NACSET PROJECT

February 16, 2022

Funded by the European Union

PROJECT OVERVIEW

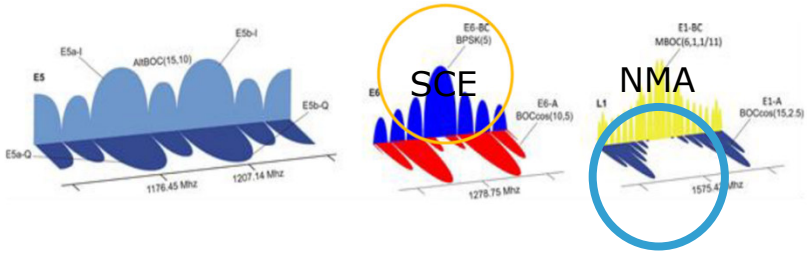
PROJECT CONTEXT

Galileo will provide two authentication services

1. Open Service Navigation Message Authentication (NMA) in E1B for receivers having the public key
2. Commercial Authentication Service (CAS) by spreading code encryption (SCE) in E6C for receivers having the encryption/decryption keys

Next generation resilient receivers will use these signals in combination with other receiver measures. The main challenges are:

1. How future resilient receivers will manage cryptographic operations required for authenticated signals
2. How to optimally combine data and signal authentication with receiver-based protection measures



WHAT IS NACSET?

- EC started the Navigation Authentication through Commercial Service-Enhanced Terminals (**NACSET**) project in Jan 2017

Objectives:

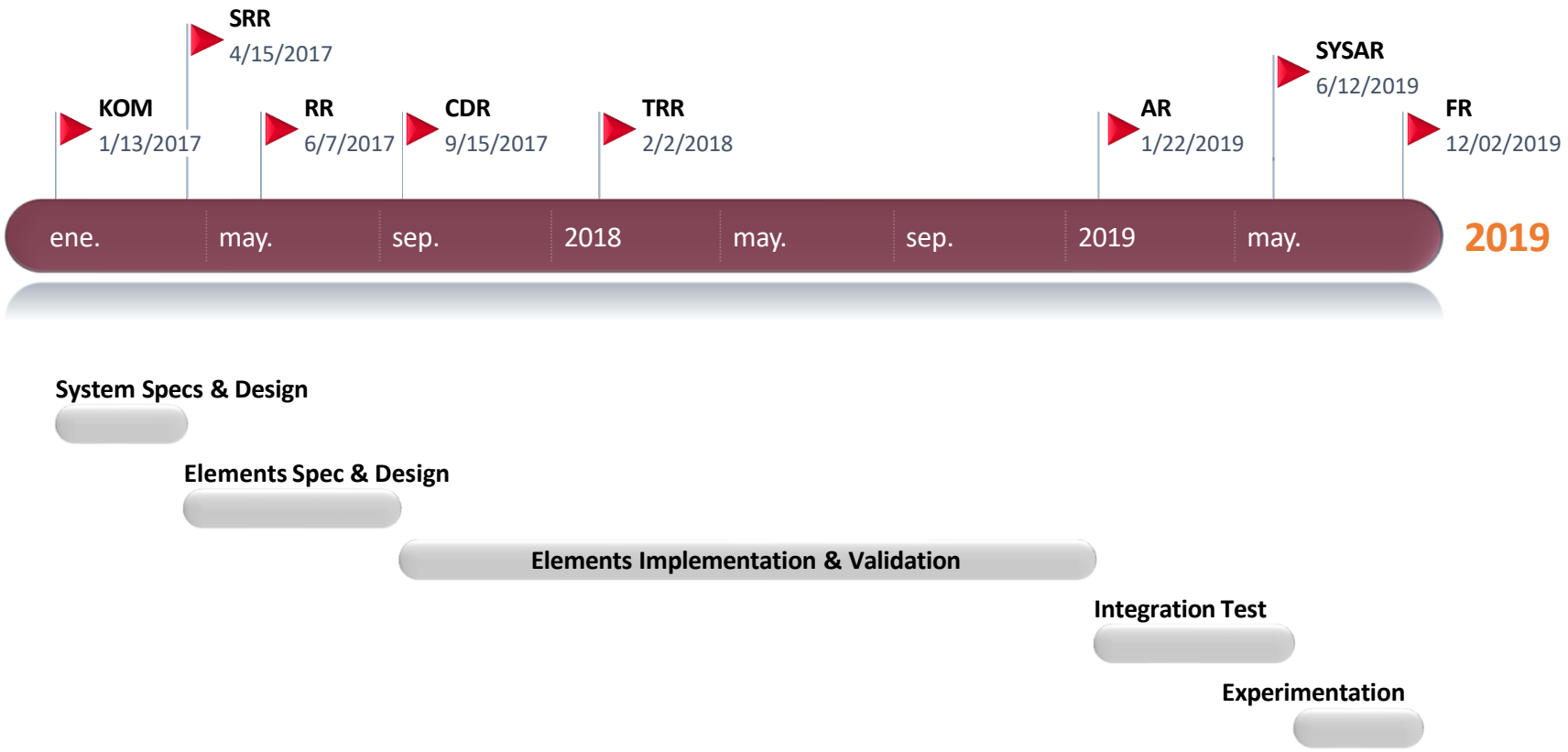
- Develop and test a secure **Key Management Simulator** for the Galileo CS and OS keys
- Develop a platform resilient to malicious and spoofing attacks
  - **Resilient User Terminal**
    - Anti-spoofing techniques
    - Accurate Time synchronization
    - Inertial Measurements Unit (IMU)
    - Signal Authentication (**Anti-replay protection**)
  - **Synchronization and Authentication Server**
    - Time Synchronization provision
    - Navigation message aiding channel
    - Assisted Signal Authentication provision

- Keep research on Galileo to define future evolutions.

PROJECT CONSORTIUM

COMPANY	OVERVIEW OF COMPANY ROLE
	As Prime and Sole Contractor with the European Commission, GMV was in charge of the overall project management under WP1000, including product assurance, configuration and documentation management, security management, consortium management and technical coordination. GMV was also the coordinator of the CS Resilient PVT Platform Development and will thus lead WP3000. GMV also lead the CSRPP System Level Activities & Maintenance (WP3300) and contributed to the User Terminal development, being in charge of the PVT client development (WP3260) and the IMU integration (WP2370) and the AntiReplay technique implementation. GMV also contributed to WP4100, led by QASCOM, giving support to the execution of part of the experimentation activities. Within WP5000, GMV lead the requested support efforts to the European Commission, coordinating the Support for threat testing of the CS-RPP platform (WP5100) and the ad-hoc engineering support (WP5200).
	CGI lead the Key Manager Simulator development and experimentation (WP200). Within WP5000, CGI coordinated the support for system accreditation and other security related aspects (WP5300).
	QASCOM was the proposed leader for the CSRPP experimentation to be performed under WP4000, being responsible for the overall coordination, planning and reporting. Within WP3000, QASCOM was responsible for the Synchronization and Authentication Server Development (WP3100) and supported IFEN and GMV in the development of the User terminal (WP3200) and also in CSRPP system level activities (WP3300). QASCOM also provided support to CGI in the definition of the KMS interfaces within WP2100. Finally, QASCOM contributed to WP5200 for the ad-hoc engineering support activities.
	IFEN lead the development of the User Terminal under WP3200, including requirements and design definition, interfaces definition, procurement of COTS, the CS Receiver Development and Time synchronization and integration and validation activities. Also within this WP3200, IFEN supporedt GMV integration of IMUs in the User Terminal. Additionally, IFEN also contributed to the CSRPP system level activities under WP3300. IFEN provided support to CGI in the definition of the KMS interfaces within WP2100. Finally, IFEN contributed to WP5200 for the ad-hoc engineering support activities.

PROJECT SCHEDULE OVERVIEW



NACSET PLATFORM

NACSET PLATFORM OBJECTIVES

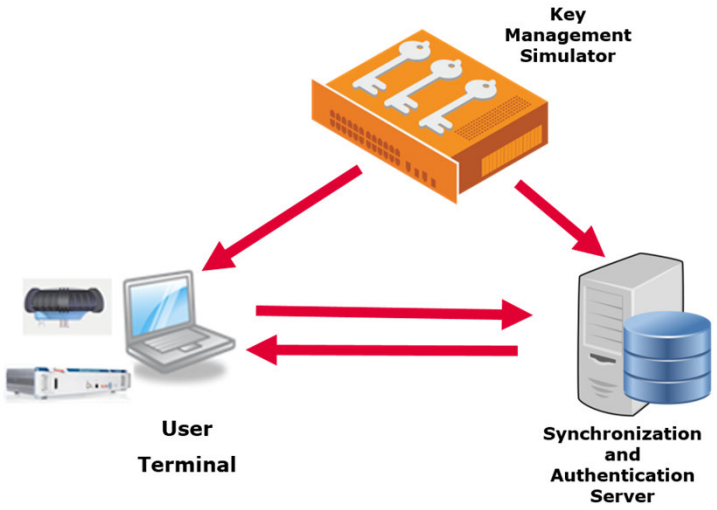
Objectives

Analyze potential threats at user-level and propose detection and/or mitigation actions.

Design and evaluate standalone protection techniques implemented using the features available in the user-terminal.

Assess assisted-based authentication and fine synchronization techniques

Develop and assess different key management schemes for future services

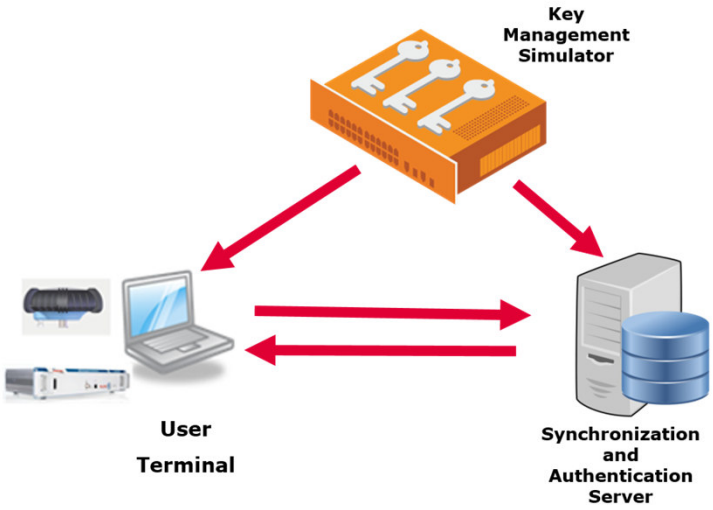


NACSET PLATFORM OBJECTIVES

Objectives

Demonstrate the achievable performances at PVT-level taking advantage of the authentication and synchronization information provided by the implemented techniques.

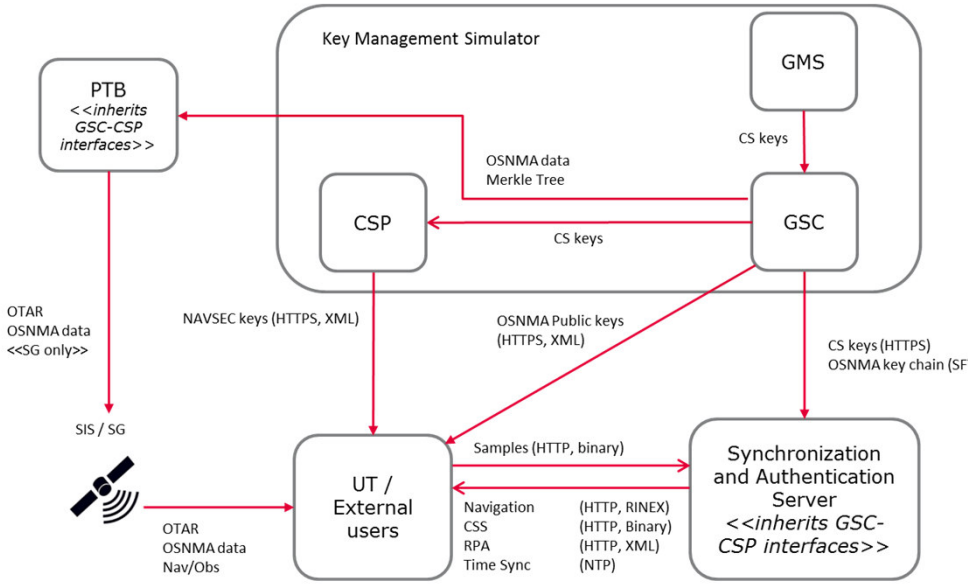
Define and carry out an experimentation campaign aiming to test the performances of the end-to-end system and the implemented techniques in standalone and combined modes. It shall consider simulated and real signals, in nominal and under-attack conditions.



PLATFORM OVERVIEW

Main Elements

1. **Galileo CS Resilient PVT Platform (CS-RPP):**
   - **User Terminal (UT)**
   - **Synchronization and Authentication Server (SAS)**
2. **Key Management Simulator (KMS)**
3. **CS Signal Generator and Threat Simulator (SG)**

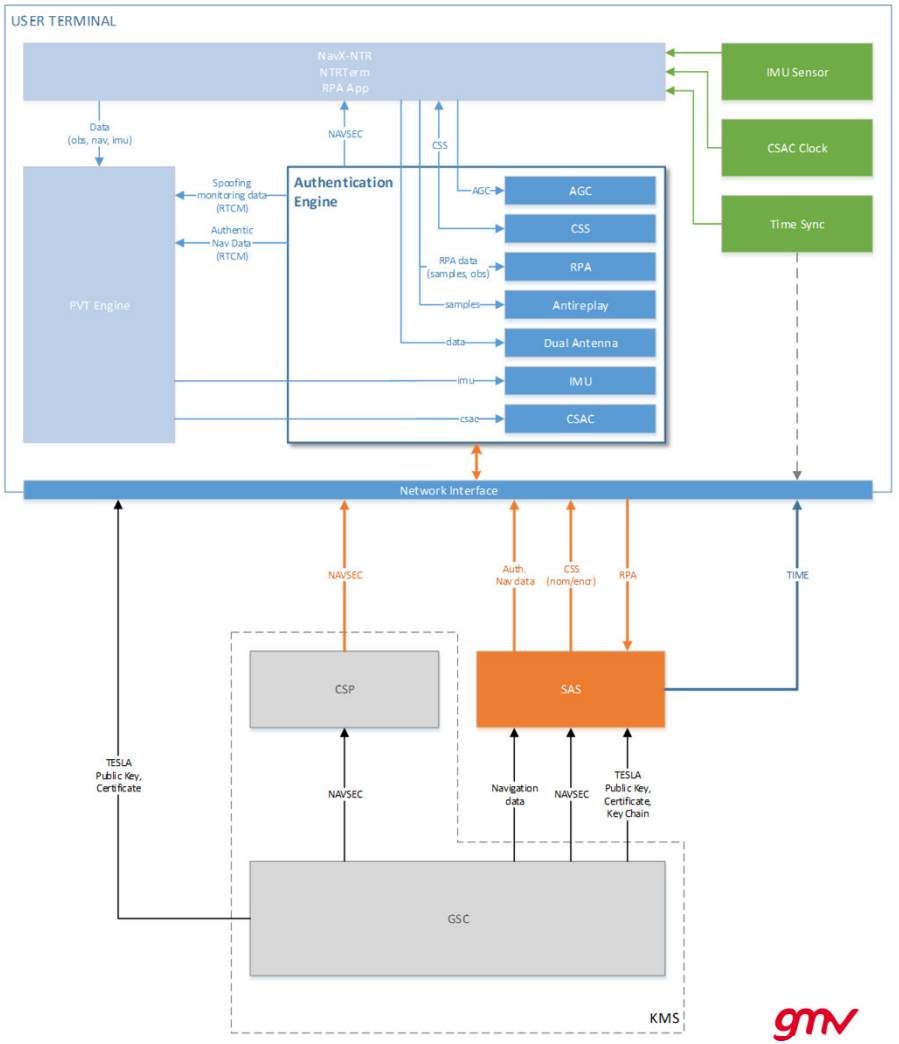


CSRPP OVERVIEW

UT and connections

High-level logical connections scheme, with particular focus on the links with the Authentication Engine.

Data exchange with the infrastructure that includes the SAS, CSP and the GSC.



CSRPP OVERVIEW

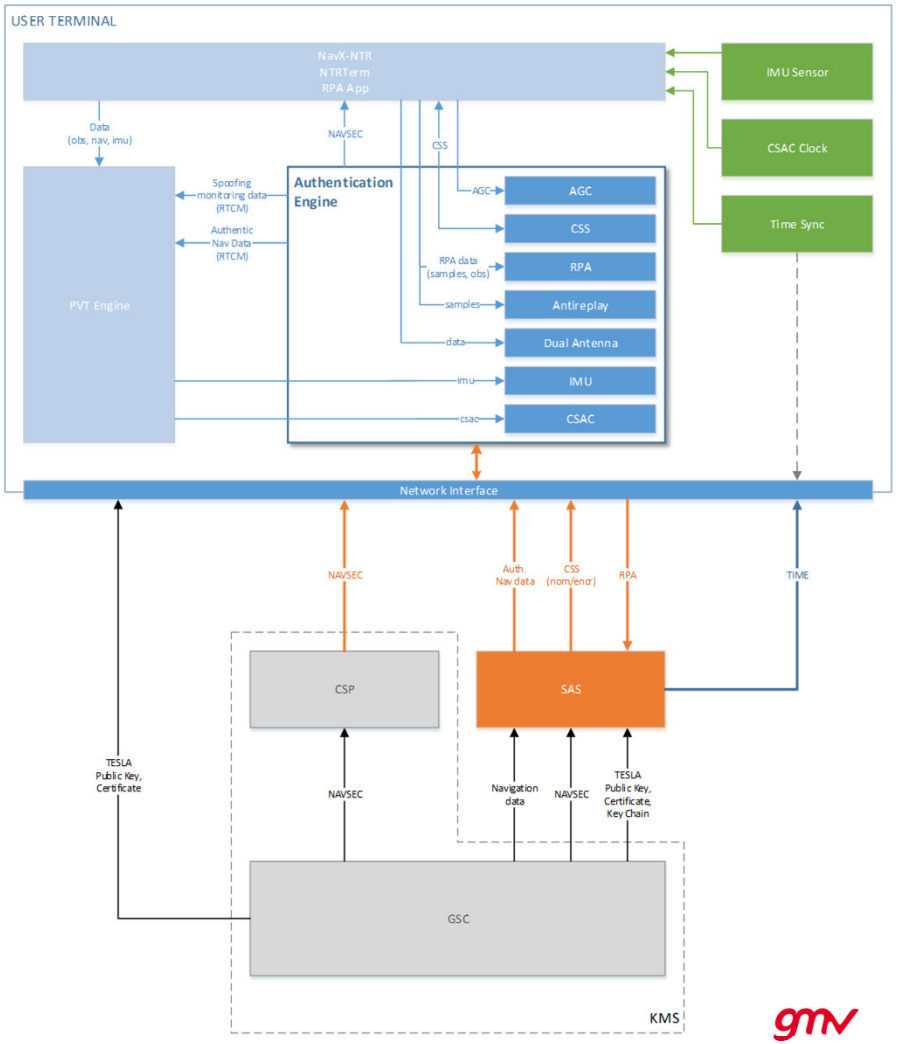
UT Techniques

Autonomous:

- **Dual Antenna Spoofing Detector:**
- **IMU Spoofing Detector**
- **CSAC Spoofing Detector**
- **AGC Spoofing detector**
- **Anti-replay**

Remote server support:

- **CSS authentication (delay, multicast, re-encrypted)**
- **RPA authentication**



KMS OVERVIEW

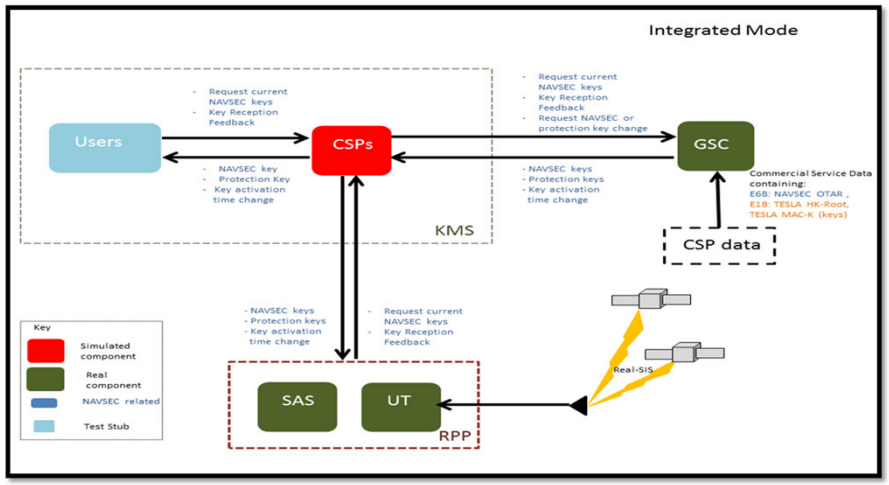
Key management simulator

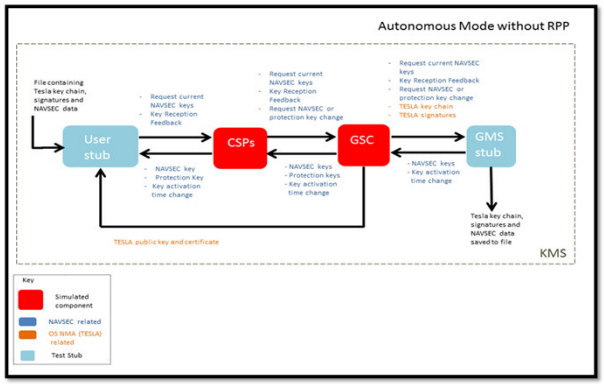
Main key management services simulated:

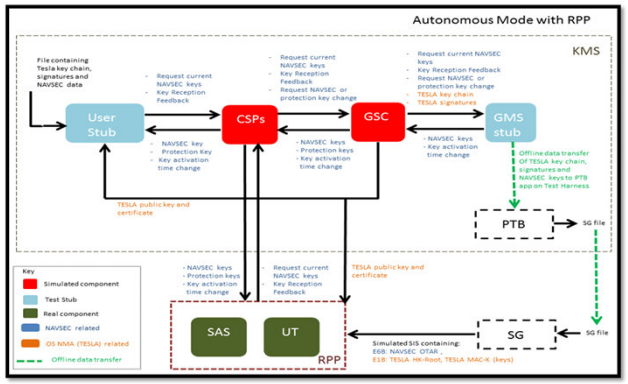
- CS encryption keys (NACSEC keys)
- OSNMA Keys (TESLA keys, public/private keys)

Allows testing:

- Fully autonomous
- Integrated with the CSRPP only
- Integrated with GSC



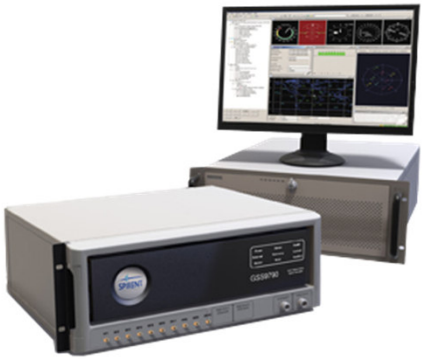




NACSET EXPERIMENTATION

CSRPP EXPERIMENTATION

The objective of the experimentation campaign is to be able to test the anti-spoofing techniques implemented in the CS-RPP in a controlled manner making use of real data (recorded or SIS) and simulated signals.



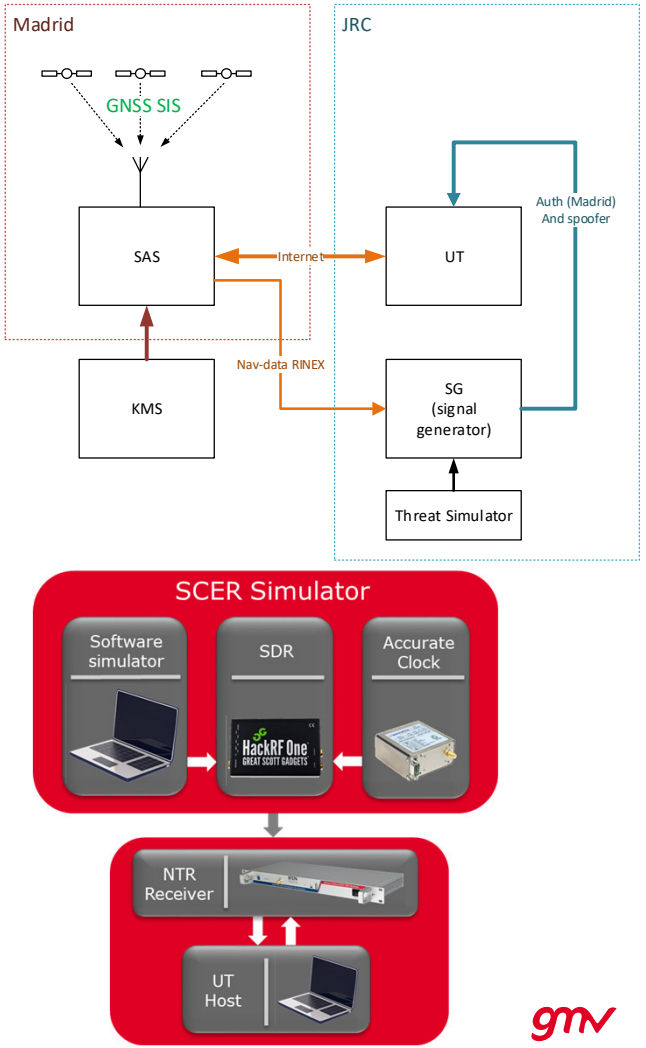
The CS-RPP experimentation campaign includes:

- **Testing the system in nominal conditions using real SIS or simulated data.**
- **Testing the system under attack conditions simulating the spoofing attacks with in-lab testing. The threats to be simulated under the NACSET experimentation campaign will be the following:**
  - Data bits manipulation spoofing attacks
  - Observables modification spoofing attacks
  - Spreading sequences and carrier generation attacks
  - Meaconing attacks

CSRPP EXPERIMENTATION

Experimentation performed between GMV (Madrid) and JRC (Ispra)

- Test were executed with simulated signal and real SIS to tests all the user techniques implemented under spoofing condition
- Different setups developed to be able to simulate all the authentication services together with synchronization services and under spoofing attacks
- Spoofer simulation capabilities developed in the Project, especially to simulate SCER attacks
- First test setup with reencrypted sequences using simulated OSNMA data successfully tested



CSRPP PROTECTION TECHNIQUES CONCLUSIONS

Technique	Advantages	Disadvantages
Remote Processing Authentication (RPA)	Trajectory spoofing is optimally detected. Not needed NAVSEC keys at UT to take advantage of the E6 encrypted signals.	Not autonomous, needs an external service. Bi-directional communication with users. Not able to detect timing spoofing
Cheap Spreading Sequences (CSS)	Not needed NAVSEC keys at UT to take advantage of the E6 encrypted signals. Good performances detecting spoofing.	Latency on the reception of the CSS is critical for the system. Not practical to provide service for many users.
Re-encrypted CSS	Good performances detecting spoofing. Not needed NAVSEC keys at UT to take advantage of the E6 encrypted signals. Can store long batches of CSS without compromising the system. Compatible with OSNMA service.	Latency increased by the decoding of the TESLA keys from the SIS. Service availability depends on the Open Service (OSNMA).

CSRPP PROTECTION TECHNIQUES CONCLUSIONS

Technique	Advantages	Disadvantages
CSAC monitoring	Very good performance to detect attacks when the receiver is tracking first the real signal. Autonomous technique, only needs the PVT computation.	Difficult to detect an attack in cold start conditions. CSAC are not available in standard receivers.
AGC monitoring	Fast at detecting different kind of attacks Simple to be implemented	Difficult to detect very complex attacks
Anti-replay detection	It is able to detect optimally very complex attacks like the zero-delay attacks. Provide signal replay protection without encrypting the signal. Compatible with OSNMA service. Does not degrade significantly in degraded environments.	Depends on OSNMA performances, without data authentication the scheme will not work. Need to be used with other techniques to detect simple attacks. Only focused on zero-delay attacks.

CSRPP PROTECTION TECHNIQUES CONCLUSIONS

Technique	Advantages	Disadvantages
Dual antenna	Very powerful technique to detect all kind of attacks as the spoofer is probably using only one source for signal transmission GPS+GAL compatible.	Needs at least two antennas separated less than the wavelength. If several spoofers are used, the attack will not be detected
IMU hybridization	Able to detect attacks even in cold start conditions. Autonomous technique.	The tightly couple approach may not be the most optimal to detect spoofing attacks. Attacks were the trajectory is modified progressively in small steps are difficult to detect.

KEY MANAGEMENT EXPERIMENTATION

The focus of the KMS Test Plan has been to verify the KMS simulation components compliance to requirement.

The focus of this experimentation campaign is to provide an enhanced assessment of the proposed NACSET Key Management solution architecture, to reflect on its fitness for purpose and try to identify possible enhancements or practices to complement the solution.

The experimentation was divided in two main services:

- CS Key Management
- OSNMA Key Management

Experiment Assessments
CS Key Integrity Rejection
CS Key Exposure
Recovery From CS Key Compromise
CS Receiver Scalability
Trust Levels & Crypto-Periods
OSNMA Key Integrity Rejection
OSNMA Key Exposure
Recovery From OSNMA Key Compromise
TESLA Key Size & Derivation Algorithm Analysis

KEY MANAGEMENT EXPERIMENTATION

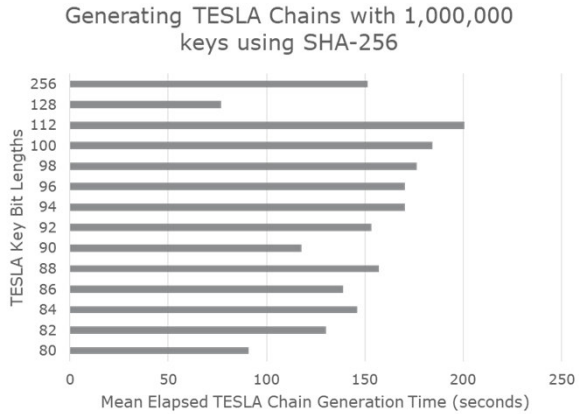
- **Galileo (GMS/GSC) approach provides a complete authentication and integrity mechanism**
  - Manual intervention of base media transmission

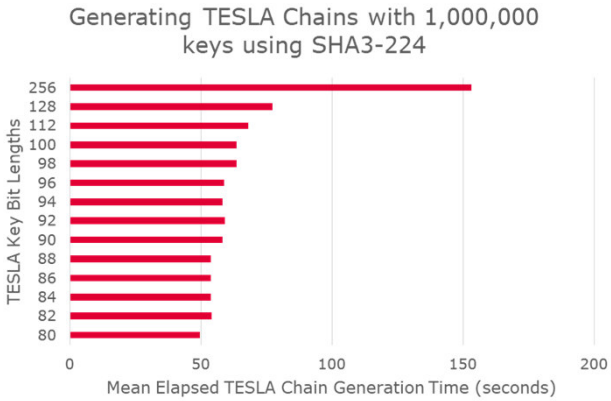
- **KMS crypto architecture provides strong protection against key exposure**
  - One-way key algorithms
  - Key revocation mechanism
  - Group trust policy for end receivers

- **Solution provides scalable receiver management**
  - Binary tree group key model provides exponential scaling of receiver grouping with linear impact on key renewal
  - KMS limited to binary key depth of 16 (supporting 32768 receiver groups) per CSP

KEY MANAGEMENT EXPERIMENTATION

- **CS NAVSEC crypto period recommendation of 1 – 10 days**
  - Emergency key replacement is operationally complex (synchronisation issues)
  - Frequent key replacement to prevent prolonged duration of potential misuse
- **Recommendation for TESLA key**
  - Additional protection of TESLA key chain delivery
  - Short key length with SHA-3 algorithm for scalable performance





PUBLICATIONS

PROJECT PUBLICATIONS

Conference	Title
ION GNSS+ 2017	Designing and evaluating next generation of resilience receivers
ITSNT 2018	ITSNT2018 Testing receiver resilience against signal replay attacks
ION GNSS+2019	Field Testing of GNSS Users Protection Technique

CONCLUSIONS AND WAY FORWARD

CONCLUSIONS

- **Key management simulator platform (KMS) has been developed, experimented and relevant feedback for Galileo have been proposed regarding key management schemes for Galileo authentications services**

- **A Commercial Service GNSS resilient receiver was successfully implemented including several state-of-the art protection techniques which enhance the experimental Galileo services**

- **Highlight achievements obtained specially with new mechanisms. Specially relevant**
  - Anti-replay technique which is the first implementation of replay attack protection based on the OSNMA service
  - Reencrypted sequences, which is a candidate for the future CAS service

CONCLUSIONS

- **Key management simulator platform (KMS) has been developed, experimented and relevant feedback for Galileo have been proposed regarding key management schemes for Galileo authentications services**

- **A Commercial Service GNSS resilient receiver was successfully implemented including several state-of-the art protection techniques which enhance the experimental Galileo services**

- **Highlight achievements obtained specially with new mechanisms. Specially relevant**
  - Anti-replay technique which is the first implementation of replay attack protection based on the OSNMA service
  - Reencrypted sequences, which is a candidate for the future CAS service

- **Recommendations for future work:**
  - Improve statistical analysis
  - Check different approaches for IMU data integration
  - Check different detector metrics for anti-replay technique
  - Additional testing in harsh environments
- **Final Review of the project on December 2019.**

Thank you

INNOVATING SOLUTIONS