During the second year of activities, the Consortium has made important progresses in several technical Work Packages (WPs).

WP2 - Design of a silicon Root-of-Trust

The final RoT in SPIRS is composed of the following hardware components (see Figure 1):

- **PUF:** a new version of the PUF module (PUFv2.2) that provides an area optimized implementation and a higher output bit rate. Additionally, the internal strategy for the challenge generation avoids the repetition of a challenge to obfuscate information against Electromagnetic Side-Channel Attacks (EM SCAs).

- **AES:** a new version of the module that combines hardware countermeasures, signature generator for Fault-Injection Attacks and Low-Entropy Masking Scheme (LEMS) for SCA.

- **SHA-256:** the hash function with 256 output bits of the SHA-2 family is chosen since it was demanded by some partners to be used in the development of their trusted applications. An enhanced hardware implementation in terms of area and timing performance is provided.

- **SHA3-512:** the hash function with 512 output bits of the SHA-3 family is chosen as alternative for partners that have required SHA-3 as hashing.

- **EdDSA:** an IP module to implement on hardware critical tasks in the digital signature scheme based on curve Ed25519.

- **SLP:** an IP module to detect fault-injection attacks due to extreme values of supply voltage and/or temperature, as well as malicious manipulations of clock and control signals at the system level.

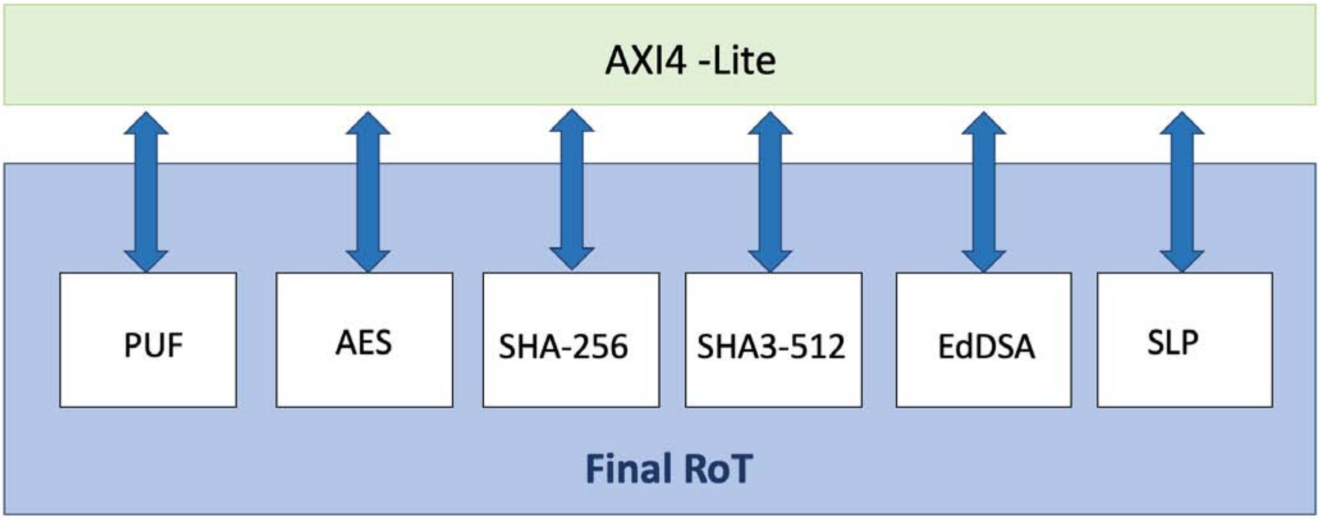


Figure 1: Final RoT in SPIRS

In order to show the right functionality of the various RoT components resulting from their interconnection with a processing system, a demo has been developed. The demo has been implemented on Pynq-Z2 and Genesys 2 development boards

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

WP3 - Design of a Trusted Execution Environment

In the context of WP3, demonstrators built on top of the second prototype of the SPIRS Trusted Execution Environment (TEE) have been developed:

- A firmware Trusted Platform Module (TPM) (fTPM) rooted in the core of the platform.
- The feasibility of integrating third party cryptography libraries like *libgroupsig* and *OpenSSL* into Trusted Applications (TAs).

Trusted Execution Environment

SPIRS TEE is based on the Keystone framework. Keystone is an open-source project for designing customized TEEs for RISC-V CPUs. This framework provides a TEE full-stack development environment that glues all the required components for instantiating or designing a TEE.

Figure 2 shows the software components of the platform. This figure includes Keystone (yellow) and SPIRS (blue) elements. The SPIRS components represent the implementation of GlobalPlatform TEE APIs on both the untrusted and trusted domains of the platform.

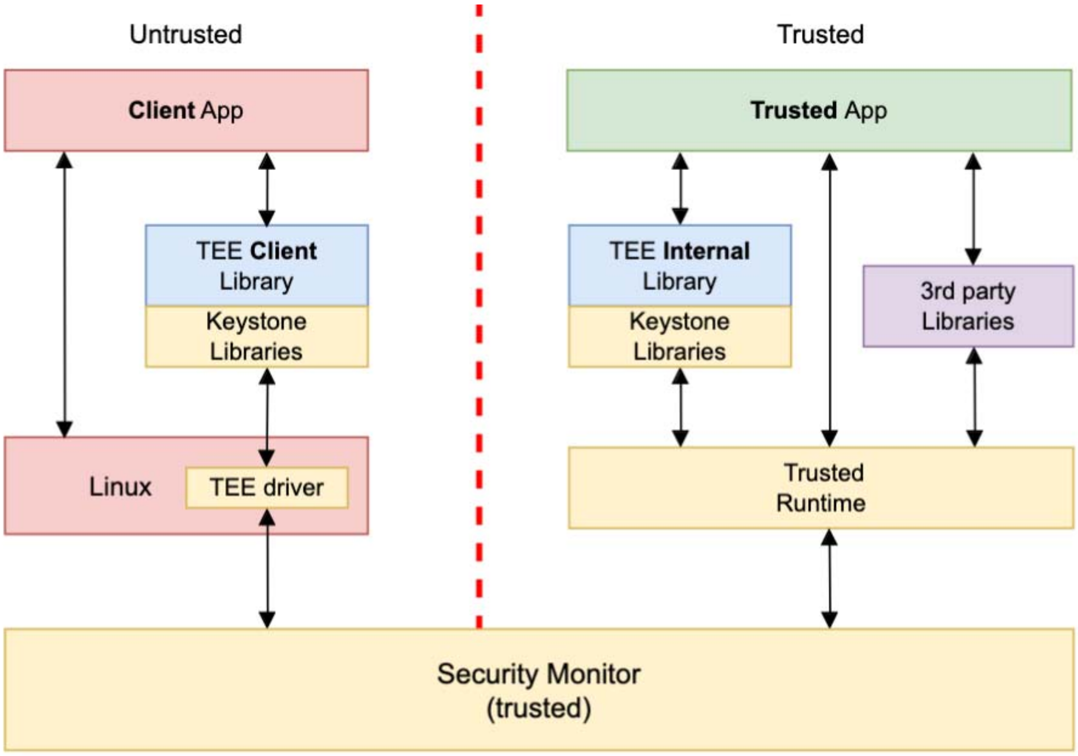


Figure 2: Basic SPIRS software stack

Secure and Measured Boot

In order to create a platform whose trustworthiness can be ensured and demonstrated, the SPIRS platform needs to include capabilities that allow Remote Attestation (RA) protocols to be enabled for all its components, hardware and software, starting from the boot up to the runtime phase. This was achieved in two steps: first of all, Secure and Measured Boot procedures were defined to ensure that the SPIRS platform booted in a trusted way; then, RA protocols were designed and implemented for all components of the SPIRS platform.

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

Secure and Measured Boot procedures need a hardware anchor upon which to base trust in the platform. In SPIRS, the device identity is the Physical Unclonable Function (PUF) resident in the hardware RoT.

The SPIRS platform is equipped with the minimum set of elements that enable Secure, Measured Boot, and RA protocols, according to the Trusting Computing Group (TCG):

- the bootrom, which will contain the first measurement procedure, thus implementing the Root of Trust for Measurement (RTM);
- the PUF, capable of giving a statistically unique identity to the device, thus implementing the Root of Trust for Reporting (RTR);
- the Physical Memory Protection (PMP) extension defined in the RISC-V standard, which allows the creation of protected memory regions within which to store measurements, thus enabling Root of Trust for Storage (RTS).

Keystone based firmware Trusted Platform Module (TPM) (fTPM)

We leverage the SPIRS TEE to build an fTPM that can be used by the platform similarly to a discrete TPM. With this approach, it is expected that existing solutions that rely on a TPM device can be transparently and seamlessly used with an fTPM. One relevant example of this is the Linux IMA subsystem which uses a TPM if it is available in the platform.

Keystone v1.0 heavily depends on Linux userspace to create a TA. The numbering in Figure 3 illustrates this process as a sequence, detailed as follows. The CA (1) initiates this procedure by using the Keystone SDK (2) libraries, which are wrappers for the Keystone TEE driver (3) in the Linux kernel. The Security Monitor (4) acts as a proxy between the security domains and creates the Trusted Runtime (5) in an isolated environment, and then finally executes the TA (6). At this point the CA and TA can exchange information using the Keystone SDK and Keystone TA libraries.

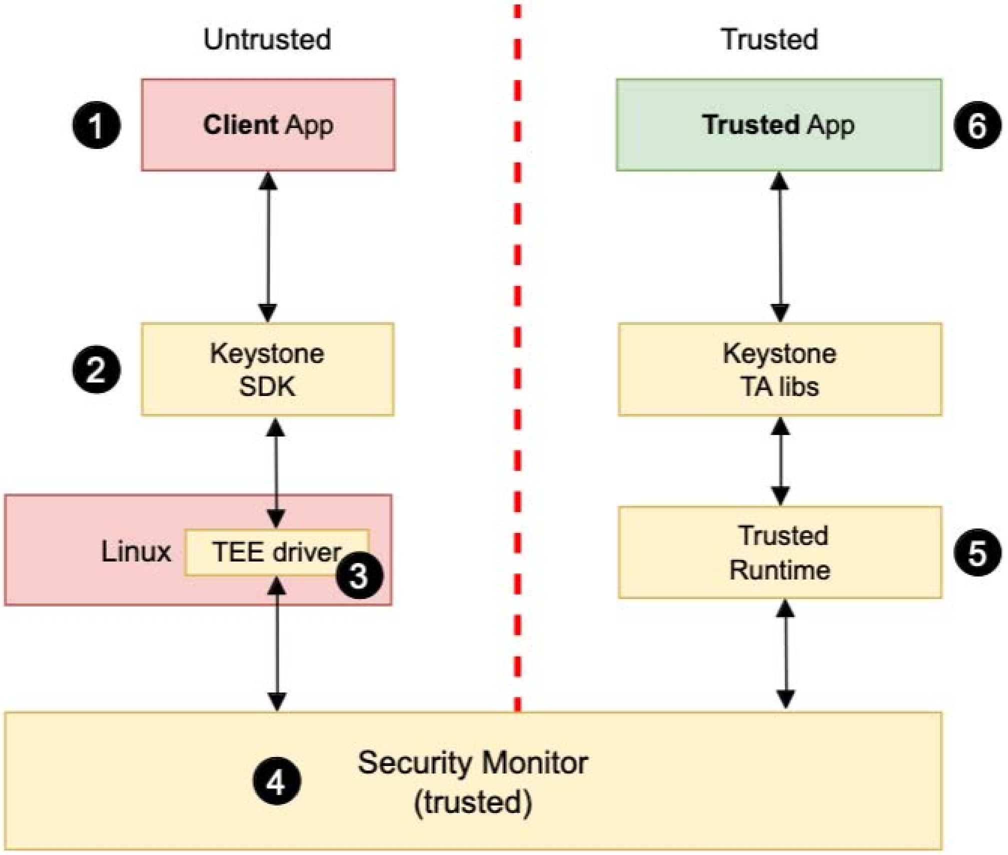


Figure 3: Keystone framework software stack

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

Group signatures schemes

A Privacy Enhancing Toolbox has been developed for such a goal, with the anonymization of users' or entities' identities as one of the functionalities of this toolbox. Two distinct group signature schemes have been selected:

- Traceable group signatures defined by Kiayias, Tsionis and Yung (KTY04) that rely on RSA and discrete logarithm assumptions
- Group signatures defined by Pointcheval and Sanders (PS16) that are based on bilinear pairings.

The selected library can be downloaded here that is is an improved version of libgroupsig.

WP4 - Integration into network infrastructures

Network integration features:

- **JOINT** Orchestration, Management and Control of 5G System and Trusted Applications on heterogeneous types of TEE-enabled TNEDs
- **EXTENSIBLE** Controller Architecture through OpenAPIs – integrates features of Resources- and Lifecycle Management, Application Deployment and Attestation in REE & TEE, and TA Configuration
- **AUDITABLE** procedure and compliance checks through logging
- **PROTECTED END-TO-END COMMUNICATION** through IPsec Overlay

Validation:

1 **From Edge Control to Trust Control**

Orchestration and Life-Cycle Management of Applications on sliced RISC-V edge platform resources

2 **Distributed Attestation**

Remote attestation of computational entities deployed on TNEDs

3 **Centrally Controlled IPsec (CCIPS)**

Management of IPsec tunnels in a 5G network protecting the communication and data treated by Trusted Applications

4 **Group Signatures**

Shows the functionality supported by the group signature library, that will be used to implement privacy respectful AAAA protocols

4 available demos:

1 Demonstrate first evolution of the Edge Controller for orchestration of Kubernetes container virtualization on a RISC-V edge resource

2 Demonstrate first evolution of remote attestation protocols for containerized workloads deployed on MNO Edge System

3 Demonstrate enhanced 5G network security by leveraging CCIPS, secure configuration handling, and protection of cryptographic data

4 Fully functional KTY04 group signature scheme in the TEE

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

WP5 - Platform integration

A preliminary FPGA implementation of the SPIRS platform has been developed:

1 To assess the correct functionality of the SPIRS platform integrating a secure CVA6-based processor (SPRITZ) and RoT components developed in WP2

2 To characterize the performance of the platform:

- Area occupation
- Power consumption

3 To implement a preliminary SPIRS platform on FPGA

- HW/SW components integration and validation

Features of the SPIRS plataform:

1 Fully compliant with "System Requirements" described in the D3.1 deliverable

2 Compliant with "Interface Requirements" described in the D6.1 deliverable

3 ALL IP modules are memory mapped to a processor compatible with RISC-V RV64GC ISA

4 ALL IP modules use a AXI4-compliant interface

INTERFACE REQUIREMENTS	DESCRIPTION	INTEGRATION STATUS
Serial Interface (UART)	Serial Interface to connect to the machine controller and retrieve/send data from/to	Complete
Serial Interface (User USB)	(Customer Side) Upload the firmware on the SPIRS Platform before securely transferring it to the manufacturer	Work-in-progress
Ethernet	Network communication	Complete
User interaction (USB HID)	User inputs	Work-in-progress
User feedbacks (HDMI or VGA)	Feedbacks on specific actions (e.g., operation started/completed)	Work-in-progress

Verification of the SPIRS platform:

1 Use of Linux boot to verify the integration of the SPRITZ processor

2 Use of low and high-level drivers to verify the integration of HW/SW RoT IPs

3 Compare the results to the golden models from WP2

4 Make the platform available for WP3 partners to conduct TEE testing

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

Demo of the SPIRS platform:

1 A preliminary version of the SPIRS platform integrating SPRITZ

2 A design flow to implement the platform on the project reference FPGA development board (Genesys 2)

3 An environment to build SW running on the HW platform

First VLSI integration of a lightweight Root-of-Trust (RoT)

A 3.57 mm2 ASIC has been taped out for integration in TSMC 65nm technology:

- to assess the viability of designing building blocks in dedicated hardware;
- to enable higher integration, with less power consumption and reduced hardware resources, yielding a lightweight version of a RoT to be used in constrained scenarios where security is a must.

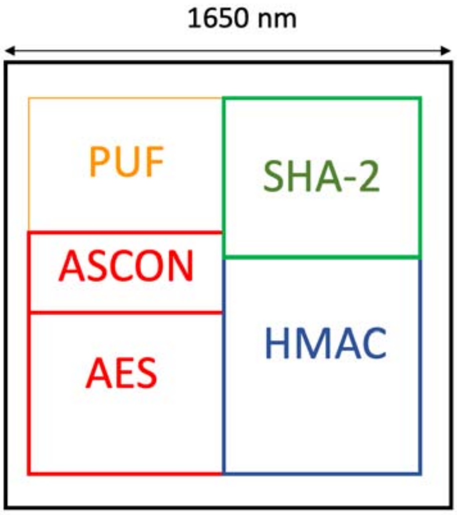


Figure 4: Distribution of the blocks in the ASIC

WP7 - Dissemination and exploitation of results

A summary of dissemination activities in numbers (first and second year):

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

Communicating and promoting SPIRS (first and second year):

- 6 promotional videos
- 7 participations in outreach activities for general audience
- Active participation in social media
- 1 whitepaper

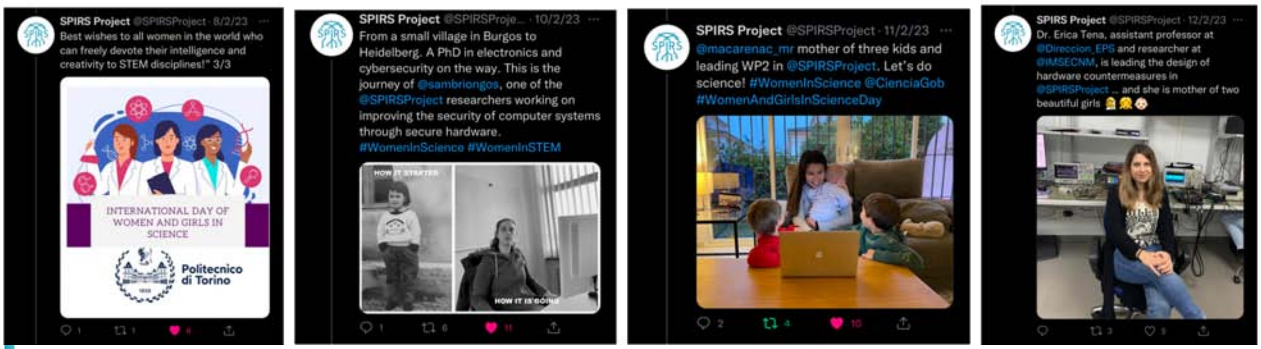
The SPIRS Project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement N° 952622

SPIRS consortium meetings for 2nd year

Description	How?	When?
Intermediate meeting	Hybrid - Heidelberg (Germany)	March 2023
First Reporting Period	Hybrid - Seville (Spain)	June 2023

SPIRS meeting in Heidelberg (March 2023)

First review in SPIRS (June 2023)



SPIRS Project @SPIRSProject · 8/2/23
Best wishes to all women in the world who can freely devote their intelligence and creativity to STEM disciplines!" 3/3

SPIRS Project @SPIRSProje... · 10/2/23
From a small village in Burgos to Heidelberg. A PhD in electronics and cybersecurity on the way. This is the journey of @sambriongos, one of the @SPIRSProject researchers working on improving the security of computer systems through secure hardware.
#WomenInScience #WomenInSTEM

SPIRS Project @SPIRSProject · 11/2/23
@macarenac_mr mother of three kids and leading WP2 in @SPIRSProject. Let's do science! #WomenInScience @CienciaGob #WomenAndGirlsInScienceDay

SPIRS Project @SPIRSProject · 12/2/23
Dr. Erica Tena, assistant professor at @Direccion_EPS and researcher at @IMSECNM, is leading the design of hardware countermeasures in @SPIRSProject .. and she is mother of two beautiful girls 👩‍🔬👧👶

Posts in social media of female researchers in SPIRS

The SPIRS Project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement Nº 952622