


Consortium

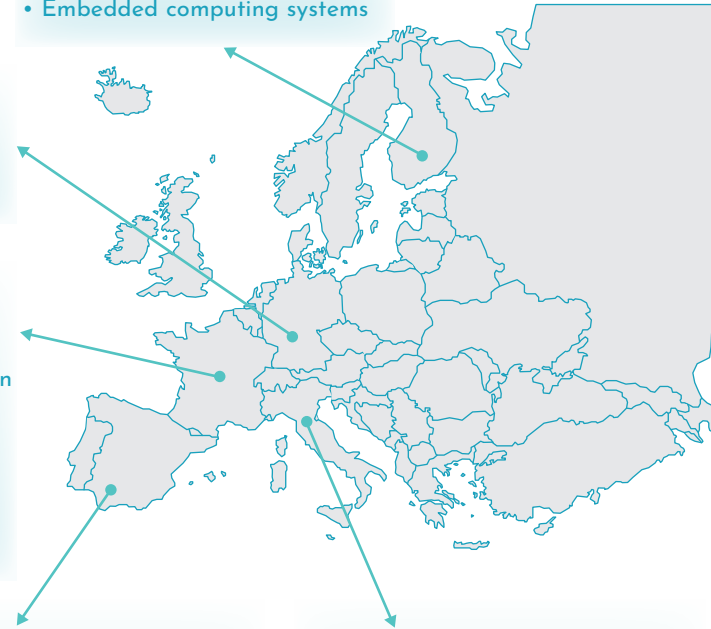


 Tampere University
• Software authenticity
• Embedded computing systems

NEC
• Validation in 5G networks

**list**
c2i tech
• Embedded systems, SoC design methodologies

THALES
Building a future we can all trust
• RISC-V core



**CSIC**
(coordinator)
• Hardware security
• Privacy-respectful protocols

 Telefónica
• Network infrastructure protection

 Politecnico di Torino
• Remote attestation protocols

**links**
PASSION FOR INNOVATION
• IoT systems /IoT interactions
• Validation in Industry 4.0

NEXT
S.p.A.
• Validation in Industry 4.0

**SECURE PLATFORM
FOR ICT SYSTEMS
ROOTED AT
THE SILICON
MANUFACTURING
PROCESS (SPIRS)**



Website



The SPIRS Project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement N° 952622

Brief Info

SPIRS

Grant agreement ID: 952622

Start date: 1 October 2021

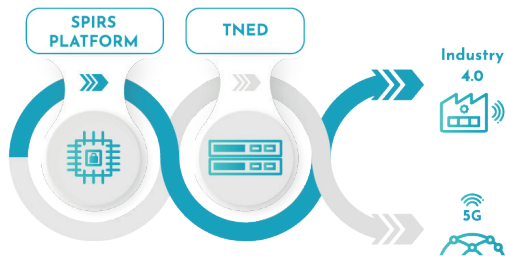
End date: 30 September 2024

Funded under: H2020-EU.2.1.1. INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)

Overall budget: € 5 041 091,25

Coordinated by: AGENCIA ESTATAL CONSEJO SUPERIOR DE INVESTIGACIONES CIENTIFICAS

 @SPIRSProject  SPIRS Project
 SPIRSProject



Concept

Our society is continuously demanding more and more intelligent devices, along with network infrastructures and distributed services that make our daily lives more comfortable. This revolution has also reached the industrial sector, transforming traditional factories into smart factories, with the objective of enhancing supply chain and manufacturing. However, the frantic adoption of Internet of Things (IoT) technologies in multiple application domains has led to widespread implementations without a deep analysis about the vulnerabilities that IoT devices are exposed to.

SPIRS addresses innovative approaches to provide security and data-privacy to future Information and Communications Technology (ICT) elements.

SPIRS encompasses the complete design of a platform, so-called SPIRS platform, which integrates a hardware dedicated Root of Trust (RoT) and a processor core with the capability of offering a full suite of security services. Furthermore, the SPIRS platform will be able to leverage this capability to support privacy-respectful attestation mechanisms and enable trusted communication channels across 5G infrastructures and the respective management domains.

RoT is implemented in hardware with a dedicated circuitry to extract a unique digital identifier for the SPIRS platform. A silicon CMOS Physical Unclonable Function (PUF)

is used to derive the device's identity. To build a complete solution, the project also features a Trusted Execution Environment (TEE), secure boot, and runtime integrity on a RISC-V processor core. Furthermore, SPIRS endeavours to the design of a blockchain-based decentralized trust management framework targeted to minimize the impact of Single Point of Failure (SPOF) risks and achieve adequate security and privacy trade-offs.

The project goes beyond the construction of the SPIRS platform and it provides solutions to integrate it in the deployment of cryptographic protocols and network infrastructures in a trustworthy way, leveraging the RoT provided by the platform. This includes the implementation of chains of trust for remote and direct anonymous attestation, and its integration with network orchestration mechanisms endorsing security and privacy protection in edge and cloud infrastructures. The SPIRS project will extend existing open-source network orchestration frameworks to demonstrate the applicability of these trusted anchors and attestation procedures in the development of IoT network gateways building a Trusted Network Edge Device (TNED).

SPIRS can be integrated in multiple sectors. To validate this, the project plans to demonstrate its results considering two different scenarios: Industry 4.0 and 5G networking.

Objectives

The main goal of SPIRS is to establish chains of trust rooted at the silicon manufacturing process for ICT systems, and apply them to improve the supply chain for networked infrastructures.

Objective 1.

Design of a platform with a tamper-proof silicon RoT.

Objective 2.

Design of a TEE using the silicon RoT.

Objective 3.

Integration of the platform into network infrastructures using the silicon RoT.

Objective 4.

Implementation of the platform.

Objective 5.

Evaluation of the platform in different scenarios: Industry 4.0 and 5G Communication Infrastructure and management systems.

