navisp

NAVISP EL1-77: Technological Enablers of Cellular Networks for PVT Assurance

12/10/23

Background 1/3

Radio frequency interference, intentional or not, is becoming more and more frequent, affecting the operations of Global Navigation Satellite System (GNSS) receivers.

The spoofing of GNSS is an evolving threat, which nowadays can be performed virtually by anyone given the wide spread of Software-Defined Radio (SDR).

GNSS are introducing anti-spoofing techniques, such as Galileo Open Service (OS) Navigation Message Authentication (NMA), Commercial Authentication Service (CAS) or GPS Chimera.

Cellular networks have various built-in security features including access control, mutual authentication, and key management, which could be evolved to provide technological enablers for Position, Velocity and Time (PVT) assurance.

Background 2/3

An effective solution to achieve ranging authentication is the use of cryptographic mechanisms to render the ranging signal unpredictable to the potential attacker.

Symmetric cryptography, for instance stream ciphers, is commonly used for this. Sophisticated key management systems or frequent rekeying for scenarios in which the users cannot be trusted are required.

Additionally, asymmetric cryptography is generally used for protecting the data exchange (e.g. digital signatures). Unfortunately, commonly used digital signatures could become vulnerable in case a quantum computer become readily available. So called post-quantum digital signatures have much longer signatures, which could be challenging to be transmitted over the limited bandwidth of GNSS.

These data exchange could be facilitated by cellular networks technologies.

In addition, cellular networks themselves have become relevant sources of Positioning, Navigation and Timing (PNT), using signals not designed to provide ranging authentication capabilities.

Background 3/3

Mobile terminals of telecommunication networks, such as 4G or 5G, store the identification and cryptographic information to access the network in either a SIM card or an eSIM, which ensures the integrity and the security of the information stored in it.

The eSIM allows the user to download the cryptographic information for a specific network on demand, while maintaining high security standards.

Similar technologies are widely used for securing low end device, such as Internet of Things (IoT), where the secure element can be used for device authentication, secure attestation, and secure firmware update.

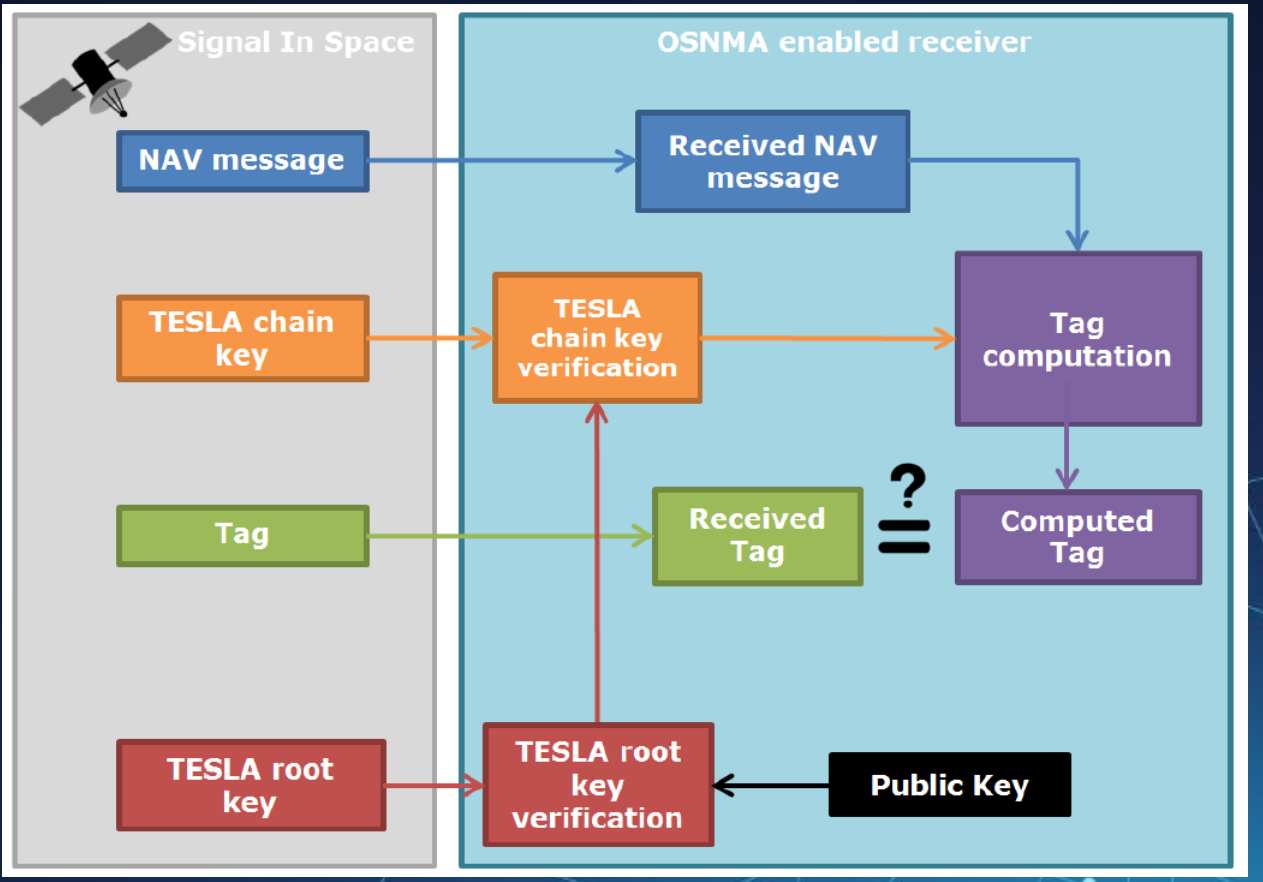
Galileo OSNMA

Provides authentication of the Galileo navigation message

It is transmitted in the I/NAV message

Based on tags computed using keys from a key chain

The key chain is authenticated using a digital signature



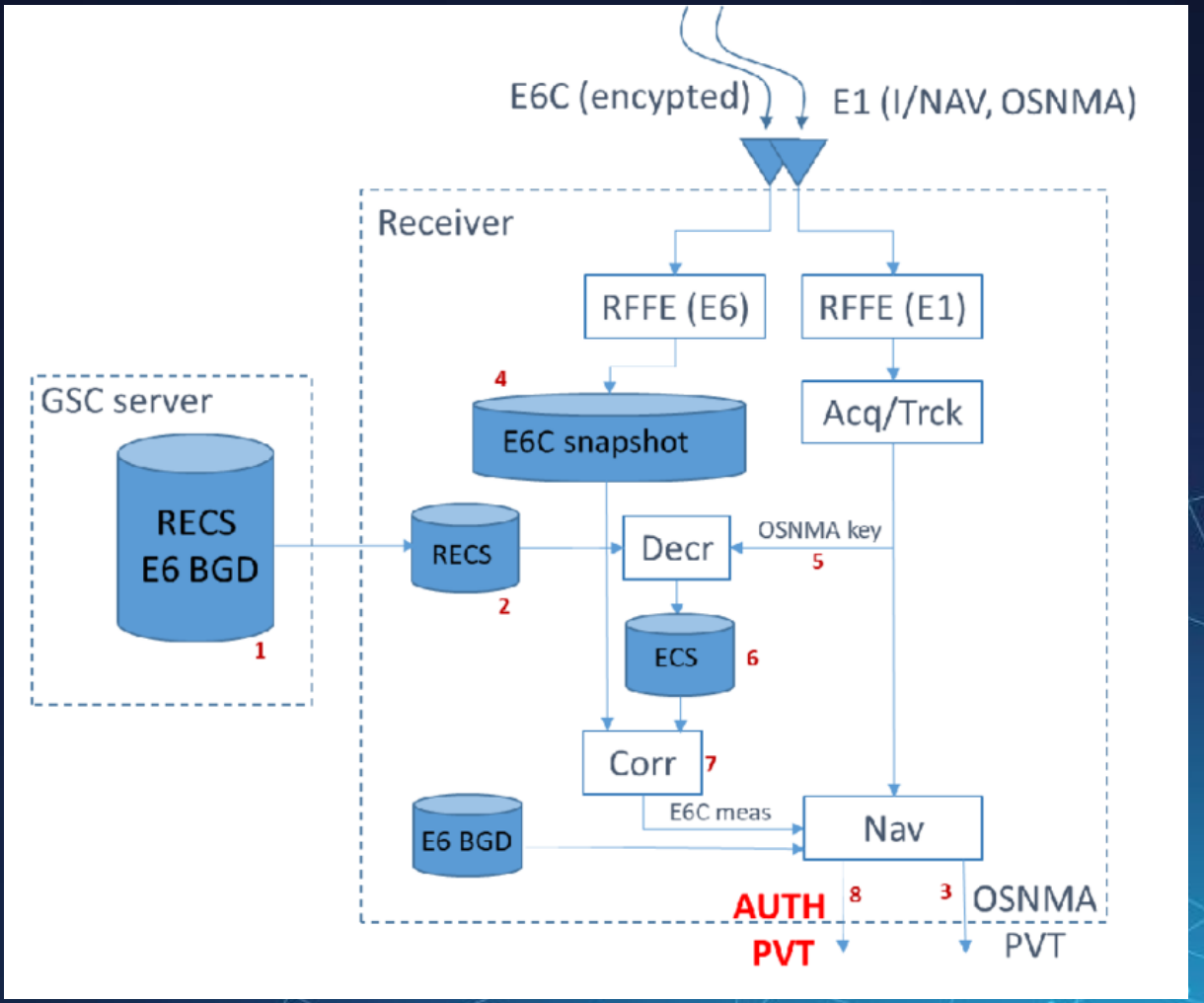
Galileo CAS

Provides authentication of the Galileo ranging signal

It is transmitted in the E6 signal

Based on the spreading code encryption

Portion of the spreading code are re-encrypted using OSNMA derived keys and made available via internet



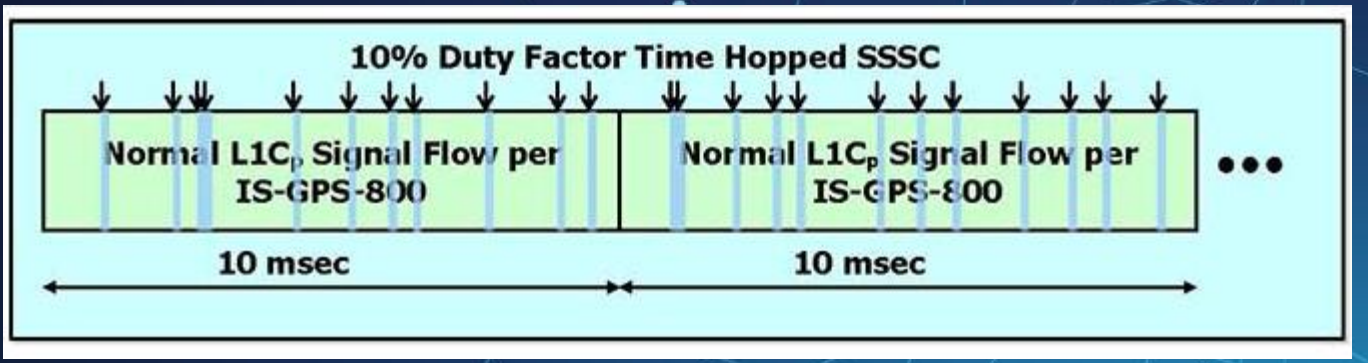
GPS CHIMERA

Provides authentication of the GPS navigation message and of the GPS ranging signal

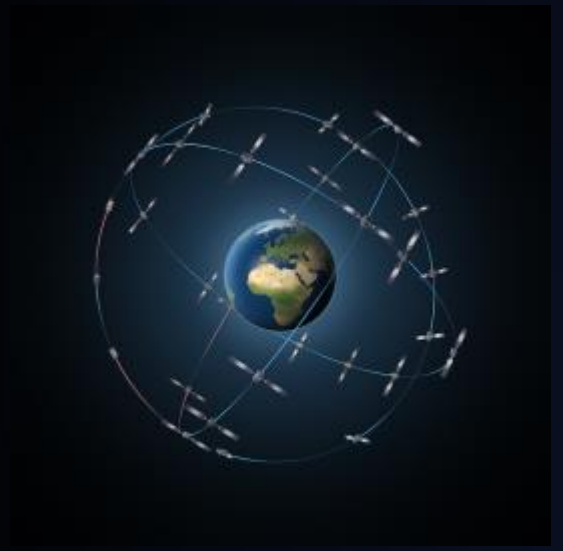
It is transmitted in the L1C signal

The navigation message authentication is based on digital signatures

The ranging signal protection is based on watermarking with encrypted code



GNSS “watermarking”



EL2-002 - GALILEO PUBLIC AUTHENTICATED SERVER-BASED SNAPSHOT POSITIONING (G-PASSION)

System for a GNSS server-based position authentication service using the Galileo signal. The system consists of the following 2 segments:

- The user segment, which is any user with a Localization Appliqué (i.e. a small device) that is able to interact with a GNSS COTS receiver (or Smartphone with GNSS capability), whose estimated PVT solution must be verified and authenticated. The user also needs to be able to communicate with a remote server centre over a secure authenticated channel and able to send its encrypted raw IF Galileo E1 snapshot (digitalized, down-converted, IF signal before the tracking loops).

- The ground segment is a remote server centre located in a secured known position estimated by a GNSS reference station (possibly a high level multi-constellation multi-frequency GNSS receiver part of a permanent GNSS network). The server also hosts an Authenticator Unit able to receive the raw IF snapshot and the non-verified PVT from the field user and judge if its position report is authentic. If it is authentic, the server sends a reply to the user including a positive PVT status flag and optionally information of augmentation, accuracy, integrity and quality of the service. Otherwise, if the non-verified PVT is not authentic (presence of interfering threats such as jamming, spoofing, meaconing or intrusion), the server shall send a negative PVT status flag within a predetermined time to alarm and optionally the estimated verified PVT of the user.

Objectives of the Activity

The objective of the activity is to study, design, and demonstrate the use of the cellular networks technologies for PVT assurance and encryption of ranging signals, considering robustness against quantum computers.

The activity shall:

- Study and design the system solutions leveraging the cryptographic information stored on the SIM card or the secure element to enable processing of encryption of GNSS ranging signals;
- Study and design the system solutions to introduce ranging signal authentication on cellular networks PNT signals;
- Evaluate the suitability of commercially available secure elements for performing the signal processing required for ranging signals;
- Demonstrate the proposed solution via proof of concept.

Example System Architecture

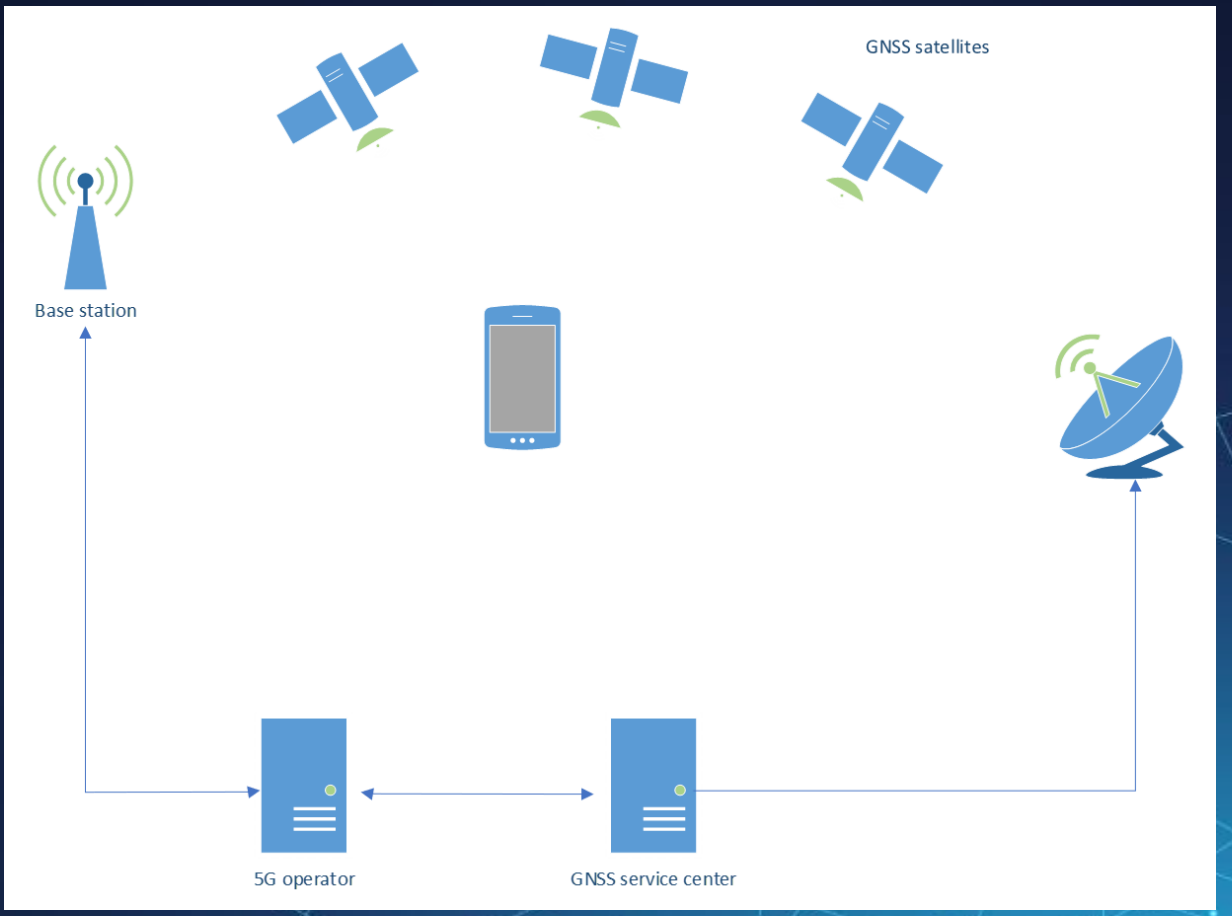
The GNSS service provider generates a set of symmetric keys.

These keys are used to encrypt the ranging signal transmitted by the GNSS satellites.

The user terminal first connects to the base station of the of his cellular network operator, and after the standard authentication and authorization process, it can ask for the PVT assurance service keys.

The user terminal can perform ranging on secure signals, significantly increasing the robustness to attacks.

Additionally, the communication channel could be used for authenticating the navigation message using post quantum signatures.



Use Cases

- UC 1: Confirmation of an initial location

Before starting the operations, the user wants to confirm the initial position.

- UC 2: Geolocation for outdoor survey

The user takes a series of measurements outdoor, possibly in the vicinity of tall buildings (which may block or degrade PNT signal). The data collected with the instrument is geotagged.

- UC 3: Transportation monitoring

The user installs a monitoring system on an asset to be transported on a sea/ground vehicle.

- UC4: Authentication of outdoor data

The user provides an instrument (e.g. a camera) containing a PNT module to an untrusted operator. The operator is required to collect data in specific locations, without the presence of the user.

Work logic

Task 1	Task 2	Task 3	Task 4	Task 5
State-of-the-art survey	Concepts tradeoffs	Testbed design & implementation	Performance evaluation	Roadmap toward industrial product
Requirements definition	Security demonstration			
Preliminary concept and CONOPS definition	System design consolidation			

Outputs

The main outputs of the activity are:

- TN discussing the suitability of commercially available secure elements for performing the signal processing required for ranging signals;
- TN with the proposed system architecture and key management scheme;
- Proof of Concept of the proposed solution using commercial products.

Note: Intellectual Property Rights ownership is with the Contractor