# PARTICLE

## «Pvt Assurance foR aTomIc management using CeLlular nEtworks»

Final Presentation
16 March 2026

© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# Copyright of final presentation

The copyright in this document is vested in QASCOM / LOCTIO / UNIVERSITY OF PATRAS.

This document may only be reproduced in whole or in part, or stored in a retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying or otherwise, either with the prior permission of QASCOM / LOCTIO / UNIVERSITY OF PATRAS or in accordance with the terms of ESA Contract No. **4000145518/24/NL/AK**.



© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# Final Presentation

- Objectives
- Use Cases
- Threat Analysis
- Testbed
- GNSS User Terminal Emulator
- 5G User Terminal Emulator
- Validation Results
- Way forward


© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# 1.

## Objectives

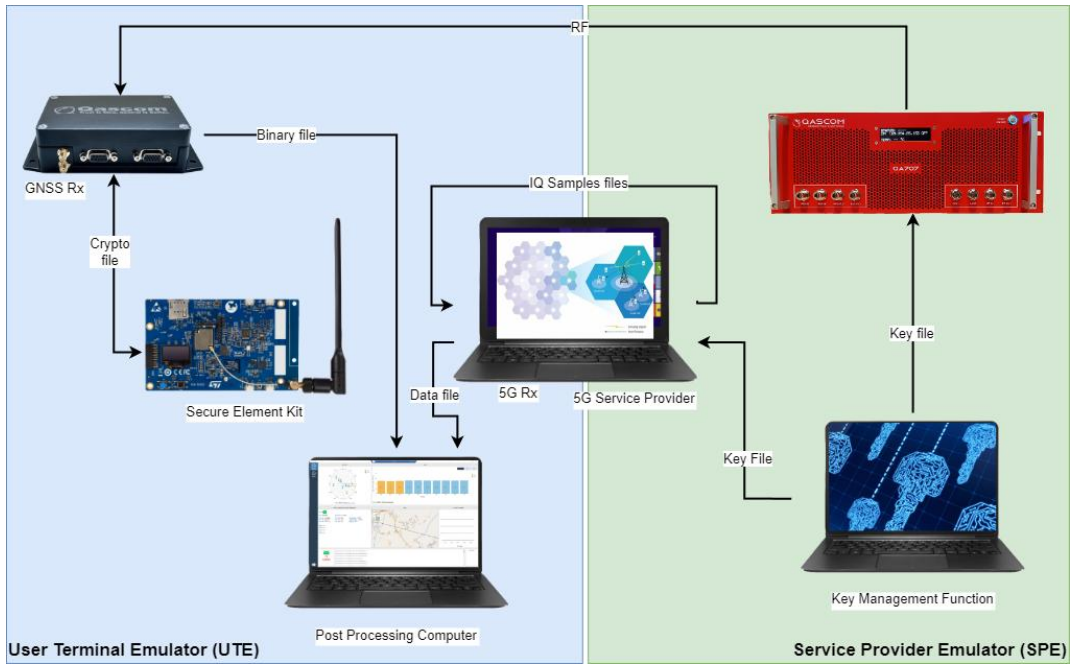
# Objectives and Solutions

## Objectives

- **Evolve PNT technology** to support the following User Needs:
  - Delivery of **Assured Position, Navigation and Time (PNT) information** & **guarantee of the authenticity** of received signals
  - Resilient User Terminal with the capability to estimate Position / Time information with GNSS and/or 5G
  - **Secure User Terminal architecture** to ensure the integrity and security of the information stored

## Solution

- Integration in Qascom GNSS receiver of **Galileo OSNMA (Data Authentication)** and **Galileo E6 SAS (Range Authentication)** in addition to Receiver-Based robustness
- Development of a Testbed to Demonstrate **GNSS/5G** positioning
- **Integration of a Secure Chip** in the receiver for the storage of cryptographic material





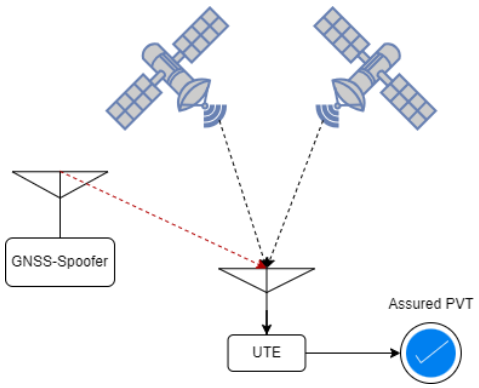

© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# 2.

## Use Cases

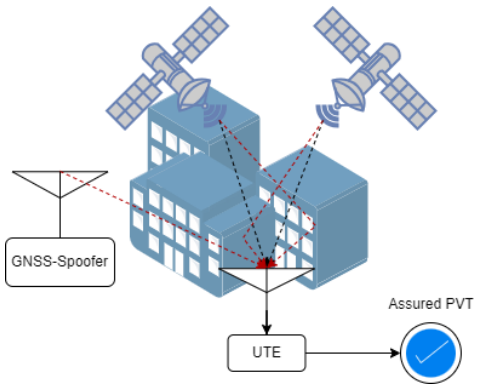
# Use Cases

### Confirmation of an initial location



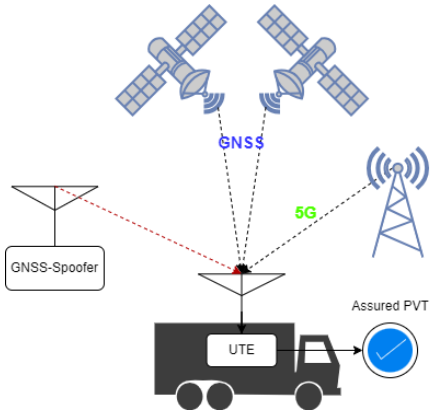

Techniques: 1,2,3

### Geolocation for outdoor survey



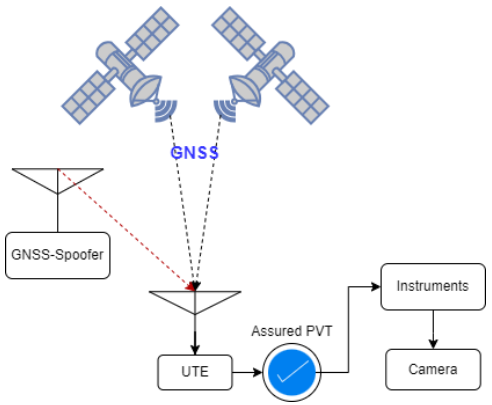

Techniques: 1,2,3

### Geolocation for and transport monitoring




Techniques: 1,2,3,4

### Authentication of outdoor data




Techniques: 1,2,3

1. **E6-XCK**: Provides information on signal coherence between E1 and E6 frequencies. If the E6 signal is not acquired or the acquisition results surpass the alarm threshold, the system raises a spoofing flag.

2. **OSNMA**: Ensures data authentication for the E1 frequency. If an advanced attack is performed, compromising OSNMA, the E6-XCK prevents the measurements from being used in the navigation solution and alerts the user.

3. **Anti-Spoofing**: Power and measurement level checks are performed to raise alerts. Power checks monitor C/N0 values, if an alarm threshold is exceeded, spoofing is declared present. Similarly, measurement consistency is monitored in time, with anomalous signals flagged as spoofed.

4. **5G**: Provides an additional layer of security and redundance from GNSS. It provides an additional navigation solution.


© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

QASCOM
AEROSPACE & DEFENCE

# 3.

## Threat Analysis

# Risk Management and Threat Analysis

- **ISO/IEC 27005** risk management process has been followed

- Risk evaluation criteria are essential for systematically identifying, assessing, and managing risks within an organization or project:
  - **Impact Criteria** determine the potential consequences
  - **Likelihood Criteria** define the probability of risks occurring
  - **Level of Risk Criteria** integrate impact and likelihood assessments
  - **Risk Acceptance** Criteria define the thresholds and conditions under which risks are considered acceptable

| Impact | Score | Description |
|---|---|---|
| Catastrophic | 5 | The effect is irrecoverable, leading to the termination of the mission. |
| Damaging | 4 | Recovery requires substantial investment and resources, significantly affecting business, legal standing, and reputation. |
| Significant | 3 | Recovery requires notable but manageable investment, impacting business, legal standing, and reputation. |
| Moderate | 2 | Recovery requires an unpleasant but manageable investment, with limited impact on operations and reputation. |
| Low | 1 | Negligible impact, with minimal investment needed for recovery. |

| Likelihood | Score | Description |
|---|---|---|
| Very Likely | 5 | Almost certain to occur |
| Likely | 4 | Highly probable to occur |
| Possible | 3 | Moderately probable to occur |
| Unlikely | 2 | Low probability of occurring |
| Remote | 1 | Very low probability of occurring. |

| IMPACT \ LIKELIHOOD | Remote | Unlikely | Possible | Likely | Very Likely |
|---|---|---|---|---|---|
| Catastrophic | Medium | High | Very High | Very High | Very High |
| Damaging | Low | Medium | High | High | Very High |
| Significant | Low | Low | Medium | High | High |
| Moderate | Very Low | Low | Low | Medium | High |
| Low | Very Low | Very Low | Low | Low | Medium |

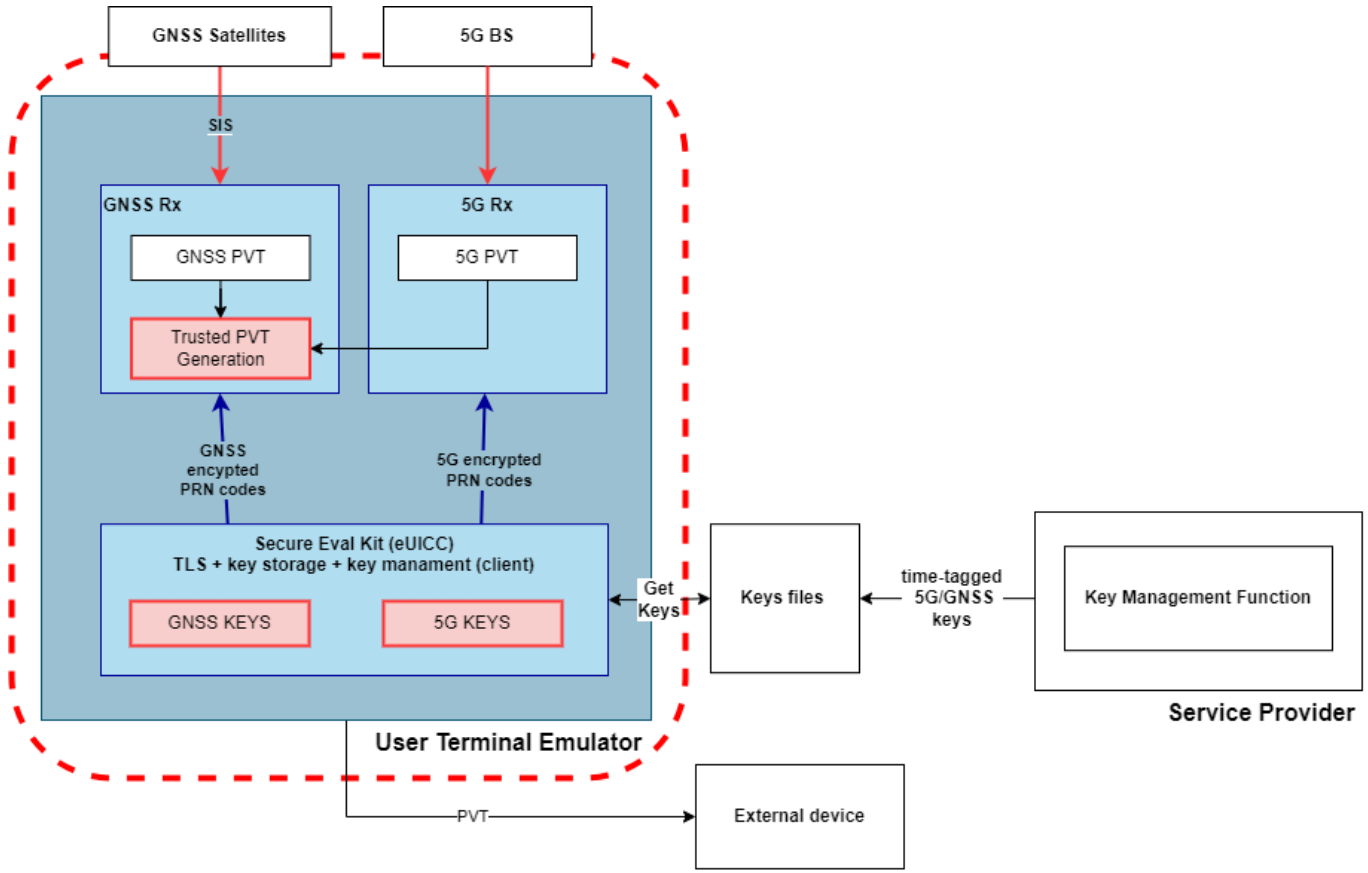
| Risk level | Accepted | Description |
|---|---|---|
| Very High | No | Requires immediate priority and significant management attention. |
| High | No | Requires priority and management attention. |
| Medium | No | May require additional management attention and mitigation measures. |
| Low | Yes | Generally acceptable but may require further analysis and minor mitigation. |
| Very Low | Yes | Considered acceptable with no further action needed. |


© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# Security perimeter delineation and assumptions

- **Identification of the security perimeter**
  - Input signals
  - Trusted PVT Generation
  - GNSS Keys
  - 5G Keys

- **Security assumptions**
  - System output is considered secure
  - Keys are securely transferred from the service provider





© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# Threat Analysis Output

- Threat Analysis output
  - Systematically analysed each identified threat in terms of impact, likelihood, and overall risk level
  - All risk magnitudes fall within medium to very high values and therefore require mitigating

| Secondary Asset | Threat | Threat impact (1-5) | Threat likelihood (1-5) | Likelihood justification | Risk magnitude |
|---|---|---|---|---|---|
| User Terminal Emulator | Sophisticated Spoofing | 5 | 3 | The attack is harder to execute, but its cost are affordable and the probability of detecting the attack is low | High |
| User Terminal Emulator | Meaconing | 5 | 4 | Meaconing is one of the simplest and cheapest means to perform deception of service | Very High |
| User Terminal Emulator | Replay Attacks | 4 | 3 | The attack is quite complex to execute, yet the attacker may have strong motivation to proceed. | Medium |
| User Terminal Emulator | Jamming | 5 | 4 | This attack is likely due to its minimal cost, ease of execution, accessibility of required hardware, and strong potential for success. | Very High |
| User Terminal Emulator | SCER Attacks | 5 | 1 | SCER attacks are very hard to perform, they require synchronization with the authentic signal, increased antenna gain and more signal processing | Medium |
| User Terminal Emulator | Exploit code vulnerabilities | 5 | 2 | Code vulnerabilities are hard to discover, and continuous software updates prevent possible exploits | Medium |


© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# 4.

## Testbed

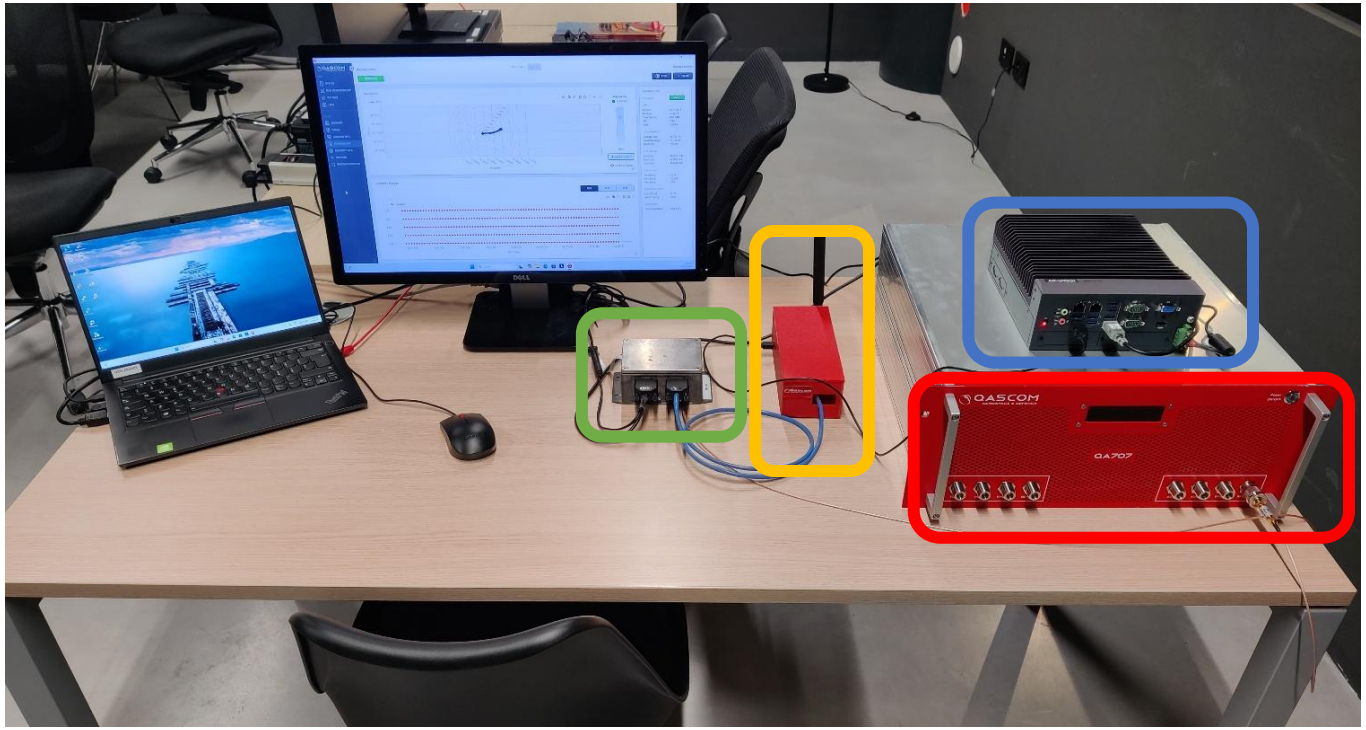
# Testbed

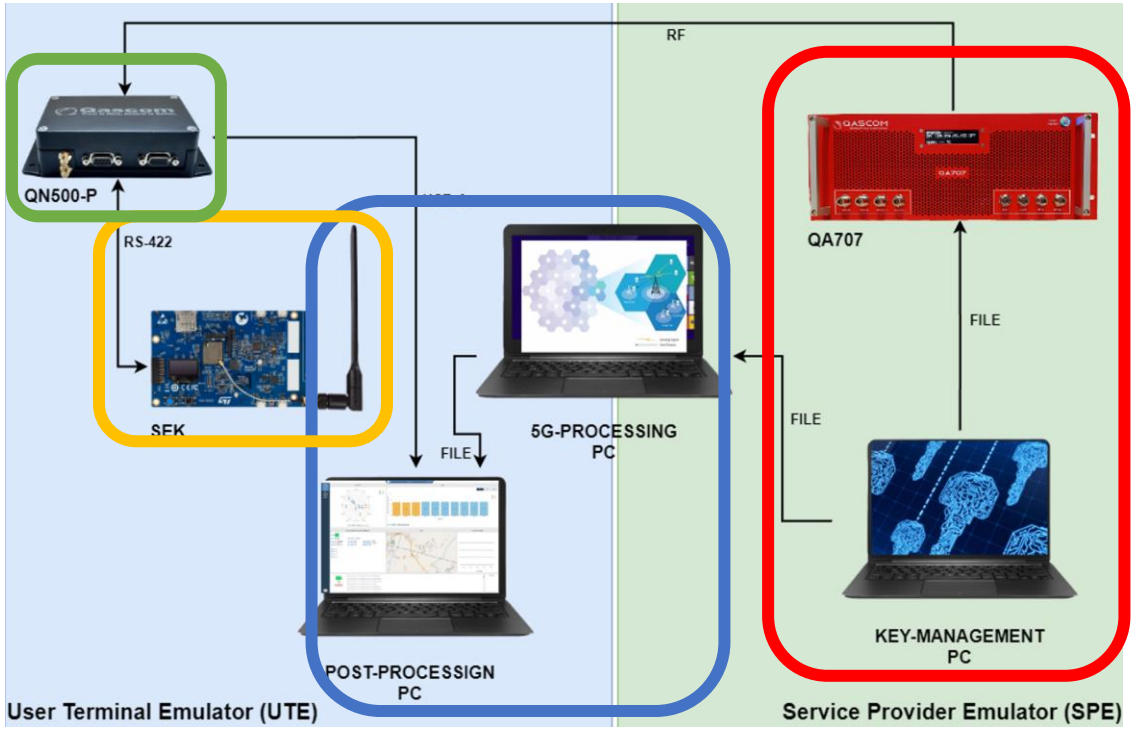


© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# Testbed overview

- Service Provider Emulator: QA707 + Key Management Function + 5G Service Provider
- User Terminal Emulator: QN500-P + Secure Element Kit + 5G receiver + Post Processing PC





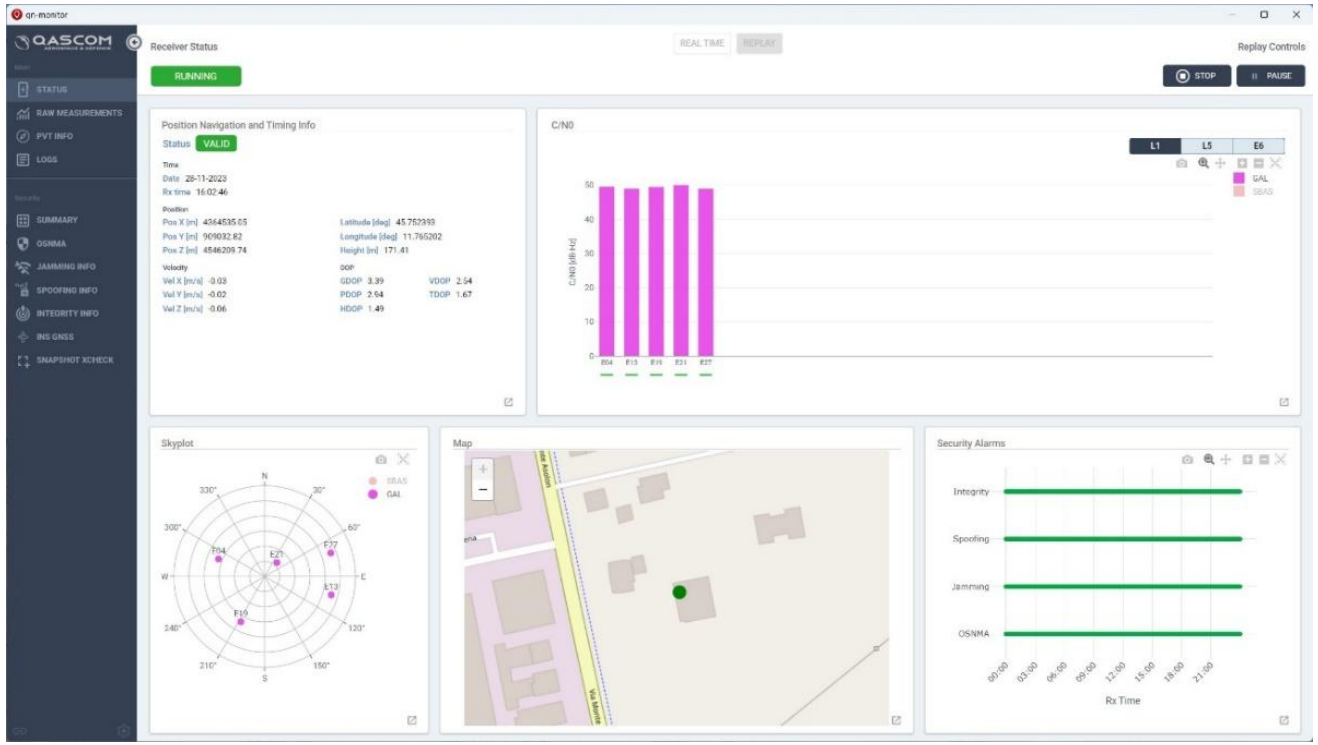


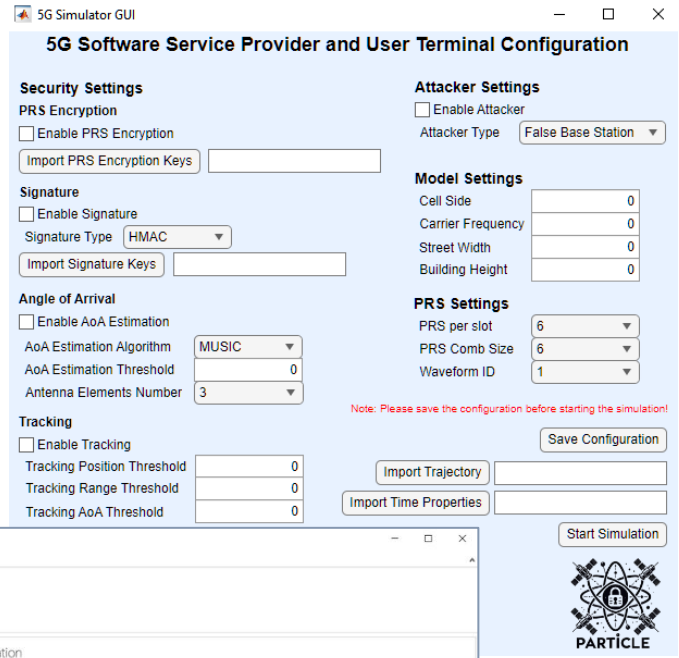

© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

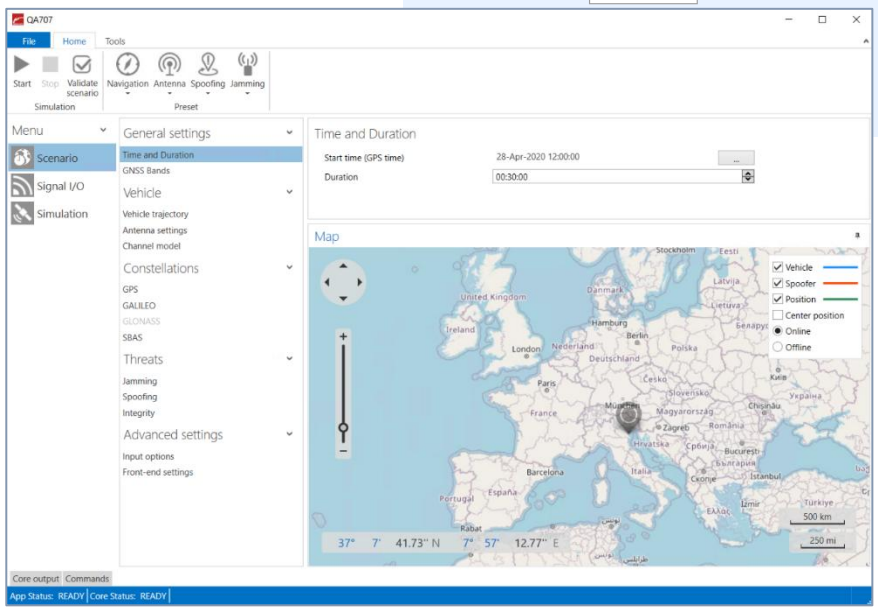
# Testbed configuration

- User configures the testbed through a set of GUIs, contolling the SPE (GNSS and 5G service providers) and UTE (GNSS and 5G User Terminals).

- The GUIs allow to see in real time relevant parameters of the operation.



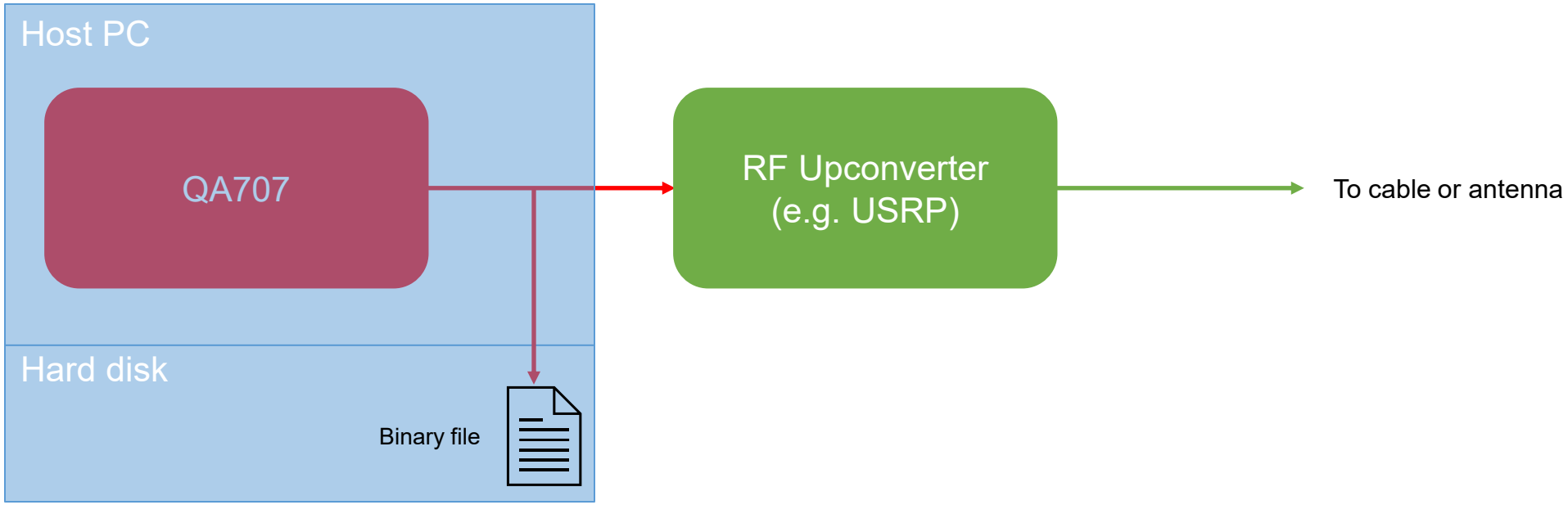






© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# GNSS Simulator Description

- Qascom's GNSS service provider emulator: QA707;
- SDR-based GNSS and interference simulator;
- Dual frequency with USRP-X300 interface.

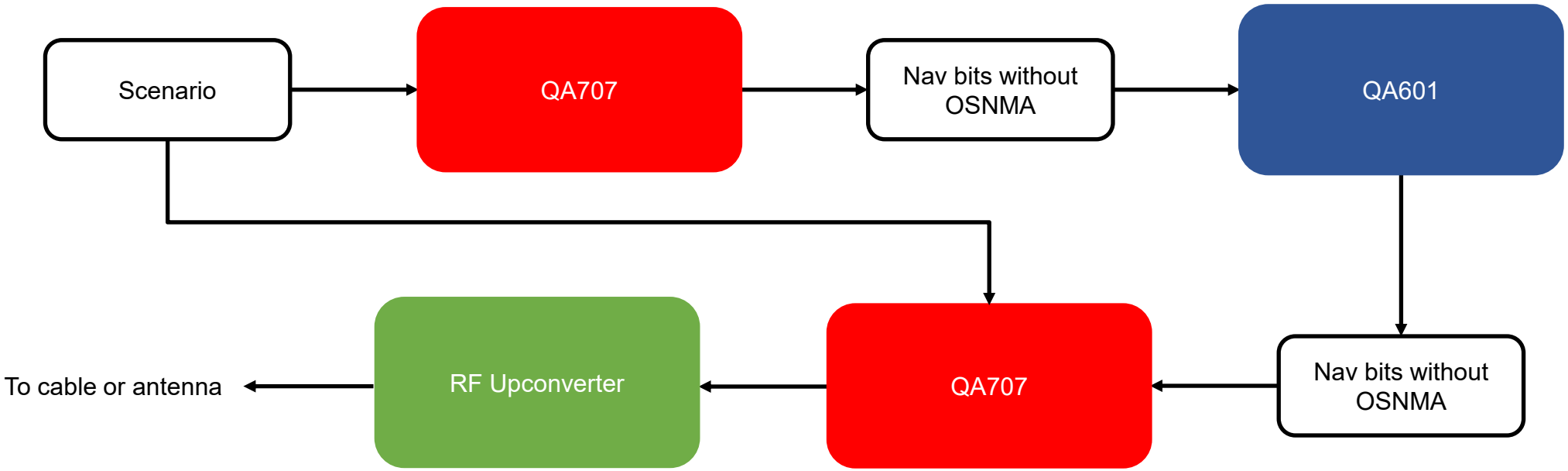





© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# GNSS Simulator Description

- Integration with QA601 OSNMA simulator.

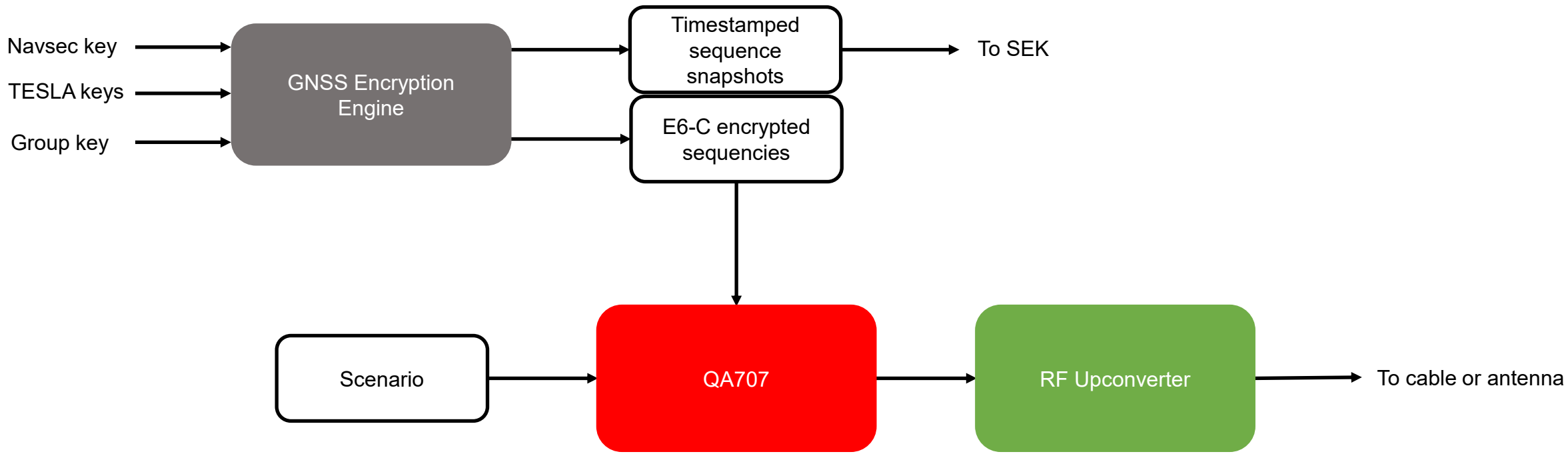




© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# GNSS Simulator Description

- GNSS Encryption Engine to compute:
  - Timestamped snapshots ➔ to SEK
  - E6-C encrypted sequencies ➔ to QA707
- Generate encrypted E6-C and transmit through RF upconverter.





© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

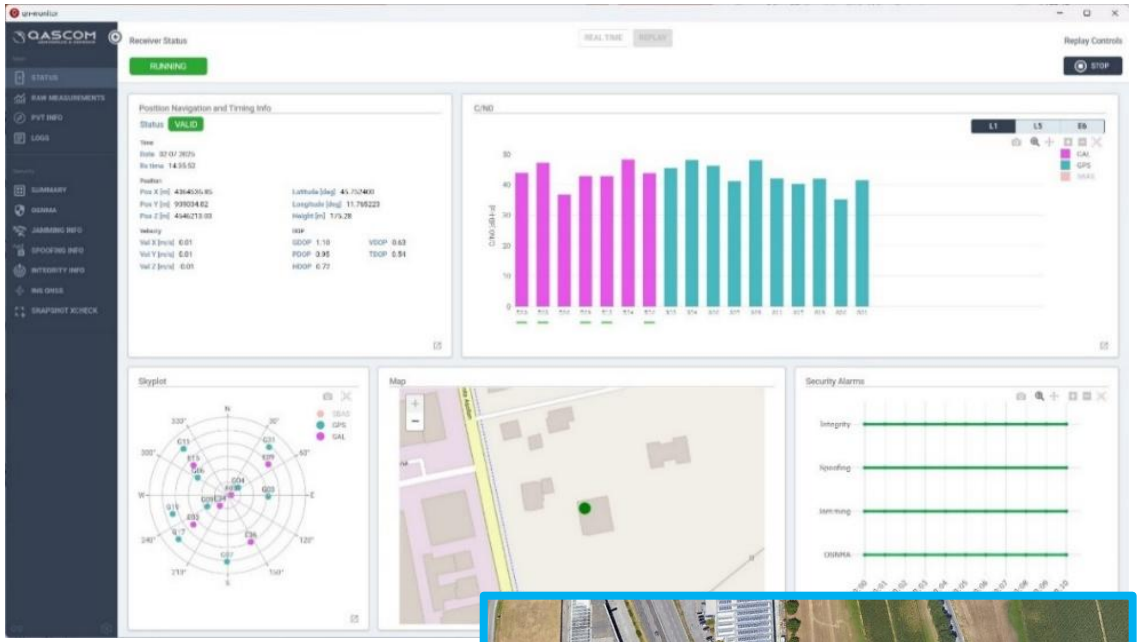
# 5.

## GNSS User Terminal Emulator

# QN500-P Robust PNT Technology Product

## QN500-P Product

- **3 Frequencies** (L1/L5/E6), **Multi-Constellation** (GPS, GAL) guarantee maximum availability in denied scenarios
- **Frequency Interference Monitoring, Detection and Exclusion**
- **Receiver Based Anti-spoofing.**
- **Advanced Integrity** based on Dual-constellation RAIM, based on Random Sample Consensus
- **INS/GNSS Sensor Fusion**
- **High Accuracy Positioning** based on Galileo HAS
- **Assured PVT with Resilience Manager**



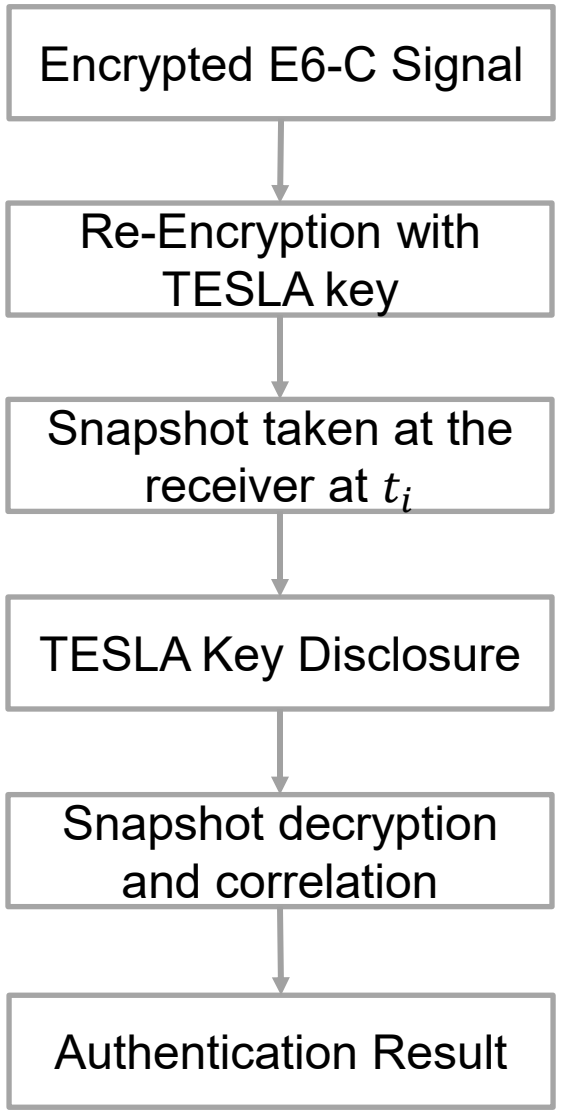

- **QN500-P has been used as starting Technology in PARTICLE NAVISP Project**



© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# E6-SAS

1. E6 Encrypted PRN Codes Generation
2. To provide further authentication capabilities, the E6-C (Pilot) signal is encrypted prior to its transmission.
3. The signal known as Encrypted Code Sequences (ECSs), are then re-encrypted using the TESLA keys provided by OSNMA on the E1-B signal, yet to be disclosed, thus creating the RECS (Re-Encrypted-Code-Sequences)
4. The RECS are then stored on the receiver for future use.
5. Once the E6-C signal is broadcast, the receiver records a snapshot.
6. Later, when the corresponding key is disclosed in the E1-B signal, the receiver can decrypt the stored RECS and correlate it with the pre-recorded snapshot.
7. A correlation peak indicates that the signal is located as expected so the signal can be authenticated.

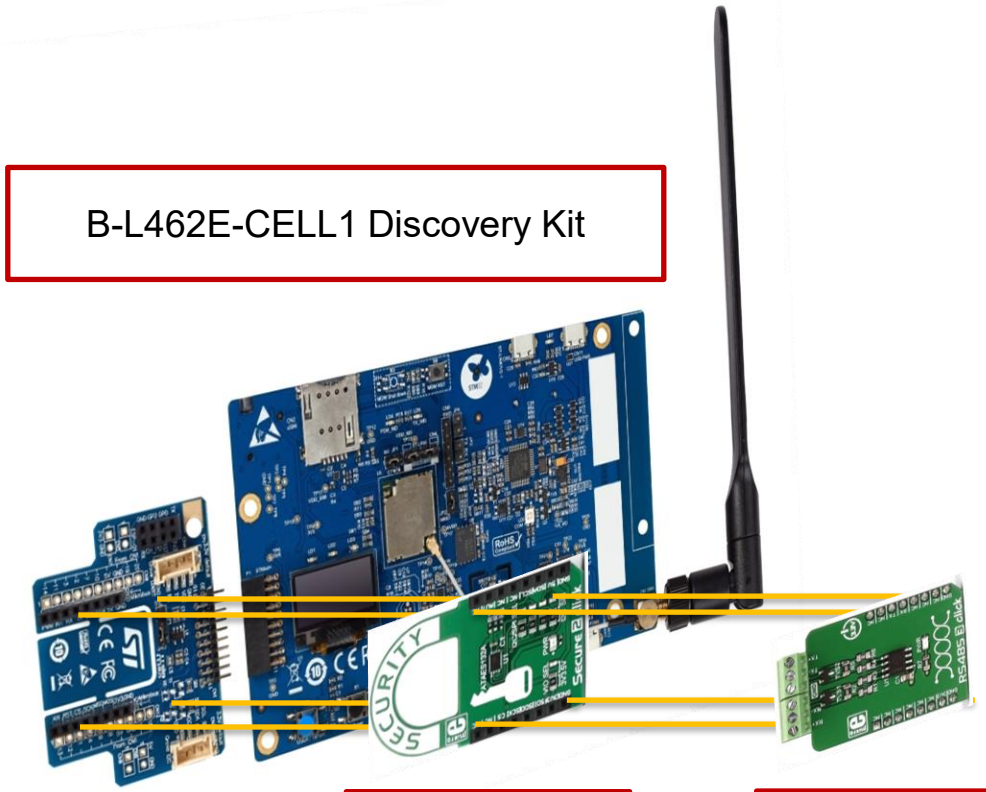




© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# SEK Module

B-L462E-CELL1 Discovery Kit



Secure 2 Click

RS485 3 Click

## Objectives of the SEK

- To Store Encrypted REC
- To Store securely the User Key
- To Decrypt the REC with the User and the Tesla Keys
- To Communicate with the receiver via Serial Interface
- To sign a message custom hash



© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

QASCOM
AEROSPACE & DEFENCE

# 6.

## 5G User Terminal Emulator

# Motivation

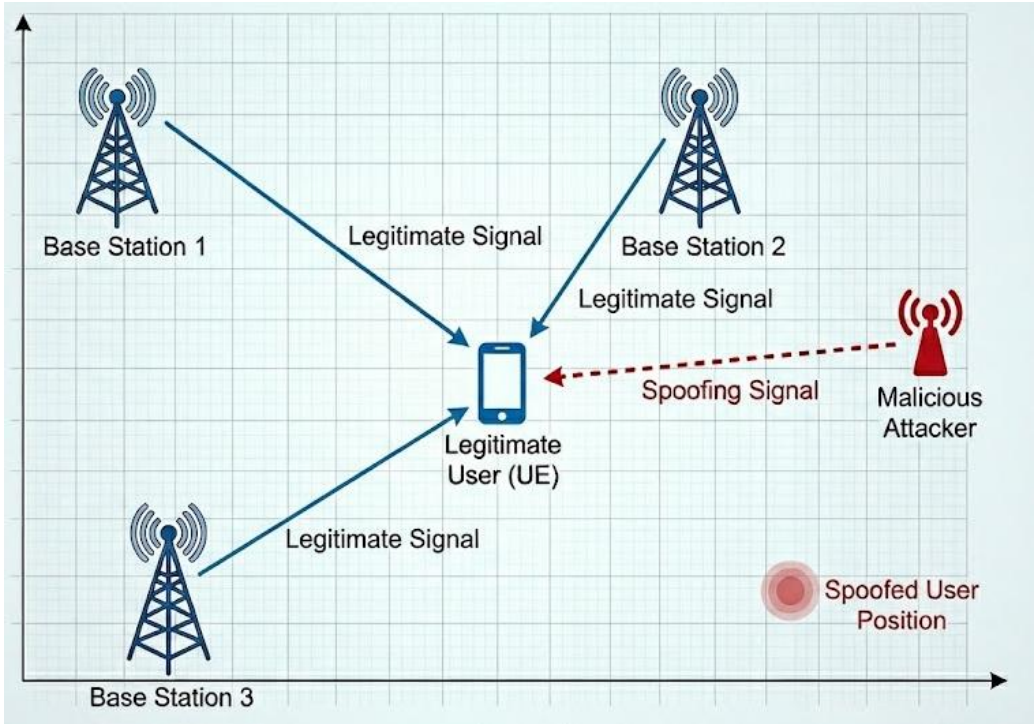
- Standard 5G positioning security assumes the threat is outside the network.

- Existing security protocols protect the network layer, but the physical layer remains highly vulnerable to attacks.

What if the attacker has already penetrated the network?

- They know the system parameters and signal structure.
  - **Assumption:** The attacker cannot have access to the cryptographic keys.

- While upper-layer data is highly encrypted, the physical layer signals used for positioning are broadcast entirely in the clear.

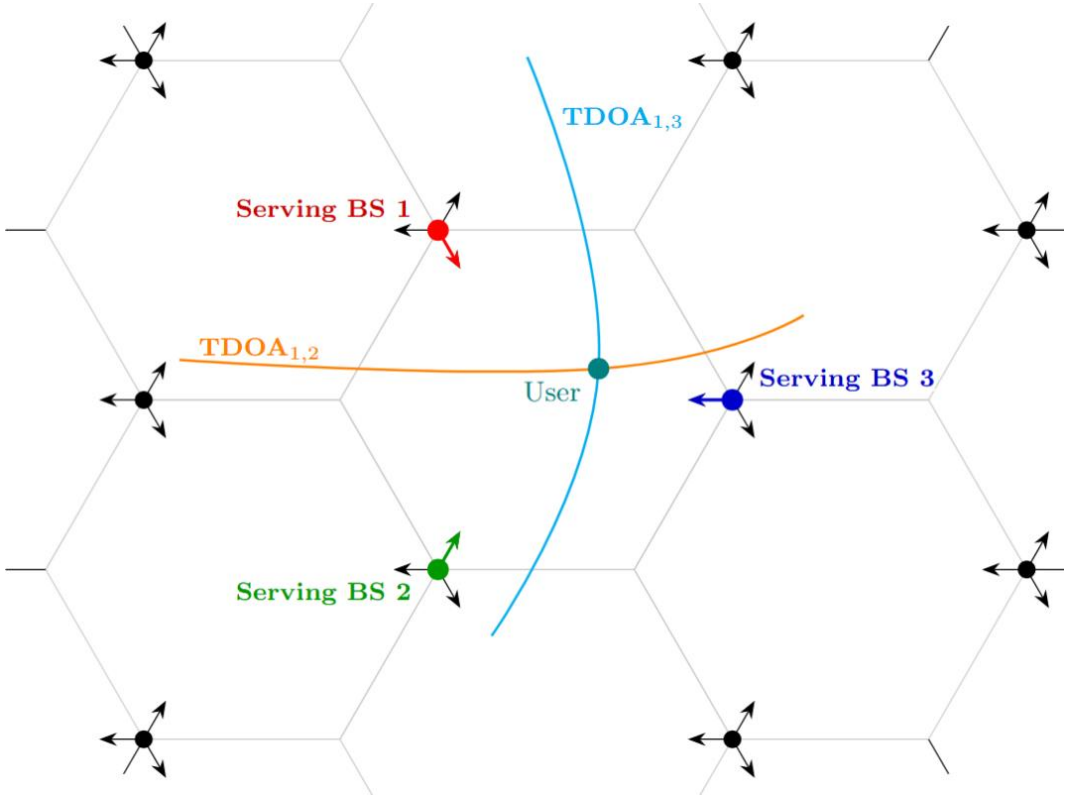




© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# Positioning with OTDOA

- DL-OTDOA (Downlink observed time difference of arrival) serves as a primary, standardized positioning technique for localizing 5G user equipment (UE).
- The localization architecture relies on a coordinated network topology where multiple base stations (BSs) simultaneously serve a single device.
- The device measures the TDOA between a reference BS and neighboring stations.
- Geometrically, each measured time difference mathematically translates into a hyperbola in a 2D coordinate system.
- The intersection of multiple hyperbolas delivers the final user position estimate.





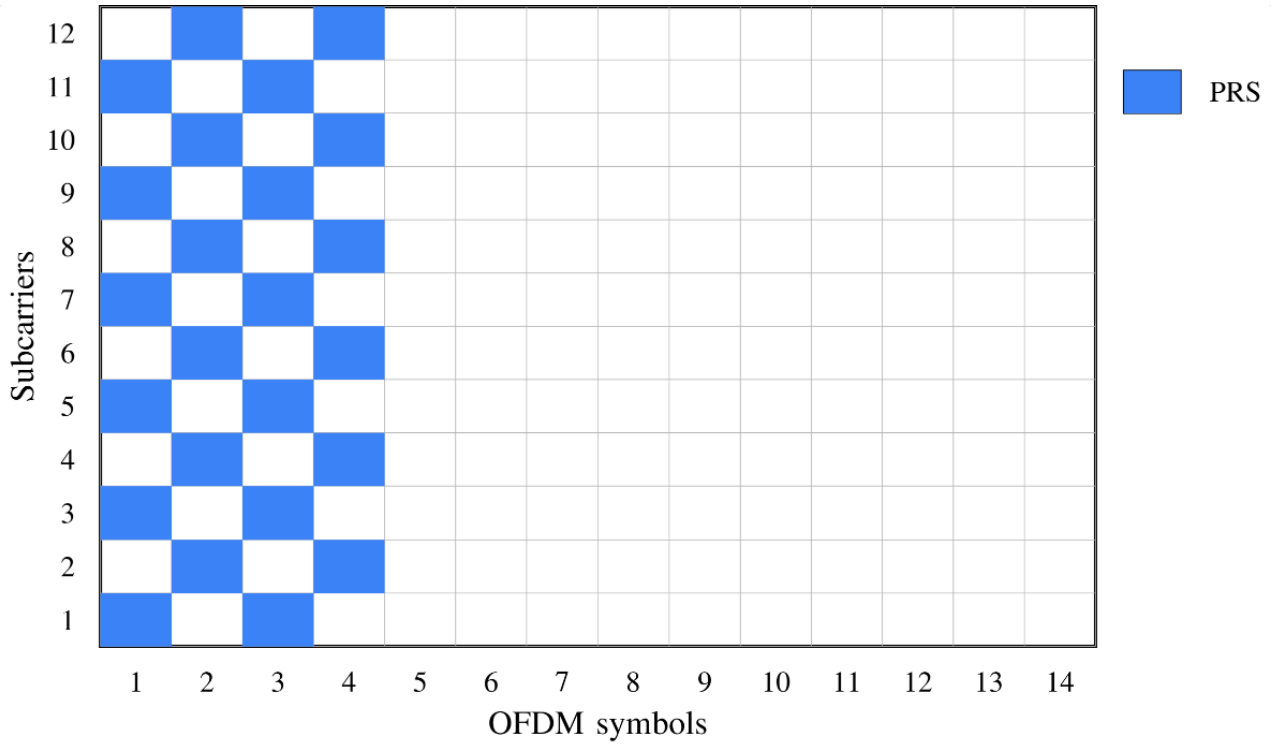
© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# The Positioning Reference Signal (PRS)

- 5G uses dedicated positioning signals.
  - PRS: Downlink transmissions
    - Pseudo-random Gold 31-bit sequence
    - QPSK modulated
    - High autocorrelation
    - Low cross-correlation
  - SRS: Uplink transmissions
    - Zadoff-Chu sequences
    - Low PAPR
    - Zero cross-correlation

- Orthogonal frequency-division multiplexing (OFDM) grid.
  - Discrete time and frequency resource elements.

- Lack of cryptographic protection introduces a critical vulnerability.





© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# Threat Model

- Operating under our assumed breach model, we defined three primary physical layer attack vectors, selected specifically for their operational simplicity and alignment with practical threat use cases:

  - A **false base station (FBS)** can spoof (or deny the service of) the system by transmitting a fake PRS (with similar properties of the legitimate signals) with higher power to artificially shift the correlation peak.

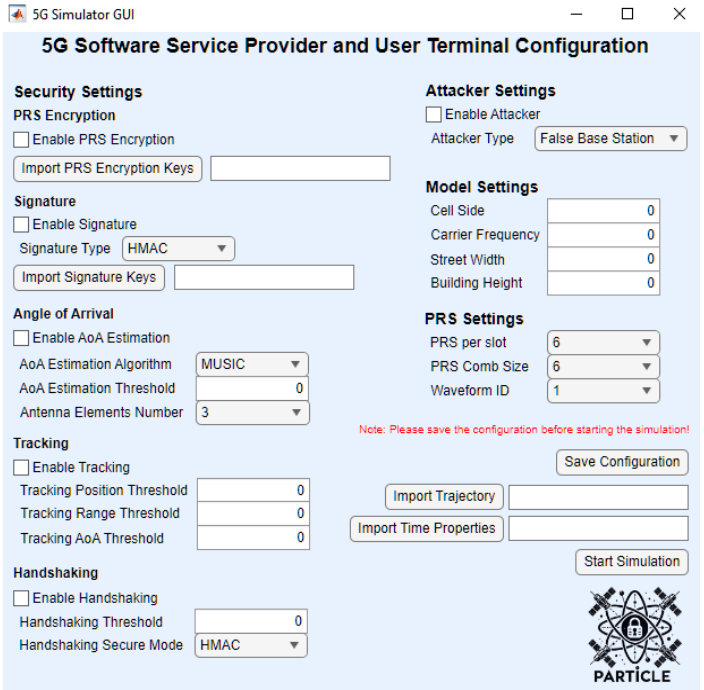
  - **Meaconing** captures and replays the legitimate PRS, deceiving the receiver without needing cryptographic keys.

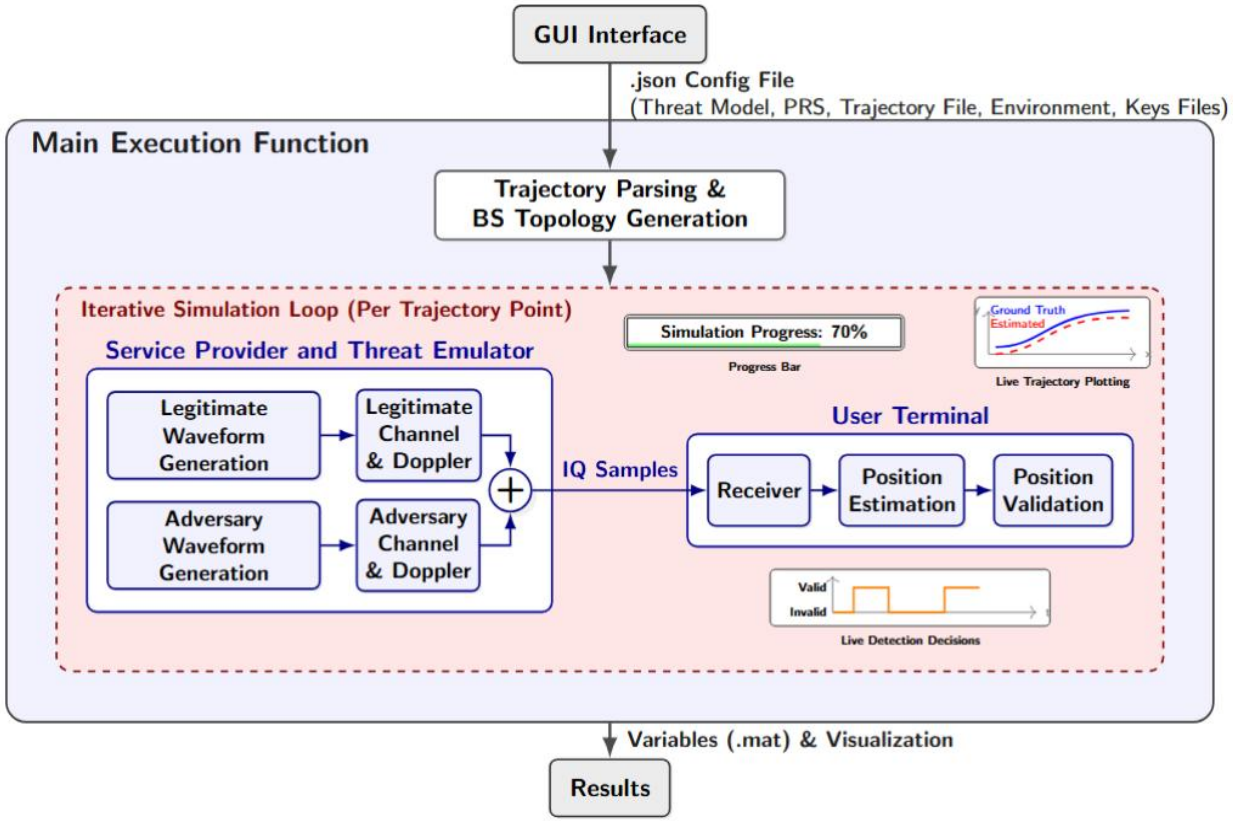
  - **Wideband jamming** overpowers the legitimate signal and causes denial of service (DoS).


© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# Detection Techniques and VeriLoc Simulator

- Identified the need for security enhancements at the physical layer in 5G positioning.
  - We propose a set of threat detection/mitigation techniques.
- VeriLoc (Verified Location): a custom MATLAB-based system-level simulator for 5G OTDOA positioning.
  - 5G Signal generation and channel propagation.
  - Allows for the injection of physical layer threats.
  - Evaluation of the proposed techniques.
  - Available at: https://github.com/loctio/veriloc





© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# 7.

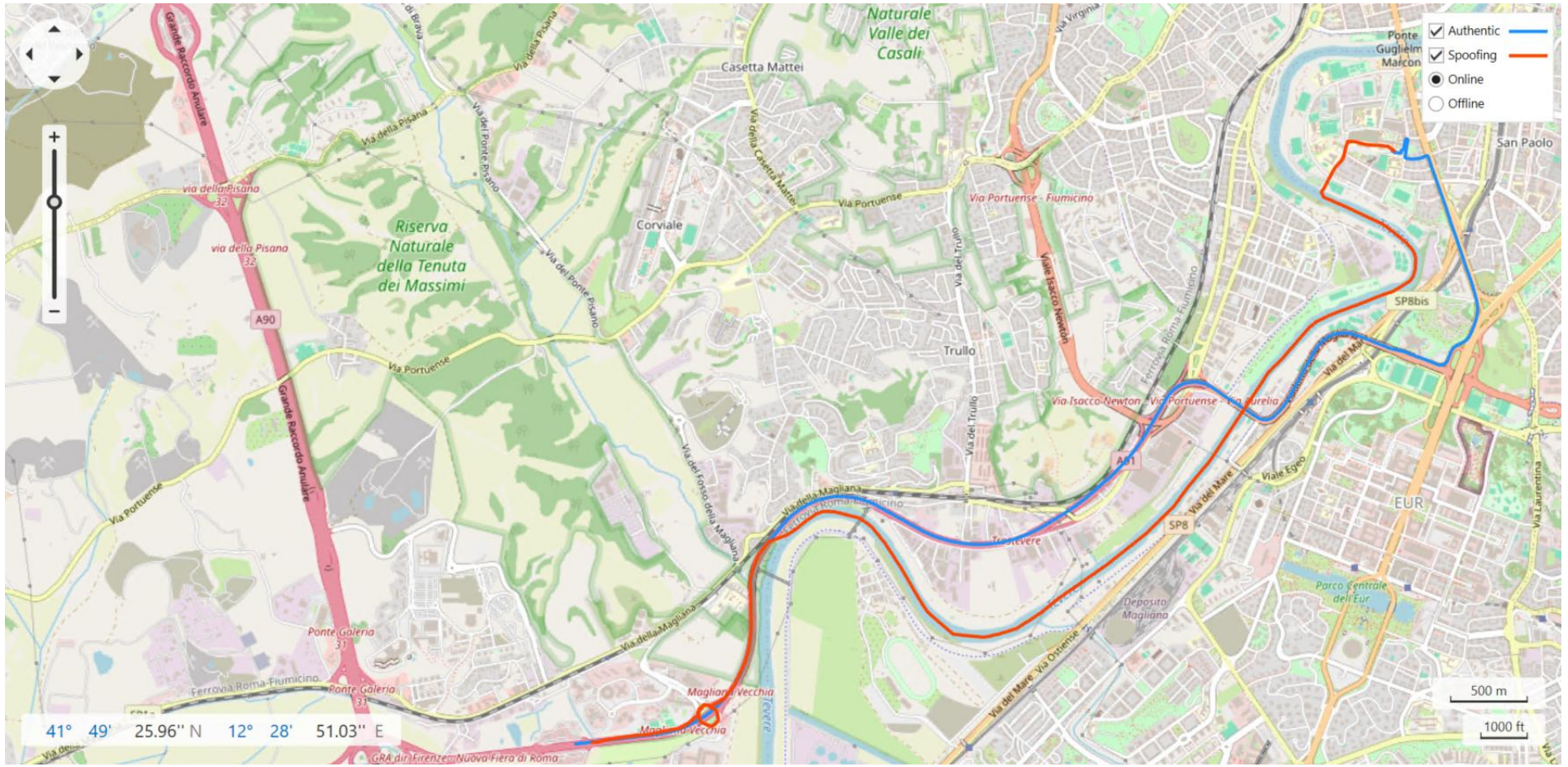
## Validation Results

# 7.1

## Test Scenario: GNSS dynamic with spoofing

# Test Scenario: GNSS dynamic with spoofing

- **Authentic trajectory / Spoofed trajectory**
- Trajectory Spoofing with authentic navigation symbols.
- Init: T0; End: T0+30min.

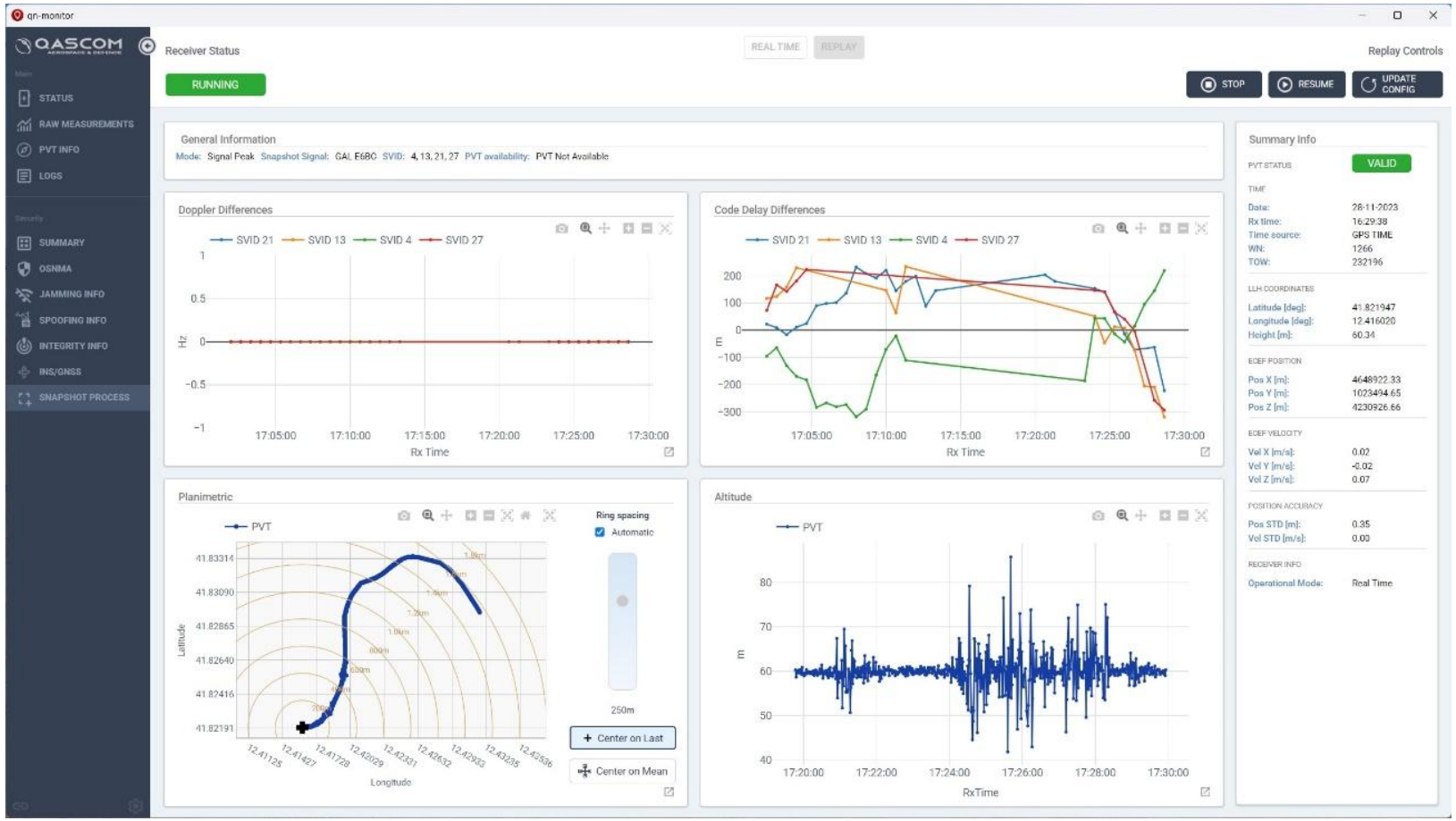





© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# Test Scenario: GNSS dynamic with spoofing

- The snapshot processing plots show in the top right how the code phase difference exceeds the set threshold.
- The lower plots show inconsistencies.






© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# 7.2

## Test Scenario: 5G dynamic with spoofing

## Proposed Techniques for Threat Detection:

- **PRS Encryption**
  - Add a layer of cryptographic protection to the transmitted signal.
    - Prevents the attacker from synthesizing valid waveforms.
- **Embed Authentication Schemes into Empty PRS Resource Elements (HMAC/DS)**
  - Enables authentication of legitimates PRS transmissions.
- **Angular-Based Authentication (ABSA)**
  - Authenticates the spatial properties of the signal based on the serving BS geometry.
- **DL-UL Handshaking (DL-UL HS)**
  - Cross-link positioning verification.
    - **Assumption:** The adversary node cannot attack UL and DL simultaneously.
- **Position Tracking**
  - Anomaly detection.

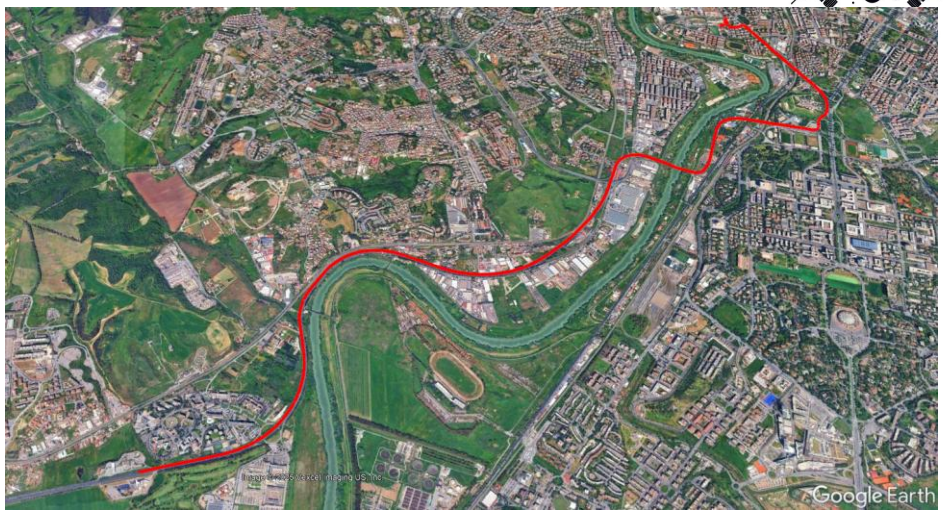
**Each technique was separately assessed to measure its individual security benefits and trade-offs against specific attack vectors.**

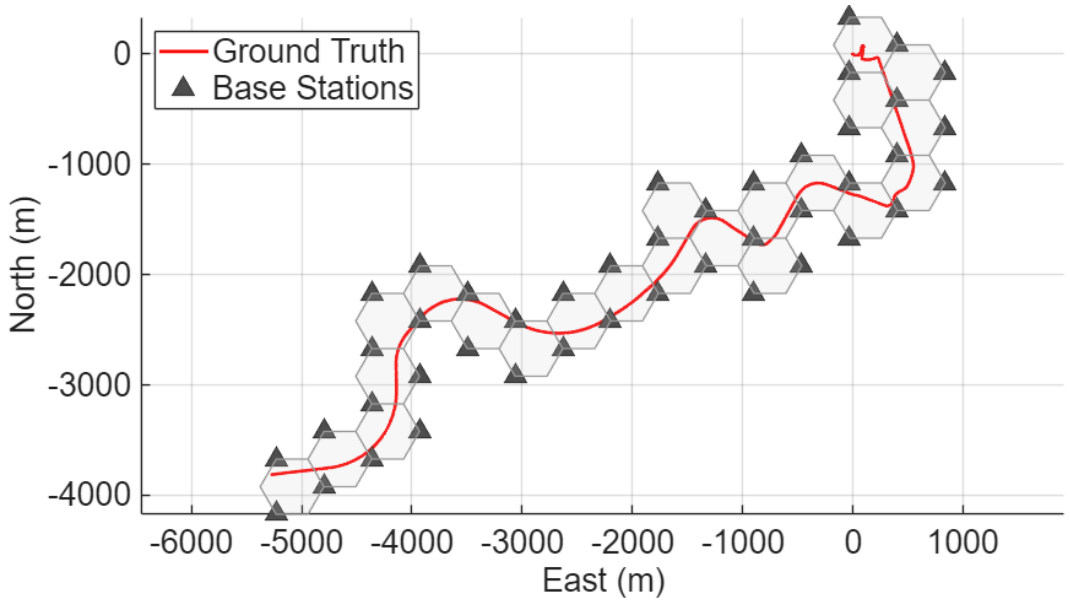
- Every technique protects a distinct dimension for robust, detection-based security for OTDOA.


© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# 5G Test Scenarios

- Transportation Monitoring with 5G Threats
  - Dynamic Trajectory
    - One Trajectory point per second
- Evaluation of three attack types:
  - Jamming
  - Meaconing (Replay Attack)
  - False Base Station (FBS)
- Proposed techniques performance assessment
  - Under threat conditions (Threat Detection)
  - Under benign conditions (False Alarm Assessment)

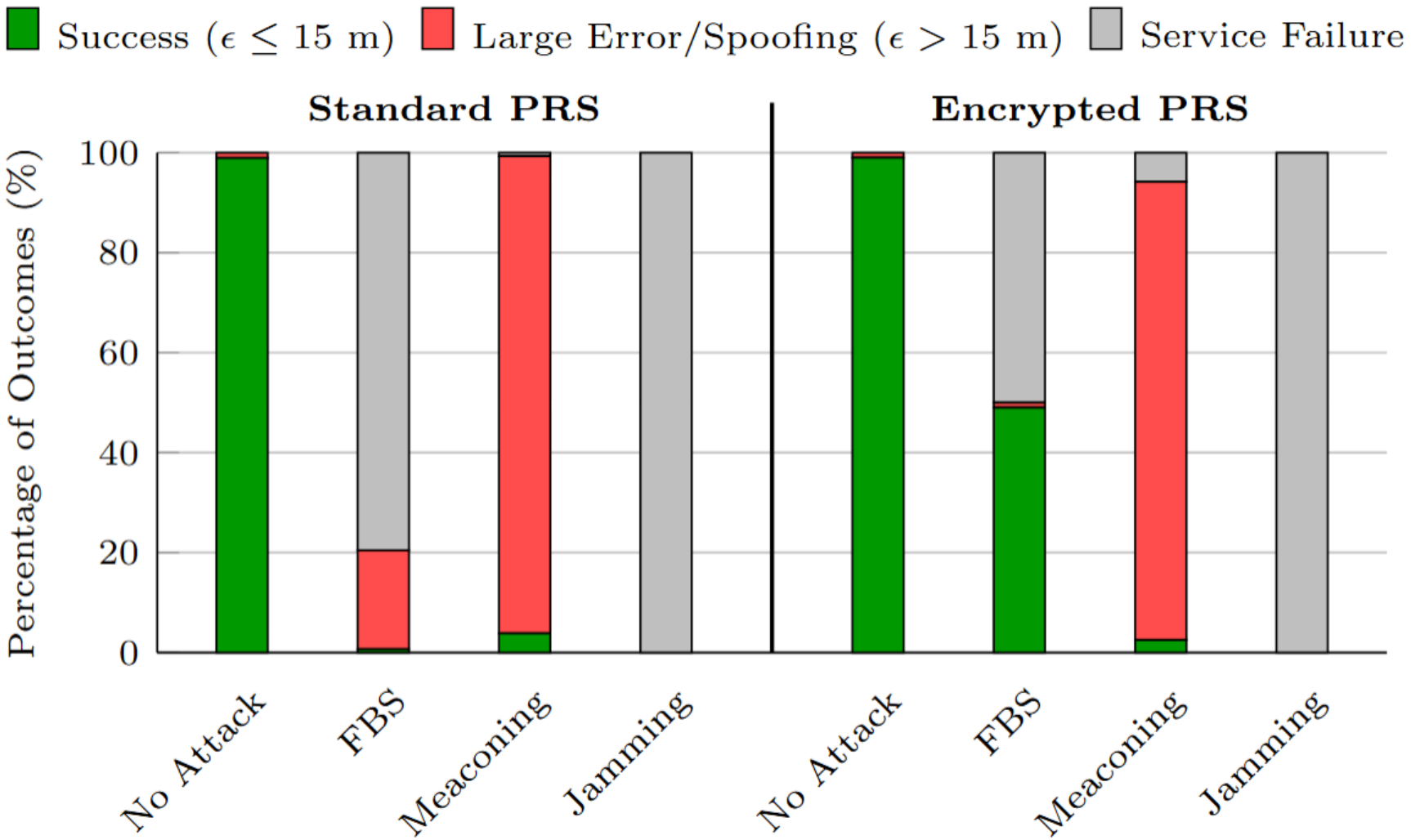




© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

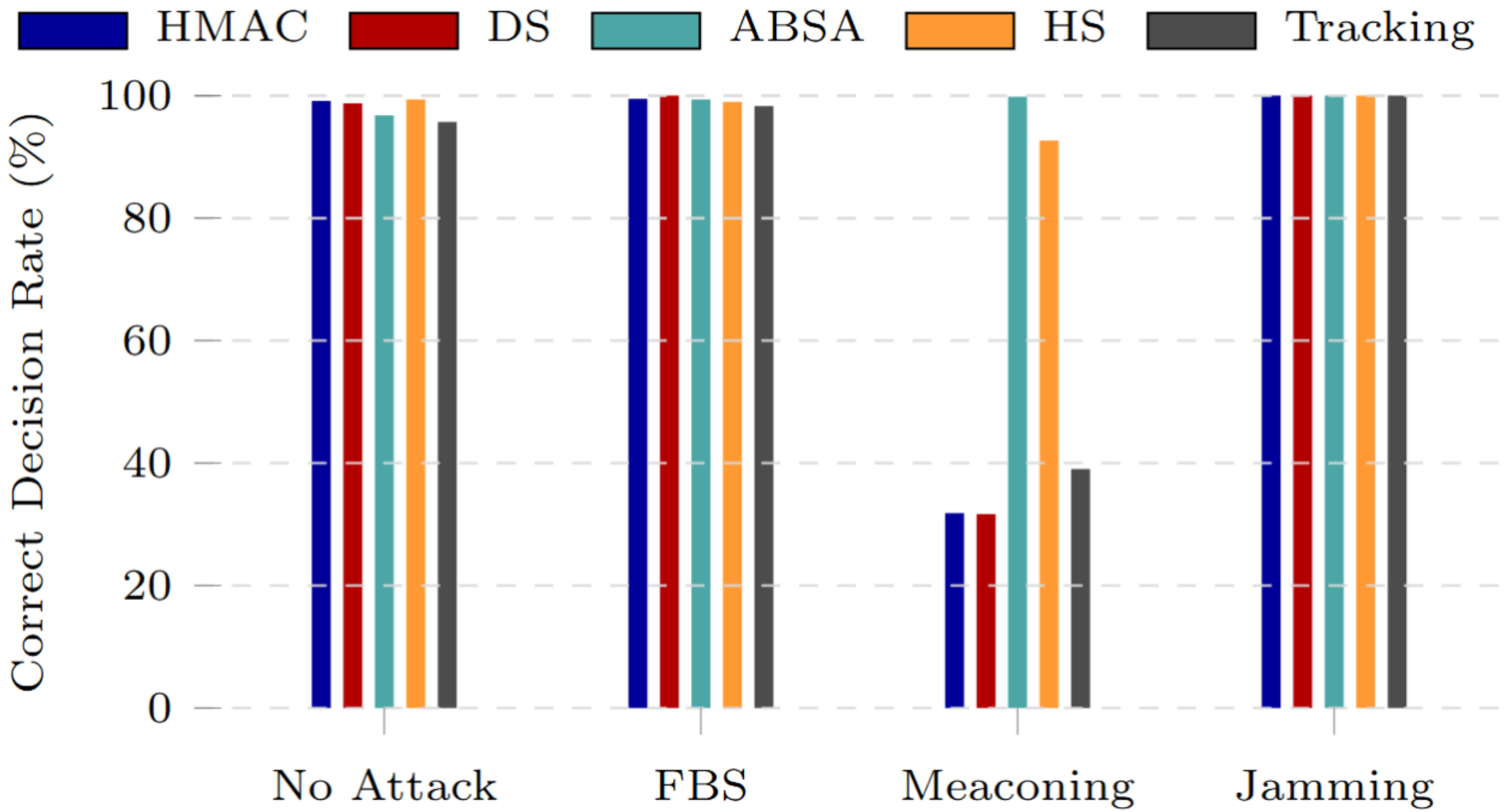
# Encrypted PRS Evaluation




- Encrypted PRS performs as standard PRS under benign conditions.
- Under an FBS attack, it neutralizes spoofing. Either computes a valid location or fails safely. A ~50% DoS rate occurs because of the attacker's high power fake signal.
- Provides zero defense against meaconing or high-power jamming.


© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

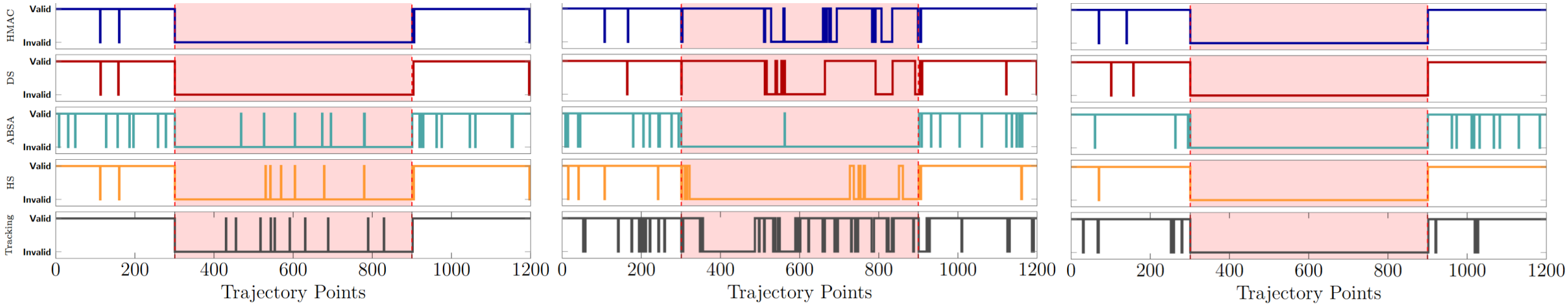
# Performance Overview






© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# Decisions per position fix




## False Base Station

- All evaluated techniques successfully detect the attack.

## Meaconing (Replay)

- Signature-based methods and Tracking fail (~40% detection).
- Angular-based authentication and DL-UL protocol successfully detect a large percentage of the attacks.

## Jamming

- All techniques achieve 100% correct decision rate.

## False-Alarm Robustness (Benign Conditions)

- HMAC/DS and DL-UL Handshaking: Near-perfect robustness
- ABSA and Position Tracking: Slightly higher false-alarm rates at the cell edges


© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# 8.

## Way forward

# Impact and Way Forward

- **Impact:**
  - Fostering the development of new IPs that target the **mitigation of potential threats**.
  - **Contribute to the standardization process**, as PARTICLE has contributed to highlighting potential vulnerabilities.

- **Way Forward:**
  - Combine and **expand the detection/mitigation techniques** targeting reliable PVT even under attack.
  - **Higher-TRL demonstration** of the proposed and new techniques.
  - To **integrate the Secure Element** cryptographic functions **inside Qascom QN500-P receiver**, by manufacturing a new board including a certified Secure Element, interfaced with the SoC for enhanced security.


© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE

# Thank you!

© Qascom / Loctio / University of Patras 2026
UNCLASSIFIED - FOR PUBLIC USE