# Final Presentation

NAVISP-EL1-060 / VALLE : NOVEL PRIVACY PRESERVING PNT PROCESSING TECHNIQUES

# Authors


Andra Sararu (GMV-RO)

Sepideh Rahimian (GMV-DE)

Inmaculada Perea (GMV-DE)

Daniel Hurtado (GMV-ES)

Javier Hernandez (GMV-ES)

Miguel Tejedor (GMV-DE)

Jie Chen (GMV-DE)

Max Herring (GMV-DE)

Raluca Prefac (GMV-RO)

Florin Mistrapau (GMV-RO)

Jedrzej Mosiezny (GMV-DE)

Alexandru Pandele (RISE)

Mihnea Ion (RISE)

Andrei Hulea (RISE)

Alexandru Budianu (ESA)

# Index


1. Project introduction
2. Use cases trade-off and selection
3. Demonstrator design and implementation
4. Performance and red team analysis
5. Conclusions and future work
6. Final Questions & comments

# Project Introduction

# VALLE Team

**Prime Contractor**

Project Management
Lead Privacy Enhancement Activities

**Subcontractors**

Lead Navigation Activities

Lead Red Team Analysis

# Scope and Objectives

- **The main objectives of VALLE:**

  - Identify, define, and consolidate a set of use cases for privacy-preserving positioning solutions or services based on sharing and processing user PNT data.

  - Define and develop multiple privacy-preserving PNT processing concepts based on the sharing and processing of different types of user PNT data.

  - Design and implement a concept demonstrator to verify and validate the proposed concepts.

# Use Cases Trade-Off and Selection

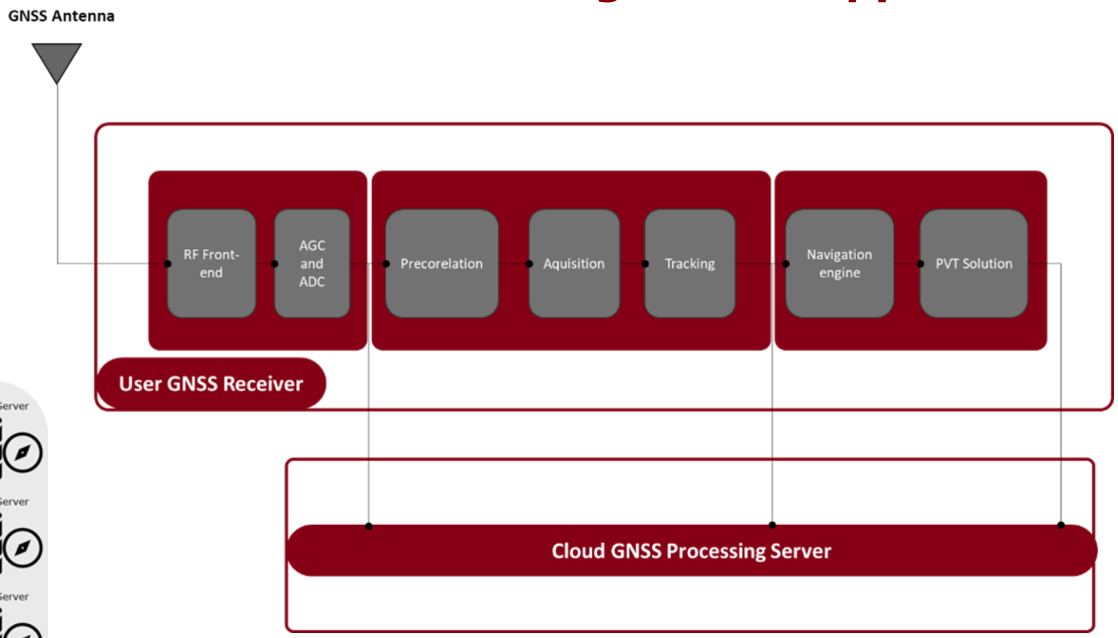
# Privacy vs functionality

- Working with data imposes a trade-off between service functionality and data privacy. Privacy may need to be sacrificed to enable certain features and vice versa.

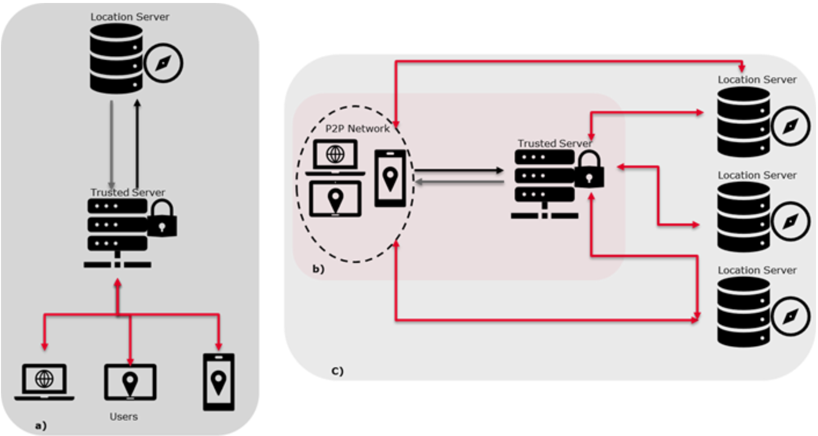

- Novel privacy enhancement techniques, such as the ones proposed in VALLE, promise to overcome this trade-off by allowing calculations without disclosing private data.

# System Architectures

## Cloud GNSS Processing Server Approach




## LBS Architectures



# Privacy Enhancement Techniques Selection

- Federated Learning
- Differential Privacy
- Secure Multi Party Computation
- Anonymization
- Homomorphic Encryption
- Zero-Knowledge Proof
- Trusted Environment Execution

# Use Cases Final Selection

| | # | Use case | Relevance | Complexity (PNT) | Complexity (PET) | Aggregate Score | Data type | PET Technique |
|---|---|---|---|---|---|---|---|---|
| ✓ | 1 | Secure collaborative positioning (Anonymisation) | High (3) | Low (3) | Low (3) | High (3.0) | Observables | Anonymisation |
| ✓ | 2 | Crowd management applications | High (3) | Low (3) | Medium (2) | High (2.75) | PVT | SMPC |
| | 3 | Tracking applications for children | Medium (2) | Low (3) | Low (3) | High (2.5) | PVT | Plain Encryption |
| ✓ | 4 | Cloud processing of data for correlation | High (3) | Medium (2) | High (1) | High (2.25) | IQ Samples | Partial HE |
| | 5 | Location for Regulatory applications (digital tachograph or road tolling) | High (3) | Medium (2) | High (1) | High (2.25) | Observables/ PVT | ZKP, SMPC or HE |
| | 6 | Geo-fencing | High (3) | Medium (2) | High (1) | High (2.25) | PVT | FHE |
| | 7 | Secure collaborative positioning (FHE) | High (3) | Medium (2) | High (1) | High (2.25) | Observables | FHE |

## Relevance Scoring

| 1 | 2 | 3 |
|---|---|---|
| Low (1) | Medium (2) | High (3) |

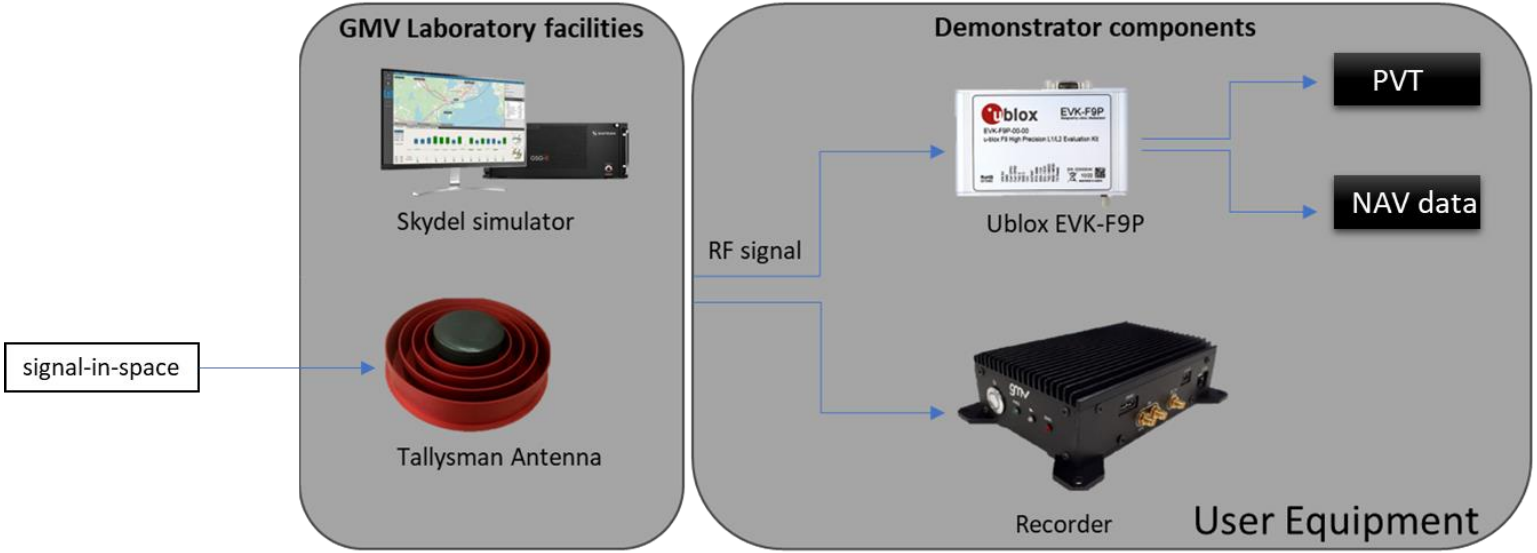
## Complexity Scoring

| 1 | 2 | 3 |
|---|---|---|
| High (1) | Medium (2) | Low (3) |

***Final score = ((Relevance) + ((Complexity PNT + Complexity PET) / 2)) / 2***

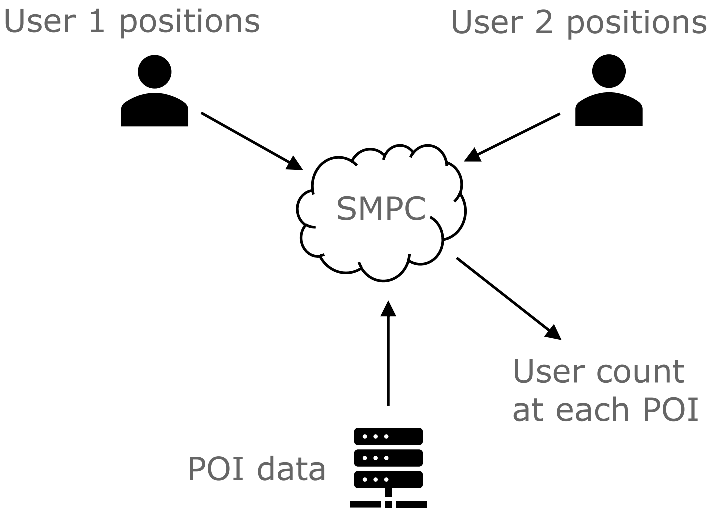
# Demonstrator Design and Implementation

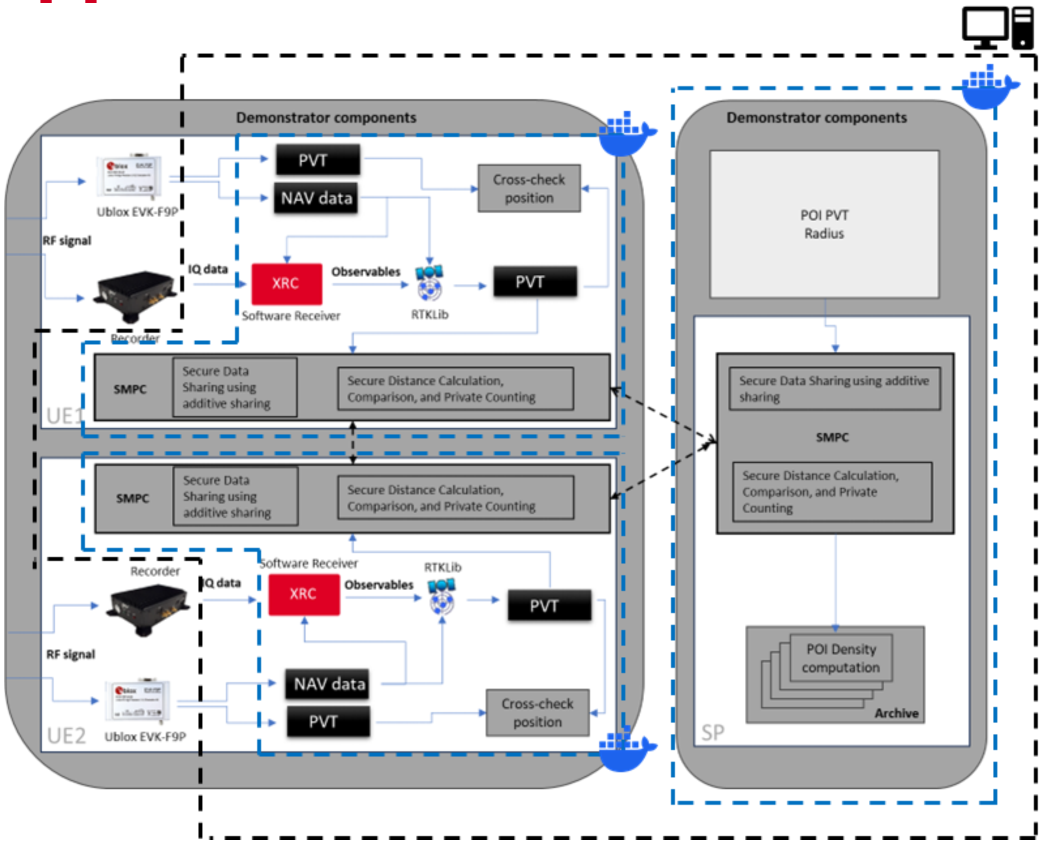
# Common workflow between use cases



# Crowd management applications

**SMPC - Secure Multi Party Computation**

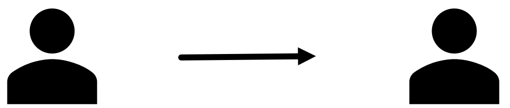


# Secure collaborative positioning

**Anonymization**
Remove or modify identifying data

**UE 1** **UE 2**

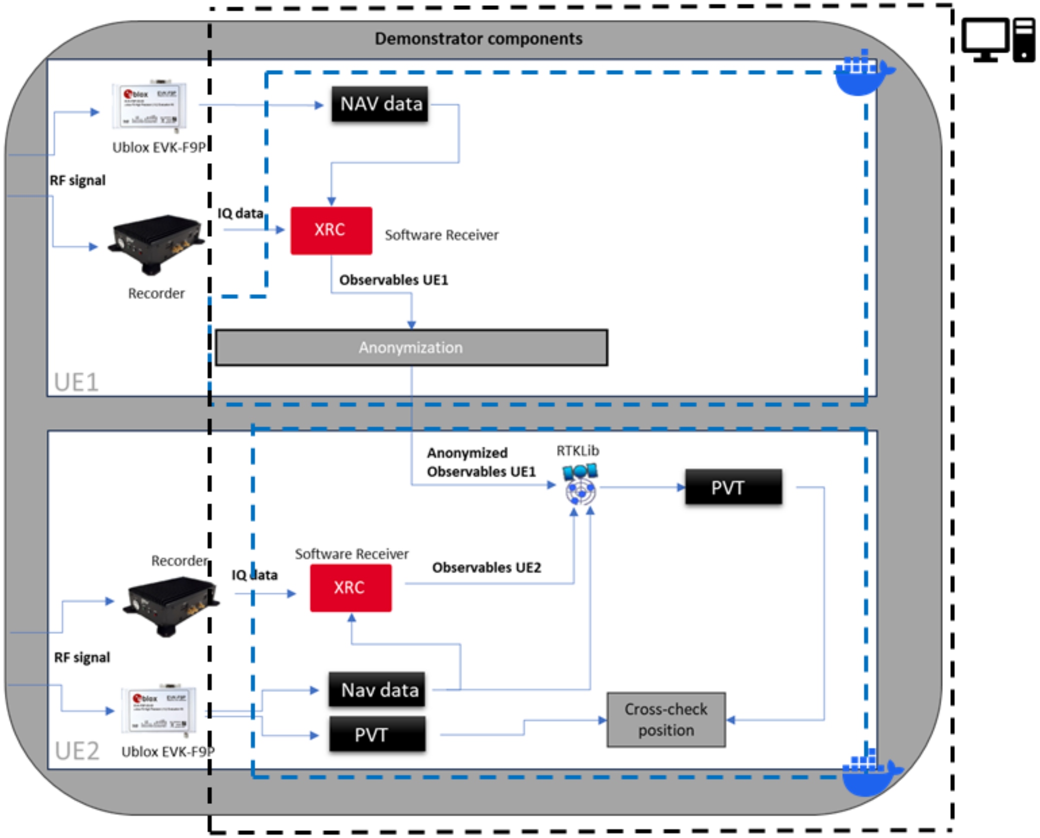


Dani
(X,Y,Z)

####
(X,Y,Z)

Anonymize headers

Improve positioning accuracy



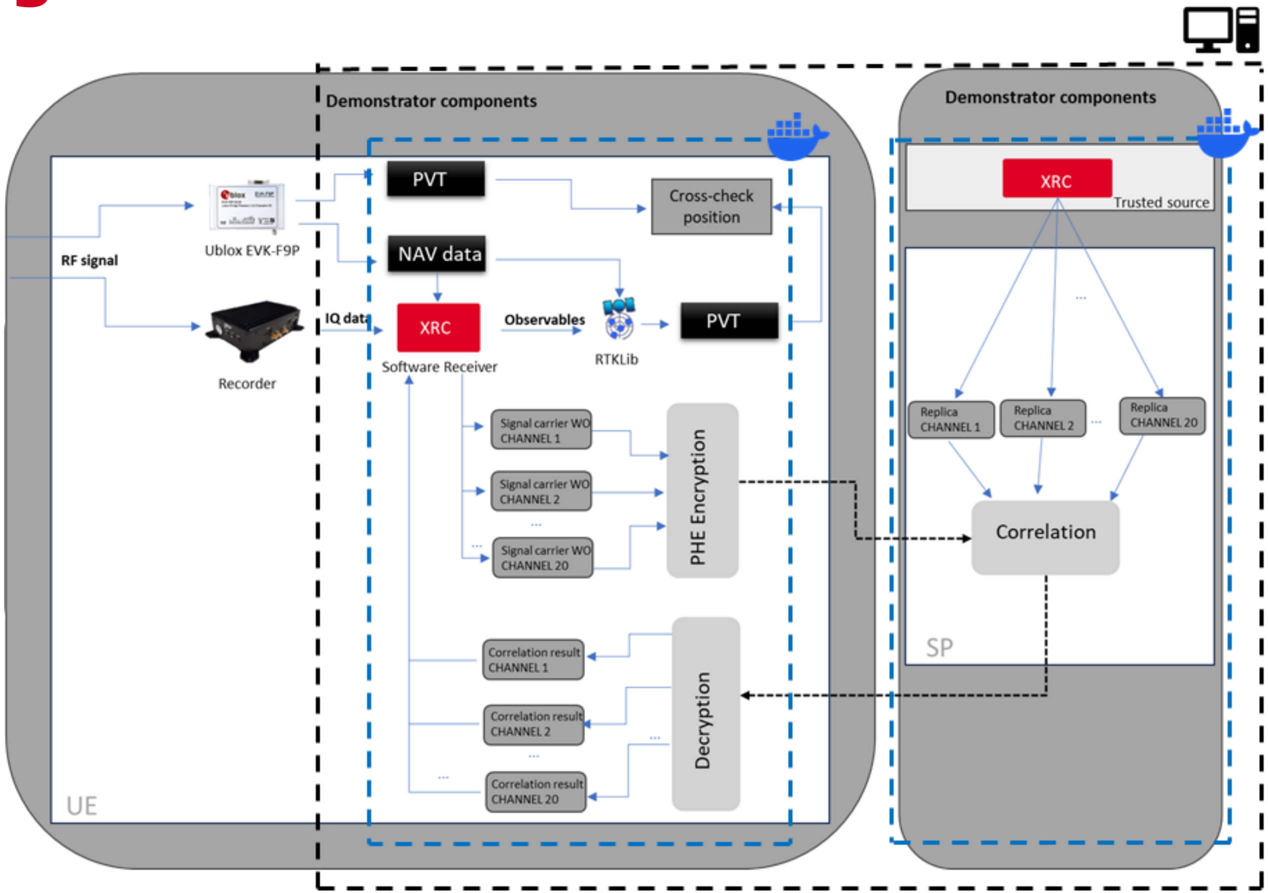
# Cloud processing of data for correlation

**Partial Homomorphic Encryption**
enc(a) ⊕ enc(b) = enc(a + b)

**UE** Encrypt IQ data

**SP** Correlate encrypted samples and plaintext replica

**UE** Decrypt correlation result



# Performance and Red Team Analysis

# Computational Performance Analysis

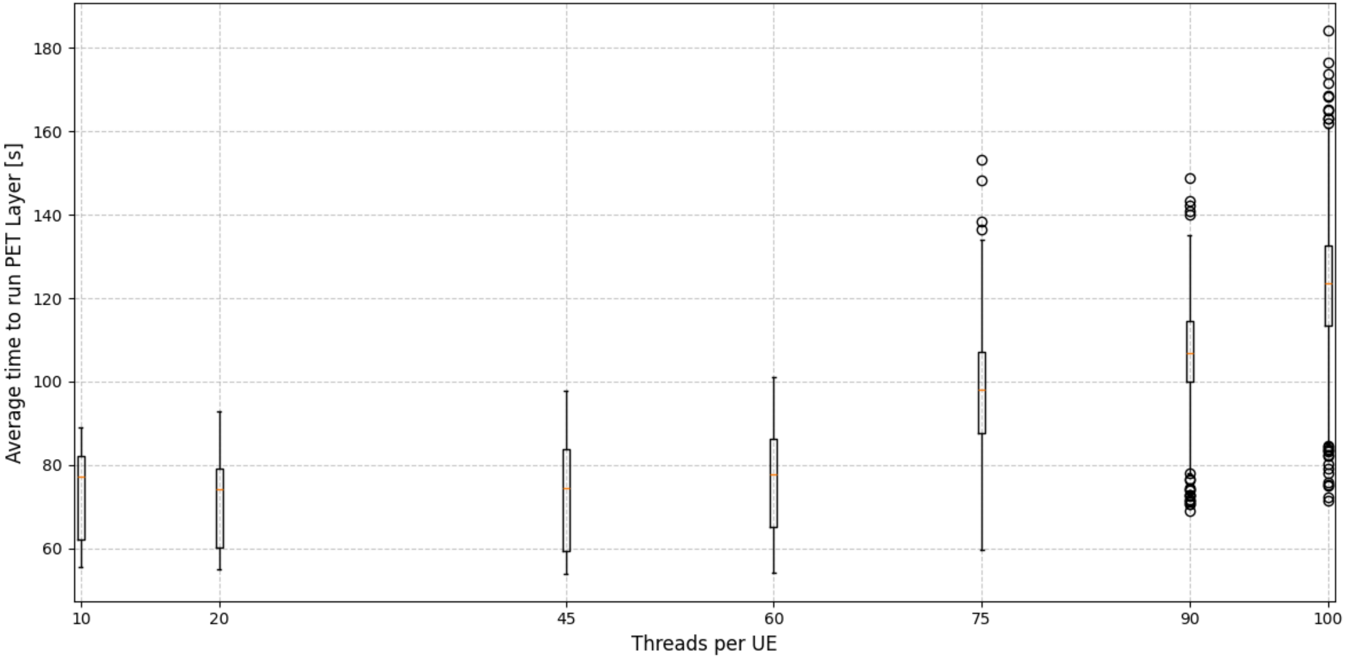
## How it was measured

- Measured on UC2: Cloud processing of data for correlation
- Used Default dataset
- Processing of 1 minute (from 10 minutes recorded)
- Performance was measured by multiple runs with different CPU Threads per UE
- Performance was measured with two batches:
  - First batch of runs was performed with PET layer
  - Second batch of tests was performed with GNSS and PET layer

| Parameter | Value |
| --- | --- |
| **Signal duration** | 10 minutes |
| **Type of signal** | synthetic |
| **Sampling frequency** | 12.5 Msps |
| **Quantization** | 8 |
| **Number of UEs** | 2 |
| **Number of SP** | 1 |
| **Constellations** | GPS and Galileo |
| **Signals** | L1C/A and E1B/C |
| **SV Tracked** | 14 |

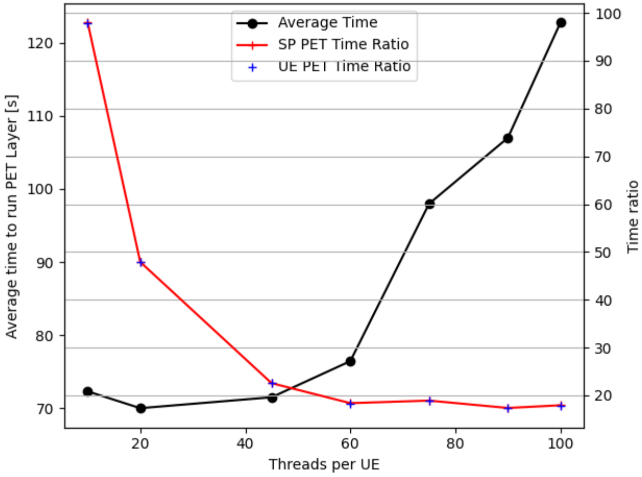
# Computational Performance - PET only

## Batch one: time to process 1s of signal on a single thread vs number of threads



# Computational Performance - PET only

## Time to process 1s of signal on a single thread and dime processing ratio vs number of threads




| Threads | Resident Memory [kB] | Elapsed time (hh:mm:ss) | Time ratio | Average time to run PET Layer [s] |
|---|---|---|---|---|
| 10 | 1341540 | 01:37:54 | 97.90 | 72.31 |
| 20 | 1139720 | 47:51.5 | 47.85 | 70.02 |
| 45 | 1214744 | 22:30.6 | 22.50 | 75.51 |
| 60 | 1246272 | 18:19.4 | 18.32 | 76.45 |
| 75 | 1537508 | 18:51.6 | 18.85 | 97.98 |
| 90 | 1311200 | 17:19.3 | 17.32 | 106.99 |
| 100 | 1339080 | 17:53.1 | 17.88 | 122.73 |

# Computational Performance - PNT and PET layers

SP | UE

PET

SP:

| Threads | Resident Memory [kB] | Elapsed time (mm:ss) | Time ratio |
|---|---|---|---|
| 90 | 510716 | 18:43.4 | 18,72 |
| 92 | 532776 | 17:24.3 | 17,41 |
| 94 | 497904 | 17:52.7 | 17,88 |
| 95 | 522220 | 17:14.0 | 17,23 |

UE:

| Threads | Resident Memory [kB] | Elapsed time (mm:ss) | Time ratio |
|---|---|---|---|
| 90 | 1391028 | 18:36.55 | 18,60 |
| 92 | 1363288 | 17:18.66 | 17,31 |
| 94 | 1449124 | 17:47.91 | 17,79 |
| 95 | 1321600 | 17:07.53 | 17,12 |

PNT

SP:

| Threads | Resident Memory [kB] | Elapsed time (mm:ss) | Time ratio |
|---|---|---|---|
| 90 | 1005776 | 12:59.5 | 12,99 |
| 92 | 1059660 | 12:38.0 | 12,63 |
| 94 | 985588 | 12:09.2 | 12,15 |
| 95 | 1004032 | 12:11.2 | 12,18 |

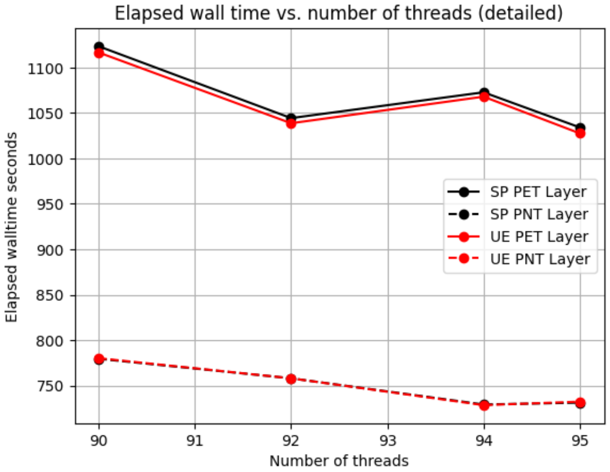
**29,41**

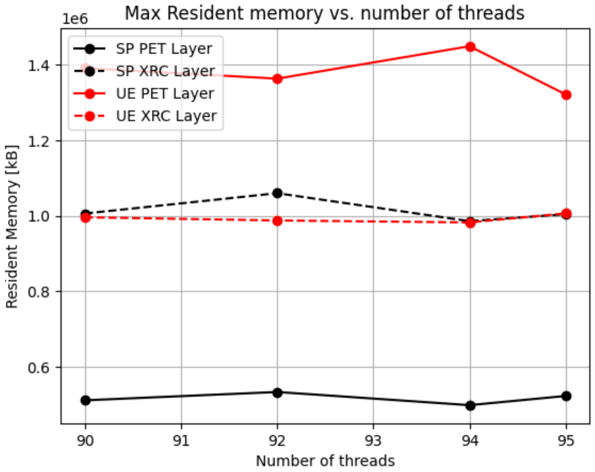
UE:

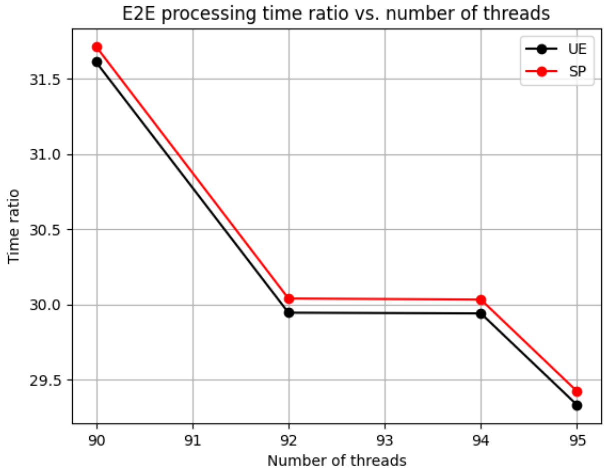
| Threads | Resident Memory [kB] | Elapsed time (mm:ss) | Time ratio |
|---|---|---|---|
| 90 | 995796 | 13:00.1 | 13,00 |
| 92 | 987412 | 12:38.0 | 12,63 |
| 94 | 982192 | 12:08.5 | 12,14 |
| 95 | 1006164 | 12:12.3 | 12,20 |

**29,32**

# Computational Performance PNT and PET layers

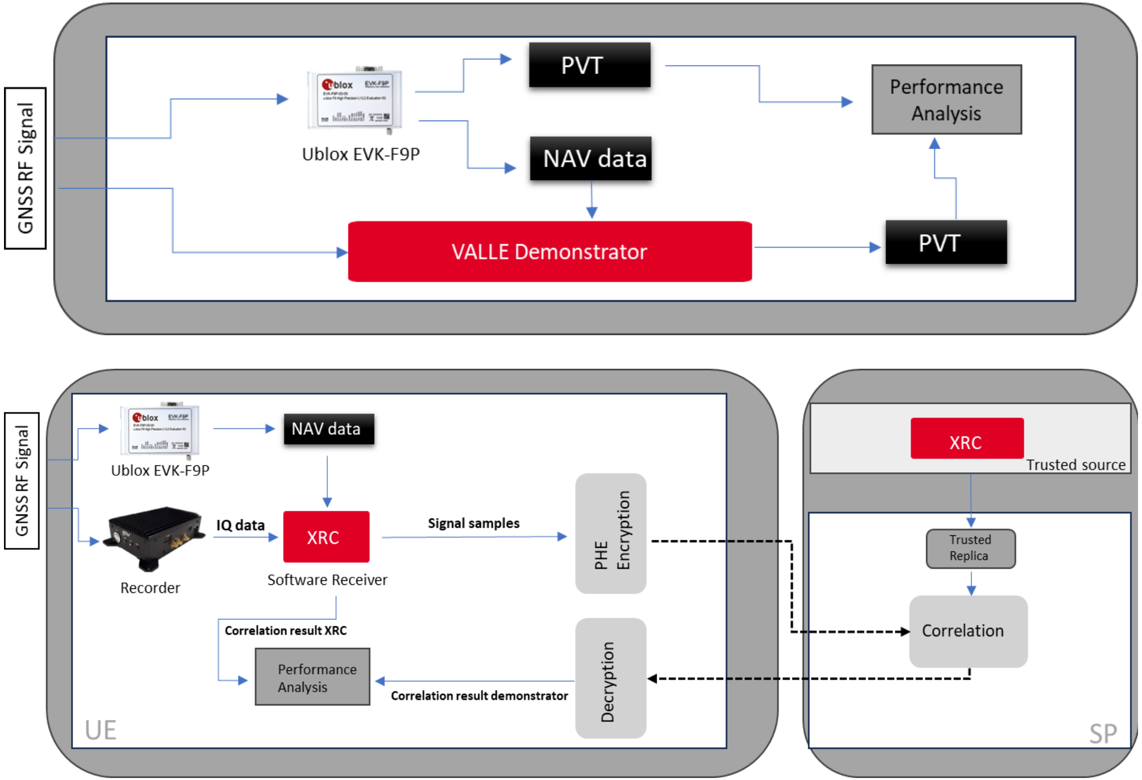


# Navigation Performance Analysis

## PVT and Correlation performance analysis workflow

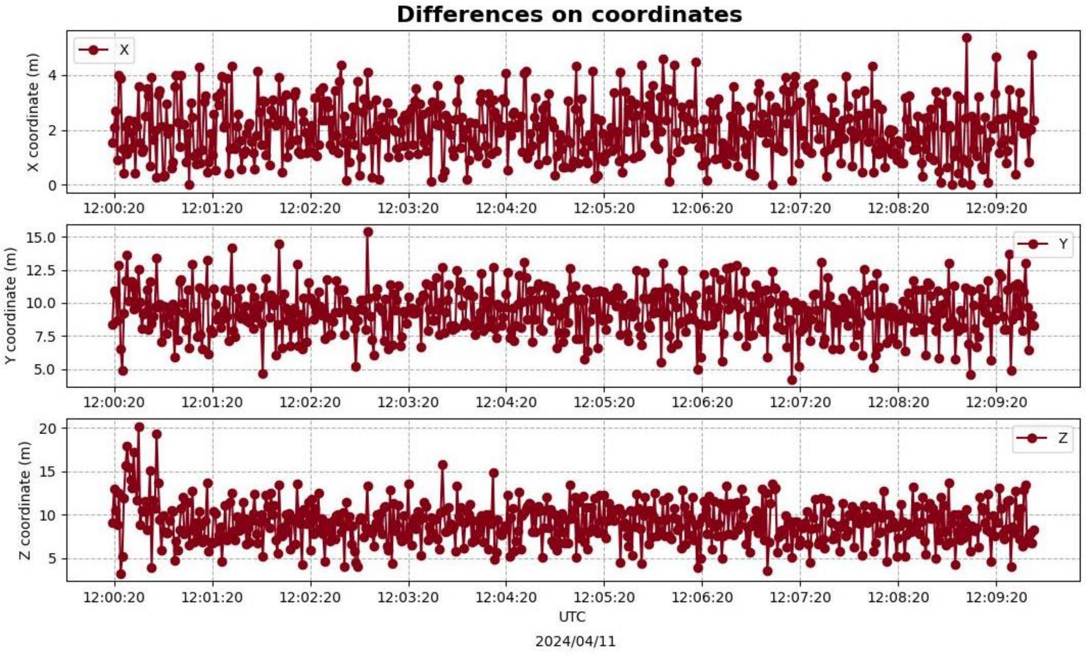



## Performance analysis datasets

| Dataset | Source | Duration | Signal | Users | Config |
|---|---|---|---|---|---|
| DS-1 | Simulator | 300 s | GPS L1C/A, Galileo E1BC | 5 | 12.5 Msps, 8 bits, 1 channel |
| DS-2 | Simulator | 600 s | | 5 | |
| DS-3 | SiS | 300 s | | 2 | |

# Navigation Performance Analysis

## Crowd Management Applications Navigation Performance Analysis



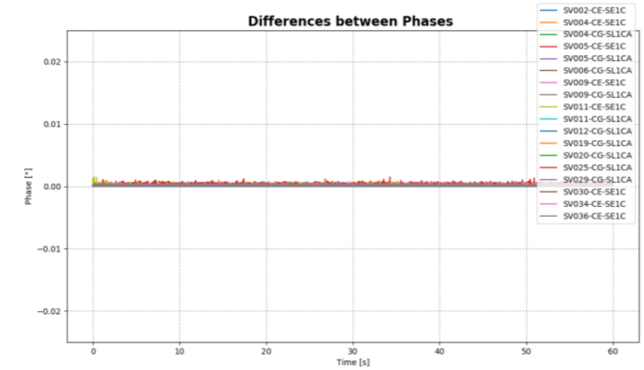

**Coordinates differences for UE5 (Dataset 2)**

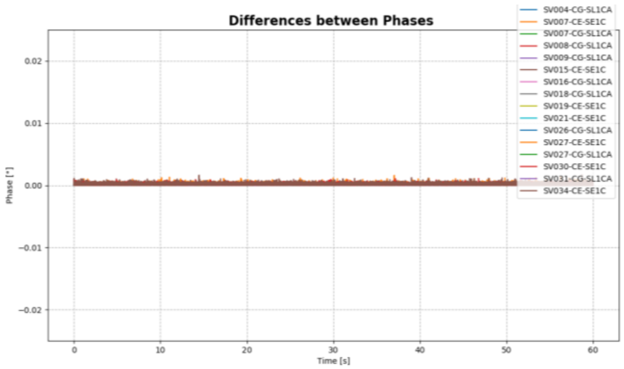
| | Pos. error (m) | X error (m) | Y error (m) | Z error (m) |
|---|---|---|---|---|
| **Mean** | 13.664 | 1.843 | 9.439 | 9.558 |
| **Min** | 5.974 | 0.002 | 3.980 | 2.979 |
| **Max** | 22.639 | 5.208 | 15.105 | 17.763 |
| **STD** | 2.638 | 0.998 | 1.772 | 2.318 |

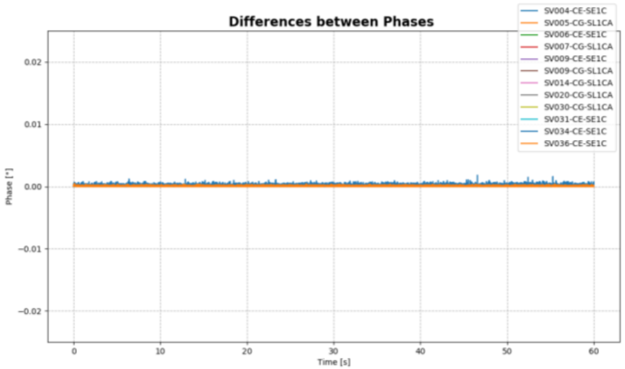
**Statistics of all 5 users**

# Navigation Performance Analysis

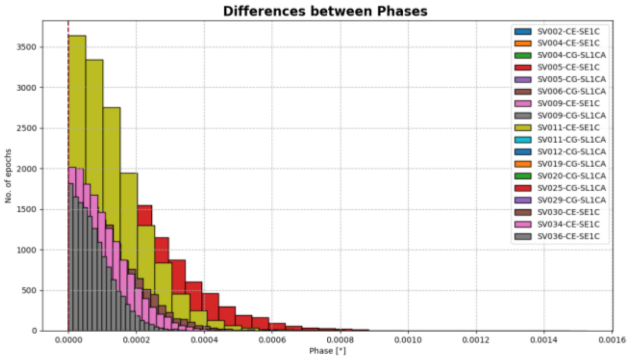
## Cloud Processing of Data for Correlation Navigation Performance Analysis

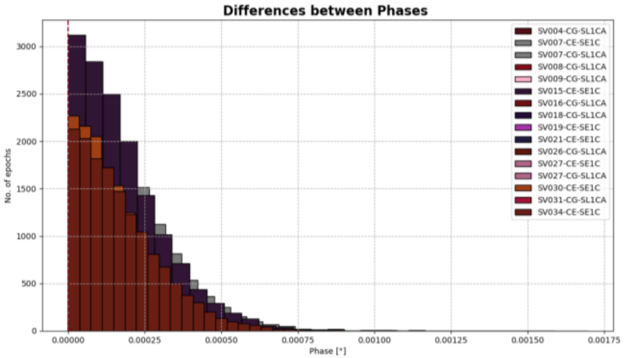


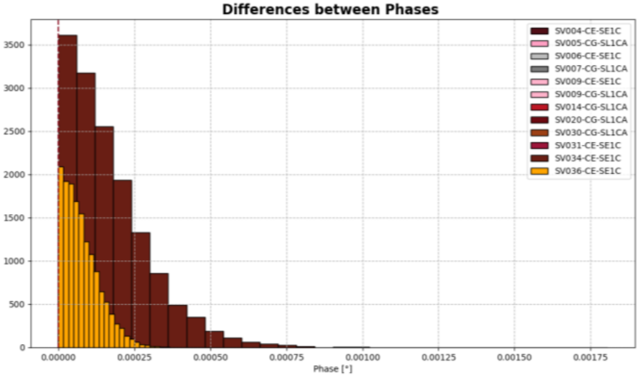




**Dataset 1** **Dataset 2** **Dataset 3**

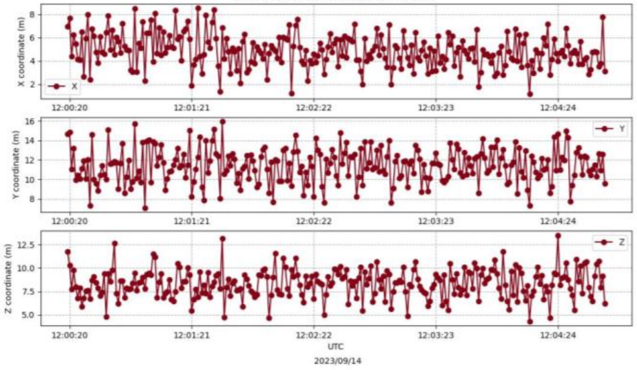


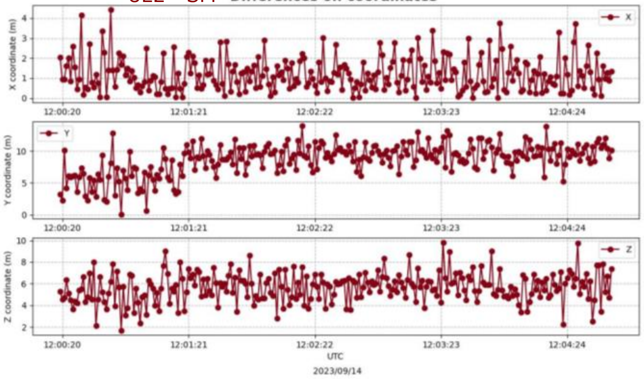



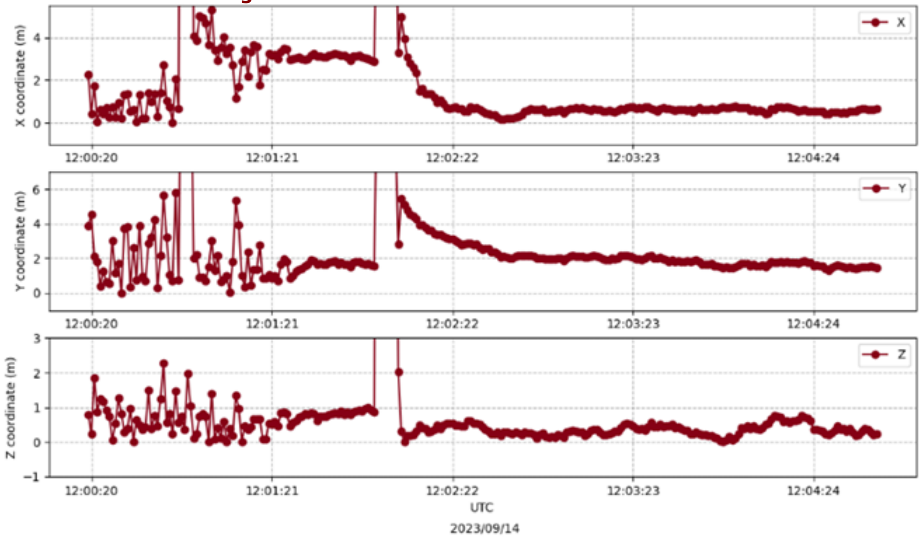



# Navigation Performance Analysis

## Secure Collaborative Positioning Navigation Performance Analysis



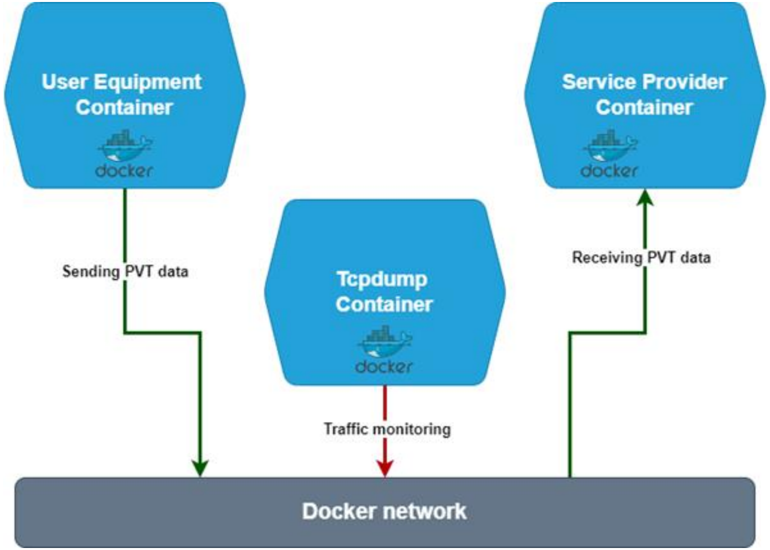




| | Pos. error (m) | X error (m) | Y error (m) | Z error (m) |
|---|---|---|---|---|
| **Mean** | 3.793 | 2.161 | 2.457 | 0.896 |
| **Min** | 0.622 | 0.016 | 0.016 | 0.005 |
| **Max** | 41.574 | 37.762 | 17.793 | 16.156 |
| **STD** | 5.596 | 4.735 | 2.389 | 2.463 |

**UE2 statistics (Moving Base)**

# Red team analysis

## Methodology



# Red team analysis

## Outcomes and Conclusion

**Protocols types:** The captured traffic contains only three protocol types: ICMPv6, mDNS, and ARP. These are commonly used for address and hostname resolution at different layers of the network stack.

**Traffic patterns:** The captured network traffic looks simillarly in all the three scenarios

**Outcomes:** The timeline of the captured packets displays noticeable gaps between them. During the analyzed timeframe the hacking container was in the same docker network with the target containers. The red team analysis analyzed the captured traffic and network protocols used by the Docker containers.

**No vulnerabilities were identified in the captured traffic.**

# Conclusions and Future Work

# Project Conclusions

## Project Achievements

- ✓ Identified, defined and consolidated a set of use cases for privacy-preserving positioning solutions and/or services based on sharing and processing user PNT data (e.g., intermediate frequency IF or baseband samples, observables, and navigation data, PNT products/trajectory information, etc.).
- ✓ Defined and developed three privacy preserving PNT processing concepts based on the sharing and processing of different types of user PNT data (e.g. IF or baseband samples, observables and navigation data, PNT products/trajectory information, etc.), and assessed the security of the proposed PNT processing concepts.
- ✓ Designed and developed a flexible concept demonstrator
- ✓ Verified and validated the proposed privacy-preserving PNT processing concepts, and benchmarked (processing time and resource usage, latency, robustness) the proposed concepts against standardized solutions

# Project Conclusions

## Use Cases Achievements

1. The project showed that use of secure multiparty computation for computation of user density is achievable and computationally feasible on a personal computer. The implemented computational algorithm allows for relatively fast securing of users position and sharing the secured data with the service provider for location based services (LBS).
2. The project showed that use of Partially Homomorphic encryption for encryption of IQ samples and performing correlation of IQ samples in the encrypted domain is feasible, computationally achievable on a single server class computer. The conducted study opened the further investigation of improving the existing algorithms to perform the correlation activities in the encrypted space
3. The project showed that use of anonymization techniques over GNSS observables enables a private collaborative positioning solution providing high accuracy PVT solutions.

# Future Work

## Potential Non-Space Applications

1. Potential non-space applications include implementation of the secure multiparty computation for novel products including crowd management applications, contact tracking, measuring of time specific crowd density in urban and rural areas, IoT and smart city features, etc.
2. Potential non-space applications of correlation of encrypted IQ samples include novel technology allowing secure correlation of GNSS signals without disclosing sensitive user data, measurements etc.
3. Potential non-space applications of anonymization techniques over GNSS observables enable the development of a distributed system performing private collaborative positioning computation based on privately shared observations and providing high accuracy PVT solutions.

The results of VALLE are promising and GMV is interested to pursue the topic of privacy preserving PNT processing concepts.

Work on evolving the Technology Readiness Level is considered and continuation options are being investigated internally in GMV.

# Working with ESA

- The development of VALLE was possible thanks to the support provided by ESA and the NAVISP Element 1 programme.
- ESA has provided valuable technical review and guidance at all stages of the project.
- ESA provides access to cutting-edge technology and expertise being at the forefront of GNSS research.
- Privacy Protection for PNT applications and VALLE technology gain increased visibility through the ESA NAVISP mechanisms.

# Q & A

# Thank you

Jedrzej Mosiezny
jmosiezny@gmv.com