NLS
FINNISH GEOSPATIAL RESEARCH INSTITUTE
FGI

An Experimental Performance Assessment of Galileo OSNMA

Toni Hammarberg

Finnish Geospatial Research Institute

Department of Navigation and Positioning

06.06.2023

ESRIUM project background

- Work done in Horizon2020 funded project ESRIUM
- Goal: create road-wear map with accurate information about the position and shape of the road damage
- Sensor vehicle with LiDARs (road damage estimation) and GNSS (positioning)
- Galileo is used for positioning the sensors vehicle, Galileo OSNMA is used increase the security and robustness of the solution
    - Therefore practical understanding of OSNMA characteristics was important for us

ESRIUM

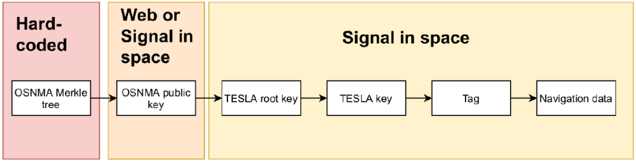
SAFE AND EFFICIENT ROADS

This project has received funding from the European Union Agency for the Space Programme under the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004181.

The content of this presentation reflects only the author's view. Neither the European Commission nor the EUSPA is responsible for any use that may be made of the information it contains.

The shortest intro to Galileo OSNMA

- OSNMA = Open Service Navigation Message Authentication
  - Goal is to verify that the received satellite data is both authentic and unmodified
- Variety of well tested cryptographic methods adapted to the satellite data use case are used to achieve this
  - Keys to authenticate the navigation data are transmitted in the signal-in-space
  - Key and navigation data are used to compute a tag: received tag and computed tag are compared
  - Keys form a hash chain: enables the verification that the key is coming from the same source as the previous
  - Public key cryptography is used to verify the first chain key (= root key)
  - The public keys are verified by a Merkle tree



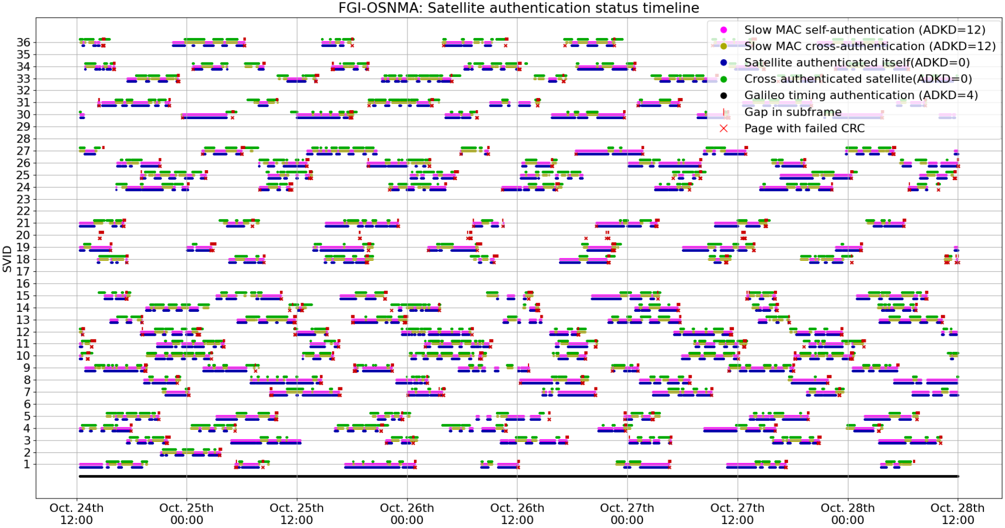
Experimental setup

- Data collection in static open sky condition during 24.10-28.10 in Espoo, Southern Finland
  - Approximately 95h of data
  - Represents best case scenario
- Septentrio Mosaic X5 receiver
  - The Galileo raw navigation bits can be obtained from this receiver, which enables OSNMA processing
- All of the processing has been done by our own OSNMA implementation, tentatively named FGI-OSNMA

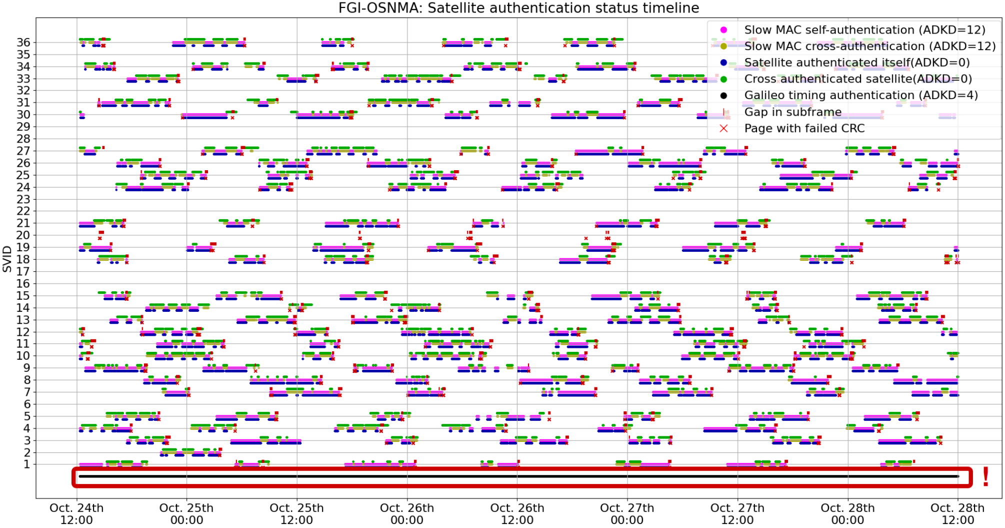
FGI-OSNMA

- Written in Python, made with special emphasis on modularity, and usability in real-time, and integrability as a library in third-party applications
- Validated with the so-called test vectors published by EUSPA, and by comparing the results to other available OSNMA implementation, such as OSNMAlib
- Will be made open-source in the near future

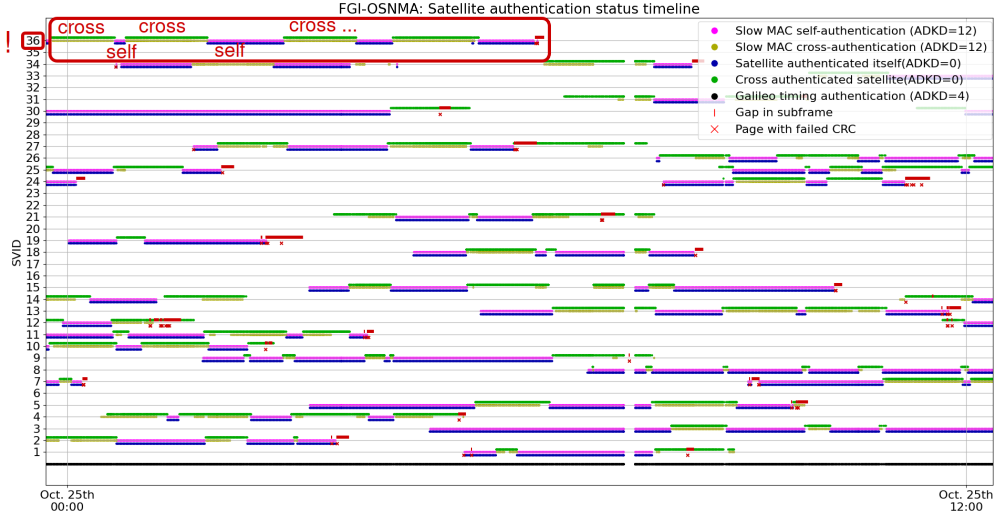
Results: authentication and data transmission events visualized



Galileo constellation timing data (ADKD=4) authentication



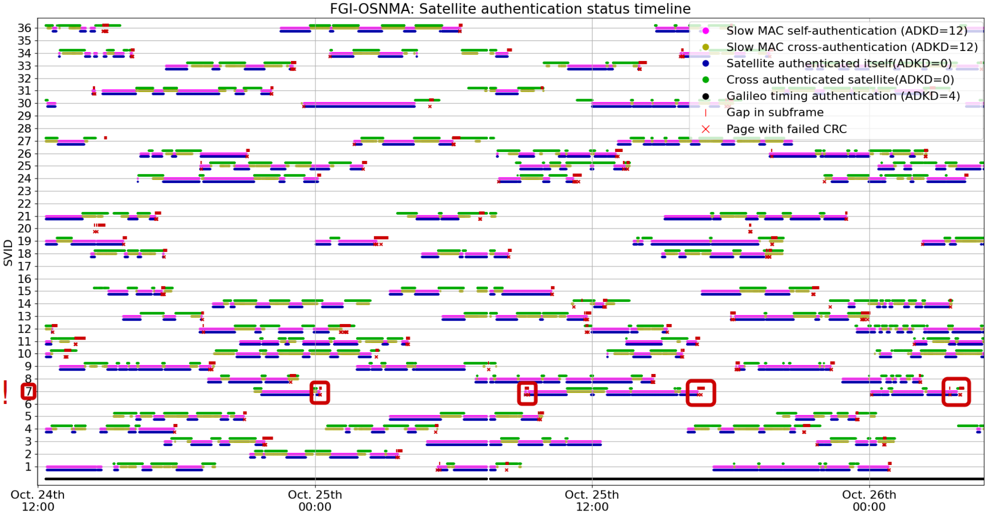
Alternation between self-authentication and cross-authentication


FGI-OSNMA: Satellite authentication status timeline

Satellite elevation and CRCs

- Satellite elevation is very visible in the timeline: when a satellite reaches low elevation, there will be data reception problems, and the receiver will receive pages with failed CRCs, and hence there will be gaps in the subframes
- Shortly after the data reception problems the satellite vanished below the horizon, hence it will no longer be authenticated or even visible
- Data reception problems from low elevation satellites is widely known, and similar behavior can be expected in any satellite application, this is not specific to OSNMA

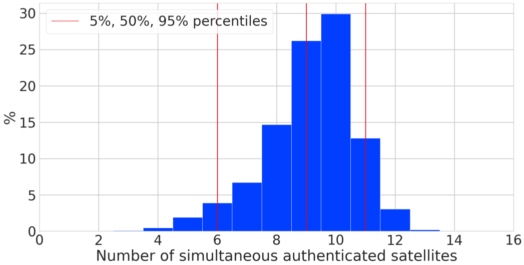
Satellite elevation and CRCs



FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

Statistics related to authentication

Statistic	Value
Simultaneous authenticated satellites: 5% percentile	6
Simultaneous authenticated satellites: average	9.14
Simultaneous authenticated satellites: 95% percentile	11
Percentage of authenticated fixes	99.74%
Self-authentications out of all ADKD=0 authentications	37.91%
Cross-authentications out of all ADKD=0 authentications	62.09%

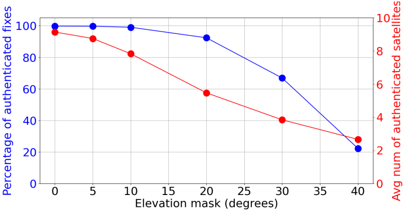


KPIs as a function of the elevation mask

- Previous results are excellent, but they represent the best case scenario (= static open sky)
- How does satellite visibility effect the results?
  - We apply an elevation mask to OSNMA processing: the OSNMA engine is run, but the data from satellites below the elevation mask is discarded
    - This approximates situations with limited satellite visibility. For example, buildings in urban areas block signals $\implies$ higher elevation mask

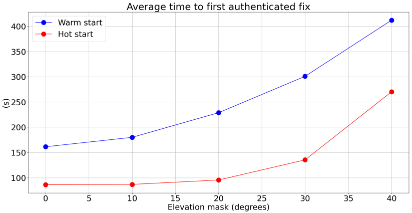
KPIs as a function of the elevation mask

Elevation mask	**Number of authenticated fixes**	**Authenticated sats. count Percentiles: 5%, 50%, 95%**
0°	99.74%	6, 9, 11
5°	99.66%	6, 9, 11
10°	99.0%	5, 8, 10
20°	92.33%	3, 6, 8
30°	66.83%	2, 4, 6
40°	22.24%	0, 3, 4



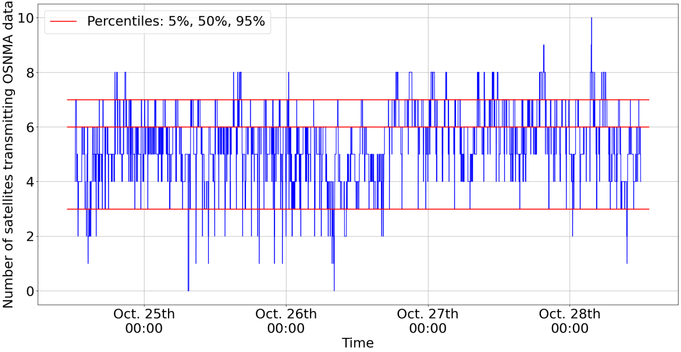
Time to first authenticated fix as a function of the elevation mask

Elevation mask	**Warm-start (Percentiles: 10%, 50%, 90%)**	**Hot-start (Percentiles: 10%, 50%, 90%)**
0°	104, 150, 232	74, 86, 98
10°	116, 166, 262	74, 86, 98
20°	136, 208, 338	74, 88, 116
30°	168, 262, 424	78, 102, 152
40°	200, 318, 570	86, 128, 454



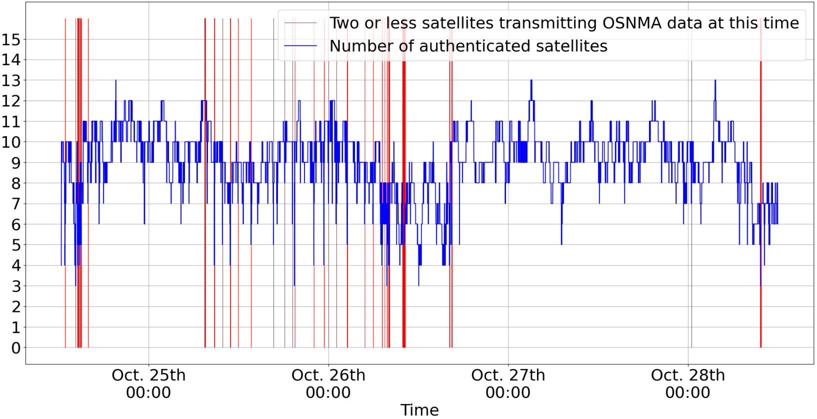
What happens in situations where we fail to get authenticated fixes?

- In our dataset the problem is that occasionally there are very few visible satellites transitting OSNMA data
  - Little to no OSNMA data $\Longrightarrow$ Very few tags $\Longrightarrow$ Very few authentications $\Longrightarrow$ Unable to get authenticated fix



Correlation of OSNMA data transmission and number of authentications

- Very few satellites transmitting OSNMA data (red lines) ⟹ Drop in the number of authenticated satellites (blue line)



Observations and conclusion

- OSNMA performance is good, satellite visibility can affect this greatly
- Only challenge during this test campaign was the occasional low number of satellites transmitting OSNMA data
  - OSNMA is still in its test phase: this can be improved in the future
- Cross-authentication has many benefits (redundancy, robustness)
  - Each satellite is responsible for authenticating multiple satellites $\Longrightarrow$ dropping one of these authenticating satellites (for example due to poor signal reception quality) can lower the amount of authenticated satellites significantly $\Longrightarrow$ this can be a difference between authenticated fix and a non-fix
    - This explains the elevation mask test results: elevation mask can make you drop satellites these authenticating satellites
    - It is common to apply an elevation mask when calculating positions, however, no mask should be applied to OSNMA data reception

Thank you for your interest!

- Questions?