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

SPIRS Whitepaper:
Concept and Use Cases

Public and summarized version of the submitted material in Deliverable 6.1 that is under revision by European Commission

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

Abstract

The SPIRS project targets the design of an ICT platform integrating a Root of Trust to provide security services. This document defines several use cases, for two relevant environments identified: Industry 4.0 and 5G Networks.

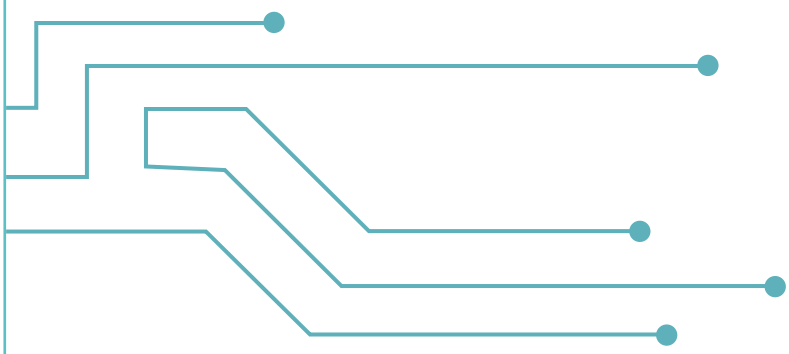
In each of the use cases, multiple components and associated functionalities are proposed to guarantee a high level of security. Among those functionalities identified are Secure Boot, Governance Schemes, Remote Attestation or the Trusted Execution Environment.

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

Contents

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

1. Introduction



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

1. Introduction

This project encompasses the complete design of a platform, called the SPIRS (Secure Platform for ICT systems Rooted at the Silicon Manufacturing Process) platform, which integrates a dedicated hardware Root of Trust (RoT) and a processor core capable of providing a complete set of security services. The SPIRS platform will support privacy-friendly attestation mechanisms and enable trusted communication channels in 5G infrastructures.

RoT is implemented in hardware with a dedicated circuit to extract a unique digital identifier for the SPIRS platform throughout its lifetime. To build a complete solution, the project also features a Trusted Execution Environment (TEE), secure boot and runtime integrity.

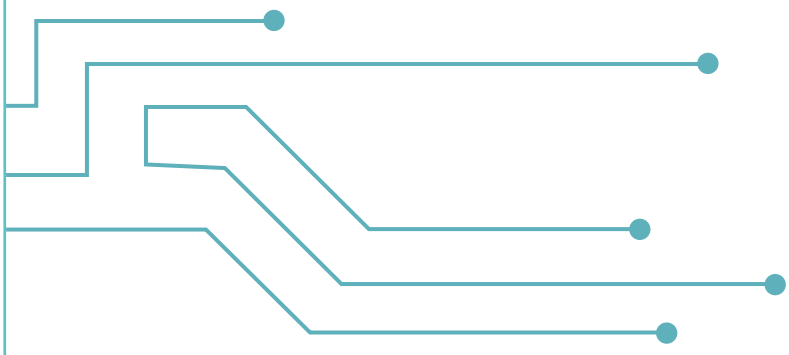
The project goes beyond building the SPIRS platform and provides solutions to integrate it into the deployment of cryptographic protocols and network infrastructures in a reliable way, taking advantage of the RoT provided by the platform.

SPIRS considers two different scenarios: Industry 4.0 and 5G technologies, for testing and validation. This documents details the initial use case and related components.

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

2.

SPIRS TNED



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

2. SPIRS TNED

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.

2.1 Software architecture

The SPIRS Trusted Execution Environment provides a series of software components (e.g., interfaces, APIs, etc.) to ensure that part of the applications can run in a secure environment. The platform defines the following components, which are represented in figure 2.1:

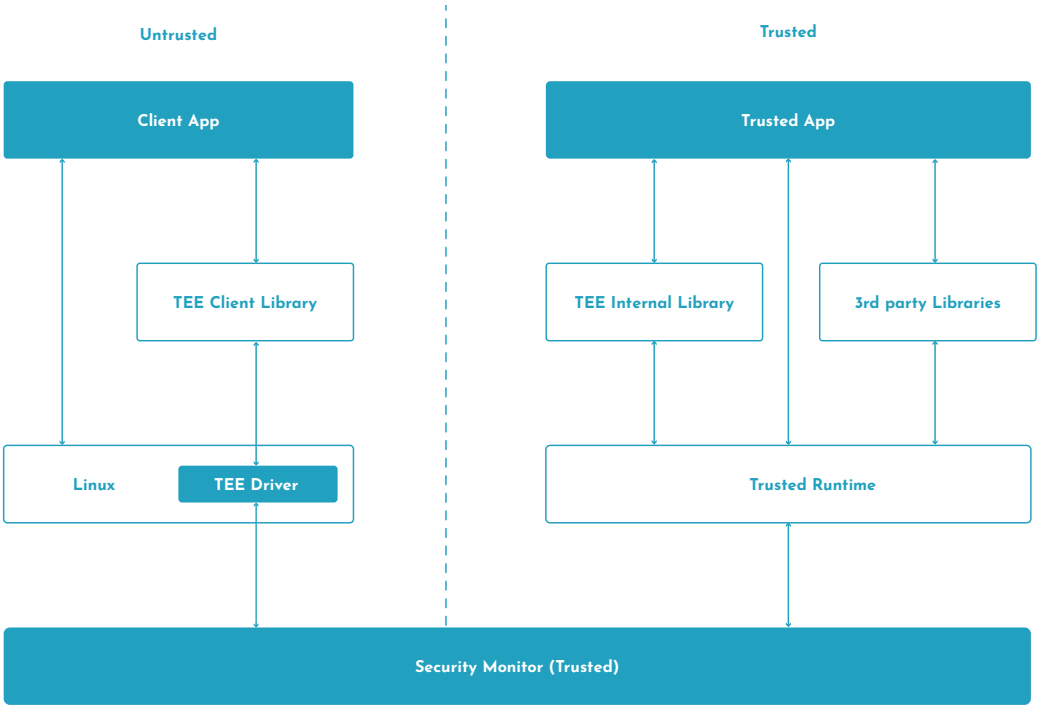


Figure 2.1: Basic SPIRS software stack.

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

- Security Monitor (SM): trusted component of the platform which has the highest privilege. This software orchestrates the platform's security and acts as a link between the trustworthy and untrusted domains. The SM relies on the RISC-V Supervisor Binary Interface (SBI) to communicate with higher immediate software layers. This increases the compatibility across the RISC-V ecosystem and existing software frameworks.

- Linux and Linux TEE driver: current implementation is based in Linux kernel version 5.7. TEE interaction from the High Level Operating System (HLOS) relies in a TEE driver, used to call the corresponding SM SBI providing a secure communication between the Client and Trusted Apps.

- Client and Trusted Applications (TAs): Client-server architecture where the client runs in the untrusted side and the server in the trusted side. This communication is handled by specific APIs defined in the TEE Client library and TEE internal library. Applications developed for the SPIRS platform can run any Linux/RISC-V supported framework.

- TEE Client library: to communicate with the trusted side, applications must follow a specific API. In this case it has been selected the "GlobalPlatform Client API v1.0" [1], providing a Remote Procedure Call (RPC) interface between client and trusted applications.

- TEE internal library: API based in on "GlobalPlatform TEE Internal Core API Specification v1.1.2" [2] which provides the communication between the Trusted applications and the Client applications. It supports access to the RoT of the devices, giving access for example to the hardware random number generator.

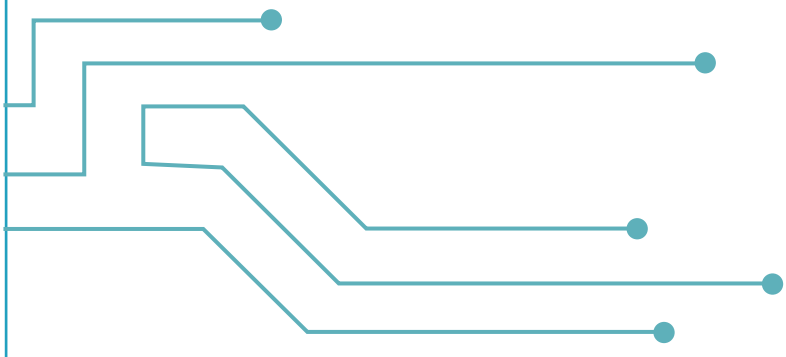
[1] "TEE Client API Specification v1.0," GlobalPlatform Inc, 2010.

[2] "TEE Internal Core API Specification v1.1.2," GlobalPlatform Inc., 2016.

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

3.

General functionalities



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

3. General functionalities

3.1 Initial setup and provisioning

- SPIRS platform is a multi-component system which can be modelled through a layered architecture, like the one presented in figure 3.1. The architecture allows us to adopt the Device Identifier Composition Engine (DICE) standard [3]-[4] 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.

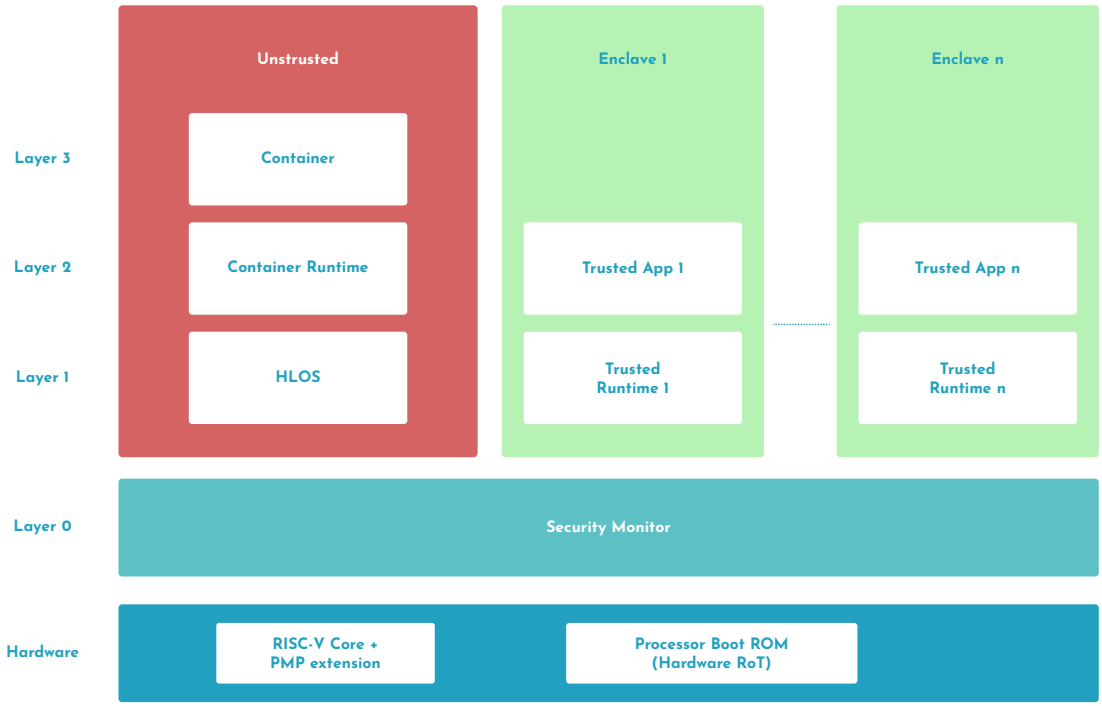


Figure 3.1: SPIRS platform layered architecture.

[3] Trusted Computing Group (TCG), "Hardware Requirements for a Device Identifier Composition Engine,"March 2018.

[4] "DICE Layering Architecture," July 2020.

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

3.2 Secure boot

It ensures that a platform has been booted into a trusted environment. 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).

3.3 fTPM

The SPIRS platform is not equipped with a TPM chip so it cannot rely on Trusted Platform's established procedures to build the RoT. The firmware Trusted Platform Module (fTPM) presented in figure 3.2, 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).

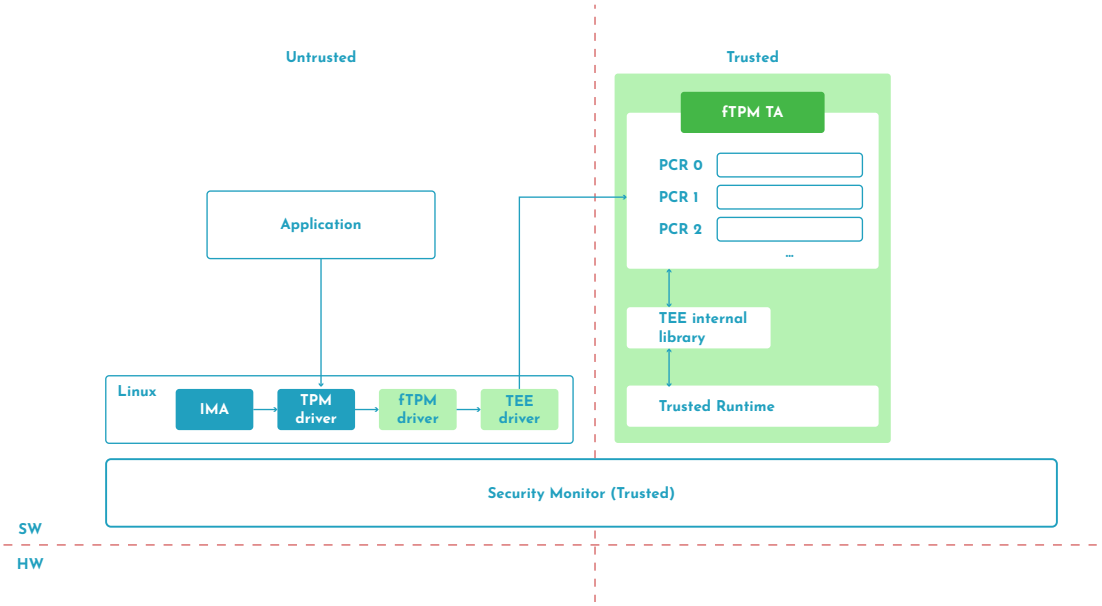


Figure 3.2: SPIRS fTPM.

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

3.4 Remote Attestation

This component 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. The attestation process begins when the RA sends to the Trusted Platform Agent (TPA) an integrity challenge (protected against replay attacks). When the request is received, the TPA generates an Integrity Report containing tamper-proof evidence on the integrity status of the HLOS (i.e., the fTPM quote) and the log of measurements collected at runtime by the IMA module. Then, the Remote Attestor evaluates the trustworthiness level of the HLOS based on the Integrity Report received from the TPA.

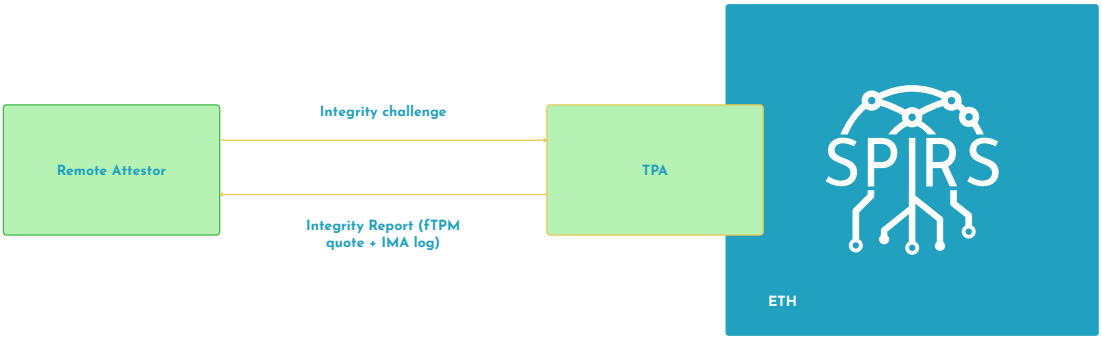


Figure 3.3: HLOS remote attestation.

3.5 Governance Schemes

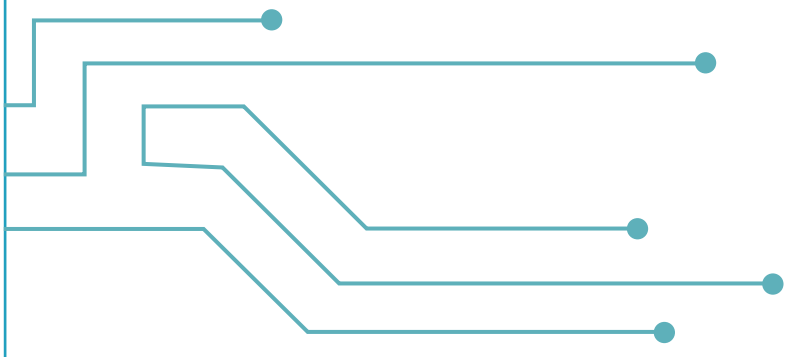
This component defines a set of roles and permissions and tracks every modification of the state of the entities taking part in the system. It is based on a Distributed Ledger Technology (DLT) which allows users of the system to retain a certain degree of anonymity providing they are not a malicious entity. In those cases, the established agreement will be broken revoking the anonymity. This solution, makes uses of groups signatures and a modification of the X.509 for building the governance scheme. The device on-boarding is similar to the one proposed by the Fast Identity Online (FIDO) Alliance [5].

[5] FIDO Alliance IoT TWG, "FIDO Device Onboard: A specification for automated, secure IoT provisioning technology," FIDO White Papers. [Online]. Available: https://media.fidoalliance.org/wp-content/uploads/2021/04/Introduction-to-FIDO-Device-Onboard-1.pdf

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

4.

SPIRS Use cases



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

4. SPIRS Use cases

SPIRS proposes two Use Case (UC) families, one for the Industry 4.0 scenario (i.e., UC1 and UC2) and another for 5G technologies (i.e., UC3). Each use case is described including the actors and the trusted applications envisioned.

4.1 UC1 - Trust in Manufacturing Machine

4.1.1 Description

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.).

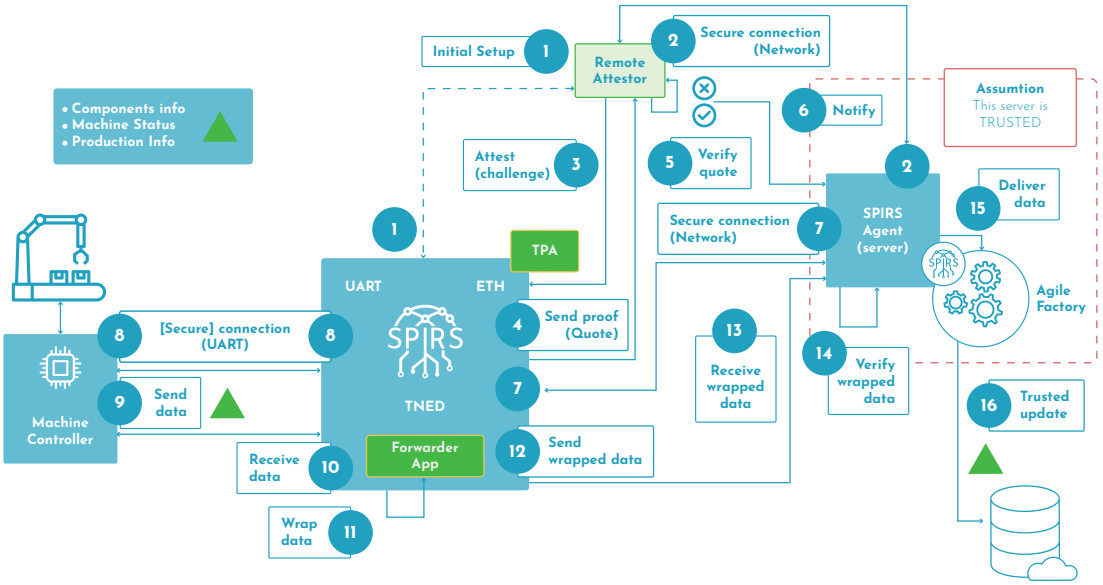


Figure 4.1: Illustration of operational setps for UC1.

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

4.1.2 Actors and roles

- Remote Attestor (RA): external application that can assert the integrity and status of the TNED against software manipulations and notify the Spirs Agent (SA) with the results during the attestation procedure.
- Trusted Platform Agent (TPA): application running in the TNED used to communicate the attestation data to the RA.
- Forwarded (FWD): application running in the TNED which ensures the secure data transfer from the Machine Controller and the MES server.
- SPIRS Agent: application running in the MES servers which receives the secure data transfer from the TNED and interfaces with the Agile Factory software.

4.1.3 Trusted application

FWD is the secure application which runs on the TNED with the objective of securing data transfers between the Machine Controller and the SPIRS agent (installed on the MES Server). During a secure transfer, data must be wrapped (i.e., encrypt and sign) to ensure the integrity and protect it against a potential eavesdropping attack. As described in figure 4.2, the application shall be able to securely connect through the UART port (present in the TNED), to the custom hardware of the Machine Controller, so it can receive the incoming data from the Machine Controller and protect it. Note, that the UART shall be trusted, so it belongs to the trusted domain. Furthermore, this application must be able to securely connect to the SPIRS Agent on the MES Server through the ETH port and transfer protected data to the SPIRS Agent.

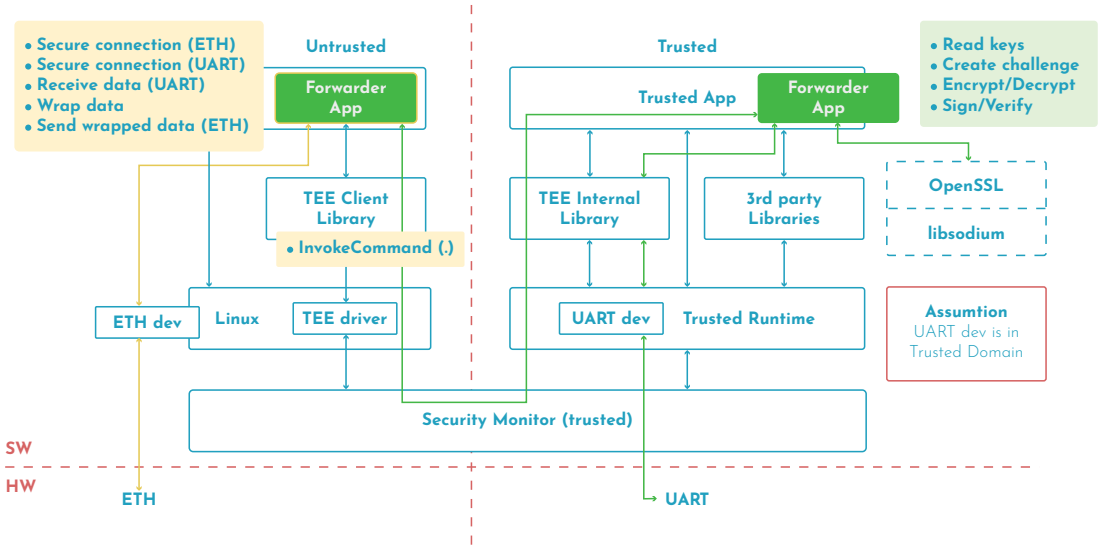


Figure 4.2: Forwarder Application.

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

4.2 UC2 - Trusted Firmware Loading

4.2.1 Description

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 as presented in figure 4.3 in order to establish the secure communication, in the customer premises and also in the manufacturer production line dedicated for firmware loading.

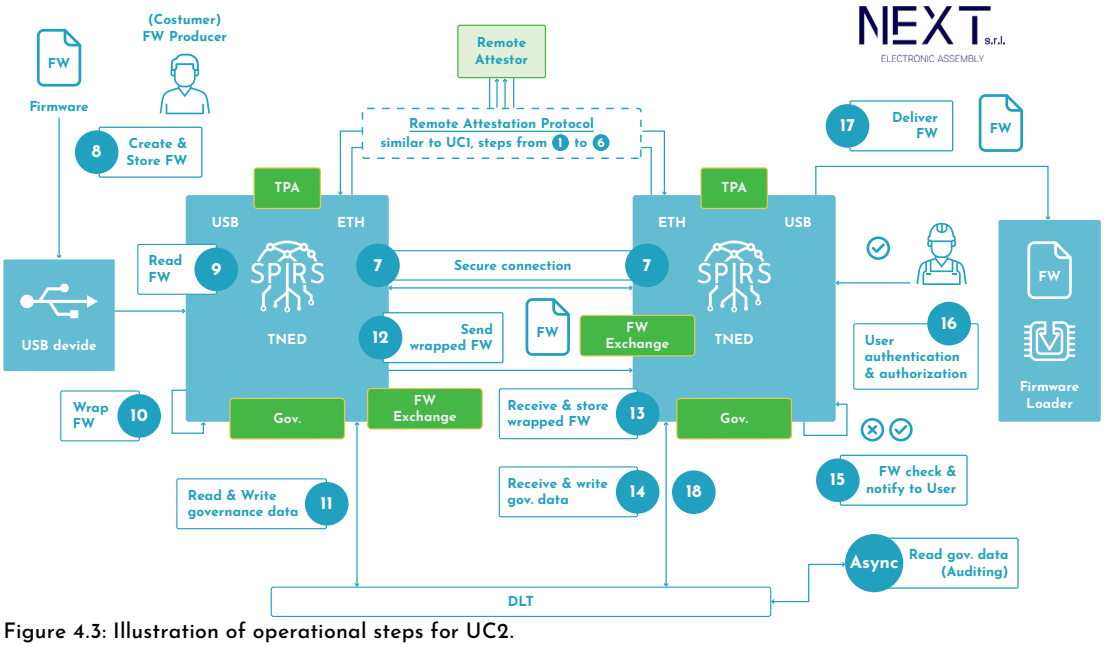


Figure 4.3: Illustration of operational steps for UC2.

4.2.2 Actors and roles

- Remote Attestor (RA): external application equivalent to the one needed for UC1, but capable to communicate with two different TNEDs and assert their integrity status against software manipulations.
- Trusted Platform Agent (TPA): application running on the TNEDs used to communicate the attestation data to the RA.
- Firmware Exchange (FWE): application running on the TNEDs, capable to securely transfer a binary application FW between two endpoints.
- Governance Application (GA): application running on the TNEDs employed to store and retrieve governance metadata from a Distributed Ledger Technology (DLT).

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

4.2.3 Trusted application

Firmware exchange application runs on the TNED, providing the secure transfer of a binary application firmware between two endpoints while maintaining its integrity during this process. The application is divided into the trusted and untrusted domains of the TNED as presented in figure 4.4. On the untrusted part, the application shall be able to securely connect through ETH port to the remote TNED so it can read the binary provided by the Customer endpoint through the USB interface. Once received, the binary must be protected (i.e., encrypt and sign in the trusted part) so it can be transferred to the Manufacturer endpoint through the ETH interface.

At the manufacturer endpoint, the application must receive the wrapped data, so it can be decrypted and verified by checking the signature. After proper user authentication and authorization, the application shall write the plain text binary application firmware on the USB interface at the manufacturer endpoint. In addition, the Firmware Exchange Application must be able to trigger the execution of the Governance Application.

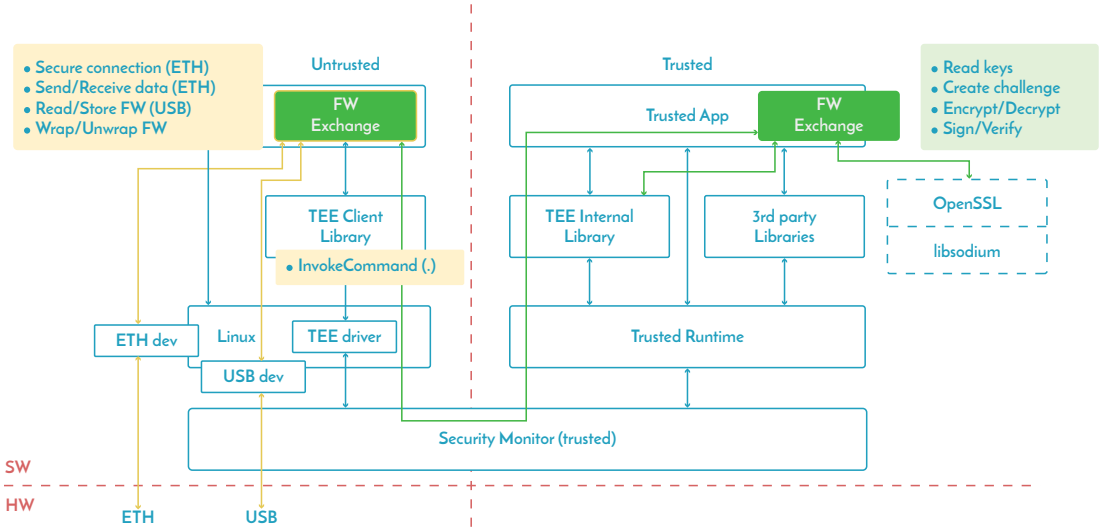


Figure 4.4: Firmware Exchange Application.

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

4.3 UC3 - 5G Network Use Case - Full End-to-End Zero Trust Enablers and Deployment

4.3.1 Description

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 as it is presented in figure 4.5. To provide these functionalities this use case takes advantage of the following pillars:

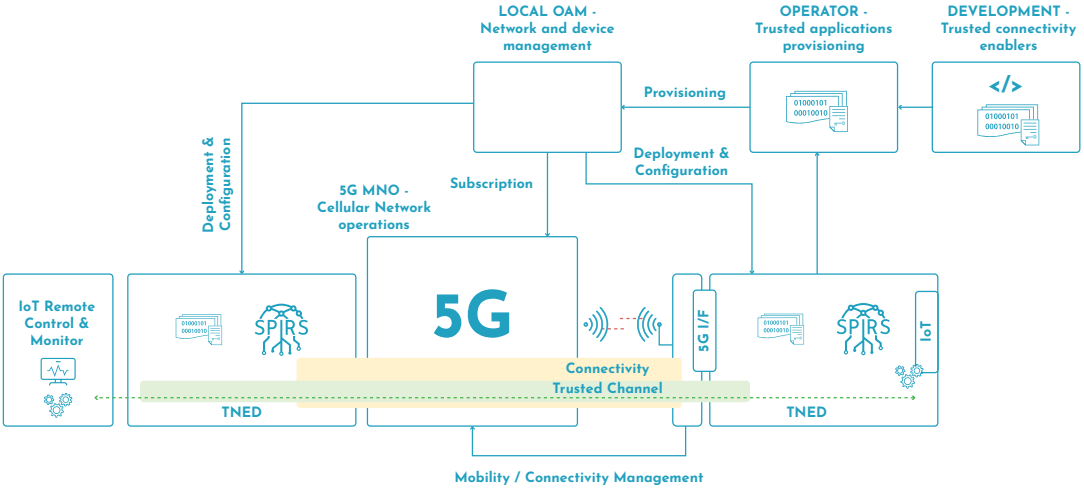


Figure 4.5: High level description of the 5G use case.

- 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).

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

4.3.2 Actors and roles

- Operations, administration, and management (OAM): set of mechanisms and resources that may be shared between the PN and the NPN. It handles the validation of the quotes or attestation messages signed by the different TNED devices, the deployment of the necessary VNFs using a MANO (i.e., Open-source MANO) and provides the configuration values through the I2NSF Controller to establish the I2NSF IPsec functionalities between both TNEDs.

- Software Developer: design and build the different trusted applications to be executed in the TNEDs to provide the I2NSF functionalities.

- Software Operator: entity that holds the trusted applications, later deployed, and executed in the different TNEDs.

4.3.3 Trusted application

I2NSF IPsec application will be used to verify, protect and setup the security policies and associations sent by the controller to establish a secure communication using IPsec across two endpoints. It is divided in two security domains, the untrusted "I2NSF agent" application and trusted environment "I2NF enclave" as presented in figure 4.6. The I2NSF agent is in charge of handling the incoming requests from the controller, passing the ciphered values to the enclave and handling the kernel calls to setup the IPsec rules and monitor the current status of the tunnel.

On the other hand, the I2NSF Enclave is the TA that must handle the decryption of the ciphered values sent by the controller, process the policies and associations received, and verify that the current ones installed into the kernel have not been tampered. To verify that the rules have not been modified, the TA must keep a copy of the rules that have been processed and setup into the kernel, so if they have been modified they can be compared and generate an alert based on the result of the verification.

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

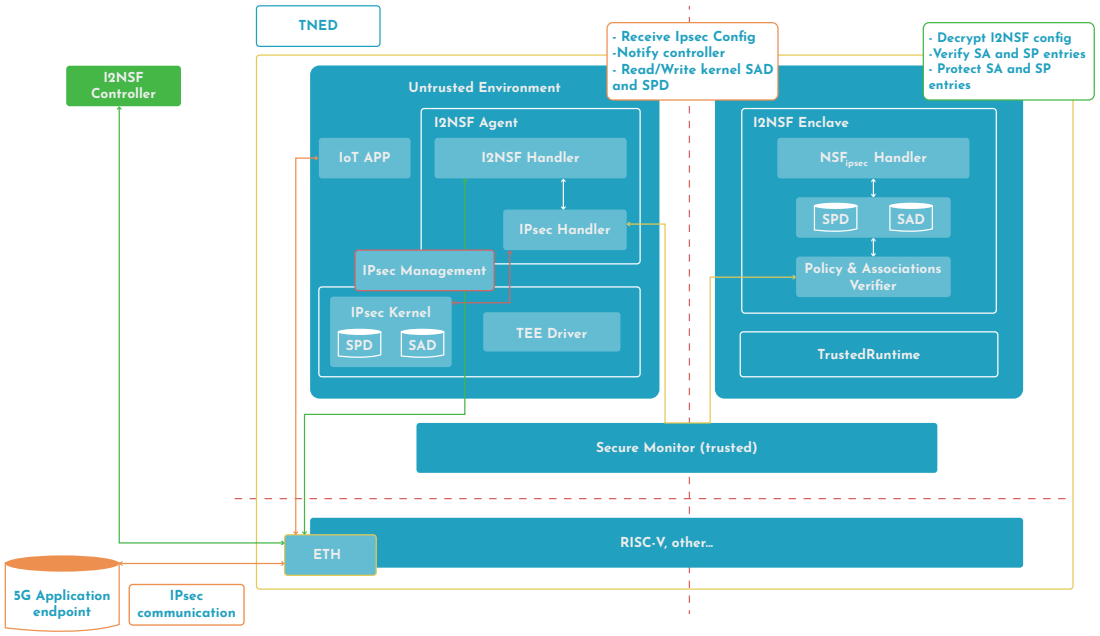


Figure 4.6: 5G I2NSF IPsec Application.

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

SPIRS project
December 1, 2022
SPIRS-0.X/1.0

Horizon 2020

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