Qascom
Trust is Nice, Control is Better.

DEFCON

Summary Report

Issue 1.00

Code	D101-ESA-QAS-DEFCON-SR
Document	Summary Report
Issue	1.00
Date of Issue	27/08/2021
Project	DEFCON
Project (full)	Dynamic tEstbed For seCur Open Service Navigation
Status	Authorized
Pages	14
Contract n.	4000123996/18/NL/CRS/as

UNCLASSIFIED
COMMERCIAL IN CONFIDENCE

QASCOM, Srl
Via O.Marinali 87, 36061 Bassano del Grappa (VI), Italy
Phone: +39 0424 525 473
Fax: + 39 0424 230 596
info@qascom.it
www.qascom.com

DOCUMENT CHANGE STATUS

Issue	Date	Change record
1.00	27/08/2021	First issue.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

1 PROJECT SUMMARY

1.1 OBJECTIVES

The risk of spoofing of the GNSS signals is increasing rapidly in different market segments such as workforce, fleet, traffic, asset management or due to a spill-over of military spoofing into civilian areas. This is due to the vulnerability of the GNSS signals and their widespread use, combined with the evolution of spoofing machines which nowadays can be realised with low-cost COTS devices.

In the last decades, the GNSS community has focused the attention on the study of potential solutions at system and user level capable to ensure robust and resilient PNT solution. ESA itself has been involved both with the TEC department, Galileo Evolution and G2G in several studies and programs for Galileo authentication.

DEFCON is an ESA project, led by Qascom in collaboration with the Universität der Bundeswehr München (UNIBW), Cillian O'Driscoll Consulting Ltd (CODC) and the Centre For Secure Information Technologies (CSIT) of the Queen's University Belfast. The scope of the DEFCON project was to go beyond state of the art of all authentication developments, explore new techniques, and identify new opportunities and ideas, still maintaining a baseline requirement of applicability to Galileo. All results are derived and supported by an end-to-end simulation including a constellation simulator and a GNSS receiver. In support to the stated work described, the project also extended and improved the tools to process and analyse the GPS P(Y) and the CHIMERA protocol.

1.2 KEY ACHIEVEMENTS

The DEFCON project has successfully hosted a comprehensive study on data and signal authentication protocols for the GNSS Open Service, taking as study cases Galileo and GPS to set reasonable and realistic system parameters.

The project firstly produced a detailed description of the state of art and a theoretical analysis of the fundamental elements of the GNSS signals that can be exploited for data and signal authentication.

The project also produced the detailed design of three authentication paradigms with the corresponding protocols and several possible configurations. The three paradigms are:

1. **SECUR**: authentication service based on encrypted signals, exploiting a remote server.
2. **SECOS-1**: data and signal authentication service based on two new signal components, one for data broadcast and one modulating an encrypted code. The data carries the digital signatures of the nav-data (e.g., the I/NAV message) and seeds for the reconstructions of the encrypted spreading code.
3. **SECOS-5**: data and signal authentication service based on one new signal component modulating a fully encrypted code. A hardware secure module (HSM) is used to verify the authentication tags computed on the data, and to reconstruct the encrypted code. The scheme presents a novel approach with the correlation of the encrypted code in the HSM, to improve the security of the receiver.

All the solutions have been developed using a SDR simulator, namely SECGEN, based on Qascom QA707. The corresponding reception chain has been developed adapting the MuSNAT software receiver from UNIBW; the SECUR verification process has been developed as well as an independent module.

Considering the solution SECOS-5, this activity represents the first successful implementation of an open service authentication with a symmetrical approach, designed to fit a SIM card. From the generation side, the

SECGEN was interfaced with a microcontroller emulating a hardware security module (HSM); from the receiver side, the HSM was plugged and used not only to regenerate the authentication tags and the spreading codes, but also to compute the correlation with the signal. This is the first implementation of a receiver with open service signal authentication done within a HSM itself.

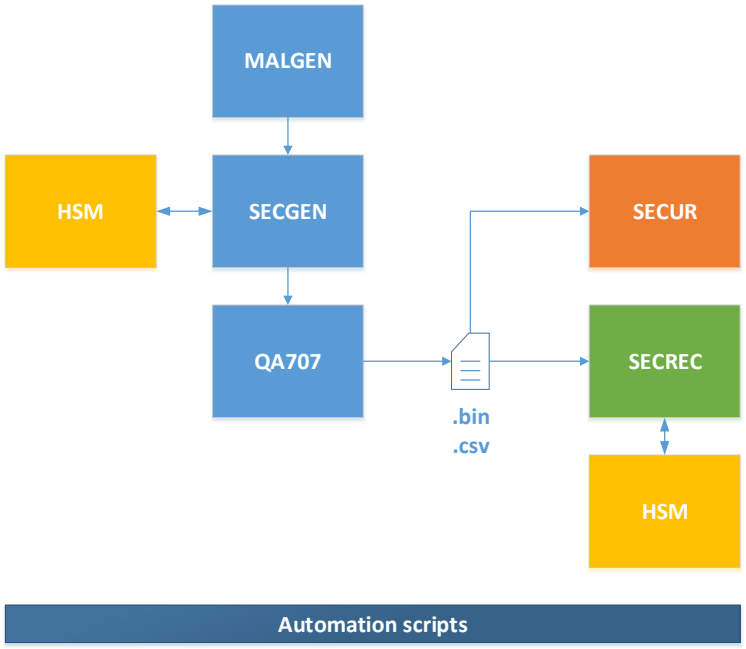

Figure 1-1: High-level architecture of the overall simulation and testing environment.

The tools have been extensively used to test the authentication solutions and to assess the receiver performance in AWGN and LMS (Land Mobile Satellite) environment conditions.

The results have been used to furtherly improve the protocol and the overall performance: for example, one of the main outcomes was the necessity of improving the demodulation and decoding performance of the data channels to guarantee the availability also in harsh environment. Channel coding and data redundancy among the satellite were two viable options.

Considering the lessons learnt from the experimentation campaign in nominal conditions, the receiver concepts of operations have been drafted. In parallel, the analysis allowed to identify viable strategies for the execution of the authentication verification, and it also provided the statistical data necessary to model the false alarm probability and to derive detection thresholds.

In addition to tests in nominal conditions, the experimentation campaign also included tests in adversarial conditions, assuming the presence of some malicious transmitter capable to estimate the unpredictable symbols (data or chips) and retransmit them.

As final step of the project, the CHIMERA protocol proposed for GPS has been implemented and tested.

In summary, the DEFCON project proposed several authentication solutions studied for future generations of Open Service GNSS, taking as study cases Galileo and GPS to set reasonable and realistic system parameters. The authentication solutions have been developed using QASCOM GNSS simulator QA707, and the processing have been done using the software receiver MuSNAT from UNIBW and the SECUR tool. In addition, the CHIMERA protocol of GPS has been developed and processed using the same tools. Novel

authentication concepts have been developed, together with advanced tools that may help the future work towards the definition of new authentication services future GNSS systems.

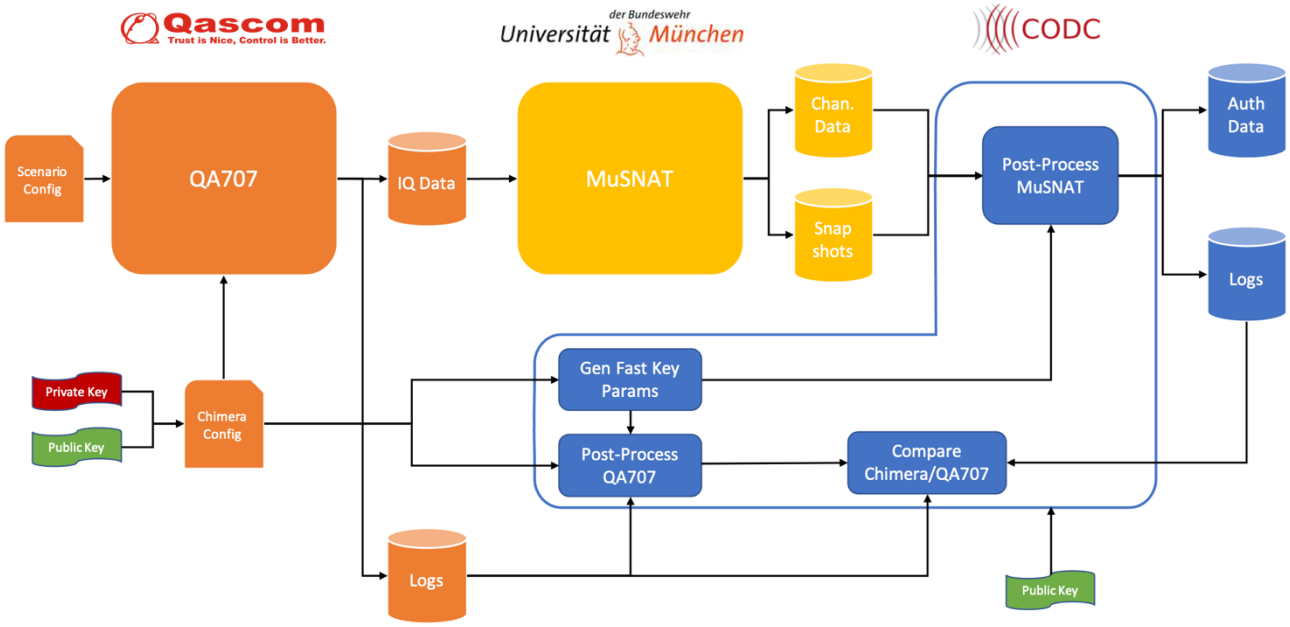

Figure 1-2: Evolution of the DEFCON tools for simulating and testing GPS CHIMERA.

1.3 PROJECT APPROACH

In the DEFCON project, the main activities have been conceptually divided as follows:

1. **[Analysis and design]** Preliminary analysis of the existing proposals for GNSS authentication, and analysis of the most promising techniques, beyond the state of art and the traditional approaches. This work eventually demonstrated that the fundamental element to be considered is the energy of the symbol/chip/bit, regardless the modulation type. Secondly, the message bandwidth reserved to authentication data is essential to achieve good authentication rates.

   From this analysis, 5 authentication techniques have been proposed, with several options. In the final stage, two main approaches have been selected.

   a. The first solution, named **SECOS-1**, is based on the full encryption of a dedicated signal component 10 dB weaker than Galileo OS, supported by the broadcast through SIS of the data necessary to reconstruct the secret sequence. Broadcast data is in turn modulated on a new data signal-component and protected by digital signature.

   b. The second approach, named **SECOS-5**, is based on the full encryption of a signal component, and the spreading code is generated and correlated within a smart-card, using symmetric schemes.

   In parallel to the study of the SECOS, a baseline scheme, **SECUR**, has been designed under the assumption that no modification is made to the GNSS system. This means that no new signals or navigation messages needs to be exploited. With those constraints, the SECUR has been developed to process existing fully encrypted signals, assuming that they are related to the open service in a deterministic way. One example is the signal of the Galileo Commercial Service.

2. **[Development]** The three approaches SECOS-1, SECOS-2 and SECUR have been fully designed and developed. They have been realized exploiting baseband signal simulation and processing, based on a customized software receiver and an emulated remote-processing service. The corresponding elements used in the project are:

    a. the **SECGEN** that is Qascom's QA707 SDR GNSS Simulator equipped with extensions for simulating the authentication signals, the channel impairments (named CHGEN), and the malicious signals (named MALGEN).

    b. the **SECREC** that is a customization of UniBW MuSNAT software receiver capable of processing the authentication signals.

    c. the **SECUR** that is a benchmark platform emulating a server-side service based on remote processing of GPS P(Y), as simulated by QA707 (random codes).

    Improvements of SECGEN and SECREC have been developed to generate and process the authentication signals and protocols and to interface with a microcontroller emulating a smart card. The latter element is the (d) **DEFCON-HSM**, implemented in the NUCLEO-F103RB, a STM32 Nucleo-64 development board with STM32F103RB microcontroller unit (MCU) from STMicroelectronics.

3. **[Experimentation]** All the authentication techniques have been tested in nominal conditions with no attack ongoing, under AWGN and LMS channel conditions. The urban model has been used for the LMS channel and results showed the main limits, mostly related to the data channel. In particular, the high number of errors in the decoding process causes availability drops, when every satellite broadcasts its own data. For this reason, the data protocol has been improved using shared data among the satellite, with great benefit in term of availability; additional improvements have been furtherly proposed to optimize the data protocol, with slower broadcast to allow more energy per symbol, or longer messages to improve turbo decoding capabilities.

The approach here described has been used to identify two possible and viable solutions to implement authentication of the GNSS signals, not just for the data but also for the ranging. The solutions have been analysed and designed considering the state of art of GNSS as presented in the literature.

As a final step, the project also analysed in detail the alternative solution for GNSS open service authentication, currently proposed for GPS, which is CHIMERA. To this aim, the simulator SECGEN has been furtherly improved to simulate the GPS L1C signals and the full CHIMERA protocol, including the authentication broadcast data and the watermarking component. In addition, the SECREC has been upgraded to process GPS L1C and a CHIMERA post-processing tool has been developed.

2 AUTHENTICATION SOLUTIONS

This section reports a summary of the authentication techniques developed in the DEFCON project. It is remarked that the project documentation reports:

- The detailed design, with development considerations.
- An extensive report of the performance in realistic navigation conditions and under spoofing attack.
- A preliminary analysis of the concepts of operations at system and user level.

2.1 SECUR

2.1.1 DESCRIPTION

The motivation for the SECUR scheme is to establish a baseline authentication mechanism, requiring no modifications at system side, against which all other schemes can be compared. This necessitates taking advantage of the existing signal-in-space and utilising existing communications infrastructure. The first major drawback of SECUR is that it can never be a standalone GNSS scheme but will rely on the availability of a reliable (two-way) communications channel with the authentication server.

SECUR is a remote processing authentication approach wherein the User Terminal (UT) tracks an existing open service and takes occasional snapshots of the sampled RF spectrum containing an encrypted signal synchronized with the open one. The snapshots are annotated with the C/A tracking information (pseudorange, Doppler, phase, C/N_0) and are transmitted over a standard wireless communications channel to a trusted Authentication Server (AS). The AS has knowledge of the chips (either through access to a security module, or by estimating the chips by other means) and uses this knowledge to cross-correlate the raw samples received form the UT and, hence, to detect the presence of the encrypted P(Y) signal. This service provides signal level authentication only, but it is to be assumed that the AS has access to an authenticated navigation message, for example, by comparing navigation messages received from a variety of observation stations distributed over a wide geographic area.

2.1.2 DATA GENERATION

SECUR requires no extra data generation by the system.

2.1.3 DATA PROTECTION

SECUR provides no protection of the navigation data, however, the AS component must have a mechanism to obtain clock and ephemeris data that it considers trustworthy.

2.1.4 RANGING PROTECTION

The ranging protection provided by **SECUR** is based on the unpredictability of the encrypted code. To prevent a replay attack, an additional constraint can be placed on the UT requiring that the snapshot samples be received at the AS within a short (100 ms) time frame. This puts an extra constraint on the attacker, requiring them to estimate, re-generate and broadcast a spoofed/replayed signal within a short period of time.

2.2 SECOS-1

2.2.1 DESCRIPTION

SECOS-1 is a combination of:

- **Navigation Message Authentication (NMA)** for the protection of the navigation messages, specifically INAV data broadcast on Galileo E1-B (and E5b).
- **Autonomous Spoofing Protection (ASP)** or Anti-Reply Protection (ARP) for the protection of the ranging measurements.

The protection of the navigation messages is based on digital signature. The ASP protection is achieved through a combination of:

- Full encryption,
- Partial encryption (watermarking),

where the cryptographic data for the reconstruction of the signal is provided with some delay (posterior verification). A summary of SECOS-1 is illustrated in Table 2-1, with its two sub-options.

Since the project uses Galileo GNSS signal parameters as case study, for sake of simplicity the GNSS signals which implements the SECOS solutions are called E1N. Figure 2-1 shows the structure proposed for E1N signals, in parallel with legacy Galileo signals which are all broadcast on the E1 centre frequency.

	Option	Data component				ASP Service		
		Power [dBW]	NMA for data	NMA for SCA seed		Modulation	Encryption	Power [dBW]
			Sign. Size [bits]	Seed Size [bits]	Sign. Size [bits]			
SECOS_1	A	-160	912	128	512	BPSK(1)	Full	-170
	B	-160	912	128	512	BPSK(1)	Watermark	Part of data

Table 2-1: SECOS-1 proposed scheme.

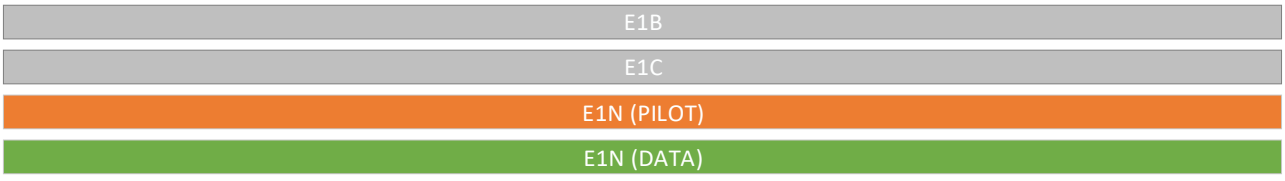

Figure 2-1: Broadcast signal components.

2.2.2 DATA GENERATION

For the combined protection of data and ranging signal, the available bandwidth in E1-B is considered not adequate. Therefore, a new signal component is proposed specifically designed for broadcasting the authentication data. Another signal component is also proposed for ranging protection.

2.2.3 DATA PROTECTION

This scheme protects the navigation data, and the spreading code seeds with EC-Schnorr digital signature. The specific implementation selected within the project is EdDSA available in OpenSSL. In detail, the following curves have been used:

- **EVP_PKEY_ED448** for the signature of the navigation data (NMA),
- **EVP_PKEY_ED25519** for the signature of the ASP seed.

The curve chosen for NMA provides a security level of 224 bits. The curve used for the signature of the ASP seed has a security level of 128.

It is remarked that the initial plan was to target a security level of 256 bits. The reduction has been discussed and agreed to reduce the impact on the bandwidth usage. This has been traded off especially for the ASP seed whose life is very short, in the range of some seconds, and the corresponding signatures need to be recomputed and broadcast frequently.

In all cases, a security level of 128 bits is today considered the minimum for a service targeting a lifetime of 20/30 years, therefore the choices are considered adequate. Considerations on the quantum risk have been done, however in the scope of the project no post-quantum techniques have been chosen for the digital signature algorithms that are known to be un-secure when attacked with specific algorithms designed for quantum computers.

2.2.4 RANGING PROTECTION

The ranging protection is provided by the ASP component. A summary of the two ASP options is given below:

A. Option A uses a lower power signal with full encryption (the random sequence is generated iteratively using block/stream cipher).
B. Option B is based on a partial encryption where part of the spreading code carrying the data component are encrypted at spreading code level (based on a block/stream cipher).

2.2.5 CONSIDERATIONS

For the solution SECOS-1, considerations on the proposed design shall be evaluated for the implementation in the signal in space:

1. The ASP component has been designed and implemented with BPSK(1). This choice is motivated by the reduced sensitivity with respect small misalignment due the tracking of the pilot component in harsh environment and the necessity of having a signal that could be generated and processed with optimized power consumption. For both conditions, requirements from the applications and from the manufactures shall be considered to feed the design process.
2. The capability of correctly decoding the bits of the authentication data component is crucial for the availability of the service. This is the reason why the seed for the generation of the ASP component is shared among all PRNs. However, this limitation can affect the proper reception of the signature of the navigation data, which is different for every satellite. Therefore, again considering the requirements of the service imposed by the applications or other analysis, the energy per data symbol should be increased.

2.3 SECOS-5

2.3.1 DESCRIPTION

SECOS-5 is a combination of:

- **Navigation Message Authentication (NMA)** for the protection of the navigation messages, specifically INAV data broadcast on Galileo E1-B (and E5b).
- **Autonomous Spoofing Protection (ASP)** or Anti-Reply Protection (ARP) for the protection of the ranging measurements.

The protection of the navigation messages is based on Message Authentication Codes (MACs). The Anti-Spoofing Protection (ASP) is achieved through spreading code encryption and low broadcast power. The authentication service is supported by a physical hardware security module (HSM), such as a smart card or secure processor. The protocol is served by a symmetric scheme, where the keys are stored within the smart card allowing fast, energy efficient algorithms to be used.

SECOS-5 scheme foresees that the HSM provides the keys for verifying the signature of the navigation data. The ASP verification is done correlating the signal with the encrypted spreading code. In SECOS-5, the correlation process is physically performed inside the HSM, to prevent any leakage of secret data.

Figure 2-2 shows the ASP signal in parallel with legacy Galileo signals, which are all broadcast on the E1 centre frequency.

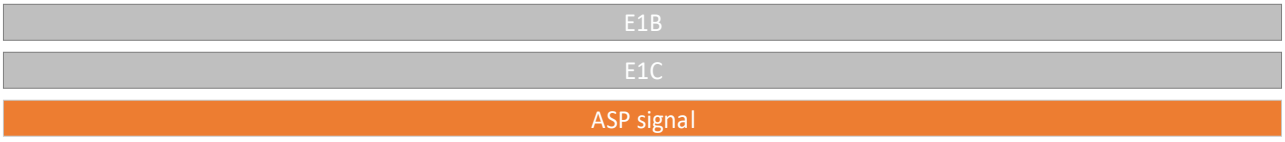

Figure 2-2: Broadcast signal components

2.3.2 DATA PROTECTION

This scheme protects the navigation data with symmetric MACs using a pre-shared secret key stored on a HSM such as a smartcard or secure processor. For the navigation data a security level of 128-bits has been selected, which is deemed sufficient given the expected lifetime of the system, as well as the short lifetimes of each message verification tag. The MAC function used is the HMAC-SHA-256, which provides the required 128-bits of security using the keyed-hash message authentication code (HMAC) construction and the secure SHA-256 hash function.

The MACs are delivered through the legacy Galileo signal E1B.

2.3.3 RANGING PROTECTION

The spreading code is generated in the HSM using the AES block cipher in counter mode. AES-CTR-128 operates as a stream cipher to output the required encrypted chips that can be mixed with the received signal in order to verify its authenticity. The spreading code is fully generated by the smart card once the time and identity (PRN) of the satellite are received.

In SECOS-5, the baseband correlation is performed within the HSM such that the derived encrypted spreading code never leaves the security boundary.

2.3.4 CONSIDERATIONS

The development of a service based on a smart card imposes constraints on how the critical data is used, stored, and renewed in the hardware device. In this case, depending on the requirements of the application, the lifetime of the keys should be modulated accordingly, and renewal policies shall be specifically designed. For example, the smart card should have a well-defined lifetime and when expired it shall be substituted. In any case, tamper resistant technology shall be adopted, and for this reason the ST33 platform has been proposed.

Additionally, the service is highly dependent on the technology because the data exchange and processing power impose limits on the overall authentication performance, device complexity and power consumption.

END OF DOCUMENT