SPIRS was officially kicked off on 1st October 2021. During the first year of activities, the Consortium has made important progress in several technical Work Packages (WPs).

WP2 - Design of a silicon Root-of-Trust

The Root-of-Trust (RoT) initial components are:

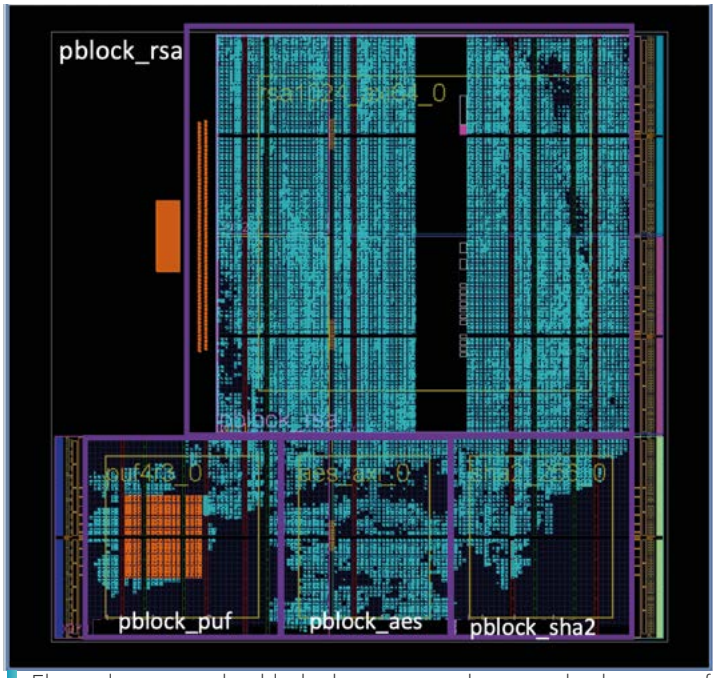
- A Physical Unclonable Function (PUF) to retrieve digital identifiers and generate random numbers.
- AES-256 as symmetric cipher for data encryption and decryption.
- SHA-2 (256) as hashing algorithm.
- RSA-2048 to generate and verify digital signatures.

RO-PUF design offers a compact and efficient implementation that has been evaluated to retrieve digital identifiers and generate TRNGs using different test systems. The performance of the PUF has been evaluated under temperature and voltage variations of the supply source.

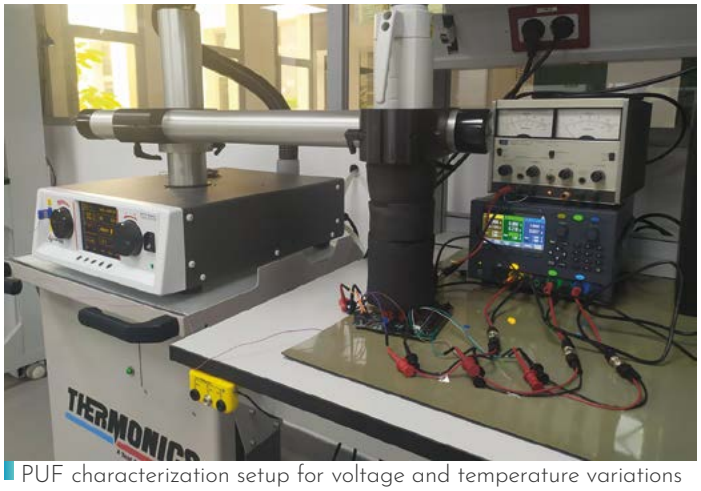
The proposed architectures for **AES**, **SHA-2**, and **RSA** algorithms provide area optimized implementations, which have been verified using NIST validation testing programs for cryptographic algorithms.

All RoT components have been encapsulated as IP cores and use a standard communication interface based on the AXI4-Lite bus to ease their characterization and re-usability on different System-On-Chips (SoCs). Low and high-level drivers are provided to facilitate the development of user applications for all RoT components. These drivers include routines to provide inputs to each RoT component and access to its corresponding responses.

A demonstrator that shows the design flow to implement a test system including several RoT components, as well as simple functions and applications to corroborate all RoT components will be available to the community.



Floor planning with pblock directives used to set the location of PUF/TRNG, AES, SHA-2 and RSA IP cores, and FPGA resource distribution



PUF characterization setup for voltage and temperature variations

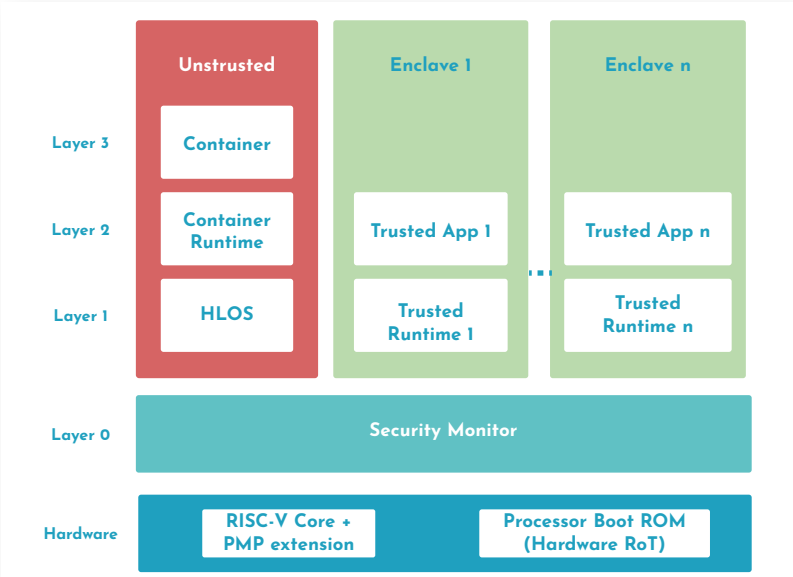
The SPIRS Project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement N° 952622

Follow us

WP3 - Design of a Trusted Execution Environment
WP4 - Integration into network infrastructures

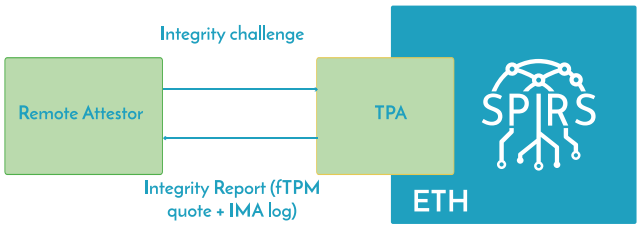
The Trusted Network Environment for Devices (TNED) is a framework developed for the SPIRS platform capable of running a Trusted Execution Environment (TEE) by providing a set of communication interfaces and access to the RoT for attestation purposes. Current SPIRS TEE implementation is based in RISC-V, running a Security Monitor (SM), which provides an Application Programming Interface (API) so Trusted Applications (TA) can run in a protected environment while having a communication with the applications running in the untrusted side of a device.

SPIRS platform is a multi-component system which can be modelled through a layered architecture. The architecture allows us to adopt the Device Identifier Composition Engine (DICE) standard proposed by the Trusted Computing Group (TCG) which provides a secure identity to the devices that are not equipped with a Trusted Platform Module (TPM) chip. In the SPIRS platform the DICE specification is applied to associate to each platform level its Compound Device Identifier (CDI) leveraging the RoT. This approach ensures reliability of transitions between components that are part of the Trusted Computing Base (TCB) of the platform and provides secure identities to the platform components both for remote attestation and the creation of trusted communication channels.



SPIRS plataform layered architecture

Secure boot. Divided in two phases, the Secure Boot of Security Monitor (Layer 0) and the Secure Boot of HLOS (Layer 1). The first one is performed by the code stored in the DICE boot ROM and executed at system startup. The Secure Boot of the HLOS is performed by the SM, which carries out some measurements into the kernel image, data configurations and boot parameters, so they can be compared by the reference values (considered trusted before launching the HLOS).



HLOS remote attestation

Firmware Trusted Platform Module (fTPM). It takes advantage of the system file measurement capability, made available by the Integrity Measurement Architecture (IMA) module which is provided by the Linux kernel. This will be used to monitor what is happening in the untrusted world so an external malicious entity (which may exploit any flaw present in the TEE libraries) can be detected as soon as possible. It will be running directly on the CPU, in a protected execution environment separated from other programs and is accessible by the IMA module through a specific driver (fTPM driver) added to the HLOS kernel, in order to allow it to store the acquired measurements inside fTPM's Platform Configuration Registers (PCRs).

Remote attestation. It has the task of monitoring the software and configurations loaded into the SPIRS' HLOS. In the event of an anomaly detection, the Remote Attestor (RA) must send a notification to the other components so it can isolate the compromised platform and restore its security posture.

Governance schemes. This component defines a set of roles and permissions and tracks every modification of the state of the entities taking part in the system. It is based on a Distributed Ledger Technology (DLT) which allows users of the system to retain a certain degree of anonymity providing they are not a malicious entity. In those cases, the established agreement will be broken revoking the anonymity.

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

Follow us

WP5 - Platform integration

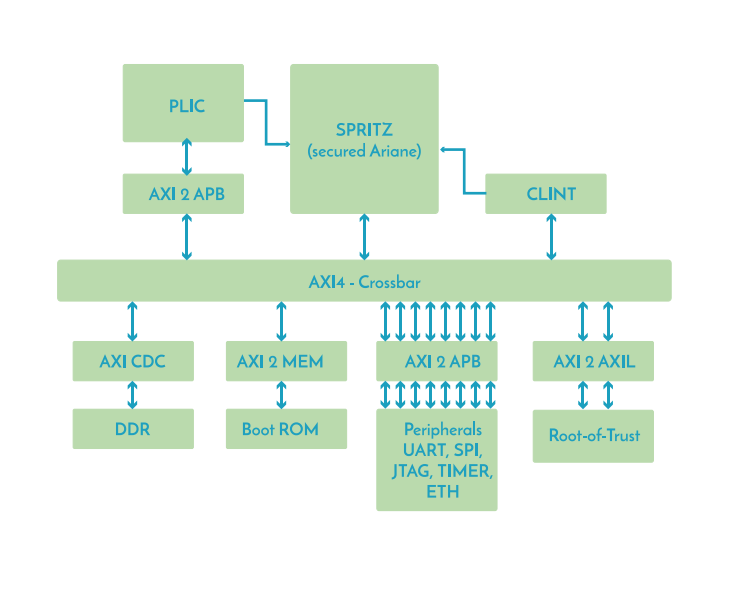
SPIRS platform is being developed using the Genesys 2 development board. The main milestones of the development are:

- Integration of the hardware IP modules of RoT
- Integration of a RISC-V secure processor
- Software validation of the platform integrating the secure processor and the RoT

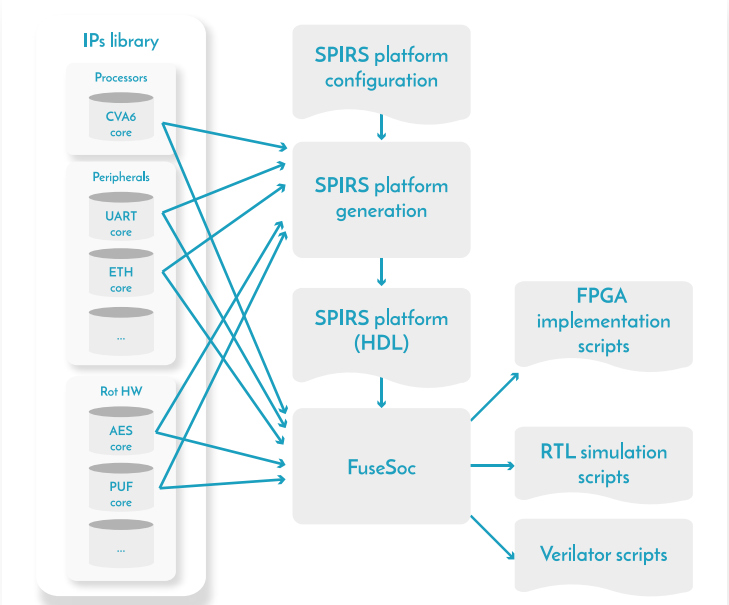
Methodology and tools to automate the design of the SPIRS platform

We are evaluating existing open-source tools:

- FuseSoC (as a package manager)
- Litex (as an example of a platform generator)



Block diagram of the SPIRS platform



Methodology to automate the design of SPIRS platform under developent

WP6 - Validation of the platform

• Use Case 1 - Trust in Manufacturing Machine

The first use case focuses on the data exchange between the machines of a production line (e.g., pick-and-place machinery) and the monitoring Manufacturing Execution System (MES) server, which is designed to control and monitor the machines for the Surface Mount Device (SMD) production lines. The MES will be running the software application which provides a series of interfaces to handle the communication with the central database. At the moment, such communication lines are fully unprotected, making them vulnerable to attacks that would maliciously alter data as it is being transmitted. By installing an SPIRS Agent (SA) and handling the communication between the MES server and the machine controller through a TNED, it can be established a secure and trusted communication channel providing safe data exchange (e.g., components information, status of the machine, production information, etc.).

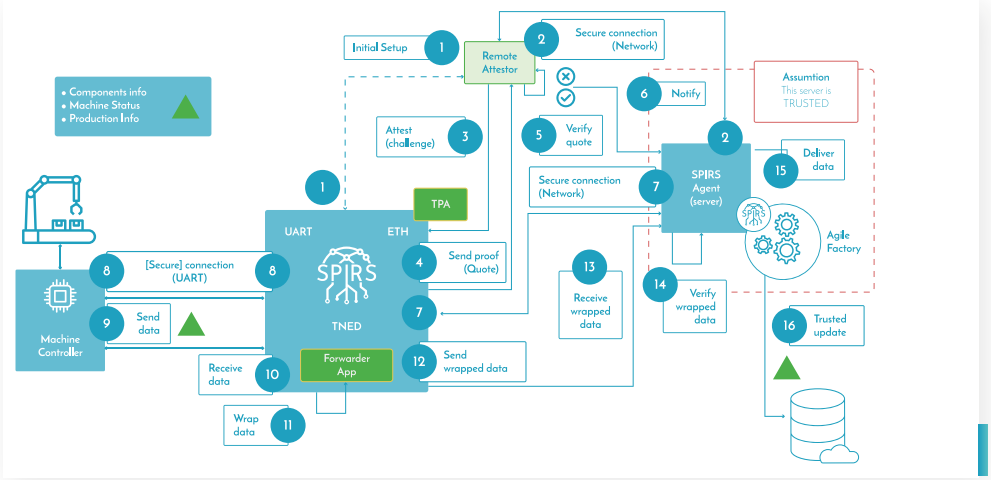


Illustration of operational steps for Use Case 1

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

Follow us

• Use Case 2 –Trusted Firmware Loading

Firmware (FW) pre-loaded on specific boards must be provided by the customers directly to the "manufacturer". During this process the software can be eavesdropped, which could lead to software stealing or even software manipulation for malicious purposes if the firmware loading process and communication channels are not correctly protected. This use case requires to install two TNEDs in order to establish the secure communication, in the customer premises and also in the manufacturer production line dedicated for firmware loading.

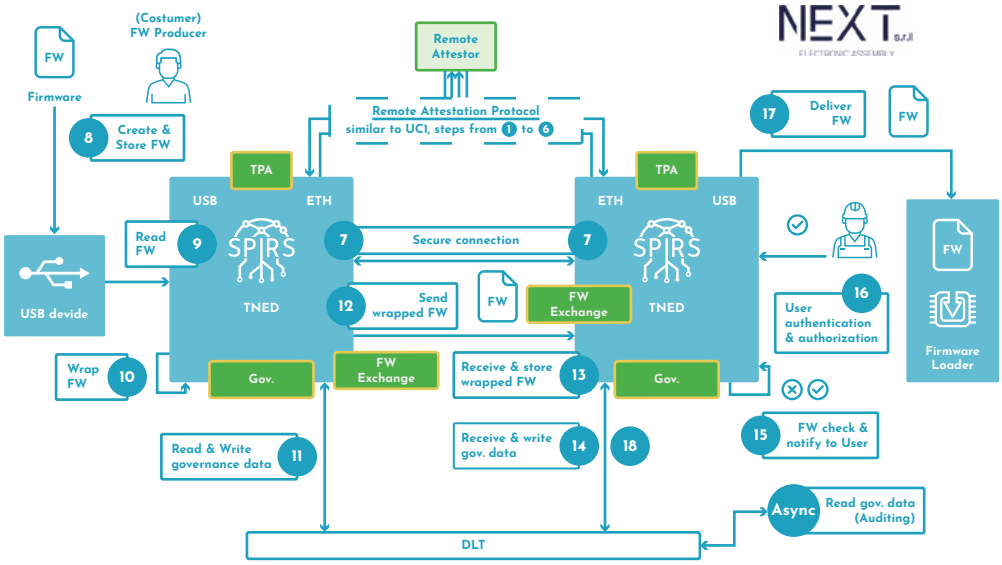


Illustration of operational steps for Use Case 2

• Use Case 3 – 5G Network Use Case – Full End-to-End Zero Trust Enablers and Deployment

The 5G use case applies to Public Networks (PN) and Non-Public Networks (NPN) coupled deployment and realizes fundamental mechanisms for a full end-to-end zero-trust solution. This will enable a secure communication between IoT devices in an NPN and the corresponding applications in the 5G PN.

To provide these functionalities this use case takes advantage of the following pillars:

- TNED mechanisms to provide deployment and attestation of fundamental software.
- Distributed functions for attestation and provisioning of software on a TNED.
- Federated or local Orchestration, Administration and Management (OAM) and Interface to Network Security Functions (I2NSF).

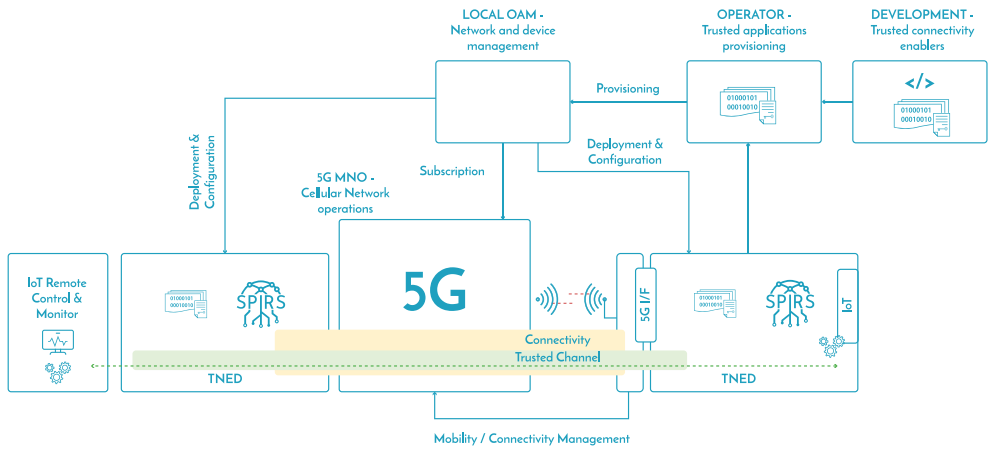


Illustration for Use Case 3

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

Follow us

WP7 – Dissemination and exploitation of results

A summary of dissemination activities:

- 8 publications in peer-reviewed international journals
- 13 participations in peer-reviewed conferences
- 12 talks in seminars and webinars
- 1 whitepaper

Communicating and promoting activities:

- Web-site activation
- 4 promotional videos
- 4 participations in outreach activities for general audience
- Active participation in social media

SPIRS consortium meetings (1st year)

Description	How?	When?
Kick-off meeting	Hybrid - Seville (Spain)/Virtual	October 2021
Intermediate meeting 1	Virtual	March 2022
Intermediate meeting 2	Hybrid - Tampere (Finland)/Virtual	June 2022
Annual meeting	Hybrid - Madrid (Spain)/Virtual	October 2022

Kick-off meeting

Intermediate meeting 2

Annual meeting

Participation in 11th Conference of EU Research & Innovation framework programme

Participation in 2022 European Researchers' Night

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

Follow us