo Programme Public Observation Test Phase only.

Please refer to the OSNMA Public Observation Test Phase Terms and Conditions.

The file was published on: 2021-09-20 13:30:39

Message ID	1
Public Key ID	2
Public Key Point	MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAErZl4QOS6BOJl6zeHCTawGpmgYHEb gezdrKnYu/ghBqHcKerOpF1eEDAU1azJ0vGwe4cYiwzYm2IiC30L1EjIVQ==
Public Key Curve	ECDSA P-256/SHA-256

The file can be downloaded from the following link: pem (md5) xml (md5)

Historical record

RSS

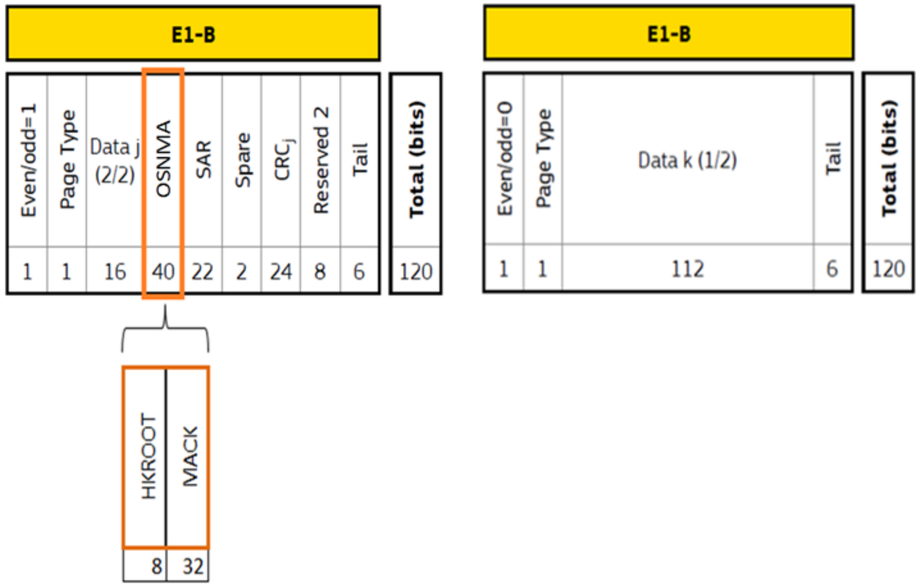
- Required time synchronisation
  - Standard OSNMA user: ~15s
  - "slow MAC" user: ~150s

- MAC types during Public Observation phase:

MAC type	Authentication Data	Key Delay
ADKD 0	I/NAV ephemeris, clock correction, Ionospheric correction, BGD, health flags	1 I/NAV subframe
ADKD 12		1 + 10 I/NAV subframes (slow MAC)
ADKD 4	GST-UTC conversion, GGTO, TOW	1 I/NAV subframe

- Capability to authenticate additional navigation message data has been verified
  - GPS navigation message data
  - Galileo F/NAV navigation message data

OSNMA configuration for the Public Observation Phase



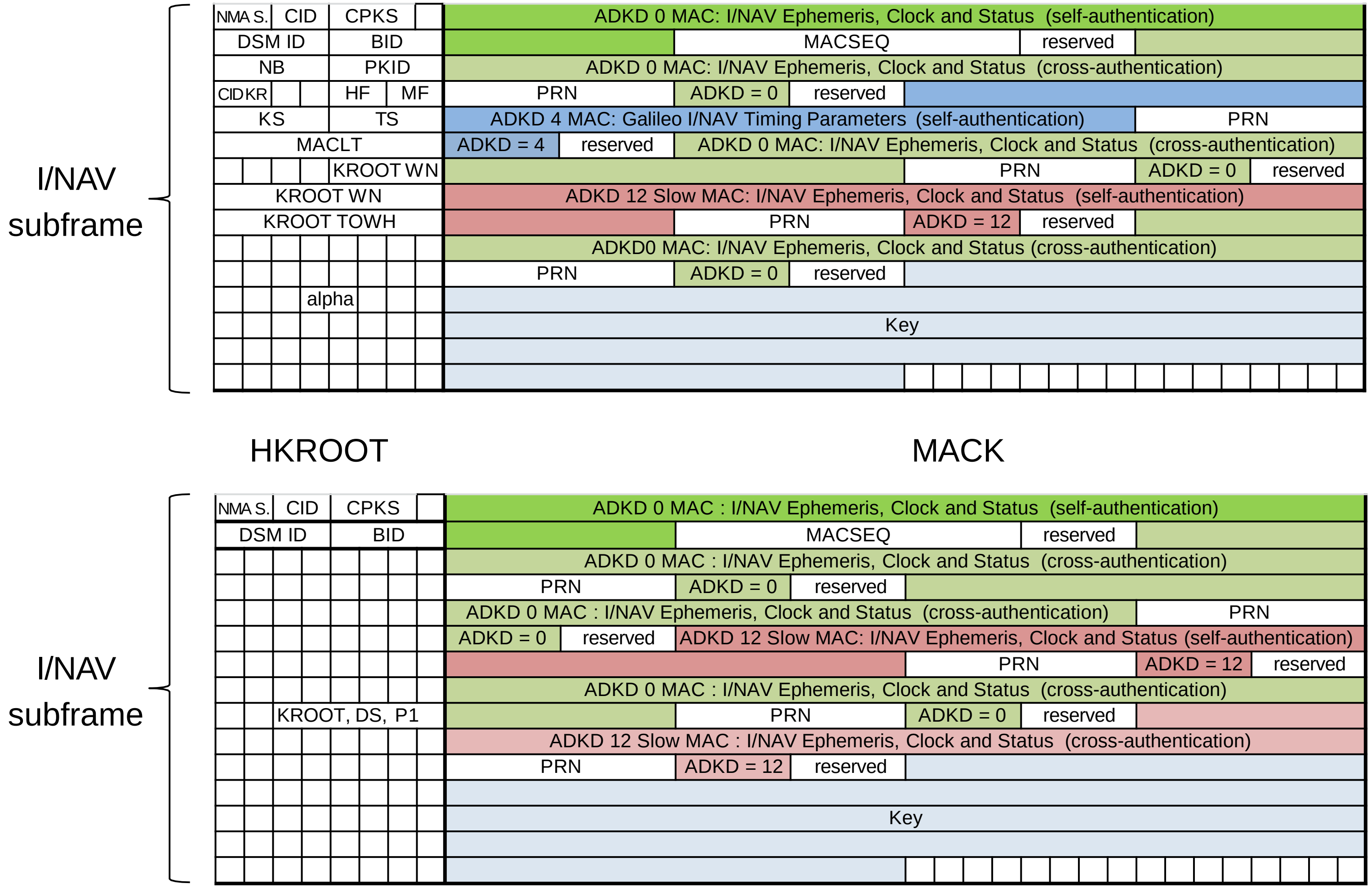
E1-B									Total (bits)
Even/odd=1	Page Type	Data j (2/2)	OSNMA	SAR	Spare	CRC_j	Reserved 2	Tail	
1	1	16	40	22	2	24	8	6	120

OSNMA	
HKROOT	MACK
8	32

E1-B				Total (bits)
Even/odd=0	Page Type	Data k (1/2)	Tail	
1	1	112	6	120

NMA parameter setting for Public Observation Phase

Key Size	128 bit
Tag Size	40 bit
Tesla Key Verification Offset	1 I/NAV sub-frame
Min. equivalent tag length	80 bit



I/NAV subframe

NMA S. | CID | CPKS | ADKD 0 MAC: I/NAV Ephemeris, Clock and Status (self-authentication)

DSM ID | BID | MACSEQ | reserved

NB | PKID | ADKD 0 MAC: I/NAV Ephemeris, Clock and Status (cross-authentication)

CIDKR | HF | MF | PRN | ADKD = 0 | reserved

KS | TS | ADKD 4 MAC: Galileo I/NAV Timing Parameters (self-authentication) | PRN

MACLT | ADKD = 4 | reserved | ADKD 0 MAC: I/NAV Ephemeris, Clock and Status (cross-authentication)

KROOT WN | PRN | ADKD = 0 | reserved

KROOT WN | ADKD 12 Slow MAC: I/NAV Ephemeris, Clock and Status (self-authentication)

KROOT TOWH | PRN | ADKD = 12 | reserved

ADKD0 MAC: I/NAV Ephemeris, Clock and Status (cross-authentication)

PRN | ADKD = 0 | reserved

alpha

Key

HKROOT

MACK

I/NAV subframe

NMA S. | CID | CPKS | ADKD 0 MAC : I/NAV Ephemeris, Clock and Status (self-authentication)

DSM ID | BID | MACSEQ | reserved

ADKD 0 MAC : I/NAV Ephemeris, Clock and Status (cross-authentication)

PRN | ADKD = 0 | reserved

ADKD 0 MAC : I/NAV Ephemeris, Clock and Status (cross-authentication) | PRN

ADKD = 0 | reserved | ADKD 12 Slow MAC: I/NAV Ephemeris, Clock and Status (self-authentication)

PRN | ADKD = 12 | reserved

ADKD 0 MAC : I/NAV Ephemeris, Clock and Status (cross-authentication)

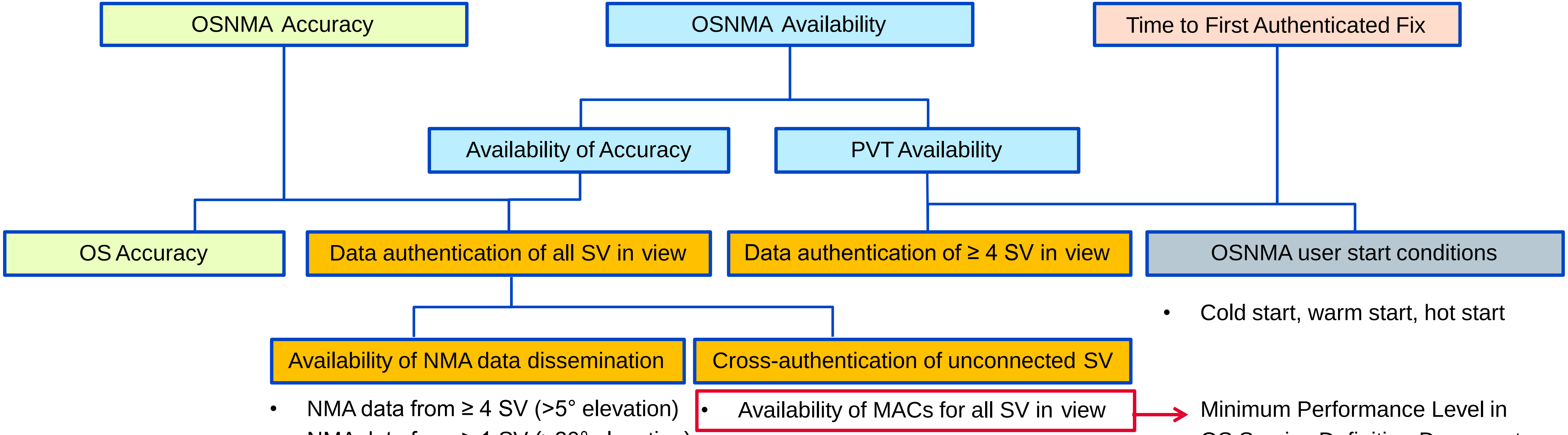
KROOT, DS, P1 | PRN | ADKD = 0 | reserved

ADKD 12 Slow MAC : I/NAV Ephemeris, Clock and Status (cross-authentication)

PRN | ADKD = 12 | reserved

Key

OSNMA service performance



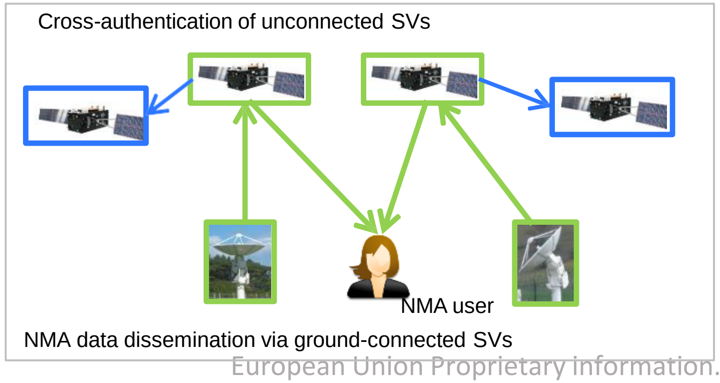
OSNMA Accuracy
OSNMA Availability
Time to First Authenticated Fix
Availability of Accuracy
PVT Availability
OS Accuracy
Data authentication of all SV in view
Data authentication of ≥ 4 SV in view
OSNMA user start conditions
Availability of NMA data dissemination
Cross-authentication of unconnected SV

- Cold start, warm start, hot start

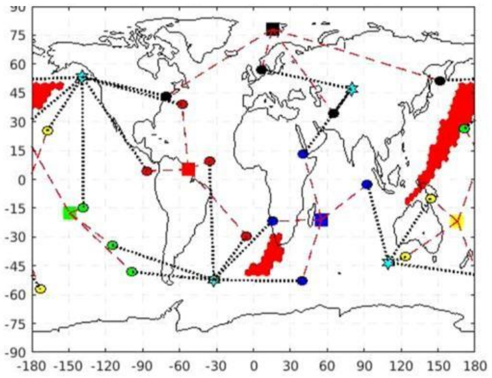
- NMA data from ≥ 4 SV (>5° elevation)
- NMA data from ≥ 1 SV (>20° elevation)

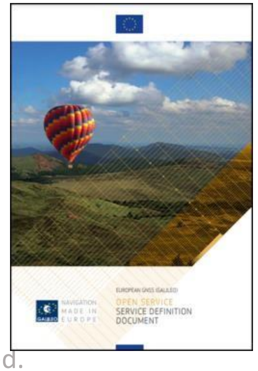
- Availability of MACs for all SV in view

Minimum Performance Level in OS Service Definition Document

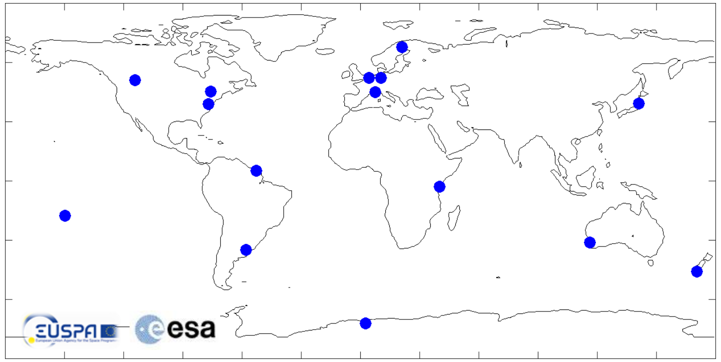


Cross-authentication of unconnected SVs
NMA user
NMA data dissemination via ground-connected SVs

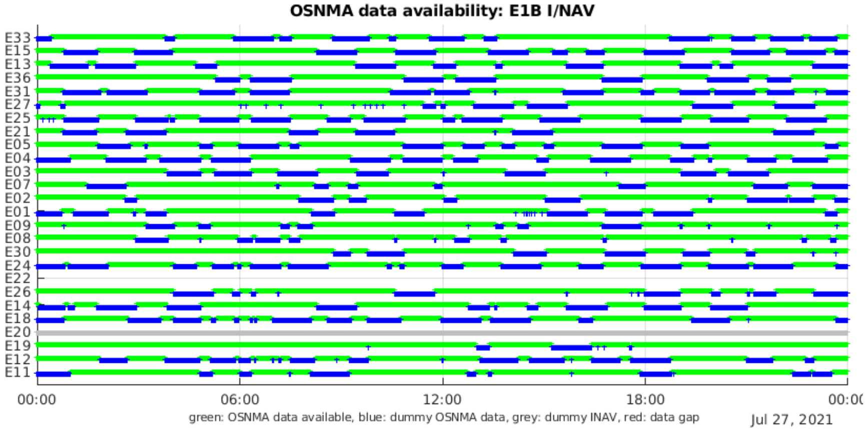




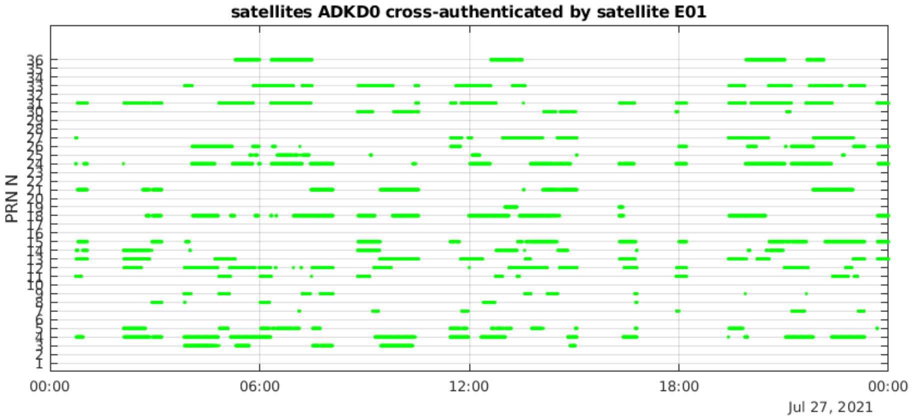
OSNMA service monitoring



- Global network of monitoring sites



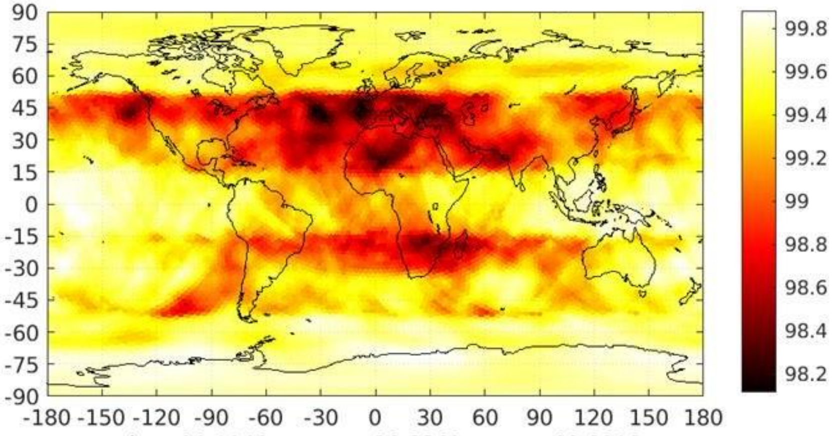
- Observed OSNMA data availability per satellite



- Observed cross-authentication per satellite

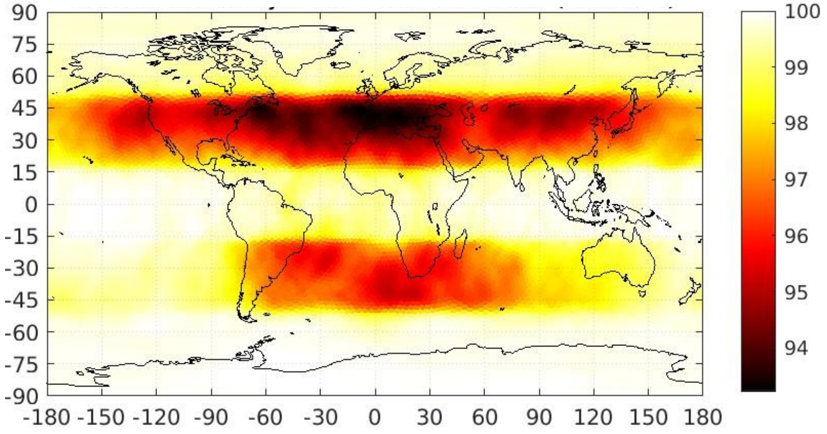
Service Volume analysis

N#MAtch



min = 98.1146, mean = 99.3369, max = 99.8818

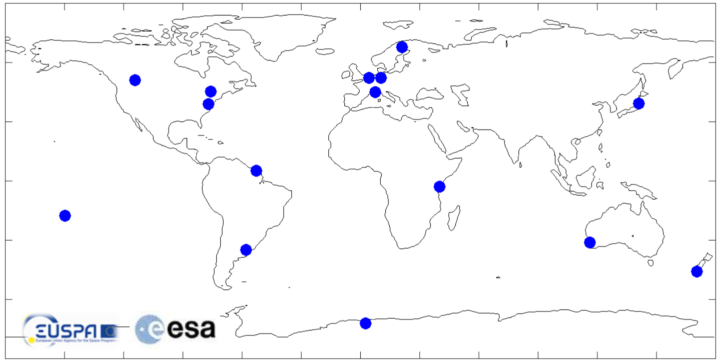
- Availability of MACs for all SV in view within 120s

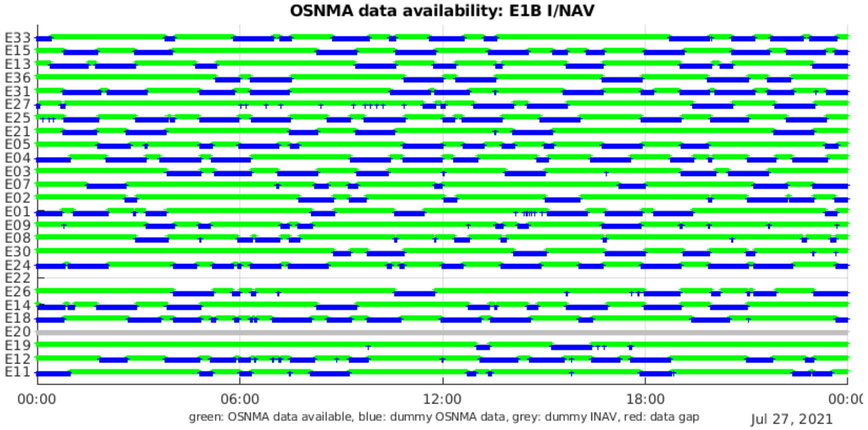


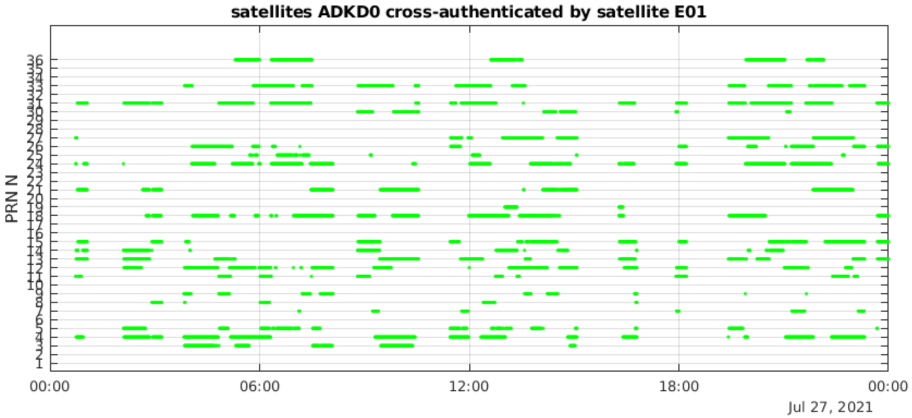
min = 93.2205, mean = 98.3948, max = 100.0000

- Availability of “slow MACs” for at least four SV in view within 240s

OSNMA service monitoring





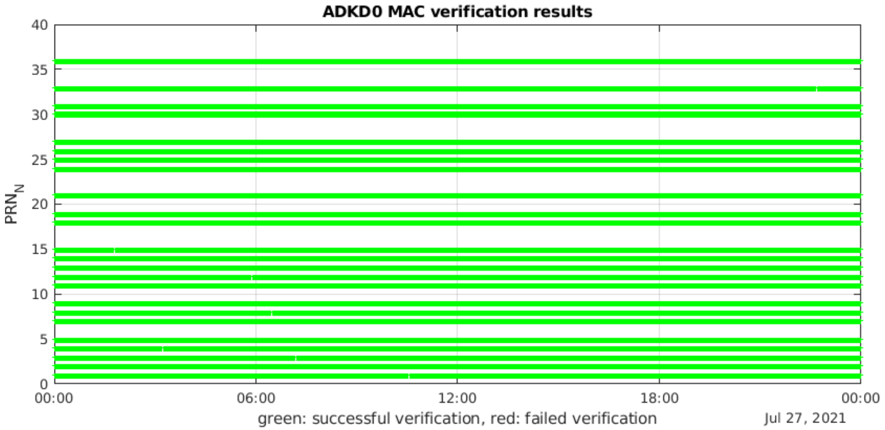


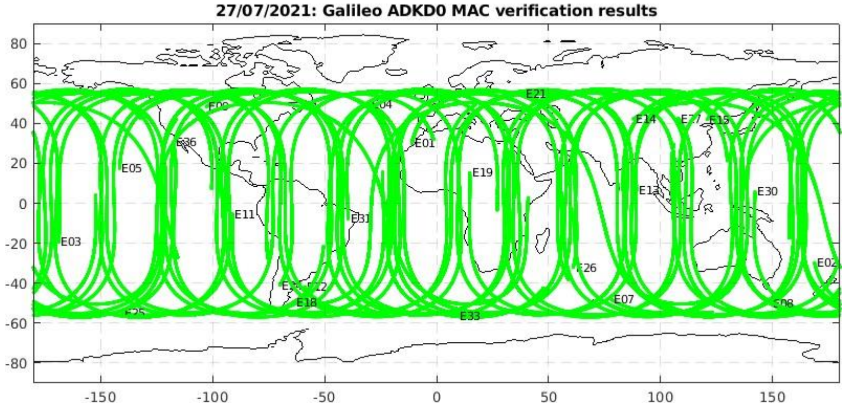
- Global network of monitoring sites
- Observed OSNMA data availability per satellite
- Observed cross-authentication per satellite

NMA data processing

OSNMA SIS ICD

N#MAtch





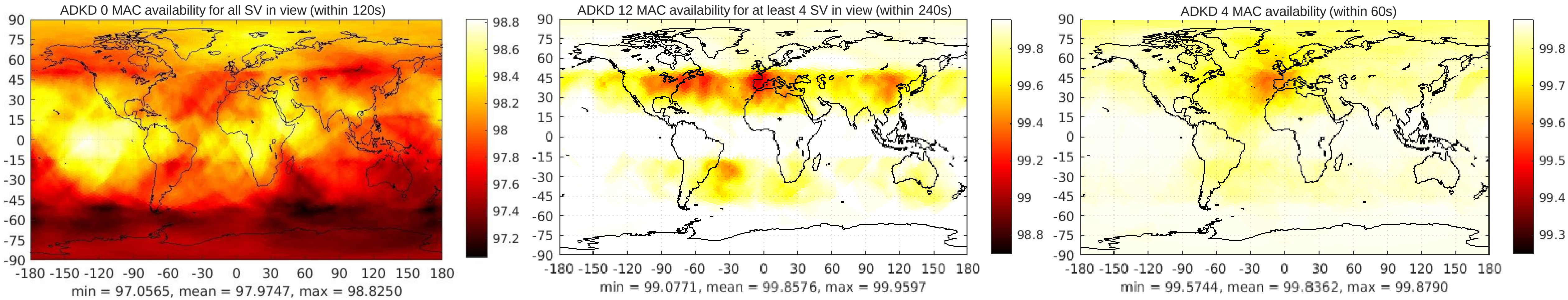
I/NAV ephemeris and clock correction: authentication results

Test Results: MAC availability, August 2021

MACs for I/NAV ephemeris and clock correction for all SV in view

Slow MACs for I/NAV ephemeris and clock correction for at least 4 SV in view

MACs for timing parameters from at least 1 SV in view


ADKD 0 MAC availability for all SV in view (within 120s)
min = 97.0565, mean = 97.9747, max = 98.8250
98.8
98.6
98.4
98.2
98
97.8
97.6
97.4
97.2
ADKD 12 MAC availability for at least 4 SV in view (within 240s)
min = 99.0771, mean = 99.8576, max = 99.9597
99.8
99.6
99.4
99.2
99
98.8
ADKD 4 MAC availability (within 60s)
min = 99.5744, mean = 99.8362, max = 99.8790
99.8
99.7
99.6
99.5
99.4
99.3
90
75
60
45
30
15
0
-15
-30
-45
-60
-75
-90
-180 -150 -120 -90 -60 -30 0 30 60 90 120 150 180

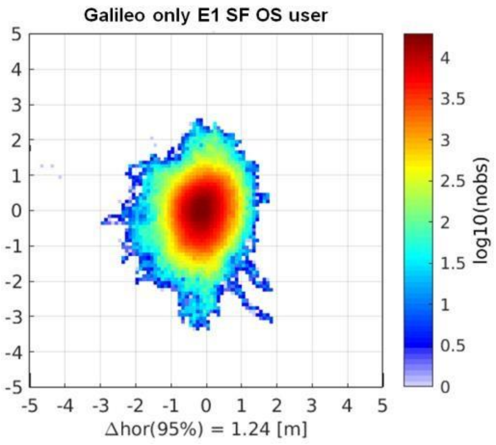
WUL: 97.06%
AUL: 97.97%
BUL: 98.82%

WUL: 99.08%
AUL: 99.86%
BUL: 99.96%

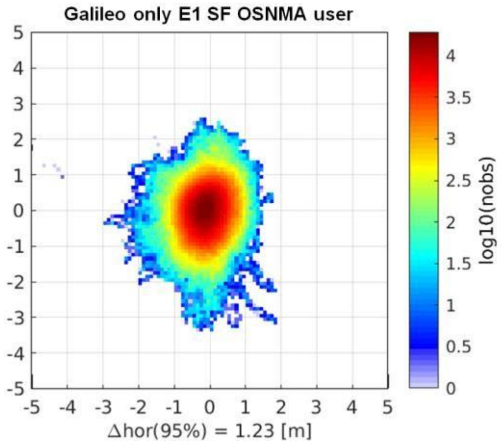
WUL: 99.57%
AUL: 99.84%
BUL: 99.88%

Test Results: Position Accuracy–Static OSNMA User

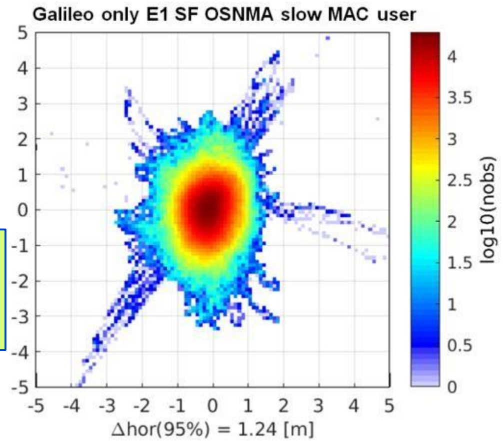
E1 SF OS/OSNMA user, open sky, fixed antenna, Airbus premises Munich, July 2021:



H: 1.24m (95%)
V: 1.83m (95%)



H: 1.23m (95%)
V: 1.82m (95%)

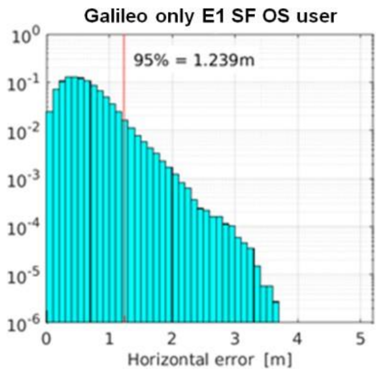


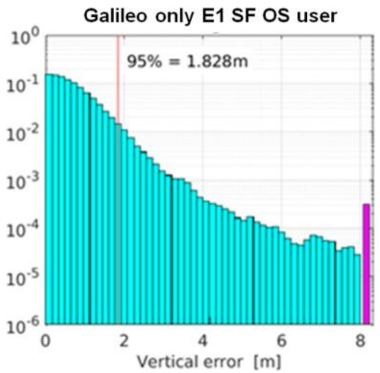
H: 1.24m (95%)
V: 1.81m (95%)

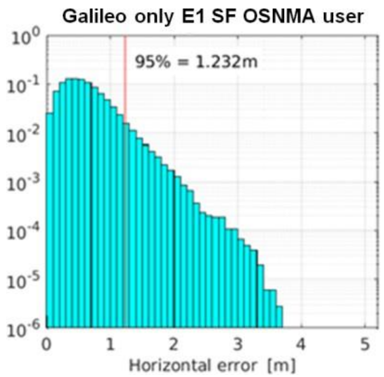
Standard OS user

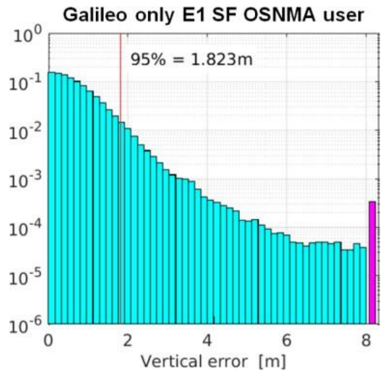
OSNMA user

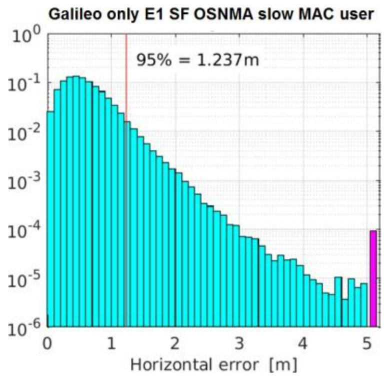
“slow MAC” OSNMA user

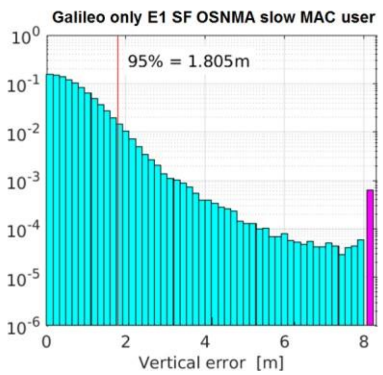








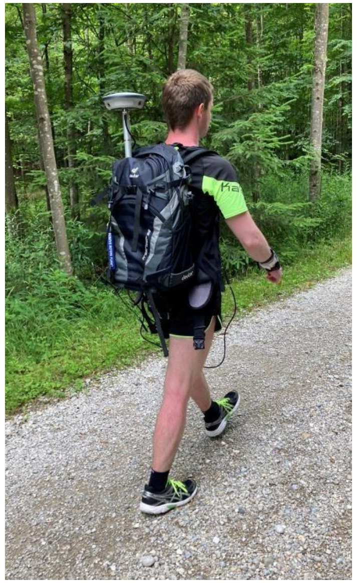


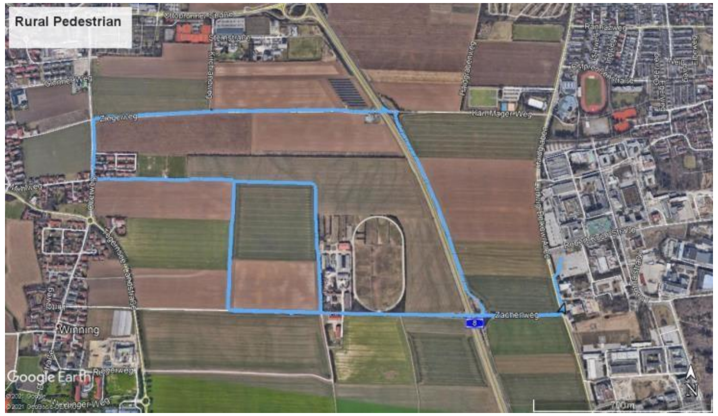


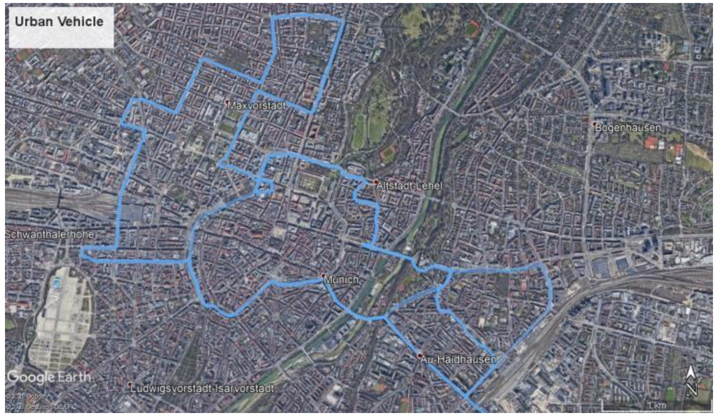
Test Results: PVT Accuracy and Availability–Mobile OSNMA User (1/2)

- Mobile user testing carried out for different use cases:
  - Rural Pedestrian
  - Urban Pedestrian
  - Rural Vehicle
  - Urban Vehicle

- Novatel SPAN GNSS+IMU for reference trajectories
- Septentrio PolaRx5 GNSS receiver for data collection





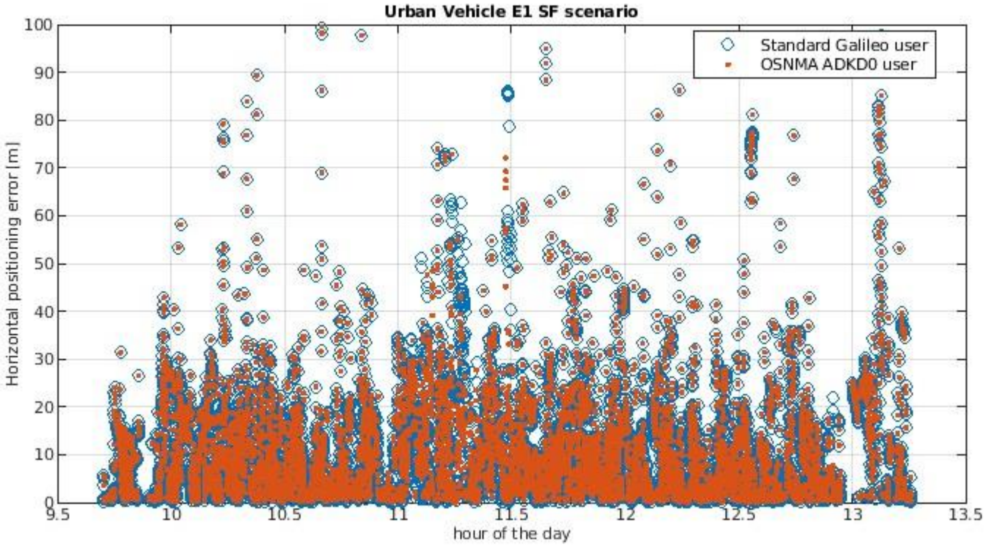


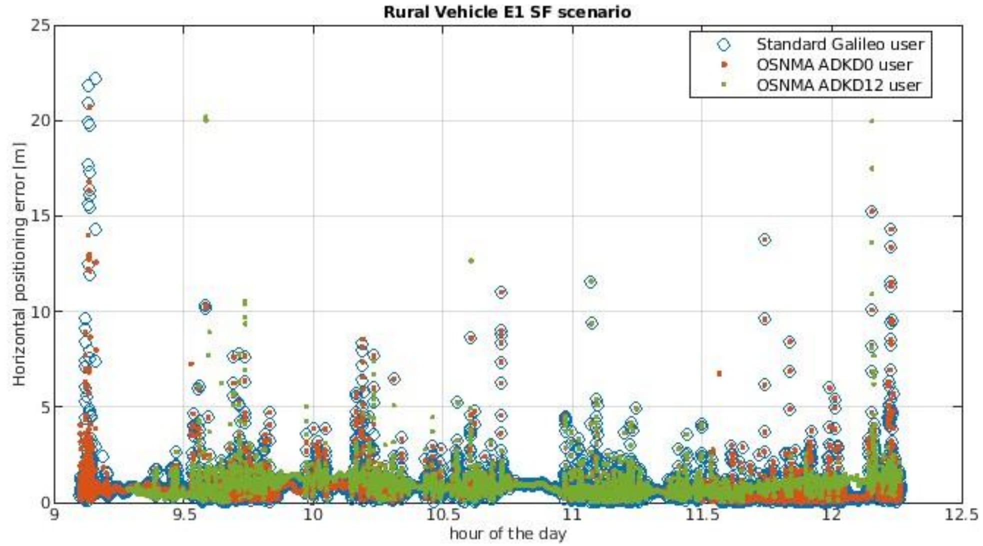
Test Results: PVT Accuracy and Availability – Mobile OSNMA User (2/2)

- Positioning accuracy and PVT availability comparable to OS standard user
- “Slow MAC” (ADKD 12) user performance:
  - Comparable to ADKD0 under good visibility conditions
  - Degraded in urban scenarios

→ OSNMA configuration for the Public Observation phase: Additional bandwidth for ADKD 12 to improve performance

Scenario	PVT Availability [%]		
	Standard	**ADKD 0**	**ADKD 12 ***
Rural Pedestrian #1	98.9%	98.9%	98.9%
Rural Pedestrian #2	99.2%	99.2%	98.9%
Rural Vehicle #1	100.0%	100.0%	94.1%
Rural Vehicle #2	100.0%	100.0%	100.0%
Urban Pedestrian #1	83.8%	81.6%	37.2%
Urban Pedestrian #2	97.4%	97.1%	37.4%
Urban Vehicle #1	96.7%	96.7%	90.1%
Urban Vehicle #2	88.1%	87.3%	41.5%

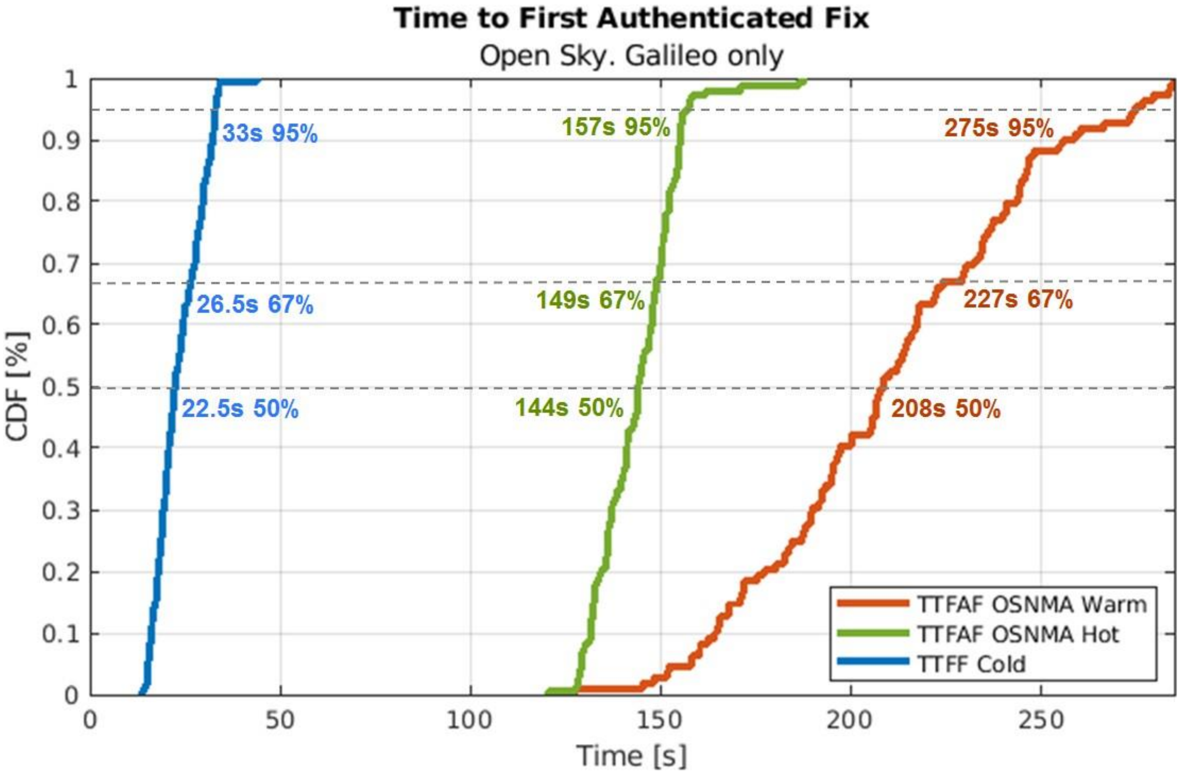




Test Results: Time to First Authenticated Fix (TTFAF)

- Startup conditions for OSNMA:
  - OSNMA Cold Start: Public Key (and Root Key) not available
  - OSNMA Warm Start: Public Key available; Root Key missing
  - OSNMA Hot Start: Public Key and Root Key available
- OSNMA-ready receiver (Septentrio PolaRx5)
  - Fixed antenna in Munich
  - Open sky
- OSNMA processing approach:
  - MAC uses only data fully transmitted before the MAC
  - MACs verified with keys transmitted in the next I/NAV subframe
  - MACs accumulated for a security level of 80 bits
- TTFAF performance of ADKD12 “Slow MAC” user was also analyzed

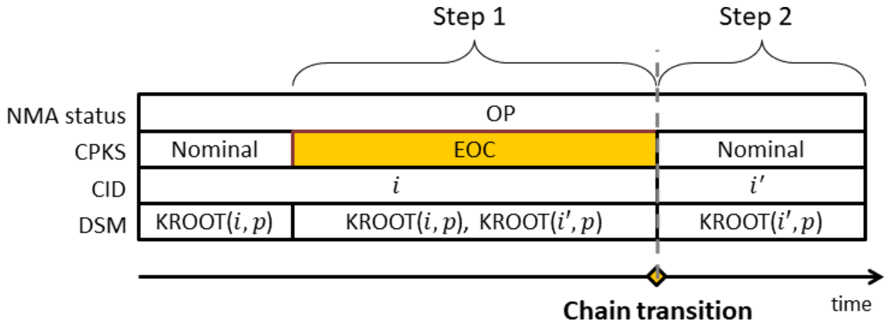
TTFAF OSNMA Hot Start [s]	50%	67%	95%
ADKD12 User	446	454	570



Results are indicative. TTFAF can be reduced with optimal receiver implementations

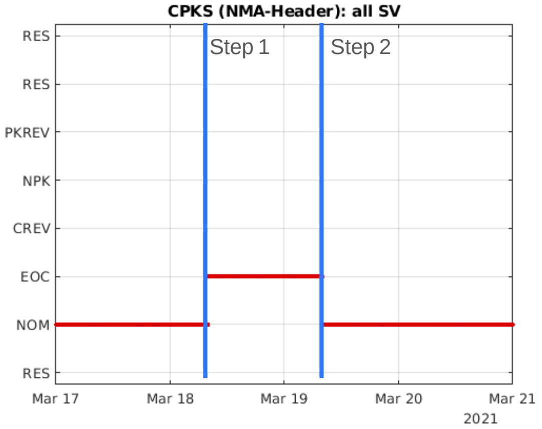
Operational aspects

- Key chain renewal/revocation

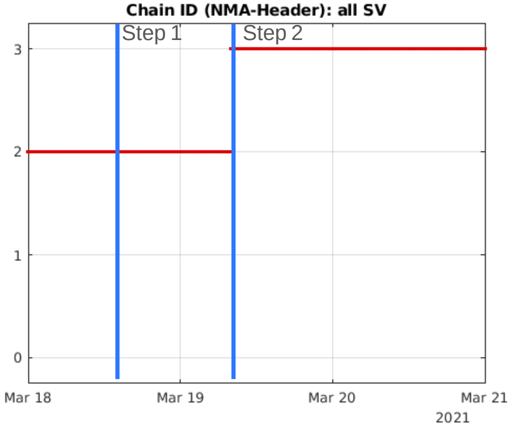


		Step 1	Step 2
NMA status	OP		
CPKS	Nominal	EOC	Nominal
CID	i		i'
DSM	KROOT(i,p)	KROOT(i,p), KROOT(i',p)	KROOT(i',p)

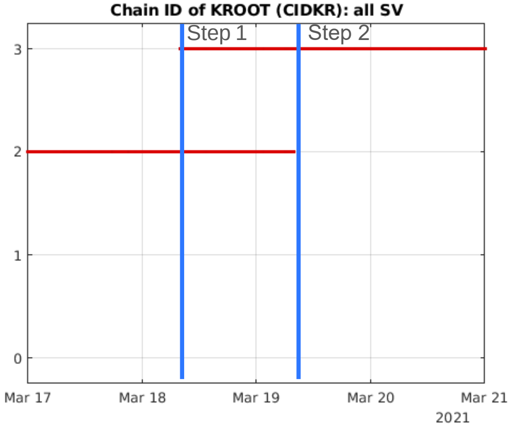
TESLA Key Chain renewal



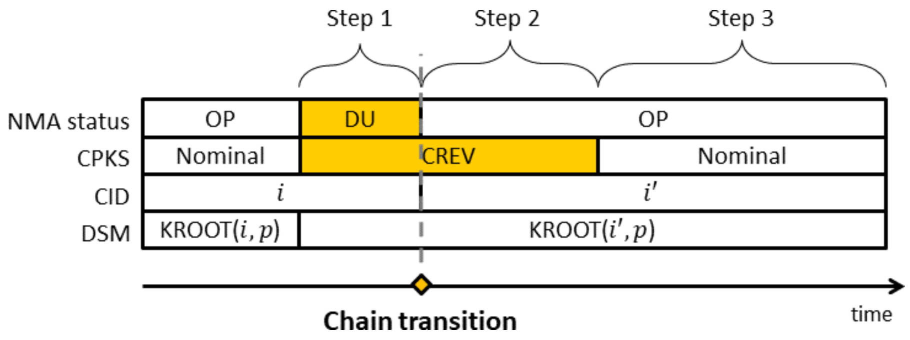
CPKS (NMA-Header): all SV



Chain ID (NMA-Header): all SV

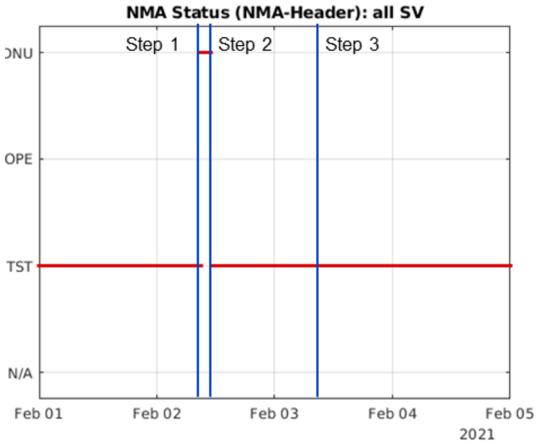


Chain ID of KROOT (CIDKR): all SV

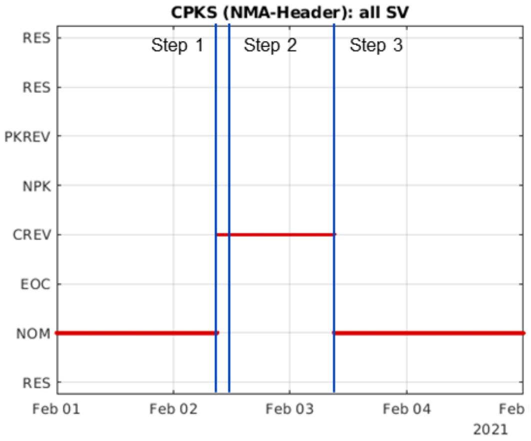


		Step 1	Step 2	Step 3
NMA status	OP	DU	OP	
CPKS	Nominal	CREV		Nominal
CID	i		i'	
DSM	KROOT(i,p)	KROOT(i',p)		

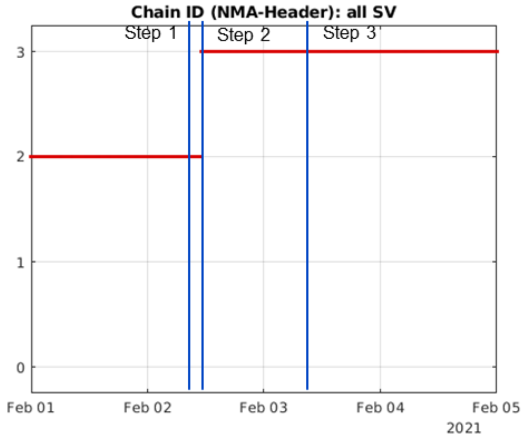
TESLA Key Chain revocation



NMA Status (NMA-Header): all SV



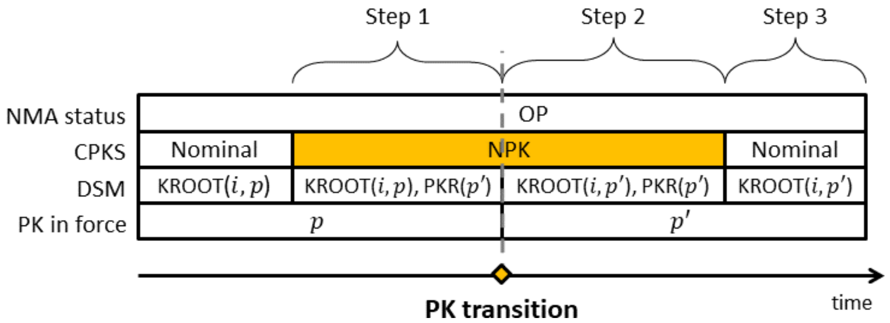
CPKS (NMA-Header): all SV



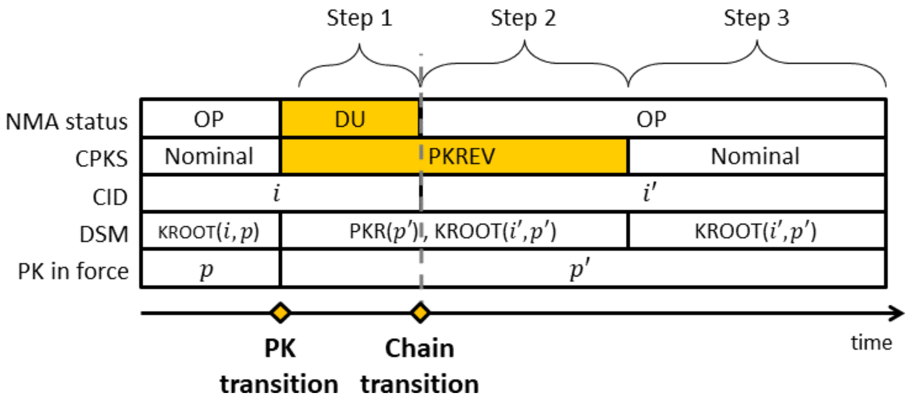
Chain ID (NMA-Header): all SV

Operational aspects

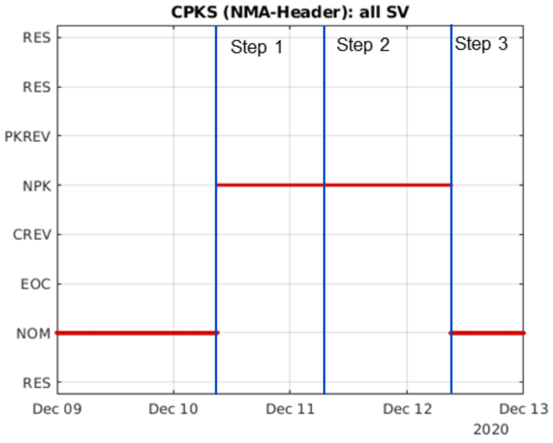
- Public key renewal/revocation

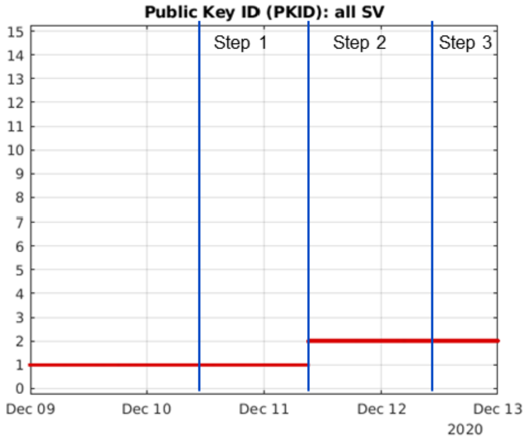


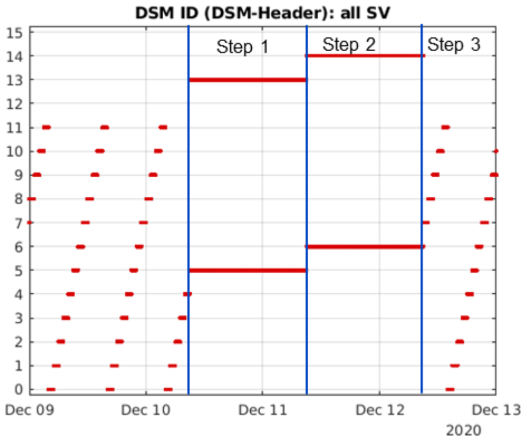
Public Key renewal

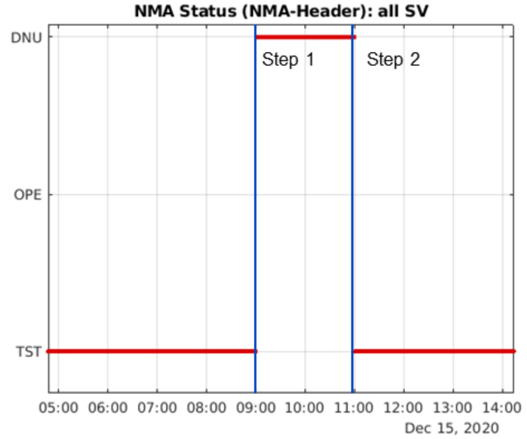


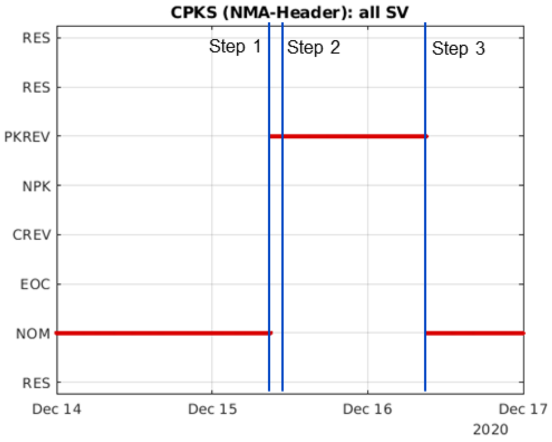
Public Key revocation

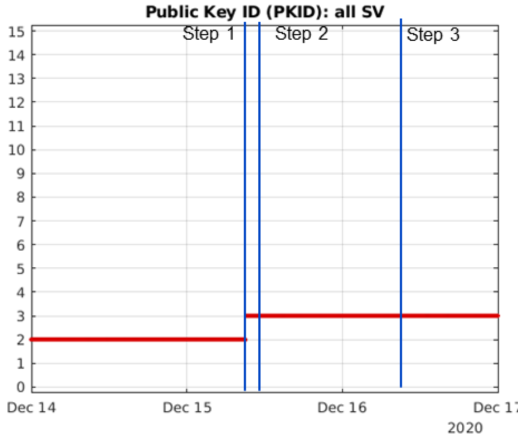






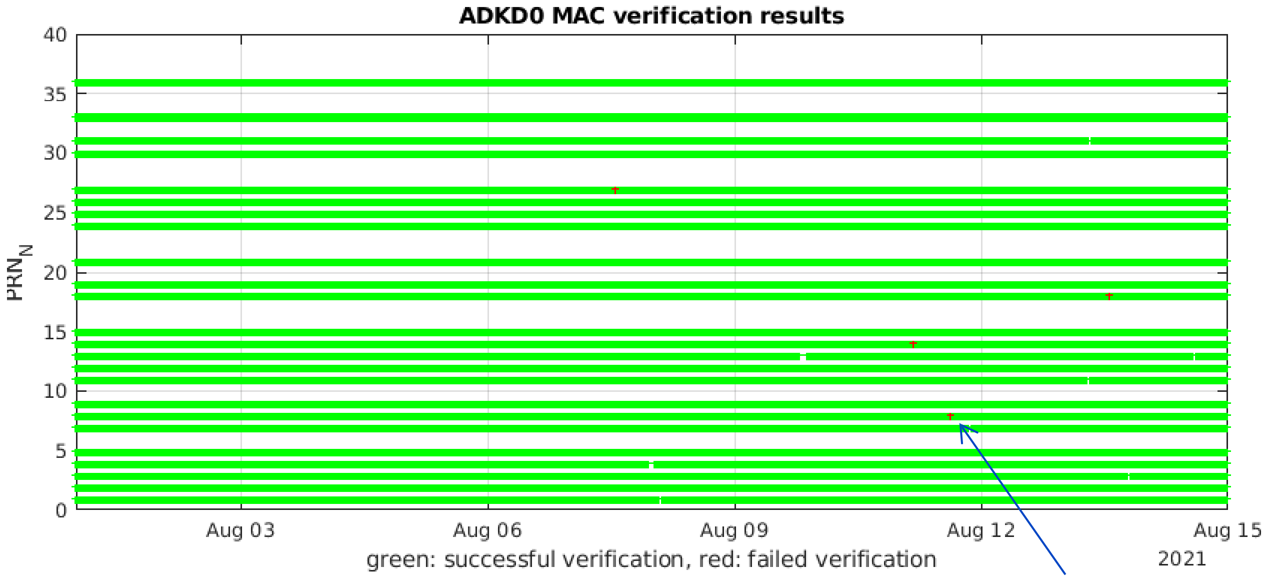






Further improvements for OSNMA service provision

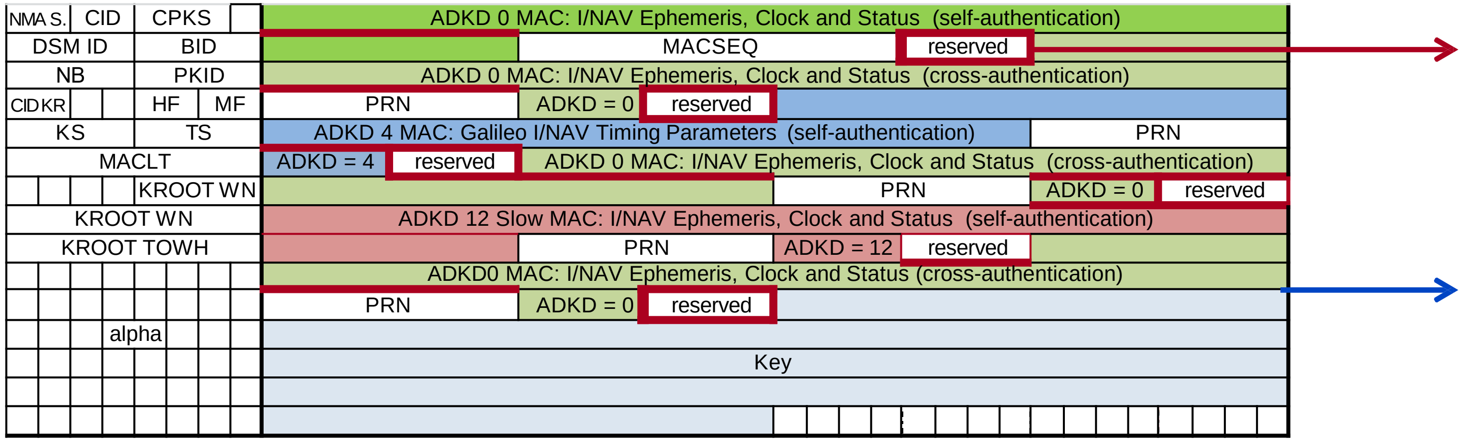
- Very sporadic MAC verification failures may still occur during the Public Observation phase at a low rate
- Root causes are known and corrective measures are identified
- Will be corrected for the service phase



Failed MAC verification

Further improvements for OSNMA service provision

- Improved Service Availability and Continuity (OSNMA data gaps)



NMA S. | CID | CPKS
DSM ID | BID
NB | PKID
CID KR | HF | MF
KS | TS
MACLT
KROOT WN
KROOT WN
KROOT TOWH
alpha

ADKD 0 MAC: I/NAV Ephemeris, Clock and Status (self-authentication)
MACSEQ | reserved
ADKD 0 MAC: I/NAV Ephemeris, Clock and Status (cross-authentication)
PRN | ADKD = 0 | reserved
ADKD 4 MAC: Galileo I/NAV Timing Parameters (self-authentication) | PRN
ADKD = 4 | reserved | ADKD 0 MAC: I/NAV Ephemeris, Clock and Status (cross-authentication)
PRN | ADKD = 0 | reserved
ADKD 12 Slow MAC: I/NAV Ephemeris, Clock and Status (self-authentication)
PRN | ADKD = 12 | reserved
ADKD0 MAC: I/NAV Ephemeris, Clock and Status (cross-authentication)
PRN | ADKD = 0 | reserved
Key

- reserved fields will be defined to provide unambiguous link between MAC and data

- “dummy” MACs will be defined in case navigation data is not available for NMA data generation

- Navigation data mask for ADKD 4 MACs (Timing Parameter) will be redefined to remove TOW

- Regular transmission of Public Key via SIS

- Merkle Tree renewal process

6/9/2021

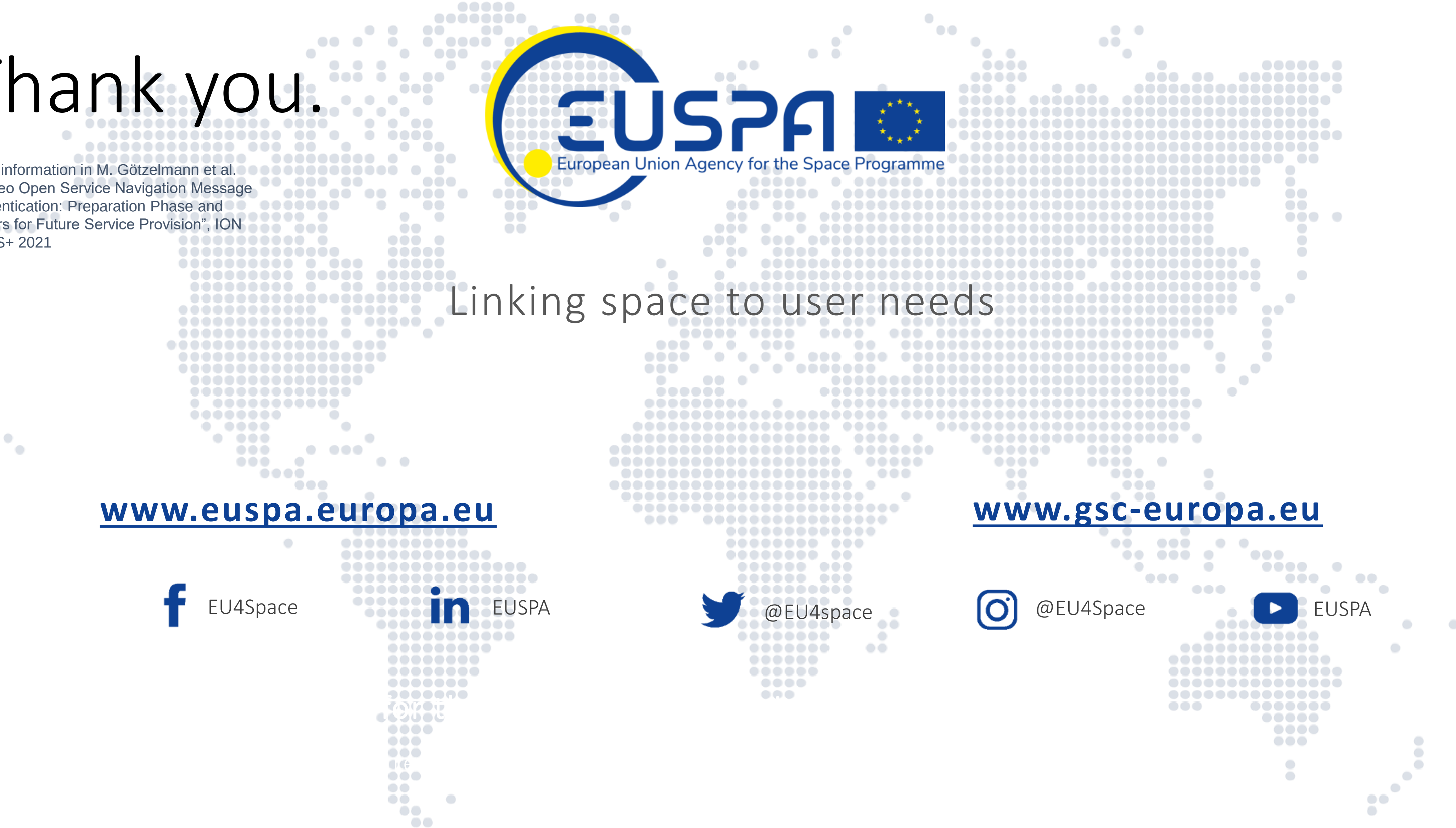
Summary and Conclusions

- OSNMA Internal Preparation Phase: a key step towards OSNMA service provision
  - Authentication of Galileo (and GPS) navigation message data successfully verified
  - Position accuracy and availability of OSNMA user are comparable to the OS
  - Some elements of the OSNMA protocol are identified for further refinement
- Sporadic OSNMA data gaps and very low residual MAC verification failure rate may occur during the Public Observation phase
  - Root causes are known and corrective measures are identified for Service Phase
- User feedback from the Public Observation phase will be taken into consideration

Thank you.

More information in M. Götzelmann et al. “Galileo Open Service Navigation Message Authentication: Preparation Phase and Drivers for Future Service Provision”, ION GNSS+ 2021

EUSPA
European Union Agency for the Space Programme



Linking space to user needs

www.euspa.europa.eu

www.gsc-europa.eu

EU4Space

EUSPA

@EU4space

@EU4Space

EUSPA

European Union Proprietary information. Unauthorised distribution, dissemination or disclosure not allowed.