



NEWSLETTER

Security Assessments for Networks and services in 5G

Welcome to the first issue of our Newsletter, where we aim to give you information on the SAND5G Project and its objectives. We describe the Challenges and the Pilot Use Cases and give you an update on our latest news. Stay tuned!

01.

7 Partners in Greece

02.

Funded by the European Union

03.

36 month project

Don't forget to subscribe so that you can receive our next issues!

[SUBSCRIBE](#)

Our Aim

The project aims to support: a) 5G stakeholders secure their systems and services; b) National Authorities and Member States' Regulators overview the security status and applied measures that implement their national cybersecurity strategies and legislation, in line with European 5G cybersecurity policies and proposed EU toolbox for 5G security.

Our Objectives

01.



Build a risk and impact assessment platform aligned with the EU toolbox for 5G security to ensure high levels of security and compliance with EU and national policies and legislation.

02.



Support National Authorities and Regulators implement their national cybersecurity strategies and legislation, in line with European 5G cybersecurity policy.

03.



Support knowledge and capacity building for relevant 5G stakeholders and their users.

04.



Validate the SAND5G platform across diverse cases and scenarios including 5G infrastructures, services, regulators, authorities etc.

05.



Engage the 5G EU industry and policy makers and guarantee sustainability of all developed solutions, tools, and training activities, beyond the end of the project.

The challenges we face

01.

European Union and its Member States need to approach cybersecurity in a comprehensive and strategic manner.

02.

In addition to enhancing resilience against supply chain attacks conducted via cyber means, it is equally important to strengthen overall resilience.

03.

Encourage Member States to work towards avoiding similar situations of unwanted strategic external dependencies in relation to ICT products and services and recognize the avoidance of vendor lock-in and the diversification of ICT suppliers.

04.

Emphasize the role and relevance of both the strategic and implementation tasks of the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centers (ECCC).



Pilot Use Cases

Use Case 01. 5G Infrastructure University of Patras & p-NET

The following will be validated for the 5G infrastructure:

- a) a complete risk and security assessment over the final 5G infrastructure (with all the new monitoring agents and security components installed) and with its security posture against a set of attacks that will be defined during the trials' setup activities;
- b) a complete risk and security assessment after the deployment of the two vertical services on top of the 5G infrastructure.

Use Case 02. Solutions for Digital Health & Wellness WINGS & OQ Technology

STARLIT is WINGS' digital health and wellness product that is a cloud-based platform powered by AI/ML, IoT, advanced wireless networks (including 5G), and, in special cases, other emerging technologies (such as AR/VR). Security is critical in such cases so as to ensure data privacy of those in need and which only personnel with correct authorization can access.

OQ Technology offers organizations the ability to develop and vertically integrate a satellite manufacturing plant from system engineering and design of COTS subsystems to integration and testing facilities. Within SAND5G, two possible network architectures for OQ satellites are proposed to be evaluated for the pilot:

- a) Transparent payload Satellite (3GPP Release 17) where the gateway facilitates satellite connection to the network
- b) Regenerative payload Satellite (Future 3GPP Releases) where Smart Satellites equipped with SDRs act as base stations.

Use Case 03. Regulators and National Authorities Hellenic Authority for Communication Security & Privacy (ADAE) and Ministry of Digital Governance

The National Authorities will be able to collect information and perform actions related to the various SAND5G instances connected to their –Special Regulatory SAND5G instance. Through this instance, the SAND5G project will evaluate various capabilities such as the level of security posture across an area, aspects for coordination and collaboration during the preparation or an incident, timing in identifying response and attack alerts.

Our latest News

SAND5G @ DSD 2024 Conference

SAND5G was presented during a Special Session on 'European Projects in Digital System Design' at the DSD 2024 Conference, held in Paris, France.

During the networking sessions, engaging discussions took place on the project and 5G security, involving researchers and professors. The conference proceedings will be available soon!



Key Facts

Project No.	101127979
Project Name	Security Assessments for Networks and services in 5G
Project Acronym	SAND5G
Call	DIGITAL-ECCC*-2022-CYBER-03
Topic	DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE
Type of Action	DIGITAL-JU-SIMPLE
Service	CNECT/H/01
Starting Date	1 January 2024
Duration	36 months

Deliverables submitted

- D1.1 Data Management Plan
- D1.2 Project Handbook
- D2.2 SAND5G requirements and architecture
- D5.1 Plan on Dissemination, Exploitation, Standardisation & Sustainability

Consortium

7 Partners in Greece



HELLENIC REPUBLIC
Ministry of Digital Governance

Follow us



The SAND5G project, "Security Assessments for Networks and services in 5G" has received funding from the European Union's Digital Europe programme under grant agreement No 101127979 and is supported by European Cybersecurity Competence Center. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.