Grant Agreement No.: 871808
Research and Innovation action
Call Topic: ICT-20-2019-2020: 5G Long Term Evolution

INSPIRE-5Gplus

INtelligent Security and PervasIve tRust for 5G and Beyond

D5.1: 5G security test cases

Version: v1.0

Deliverable type	R (Document, report)
Dissemination level	PU (Public)
Due date	31/10/2020
Submission date	04/11/2020
Lead editor	Diana P. M. Osorio (UOULU)
Authors	Ricard Vilalta, Pol Alemany, Michela Svaluto, Charalampos Kalalas, Roshan Sedar, Raul Muñoz, (CTTC), Edgardo Montes de Oca, Huu Nghia Nguyen (MI), Diana P. M Osorio, Pawani Porambage, Tharaka Mawanane Hewa (UOULU), Antonio Pastor, Sonia Fernandez (TID), Maria Christopoulou (NCSRD), Sabina Sandia, Phil Grayling, Orestis Mavropoulos, Grant Millar, Anastatios Kafchitsas (CLS), Vincent Lefebvre (TAGES), Jordi Ortiz(UMU), Cyril Dangerville, Geoffroy Chollon (TSG), Gürkan Gür, Bernhard Tellenbach (ZHAW), Chafika Benzaid (Aalto), Mohammed Boukhalfa (Aalto), Tarik Taleb (Aalto)
Reviewers	Georgios Xylouris(NCSRD), Rafał Artych (OPL), Dhouha Ayed (THALES)
Work package, Task	WP5, T5.1, T5.2

Abstract

This deliverable presents the set of test cases selected for validation on the INSPIRE-5Gplus project. This set of test cases were selected by performing an exhaustive requirements elicitation of 5G security use cases defined in WP2, stemming from the new and enhanced 5G security and trust/liability assets developed in WP3 and WP4. Herein, we perform an initial description on the requirements, key performance indicators and relationship of the test cases to the High-Level Architecture being developed in WP2. Finally, the capabilities and enhancements required for the envisioned testing environment for the integration and experimentation of the 5G security test cases is also presented.

Document revision history

Version	Date	Description of change	List of contributor(s)
v0.1	15/09/20	First complete version	All Authors
v0.2	26/09/20	First revision	Georgios Xylouris(NCSRD), Rafal Artych (Orange)
v0.3	12/10/20	First revised version	All Authors
v0.4	13/10/20	Final First Edited Version	Diana P. M. Osorio (UOULU)
v0.5	22/10/20	Second revision	Dhouha Ayed (THALES)
v0.6	23/10/20	Final Second revised version	All Authors
v0.7	26/10/20	Final editing	A. Köhler (EURES)
v0.8	27/10/20	Editorial corrections and sending out for GA approval	Diana P. M. Osorio (UOULU), U. Herzog (EURES)
v1.0	04/11/20	Document submitted	U. Herzog

Acknowledgment

The research conducted by INSPIRE-5Gplus receives funding from the European Commission H2020 programme under Grant Agreement No 871808. The European Commission has no responsibility for the content of this document.

[1] http://creativecommons.org/licenses/by-nc-nd/3.0/deed.en_US

Executive Summary

This deliverable presents the set of security test cases selected for validation on the INSPIRE-5Gplus project. This set of test cases were selected by performing an exhaustive requirements elicitation of the 5G security use cases that are being defined as part of the activities of INSPIRE-5Gplus. The identification of the corresponding Key Performance Indicators (KPIs) and service requirements is also carried out stemming from the new and enhanced 5G security and trust/liability assets developed in INSPIRE-5Gplus. A total of nine test cases were selected, and initial descriptions are presented in this document.

Specifically, the content of this deliverable includes:

- A list of generic KPIs identified for validation of the nine test cases and their mapping to 5GPPP Performance KPIs.
- A first description of the INSPIRE-5Gplus framework High Level Architecture (HLA), which is being designed and enhanced in order to support fully automated End-to-End network and service security management in multi-domain environments. This description presents the current status of the HLA in order to allow the connection of the test cases into this framework. However, the HLA is being developed and enhanced, and the final version will be presented in future deliverables.
- A methodology of selection and a detailed description of the set of test cases, emphasizing on the following aspects: objective, functional architecture, targeted KPIs, requirements for deployment and pre-conditions, related INSPIRE-5Gplus enablers, methodology and expected outputs, timeline and risks.
- A listing of the available 5G facilities and the required building blocks are identified in respect to the 5G security test cases objectives. Specifically, the architecture and components of the facility, capabilities, required building blocks for security test cases, facility limitations and enhancements required, and timeline and risks are described for each facility.

This deliverable aims at providing the first signalling on the set of test cases that will validate the 5G security assets and mechanism developed in INSPIRE-5Gplus.

Table of Contents

List of Figures

List of Tables

Abbreviations

ACCA	Anticipated Cooperative Collision Avoidance
ACID	Atomicity, Control, Isolation, Durability
API	Application Programming Interface
CCAM	Cooperative, Connected and Automated Mobility
CN	Core Network
CTI	Cyber Threat Intelligence
DBMS	Database Management System
DE	Decision Engine
DENM	Decentralized Environmental Notification Message
DLT	Distributed Ledger Technology
DVB	Digital Video Broadcast
E2E	End-to-End
E2EDE	E2E Decision Engine
E2ESO	E2E Security Orchestrator
EC	European Commission
ETA	Estimated Time of Arrival
HLA	High Level Architecture
HOA	Higher Order Ambisonics
HSPL	High-Level Security Policy Language
KPI	Key Performance Indicator
MANO	Management and Orchestration
MEC	Mobile Edge Computing
MQTT	Message Queuing Telemetry Transport
MSPL	Medium-Level Security Policy Language
MTD	Moving Target Defence
MTTC	Mean Time to Contain
MTTD	Mean Time to Detect
MTTR	Mean Time to Resolve
NFV	Network Function Virtualization
OTT	Over the Top
PSM	Policy and SSLA Management
RAN	Radio Access Network
RCA	Root Cause Analysis
SA	Security Agent

SAE	Security Analytics Engine
SD-SEC	Software Defined Security
SDC	Security Data Collector
SDN	Software Defined Network
SMD	Security Management Domain
SO	Security Orchestrator
SSLA	Security Service Level Agreement
TM	Trust Management
TRM	Trust Reputation Management
vAAA	virtual Authentication, Authorization and Accounting
vIDS	virtual Intrusion Detection System
VSF	Virtual Network Security Functions

1 Introduction

1.1 Scope

This is the first public deliverable of the INSPIRE-5Gplus project's Work Package 5 that defines 5G security test cases with focus on 5G platform scenarios ICT-17, ICT-18, ICT-19. This deliverable discusses the service and deployment requirements of the security test cases and their corresponding key performance indicators (KPIs). Moreover, the available 5G facilities for tests are also identified jointly with the required building blocks and modules to be deployed on the 5G facilities, interactions between blocks, security approaches, information and data flows.

1.2 Target Audience

The target audience of this deliverable are stakeholders and industry and academic working groups interested in security of 5G technologies and infrastructure.

1.3 Structure

The rest of this deliverable is structured as follows. Section 2 describes the considered KPIs for evaluation of the selected group of Test Cases to be demonstrated and a brief description of the High-Level Architecture (HLA) proposed by INSPIRE-5Gplus. Section 3 details the methodology followed for selecting the group of Test Cases as well as a complete description of each. Section 4 provides detailed information about the 5G security testing infrastructure available for testing. Finally, conclusions are provided in Section 5.

2 Security KPIs for validation and HLA

2.1 Description of Security KPIs

This section provides an initial overview of generic KPIs proposed in the scope of INSPIRE-5Gplus that will serve as means of evaluation for the test cases to be presented in the next section. The specific KPIs considered for evaluation of each test case are detailed in Section 3. In Table 1, we present the 5G-Public Private Partnership (5G-PPP) contractual KPIs[2], while in Table 2, we present a mapping of the relation of INSPIRE-5Gplus KPIs with 5GPPP Performance KPIs.

KPI	DESPCRIPTION
KPI1	Providing 1000 times higher wireless area capacity and more varied service capabilities compared to 2010.
KPI2	Saving up to 90% of energy per service provided. The focus will be in mobile communication networks where the dominating energy consumption comes from the radio access network.
KPI3	Reducing the average service creation time cycle from 90 hours to 90 minutes.
KPI4	Creating a secure, reliable and dependable Internet with a "zero perceived" downtime for services provision.
KPI5	Facilitating very dense deployments of wireless communication links to connect over 7 trillion wireless devices serving over 7 billion people.
KPI6	Enabling advanced user-controlled privacy.

Table 1: 5GPPP Performance KPIs

KPI	DESPCRIPTION	KPI1	KPI2	KPI3	KPI4	KPI5	KPI6
Mean Time to Detect (MTTD)	MTTD measures how long it takes the system to detect potential security incidents.	●		●	●		●
Mean Time to Contain (MTTC)	MTTC measures how long it takes the system to contain detected potential security incidents.	●		●	●		●
Mean Time to Resolve (MTTR)	MTTR measures how long it takes the system to resolve potential security incidents.	●		●	●		●
Transaction speed	Measures the number of transactions per second that can be performed (e.g. a blockchain).	●		●	●	●	●
Packet Loss Ratio	Percentage of loss packets respect the total transmitted packets.	●	●		●		
False positives	Determine the ratio of false positives with respect to the number of supposed attacks or security function failures				●		
False negatives	Determine the ratio of false negatives with respect to the number of simulated attacks or				●		

[2] https://5g-ppp.eu/wp-content/uploads/2014/02/Advanced-5G-Network-Infrastructure-PPP-in-H2020_Final_November-2013.pdf

	security function failures.						
Initial Time	Measures the initial delay until messages can be processed by the network.		●	●	●	●	
Migration time	Time required to migrate assets (i.e. NFs) or scale computing/network resources measured from the moment the last message is processed in the initial state until the first message is processed to the migrated state.		●	●	●	●	
Blocked adversarial examples rate	The percentage of adversarial examples successfully detected				●		
Automated model generation	Measures the percentage of the actual network that can be modelled automatically.	●		●	●	●	●
Automated vulnerability assessment	Measures the percentage of identified vulnerabilities that can be used to exploit the network.	●		●	●	●	●
Cyber-security insights assessment	Measures the percentage of the cyber-insights that were used to improve the security posture of a 5G network.	●		●	●	●	●

Table 2: INSPIRE-5Gplus considered KPIs and their relation to 5GPPP Performance KPIs

2.2 INSPIRE-5Gplus Framework High-Level Architecture

INSPIRE-5Gplus framework is designed to support fully automated End-to-End (E2E) network and service security management in multi-domain environments. The framework empowers not only protection but also trustworthiness and liability in managing 5G network infrastructures across multi-domains. In INSPIRE-5Gplus, a “domain” refers to the different technology domains of a mobile network, such as radio access network (RAN), core network (CN), mobile edge computing (MEC).

The INSPIRE-5Gplus framework HLA, depicted in Figure 1, is split into security management domains (SMDs) to support the separation of security management concerns. Each SMD is responsible for intelligent security automation of resources and services within its scope. The E2E SMD is a special SMD that manages security of E2E services (e.g., network slice) that span multiple domains. The E2E SMD coordinates between domains using orchestration. The decoupling of the E2E security management domain from the other domains allows escaping from monolithic systems, reducing the overall system’s complexity, and enabling the independent evolution of security management at both domain and cross-domain levels.

Each SMD, including the E2E SMD, comprises a set of functional modules (e.g., security decision engine, security orchestrator, trust manager) that operate in an intelligent closed-loop way to enable software defined security (SD-SEC) orchestration and management. Each functional module provides a set of security management services that can be exposed inside the same domain or cross-domain, to the authorized consumers, using the domain integration fabric or the cross-domain integration fabric, respectively.

In addition to a multi-domain design, the INSPIRE-5Gplus security architecture is extensible to multi-operator and over the top (OTT) environments by considering their security threats and requirements. Indeed, the inter-domain fabric provides an inherent capability for security management among disparate networks as shown in Figure 1. In what follows, we provide a concise description of the key functional modules composing the INSPIRE-5Gplus framework HLA at both domain and E2E levels.

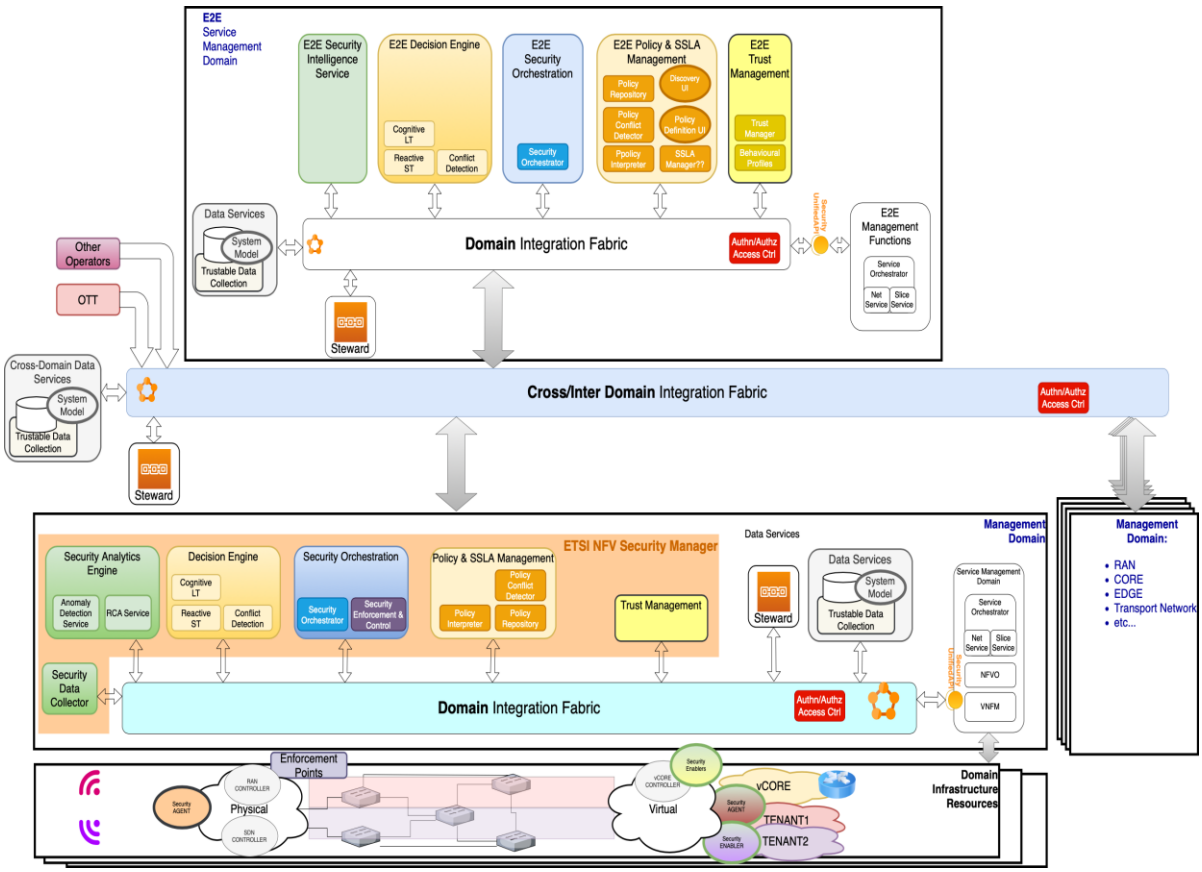

Figure 1: INSPIRE-5Gplus Framework HLA

2.2.1 Domain-Level Functional Blocks

2.2.1.1 Security Data Collector

The main function of the security data collector (SDC) is to gather all the data coming from the security enablers at the domain level, needed by the security management functions (e.g., Security Analytics Engine). The types of data collected by the SDC may include:

- Performance monitoring data (e.g., counters and statics data);
- Security monitoring data (e.g., traffic meta-data, packet capture, session data);
- Event/alarm data (e.g., system logs, application traces, system traces);
- Machine learning reference data sets;
- External data (e.g., Cyber Threat Intelligence (CTI), external data sets).

2.2.1.2 Security Analytics Engine

The main function of the Security Analytics Engine (SAE) is to derive insights and predictions on the domain's security conditions based on data collected in the specific domain or even from other domains. In the context of INSPIRE-5Gplus, the SAE provides the Anomaly Detection and the Root Cause Analysis (RCA) services. The Anomaly Detection service has the capabilities of detecting and/or predicting anomalous behaviours due to malicious or accidental actions by identifying patterns in data or behaviour that are not conforming to expected normal behaviour. The Anomaly Detection service leverages data aggregated by the SDC from the managed entities of the domain, including performance and security monitoring data, events and alarms, generated by system logs and packet traces. The RCA service identifies the cause of the observed security incidents by analysing and correlating data from other services (e.g., Anomaly Detection service) The Root Cause

is the location in the network where applying a corrective action would prevent the problem from occurring. As a result, the RCA service also provides recommended actions to correct the root cause of network incidents.

2.2.1.3 Decision Engine

The Decision Engine (DE) functional block oversees the different actions emitted by the security assets and the SAE to select the best decisions to apply for securing a running targeted service. This centric component acts as an arbitrator between security assets and the rest of the platform that manages domains.

The Decision Engine (DE) delegates the actual mitigation creation to Cognitive Long Term and Reactive Short-Term assets. Those assets contain the algorithms to build a coherent mitigation plan given a detected threat:

- The Cognitive Long-Term assets will be based on advanced AI techniques and may use past data across several sources to internally create correlations, potential forecasts and propose to the DE elaborated mitigation plans.
- The Reactive Short-Term assets will be built up on simple rules to provide quick and mundane reactions to specific events. These rules will be akin to what a human operator would do given a situation. To counter their simplicities, the mitigations resulting from those assets can be computed and enacted rapidly.

The Decision Engine (DE) relies on multiple “third-party” assets running concurrently and waits for them to emit a mitigation proposal. Those actions can then land in the Decision Engine without any given order and sometimes they may be conflicting. For example, a Reactive Short-Term asset may see a device as legitimate and authorise its traffic. Whereas a Cognitive Long-Term asset may see this specific device as a potential Ddos-er 10 minutes in the future. In such situation, the Decision Engine (DE) has to arbitrate the conflicting reactions either by using a confidence level and/or by looking at a statically priority list. Finally, as a mitigation may take times to be applied by the underlying Security Orchestrator, the Decision Engine must track selected reactions and ignores new-coming mitigation proposals to let the system stabilize.

2.2.1.4 Security Orchestration

The security orchestrator (SO) oversees the different security enablers to cover the security configuration requirements in the corresponding Management domain specified in the defined security policy. SOs are part of each Management Domain as well as the E2E Service Management Domain. Even if the Security Orchestration from a Management Domain perspective is autonomous in how enforcement occurs in the associated domain, the E2E Security Orchestration enforces E2E decisions by splicing and delegating these decisions onto Policies to be delivered to the corresponding Security Orchestrators of the Management Domain that will then enforce them with a certain degree of independence.

The SO drives the security management by interacting, through the integration fabric, with the different SDN controllers, NFV MANO and the security management services. The SO will enforce proactively or reactively the security policies through the allocation, chaining and configuration of virtual network security functions (VSF) such as virtual Intrusion Detection System (vIDS), vFirewall, virtual Authentication, Authorization and Accounting (vAAA). The SO will be fed by the evolving system model, the trust and reputation indicators coming from the Trust Management (TM) component, as well as the insights and evolved plans inferred by the DE. This cognitive behaviour will provide self-healing and self-protection capabilities to the entire managed system, allowing the orchestrator to react automatically according to the actual context, and timely trigger the adequate countermeasures to mitigate the ongoing attacks or prevent foreseen threats. Potential reactions encompass, among others, applying security policies to control the traffic (e.g., by dropping or

diverting it) through an SDN controller, and deploying, decommissioning, re-configuring or migrating the VSFs.

2.2.1.5 Policy and SSLA Management

The Policy and SSLA Management (PSM) component captures and negotiates the Protection Level and Security Level requirements and constraints expressed by consumers and providers allowing the security orchestrator to configure, deploy and manage the security services. The PSM provides specification and monitoring capabilities to define Security Service Level Agreement (SSLAs) based on policies and assess them in real-time in cooperation with other INSPIRE-5Gplus functions, such as the Security Orchestrator or the E2E Decision Engine Conflict Detection module. The SSLAs provide the mean to specify the security requirements or policies and assessing or enforcing their fulfilment to obtain the desired security level.

2.2.1.6 Trust Manager

The Trust Manager (TM) manages the trust related functions in the security framework. It contains various internal services for trust management. As a key building block, Trust Reputation Manager (TRM) service in TM assigns trust + reputation values to monitored 5G entities and provides them to security management entities and end users in 5G virtualized networks. Component Certification Service CCS provides a static evaluation of the different 5G network components by measuring adapted metrics automatically or manually. These metrics are combined for defining trustworthiness properties exposed by the components. Similarly, for trusting a slice, Slice Trustworthiness Service STS ingests slice-related data (static and dynamic properties) and scores a 5G slice based on related parameters for the end-users or other system components.

For trust in how data flows traverse a network and are processed spatially, Ordered Proof of Transit (oPoT) service verifies the correct order of nodes on the network path followed by a flow. The oPoT service brings the opportunity to create trust in the process of guaranteed slices confinement, or inter-domains trust. For the 5G networked services themselves, Service Trust Manager service is designed as a Smart Contract and it will calculate the trust and reliability of a cloud infrastructure or the services deployed on it, based on multiple values for both the infrastructure and the services. Different types of Service Trust Manager are devised (with different Smart Contracts for each of them), depending on the element the trust is being calculated.

TM also provides a wrapper service that produces the modifications on the binaries (executable file) in order to deliver the following capabilities, all delivered by the obfuscation-based protected security routine embedded and added on the protected program. The output protected binary is a modified version of the original with modifications aimed at hardening the code against various attacks in confidentiality, integrity, illicit usage and vulnerability exploit. A metadata file or data structure is enclosed in the protected VNF package and describes the various security functions applied with the parameters used for these.

2.2.2 E2E-Level Functional Blocks

2.2.2.1 E2E Security Intelligence Engine

The E2E Security Intelligence Engine derives cross-domain insights and predictions based on data collected from different domains. It has a similar role as the SAE but at the cross-domain level.

This function is necessary for analysing the data provided by the different domain Security Data Collectors or stored in the E2E Data Service to detect any anomalies that can only be detected using information from more than one domain (e.g. SIEM-type analysis that correlates events captured in logs). It generates notifications that will be used by E2E Decision Engine to trigger the necessary remediation or prevention procedures.

2.2.2.2 E2E Decision Engine

The E2E Decision Engine (E2EDE) manages the high-level security at the E2E level. This component consumes events, policies proposal from security assets or from the underlying Domain Decision Engine (DDE) to adapt and propagate the security decisions across multiple domains.

2.2.2.3 E2E Security Orchestration

The E2E security orchestrator (E2ESO) is responsible of orchestrating and managing the different security enablers from multiple domains to cover the security configuration requirements specified in the defined E2E security policy. The E2ESO maps the E2E security policy into the domain-specific policy and interacts with the SOs to apply the corresponding security policies and deploy and manage the life cycle of the required security enablers at domain level.

2.2.2.4 E2E Policy and SSLA Manager

The block provides multi-level SSLA, HSPL, MSPL and final enabler configuration translations. This module is also in charge of avoiding conflicts within the requests as well as historical active requests already enforced on the system.

2.2.2.5 E2E Trust Management

The E2E Trust Manager (E2ETM) facilitates E2E trust services across multiple domains, relying on the domain-resident TMs. It can provide across-domains versions of trust functions by aggregating trust outputs of domain-resident TMs and enriching them with inter-domain parameters. It interacts with E2E Policy and SSLA Manager, and Security Orchestrator to operate in compliance with E2E security requirements, policies and SSLAs.

2.2.3 Domain-Level and Cross-Domain Data Services

Data services allow the different functions to persist data that can be shared by functions in a domain or in different domains. They manage access to authorized consumers. In this way the data persistence and data processing are separated, i.e. enabling stateless management functions and eliminating the need for per-function data persistence and pre-processing.

The data services should support different types of storage techniques (DBMS, DLT, persistent data bus…) depending on the needs. The mechanisms or technologies used could eventually be dynamically selected.

The data is collected by the SDCs and should be handled either within the domain where it was produced or by a well-defined and controlled entity. The Data services need to implement access control, data security policies, and eventually transactions and ACID properties (Atomicity, Consistency, Isolation, Durability) particularly if multiple producers and consumers are involved.

Data types are those collected by the SDC (see list in Sec. 2.2.1.1). The captured data can be either real-time data or historical data needed for security-based analysis (e.g., risk, liability, root cause, vulnerability detection, intrusion detection)

The data can pertain to one domain or shared between domains for cross-domain security analysis and control. The data can be stored and used by different security management functions, such as SAE, DE, SO.

2.2.4 Integration Fabric

The integration fabric allows the interoperation and communication between services provided by the different functional blocks, within a domain and across domains. It provides services to register, discover and invoke security management services. The integration fabric allows the communication

between the security management services via communication channels.

2.2.5 Security Unified API

The Security Unified API aims to be a set of commands/rules that will allow the exchange of information between the Management Functions elements - i.e. Network Slices, Network Service, etc. - and the HLA components and especially with the Security Orchestrator. This API must allow the interactions to be in both directions “from and to” the HLA and the Management Functions elements. The Security Unified API is an element that may be deployed in both the E2E and the multiple management domains.

2.2.6 Security Agent

The Security Agent (SA) is a security function performing security monitoring/management with a local data capturing and/or actionable behaviour. The SAs communicate with the corresponding INSPIRE-5Gplus management plane in their security management domain based on configurable security policies. The SA may provide security data to the analysis and management functions from the traffic plane, acting for instance as active or passive probes.

Preconfigured data for initial configuration is assumed to be injected or loaded at SA instantiation (e.g. from NFV-MANO). An API for runtime configuration could also be available. The Security Agent’s main function is to provide interoperability between INSPIRE-5Gplus management plane and the security enablers in the data and control plane (active or passive). Security enablers can vary in typology and nature. In some domains they can be dedicated security network probes. In others they can be existing VNFs or PNF with security capacity. In all cases, it is expected that the Security Agent function helps translating security policies, i.e. MSPL, to specific or proprietary enabler configuration formats and generate the data required from the network to perform security analyses. This component will expand the interoperability with different vendors and solutions in the 5G domains. The Security Agent functionality will be part of security by enablers and be compliant with the defined INSPIRE-5Gplus interfaces.

3 5G security test cases

3.1 Test case selection methodology

The set of test cases were selected after conducting an analysis of the use cases that are being discussed as part of task T2.4 of WP2 (to be consolidated in deliverable D2.3). We first introduce a brief description of the methodology followed for selecting the set with a total of 9 test cases, and, in the following, each test case is described in detail.

3.1.1 Relation to 5G platforms from 5GPPP projects

The set of the 5G security Test Cases (TC) presented herein were selected by given a special focus on the 5G platform scenarios defined in ICT17 projects, vertical scenarios on cooperative, connected and automated mobility (CCAM) defined in ICT18 projects, and general vertical scenarios for ICT19 projects, addressing the major challenges for 5G security. Figure 2 illustrates the mapping of the selected Test Cases (to be described in Section 3.2) to ICT projects.

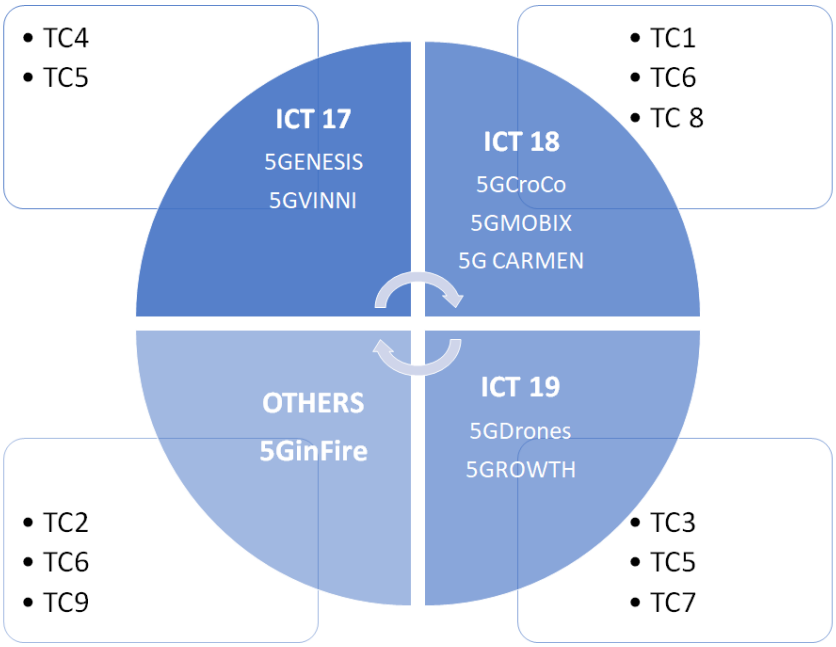

Figure 2: Mapping of INSPIRE-5Gplus Test Cases to 5GPPP projects

3.1.2 Connection to INSPIRE-5Gplus security requirements

Table 3 shows a general view on the security requirements proposed by INSPIRE-5Gplus in D2.1 that are addressed by each of the selected test cases.

Security Requirement	Requirement	Relation to proposed TCs
SEC-REQ-01	The 5G network shall provide telemetry and other auditing information relevant to the security mechanisms of the system.	TC2, TC3, TC5, TC7, TC8
SEC-REQ-02	The 5G network shall only allow authenticated users to consume the services provided by the 5G system.	TC1, TC6, TC7, TC8
SEC-REQ-03	The 5G network shall warrant measurable level of availability of its services to the relevant stakeholders.	TC2, TC3, TC6, TC9

SEC-REQ-04	The 5G network shall ensure the necessary network capacity and network resources for the critical operations of the 5G services.	TC2, TC4, TC9
SEC-REQ-05	The 5G network shall enable a secure platform for vertical services to be deployed.	TC1, TC2, TC3, TC4, TC5, TC6, TC7, TC8, TC9
SEC-REQ-06	The 5G network shall enable the state management of its platform components.	TC3, TC6, TC7, TC9
SEC-REQ-07	The 5G network shall be able to revert to previous states with minimal service disruption of deployed application in case of malicious compromise.	TC1, TC2, TC7, TC8
SEC-REQ-8	The 5G network's security mechanisms should not impact the functional requirements of critical operations for vertical applications.	TC1, TC2, TC7
SEC-REQ-9	The security mechanisms of the 5G network shall be able to be deployed in any potential 5G hardware provider without any impact on their performance or functionality.	TC2, TC3
SEC-REQ-10	The security mechanisms of the 5G network shall be able to measure/evaluate trust level of its components and platforms and share this information with verticals in a safe and trustable way.	TC1, TC5, TC6, TC8
SEC-REQ-11	The security mechanisms used in a complex 5G eco-system shall be able to identify, distribute and allocate responsibilities between 5G ecosystem stakeholders.	TC6, TC7, TC9
SEC-REQ-12	The 5G eco-system shall be able to publish security KPI measuring the compliance of stakeholder with their Security Level Commitments.	TC6
SEC-REQ-13	Technologies used to distribute over 5G eco-system (end to end) and evaluate post security incident root cause of failure are trustable.	TC4, TC5, TC8
SEC-REQ-14	The 5G system must provide security mechanisms to ensure that user (and endpoints) data are securely processed and stored wherever it is processed or stored. Both confidentiality and integrity guaranties shall be brought all along the full lifecycle of the data in transit, process and storage.	TC4, TC5, TC7

Table 3: Relation of the selected test cases to the INSPIRE-5Gplus security requirements

3.1.3 Mapping to INSPIRE-5Gplus security enablers

The purpose of the selected test cases is to validate the 5G security assets and mechanisms developed in INSPIRE-5Gplus. Specifically, the enablers to be evolved or entirely developed in the context of Work Package 3 (WP3) are related to advanced smart techniques, such as Artificial Intelligence and Machine Learning, in order to provide new security enabling technologies for provisioning intelligent and autonomic end-to-end cybersecurity services that are able to detect and mitigate both existing and new threats targeting 5G networks. On the other hand, Work Package 4 (WP4) will evolve existing security assets while developing new ones taking advantage of additional assets and techniques with a focus on trust and liability across 5G infrastructure and services. Table 4 summarizes the enablers from WP3 and WP4 considered by each test case.

Test Case	WP3 Enablers	WP4 Enablers
TC1	Secured Network Slice Manager for SSLAs	Network Slice Manager for Trusted Blockchain-based Network Slices
TC2	Monitoring probes Security Analytics Engine SSLA assessment Self-protection for triggering reaction strategies	
TC3	MMT monitoring framework Software protection techniques Smart Traffic analysis Data collector and aggregator	Software trust leveraging TEE.
TC4	Security Orchestrator SliceManager/Provider IAM i2NSFController as SDN Controller APP i2NSF agent/ vIPsec DTLS Proxy VNFM Policy Repository Conflict Detector Cognitive Long-Term Planning Data Collectors	TEE - Intel SGX
TC5	Katana Slice Manager Security Analytics Framework Moving Target Defense Controller MMT probes and monitoring framework Defense Optimization Engine (OptSFC) Security Orchestrator	
TC6	Security Orchestrator Migrate (UMU) DLT Policy Repository Conflict Detector Data Collectors Behavioural Profiles	Trust Manager TEE - Trusted Execution Environment
TC7	Network slice manager Analytics Engine SLAs manager Active/Passive Probes Auto-scaling tools Damage control component ML models robust to adversarial attacks	

TC8	Model Generation of 5G networks through network capture files Cyber-security insights assessment Automated identification of threats based on the attributes of the network Automated assessment of vulnerabilities of the network's components	
TC9	SFSBroker	

Table 4: Mapping of the enablers from WP3 and WP4 to be validated for each test case

3.1.4 Risk Assessment

On the selection of TCs for validation in INSPIRE-5Gplus, we have considered TCs that expect moderate risk on the different phases of implementation. A risk assessment is presented in more details for each TC in Section 3.2 as well as for each 5G security infrastructure in Section 4. The key aspects valued in the risk assessment are the following:

- Risk on the modelling of the Test Case.
- Maturity of technologies/enablers from WP3 and WP4.
- Risk on the timeline according to 5GPPP ICT projects.
- Risk regarding integration on the test infrastructure.

In the following sections, we provide an initial description of the set of security test cases that can be deployed to validate the 5G security assets and mechanisms developed in INSPIRE-5Gplus.

3.2 Test cases description

3.2.1 Test Case 1: Secured Anticipated Cooperative Collision Avoidance

Autonomous vehicles depend mainly on sensors placed inside and around the car in order to sense their environment, i.e, streets, buildings, signals, pedestrians, etc.- and to control the vehicles around them. However, certain situations cannot be discovered by these sensors as the situation might have happened out of their range -i.e. traffic jams, accidents, and others-. To these situations, Vehicle communications (V2X) are essential as they allow not only being aware of the situation in advance -i.e. range of Kms- but also to cooperate in order to make the emergencies services act faster than they do nowadays.

V2X involve a set of multiple elements -i.e. cars, bikes, pedestrians, etc.- moving at a different speeds and directions while exchanging information among them. Depending on the scenario -i.e. urban, semi-urban, railways, the obstacles between transmitters and receivers are very different -i.e. skyscrapers, buildings, trees, etc.-. Due to the variety of obstacles and the speed of the vehicles, the information in this type of communications must be transmitted and processed with low latencies -i.e. range of ms, with the lowest retransmissions possible while the infrastructure must be aware at any moment where each vehicle is. This test case (TC) is focused on ensuring the information exchange between vehicles and the infrastructure. To do so, the scenario is based on one of the use cases (UC) presented in the EU 5GCroco (https://5gcroco.eu/) project, the so called: Anticipated Cooperative Collision Avoidance (ACCA).

Figure 3 shows the ideal situation on which the TC will work and present its problematic situations to be solved through the INSPIRE-5Gplus framework. The idea is to have a Network Slice composed by three Network Services (NSs) to exchange traffic information: two equal NSs, each deployed into a Road-Side Unit (RSU), and the third NS in a Central Node with the biggest amount of computational resources to share the information with other domains.

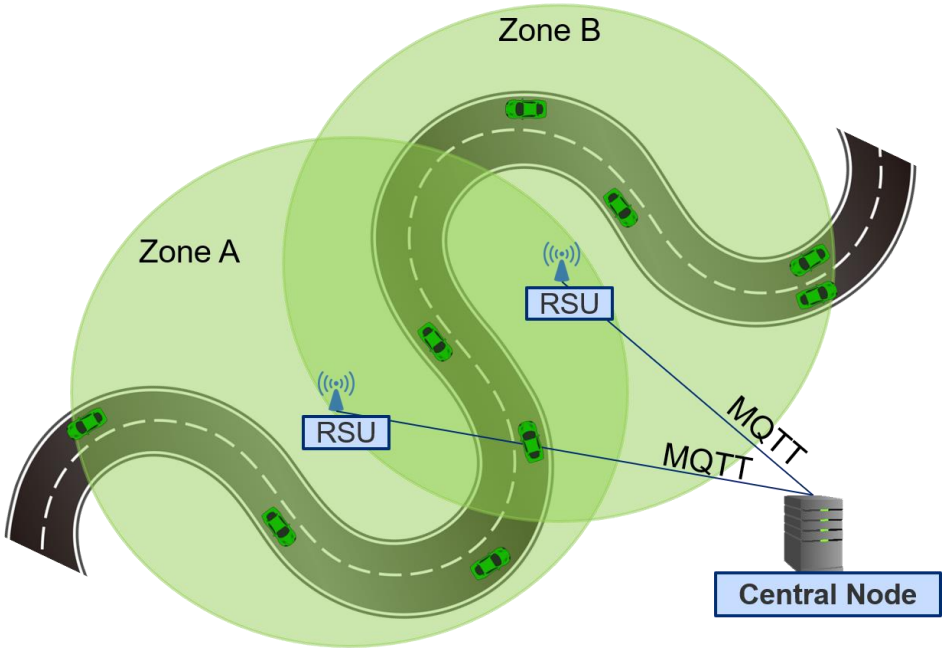

Figure 3: Ideal Scenario

3.2.1.1 Problem Description and Objective

This TC focuses first on checking that the elements composing a network slice before it is deployed are valid and they are not tampered, and secondly, how security is applied once the network slice is deployed. To show these two aspects, this TC aims to use the following two situations:

Sub-case 1: Fake Car Accident Scenario

As Figure 4 shows, the problematic scenario appears when a malign node generates information notifying for a fake car accident (red car) which will generate traffic problems on the surrounding cars as they will slow down causing possibly a traffic jam and also to those cars far away who will choose a different road to avoid the accident.

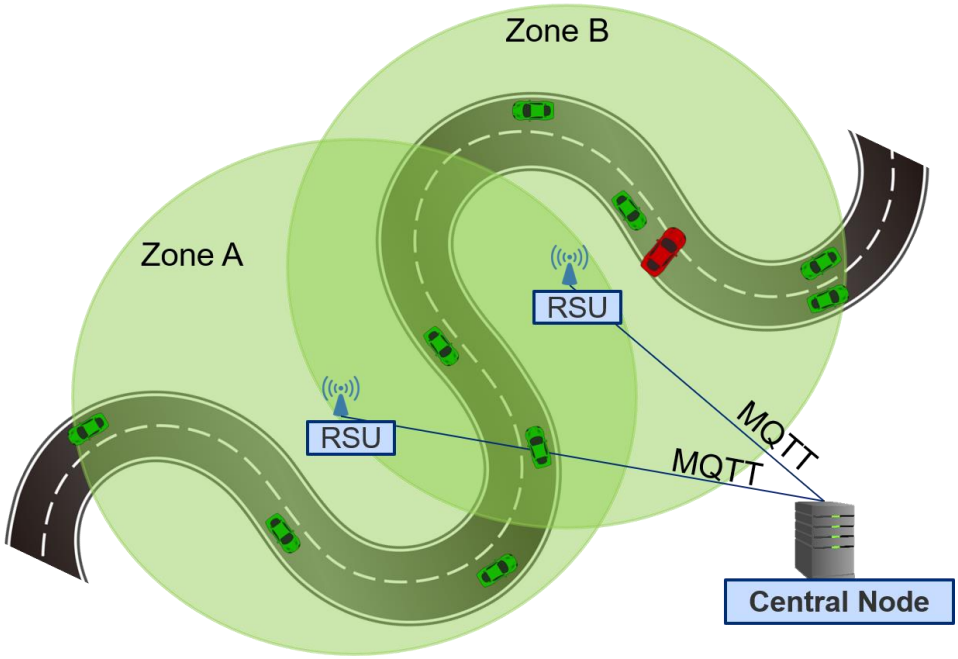

Figure 4: Fake Car Accident Scenario

Sub-case 2: Trusted network slice components scenario

The second scenario aims to use Blockchain as a solution to add trustworthiness to the elements when deploying the elements composing a network slice. By using a Validation and Verification tool, the objective is to test and validate the correctness of the elements defining a network slice -i.e. network slice templates, networks services, etc.-. If the results are correct, the information regarding the correct validation and verification of those elements would be uploaded in the Blockchain shared with Network Slice Managers. Then, when a Network Slice Manager aims to upload/add a new network slice element, if its validation is not in the Blockchain, the network slice element will not be accepted and available. Figure 5 shows the architecture for the verification and validation procedure of network slice components and a distributed Network Slice management across domains.

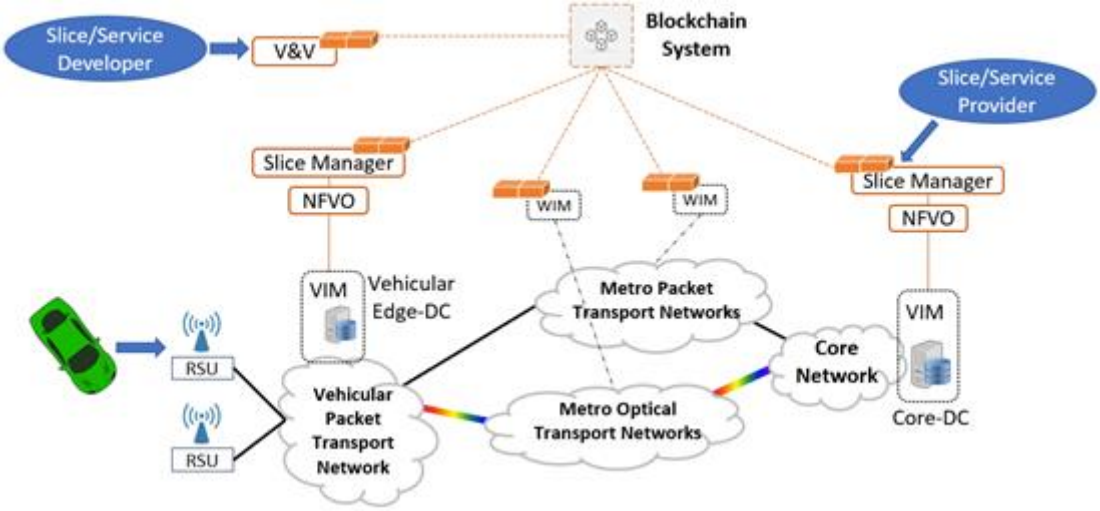

Figure 5: Trusted network slice components scenario

To address the previous two scenarios, this TC will focus on the management of an End-to-End (E2E) Network Slice composed with secured and verified NSs and their Virtual network Functions (VNFs). On the first scenario, the TC aims the use of Security Service Level Agreements (SSLA) to identify the fake information generated by the malicious node and apply the correct solution -e.g. firewall or other possibilities-. The second scenario aims to use of Blockchain as a new element to be used within the creation of Network Slices and the participation of multiple IPs in them.

Based on the previous drafted solutions, the objectives are:

1) The management and orchestration of End-to-End (E2E) Network Slices which are composed only with NSs and VNFs previously verified as secure elements.

2) The use of SSLA to monitor and verify that the E2E network Slice performs as expected.

3) The use of a Blockchain technology in order to add trust to the elements defining a network slice for vehicular services.

3.2.1.2 Functional Architecture

The functional architecture for the previous scenarios is presented in Figure 6. Based on the described situations, there will be three main elements:

- Cloud DC: It corresponds to the Central Node in Figure 4, Figure 5 (called Core-DC) and Figure 6. Its main functionalities are the management of the data generated by all the Vehicular MEC nodes -i.e. analytic, forwarding, etc.- through the use of a V2X Communications Application and the detection of malicious data generators like the fake vehicle accident in the first scenario of this TC using an Intrusion Detection System (IDS). The idea is to develop a proprietary IDS service able to identify whether a vehicle is fake or not using historical records -i.e. position, speed- based on these records, generate a self-designed metric called Trustworthiness (T) to be associated to each vehicle. If the value T becomes lower than the threshold defined in the selected SSLA, Security Intelligent System will start the proper actions (calling the SO, Policy&SSLA Manages, etc.) to update the firewalls allowed vehicles in the RSU.
- Vehicular MEC-X: This is the functionality to be done by the Road-Side Units (RSUs) in Figure 4, Figure 5 and Figure 6. Like the Cloud DC, these elements will also use a V2X Communications Application in order to communicate with the vehicles and the Cloud DC. Together, a Firewall will also be used in order to filter the traffic that the Cloud DC will classify as not acceptable.

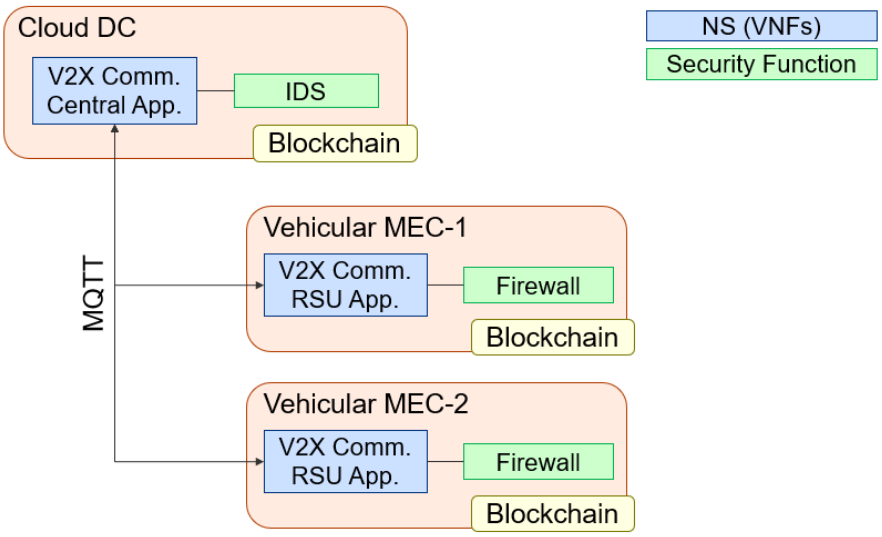

Figure 6: Functional Architecture

In all the previous blocks, there is one functionality in common, which is the Blockchain validation and verification of all the three elements. Furthermore, the last element in common is how the Vehicular MEC nodes communicate with the Cloud DC node. To do so, Message Queuing Telemetry Transport (MQTT) will be used as it allows to transmit information through a publisher & subscriber.

In order to understand better how this TC is related with the INSPIRE-5Gplus framework, Figure 7 shows how each one of the elements within the High Level Architecture (HLA) participates in the deployment of an E2E Network Slice:

1) Vertical requests an E2E network slice (slice) with an associated SSLA to the E2E Network Slice Manager (Slicer).
2) The E2E Slicer allocates each Network Service (NS) to the correct domain and requests its deployment to the specific Domain Slicer.
3) The E2E Slicer requests the SDN Controller to configure the inter-domain paths between NSs.
4) The E2E Slicer requests the associated SSLA to the E2E Policy&SSLA Manager (PS).
5) The E2E PS requests to each Domain PS to configure and associate the SSLA to the deployed NSs.
6) The E2E Slicer requests to the E2E Security Orchestrator (SO) the Security Functions (SF) deployment next to the E2E slice NSs to add the expected security.
7) The E2E SO requests to each Domain SO the specific SF deployment.
8) The E2E SO requests the E2E Security Intelligence Engine (SIE) to monitor the E2E slice.
9) The E2E SIE configures each Domain SIE to monitor the NSs security performance.
10) Once all the elements are deployed and configured, the data is saved and the E2E slice ready.

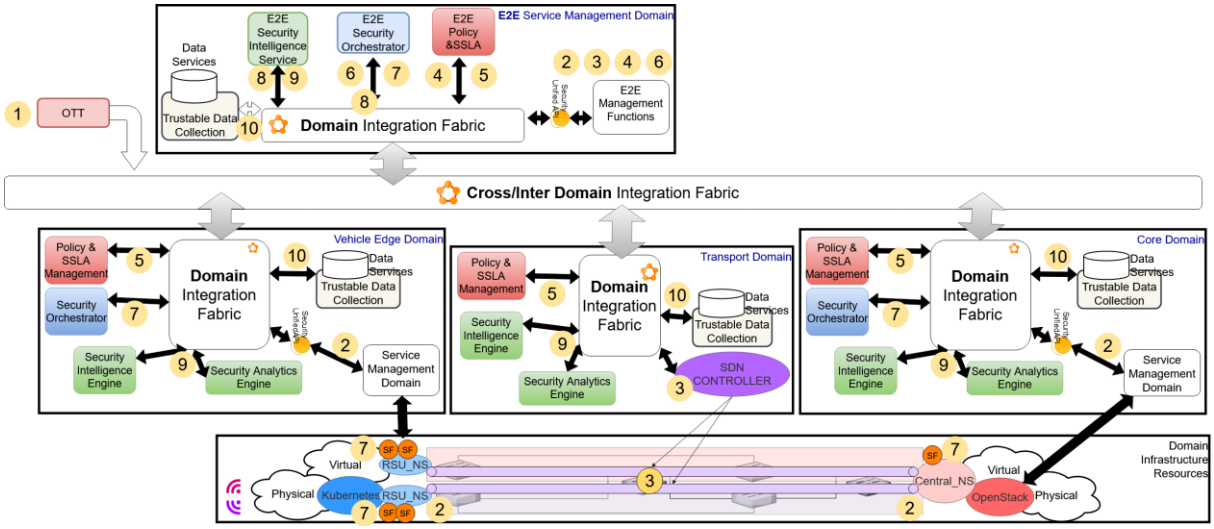

Figure 7: E2E Network Slice Deployment step within the HLA.

3.2.1.3 Target KPI

In order to evaluate the previous attack situations and ensure that the security functionalities work according to the expectations and have a good performance, Table 5 shows the selected KPI with the associated Service Level Requirements (SLRs). The selected list is intended to be an initial list of values to be used as reference, so in future works this table may be updated.

Target ACCA KPIs			
SLR Title	**SLR Unit**	**SLR Value**	**Explanation/Reasoning/Background**
Mean Time to Detect (MTTD)	[ms]	Mean value < 10 min	MTTD measures how long it takes the system to detect potential security incidents.
Mean Time to Contain (MTTC)	[ms]	Mean value < 10 min	MTTC measures how long it takes the system to contain detected potential security incidents.
Mean Time to Resolve (MTTR)	[ms]	Mean Value < 10 min	MTTR measures how long it takes the system to resolve potential security incidents.
Latency	[ms]	Time to reach destination < 100 ms.	Due to the vehicles speed, it is necessary that the information travels and reaches the destination the fastest way possible. Use of MEC should allow to send the message from the RSU node in which a vehicle is linked to the central node.
Transaction speed	[t / s]	A minimum of 12 t/s	Number of transactions per second that the Blockchain performs.
Packet Loss Ratio (PLR)	[%]	PLR =< 1 %	Percentage of loss packets respect the total transmitted packets.

Table 5: ACCA Test Case KPIs

3.2.1.4 Requirements for deployment, preconditions

The requirements and pre-conditions to properly develop this TC are:

1) VNF Security Certification using V&V: To reach the first of the three objectives, it is necessary to have a tool and a methodology to verify and certify that a NS and its VNFs are secure. The selected tool will follow the idea designed and presented in the H2020 5GTANGO project, the Validation and Verification (VnV) platform which was able to verify and validate if the functionality of a NS (and its VNFs) was the expected one. Within the context of the INSPIRE-5GPlus project, the point is to validate that the NSs and VNFs can be considered as secure by passing a set of tests.

2) Connected Vehicle authentication and authorization: The core functions involved are the Access and Mobility Function (AMF) and the Authentication Server Function (AUSF). The AMF initiates the authentication procedure with the vehicle and communicates to the AUSF the serving network name. Then, the AUSF determines whether the AMF is authorised to send this message. The AUSF also provides security features through specified security functions, i.e., Authentication Credential Repository and Processing Function (ARPF) and Security Anchor Function (SEAF). All these functions are part of the 5G core Service-Based Architecture (SBA) and can be deployed as secured VNFs.

3) Secured Multi-domain Network Slicing: The E2E Network Slice to be deployed aims to make use of the benefits offered by the different domain characteristics -i.e. low latencies, high bandwidth, etc.- and technologies -i.e. Kernel-based Virtual Machines, Containers- in order to deploy the NSs within the E2E Network Slice in the most efficient way possible. For this reason, the testbed must be composed of multiple domains and among them the two most

necessary are: Vehicular and Cloud domains.

4) Distributed Ledger Technologies (DLTs) - Blockchain: It is necessary to have a private and permissive Blockchain to have the defined scenario with the three nodes involved.

3.2.1.5 WP3/WP4 enablers

For the correct TC development and demonstration success, an existing Network Slice manager will be extended with two enabler functionalities called: “Secured Network Slice Manager for SSLAs” defined in WP3 and “Network Slice Manager for trusted Blockchain-based Network Slices” defined in WP4.

The Secured Network Slice Manager for SSLAs (WP3 enabler) for these solutions is the ability to manage SSLAs associated to the E2E Network Slices deployed and monitor them in order to ensure the safeness performance of each component within an E2E Network Slice.

The “Network Slice Manager for trusted Blockchain-based Network Slices” is the enabler to be designed and developed in the WP4 context. In this case the point is to add one more security layer to the E2E Network Slices in addition to the SSLA. By using Blockchain, this enabler aims to classify the NSs and VNFs as securely verified by passing a set Security Functions (SFs) -i.e. Probes- that will test and validate the expected NSs and VNFs operation.

3.2.1.6 Methodology and expected outputs

Methodology

The previously defined TCs scenarios will be developed using a collaborative methodology through the use public GitHub repositories:

Enabler Repository - Regarding the enablers to use in the two previously defined sub-cases will be developed and integrated in a single enabler using the following GitHub repository: https://github.com/INSPIRE-5Gplus/i5p-netslice-mgr. Furthermore, is is plan to create a secondary GitHub repository for the Virtual Machine (VM) images that will be used during the TC tests and demonstrations whose name will be: “i5p-vehicle-location-integrity-validator”.

Test Case - In relation to the TC, all the tests and KPIs among other possible necessary documentation will be managed and maintained using the following GitHub repository: https://github.com/INSPIRE-5Gplus/i5p-tc-acca. During the tests phase, it is planned to use OpenTAP as the test system to develop and control them.

The development of this TC will follow the next steps:

1. A research and an evaluation on the existing software enablers will be done in order to define what can be used and what needs to be developed.
2. With all the necessary enablers defined, a check process will be done to verify how can they be integrated following the ZSM architecture defined in WP2.
3. Design and definition step to create the Network Services and Functions, the Security Functions, the SSLA and Policies descriptors to be used in the two different TC scenarios for the final deployments.
4. With the previous steps done, then we will start developing those elements that are not available in order to integrate them with the existing enablers.
5. Realization of multiple tests in order to obtain the results and compare with the defined KPIs.

Regarding the last two steps, once the first version of the integrated enablers is done, they will be carried out in parallel in order to keep improving the deployment and integration of the multiple enablers involved.

Outputs

As this TC has two different scenarios to be studied -i.e. SSLAs and Blockchain on Network Slicing-, two are the expected outputs during the test and demonstration phases. On one hand to validate that the SSLAs are well applied by forcing situations in which the SSLA is violated and the associated solution -i.e. policy- is applied. On the other hand, to validate that only those verified and validated network slices may be available and deployed.

3.2.1.7 Timeline and risks

This TC has its origin on the EUC 5GCroCo project, an ICT-18 project started in November 2018 and that it will finish in November 2021. As Figure 8 presents, INSPIRE-5Gplus and 5GCroCo projects co-exist until November 2021. In that moment INSPIRE-5Gplus will still have 11 months more before it finishes. So, while both projects will co-exist this TC will have the support from the 5GCroCo project but, once this is finished (November 2021), the support will be reduced to the CTTC task force involved in the INSPIRE-5Gplus project.

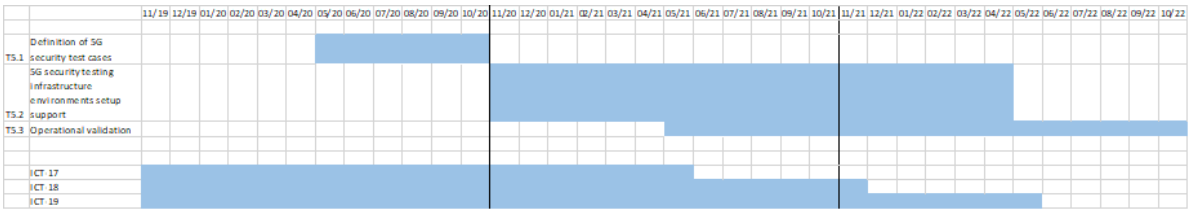

Figure 8: INSPIRE-5Gplus WP5 and ICT-X projects timeline

Based on the timeline presented in Figure 8, this TC defines three phases in order to demonstrate its evolution until the end of the INSPIRE-5Gplus project. Table 6 presents the three phases in which this TC is divided:

Phase	Time	Description	Risks
0 - Basic scenario	M12	In this phase the idea is to have 2 simulated vehicles moving near an active RSU. A Network Slice will be deployed involving the RSU and the Central Node (CN). The RSU will contain an MQTT broker and a GeoServer APP that will communicate with the CN. Associated to the Network Slice, a Security Function (SF) will be deployed. The SF will be in charge to check the vehicles location integrity. In order to have all the elements deployed, it is necessary to make us of the Network Slice Manager and the Security Orchestrator.	No risks are foreseen.
1 - Scenarios Integration and Testing	M24	During this phase, there are two main objectives: – to evolve the previous phase and integrate the enablers within the Barcelona testbed (Section 5.5.4). – to create an automated testing system in order to do the maximum tests possible and validate the	No risks are foreseen.

		integration of the enablers with the testbed network.	
2 - Scenarios Demonstration	M36	By the end of the project, the objective is to have the used enablers fully integrated in this TC. Furthermore, to demonstrate the correct functionality of the enablers through monitoring and tests activities to validate the KPIS and extract the final results.	5GCroCo infrastructure availability

Table 6: ACCA TC Phases and Risks

3.2.2 Test Case 2: Definition and assessment of Security and Service Level Agreements and automated remediation

This test case concerns the definition of SSLAs for assessing and controlling that: the security functions are correctly implemented, the security properties are not violated, and the violations trigger self-healing and self-protection strategies.

The main goal of this TC is demonstrating how: SSLAs can be defined and enforced, and how they facilitate the agreements between different constituents concerning the expected cyber-security level and remediation strategies.

This TC shows how SSLAs can be defined for formalising the requirements related to a wide variety of cyber-security issues and concerns. It goes far beyond current intrusion detection and prevention systems, as well as policy control systems, in that:

- It is based on real-time metrics that allow fine-grained or more abstract assessment of the security requirements of the different stakeholder involved.
- It allows detecting security breaches as well as malfunction of security functions.
- It integrates remediation strategies that can be triggered automatically with the goal of enforcing the specified SSLAs.

3.2.2.1 Problem Description and Objective

The ability to define and manage Security-oriented SLAs (SSLAs) is essential for operators offering managed services. Similar to the SLAs concerning performance, SSLAs is a contract between an operator and a customer that defines the services and the security levels that both parties expect. In other words, SSLAs are needed by operators, service providers and end-users to “contractualise” the requirements related to security capabilities of the provided networks, slices and services. The defined SSLAs allow controlling that the security functions are correctly implemented and that the security properties are not violated.

To better automate the process of defining and enforcing SSLAs, real-time monitoring of network, application and system activity based on distributed probes is needed. The probes, or Security Agents, capture the data, meta-data and statistics that allow measuring the parameters implicated in the specified SSLAs. Then, Complex Event Processing and Machine Learning can be used to analyse and detect breaches at the local level by the Security Agents or at the domain or cross-domain level by the Security Analytics Engine. Finally, when breaches are detected, corrective actions (e.g. self-healing or self-protection techniques) need to be taken. These actions can be triggered manually by the operators, or automatically by the Decision Engine that interacts with the Orchestrators and Controllers to perform the necessary actions.

SSLAs are defined for assessing and controlling that:

- the security functions are correctly implemented
- the security properties are not violated
- the violations trigger self-healing and self-protection strategies

SSLA metrics examples:

- Data and service availability
- Geolocalisation of data/services
- Frequency of security analysis
- Number of GTP per subscriber
- Isolation access from other slices
- Security enforcement techniques:
    - Time to deploy new technique
    - Delay in applying patches
    - Delay in reconfiguring
    - Delay in revoking users/operators
    - Delay in replicating services and switching instances.

3.2.2.2 Functional Architecture

The following diagram presents the functional architecture for the Test Case.

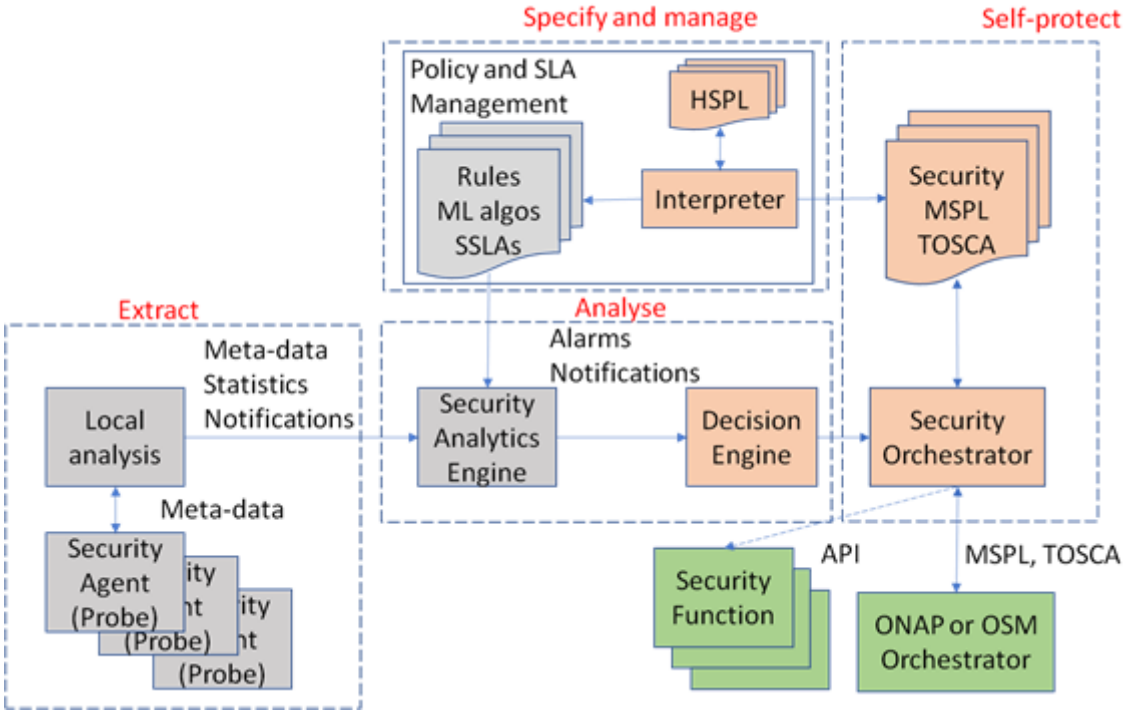

Figure 9: Use case functional architecture diagram

The main functions are depicted in red. The probes (Security Agents) provide the data analysed locally and/or by a centralised application (Security Analytics Engine) that will notify the Decision Engine. The Decision Engine will trigger the corrective actions that could involve interacting with the Security Orchestrators or directly with the Security Functions and Controllers.

3.2.2.3 Target KPI

Target KPIs			
SLR Title	SLR Unit	SLR Value	Explanation/Reasoning/Background
Number of false positives	Number	Ratio of FP < 1%	Determine the ration of FP with respect to the number of supposed attacks or security function failures
Number of false negatives	Number	Ratio of FN < 1%	Determine the ration of FN with respect to the number of simulated attacks or security function failures. This needs to be done under controlled conditions (i.e. using generated traffic that contains different types of attacks or failures)
Mean Time to Resolve (MTTR)	Time in sec.	< 10 sec.	The detection rules and algorithms should perform so that the attack is detected and blocked before it has the possibility of impacting the services

Table 7: Target KPIs for TC2

3.2.2.4 Requirements for deployment, preconditions

MMT (Montimage Monitoring Tool) security monitoring framework integrated with the 5G testbed by deploying and configuring the probes (Security Agents) and providing access to the captured meta-data to the MMT security monitoring framework.

The probes and analysis need to be configured so that:

- The probe captures the needed information:
  - Required statistics on data and control layer traffic,
  - Required operating system metrics (memory, caches, CPU…).
- SSLAs are defined to detect to unusual behaviour that can be considered malicious, such as:
  - Detection of spikes or increase in the number of sessions per second and per user,
  - % of very short sessions or incomplete sessions.
- SSLA reaction strategies defined to:
  - Generate alarms, notify Security Orchestrator, change configuration of security function, etc.
  - Limit the cost in terms of memory and CPU of the security probes,
  - Reduce or increase the number of security rules and algorithms.

3.2.2.5 WP3/WP4 enablers

MMT (Montimage Monitoring Tools) security monitoring framework with the following enablers:

- Monitoring probes (i.e. Security Agents),
- Security analysis (i.e. Security Analytics Engine),

- SSLA assessment (i.e. Decision Engine)
- Self-protection (i.e. Decision Engine) for triggering reaction strategies (e.g. interaction with the Security Orchestrator).

EPC-in-a-Box: 5G SA (Stand Alone) experimental platform based on SDR (Software Defined Radio), open-source or proprietary EPC (Evolved Packet Core) and integrating the MMT security monitoring framework.

All are available today except the Self-protection which is only partially available, and the experimental platform that is being tested.

3.2.2.6 Methodology and expected outputs

Methodology

The following steps need to be performed.

Step 1: Development and integration:

- Test and debug current MI's 5G Stand Alone platform,
- Integrate the SSLA enabler in the 5G testbed's MMT framework,
- Extend Self-protection module (optional)

Step 2: The SSLAs need to be specified and verified, as well as the reaction strategies. This could mean that it is necessary to add or modify specific protocol or data parser plugins so that the probes can capture the needed data and that the framework can trigger reactions. Eventually, the SSLAs can be managed by the Policy and SLA Management module.

Step 3: Probes need to be provided that can extract the metrics required by the SSLAs and integrate local analysis functions. They need to be able to perform real-time capture of metrics. Possible data the needs to be processed by the probes is: network data/control plane traffic, system logs, and application traces. The probes should have the ability of analysing the data using specified rules extracted from the SSLAs, and analysing statistics and behaviour using, e.g. machine learning techniques.

Step 4: The probes are deployed and configured to assess the SSLAs.

Step 5: Metrics and notifications provided by the probes need to be communicated through some channel to the Security Analytics Engine of the framework.

Step 6: The Security Analytics Engine needs the rules and algorithms that allow it to detect breaches and notify the Decision Engine of the framework when they occur.

Step 7: The Decision Engine needs the rules and algorithms that define the strategy that needs to be triggered to remediate a detected breach. The strategy can be implemented using pre-existing or generated scripts, generated Tosca or MSPL descriptions, embedded functions, or generated alarms/notifications that will be addressed by the operators manually.

Output

The non-respect of a SSLA is detected and the remediation strategy is correctly carried out.

The TC is successful if the rates of false positives and true negatives are low, and the reactions correctly remediate the security problems detected, assuring that the SSLAs are always applied as far as possible. The security problems involve both detecting malfunctioning security functions and malicious attacks (e.g. DDoS, data exfiltrations, and evasions).

3.2.2.7 Timeline and risks

Phase	Time	Description	Risks
Set up of platform	M20	Deploy the existing components in the testing facilities.	Unavailability of bug free 5G SA platform. Mitigation: Use the currently available 5G NSA version, or simulate the traffic and the attacks using some gNodeb emulators and traffic generators.
Extensions	M24	Extend the enablers	Lack of resources Mitigation: reduce the scope of the test case to focus on some important aspect (e.g. traffic related SSLAs).
Integration	M28	Integrate the different elements	
Experiments	M32	Test and evaluate the solution	

Table 8: Timeline and risks for TC2

3.2.3 Test Case 3: Network attack detection over encrypted traffic in SBA

This Test Case concerns the detection of network attacks over encrypted traffic in Software-Based Architectures as standardised in 5G [3GPP TS 23.501]. It also includes attacks on anti-malware software defined functions that can be evaded using encrypted traffic (e.g. reducing their performance, provoking malfunctioning, making attacks undetectable by DPI techniques, or attacked by tampering its integrity. The Test Case leverages the use of data and software protection techniques empowering Intel 's SGX enclave[3] to prevent two types of attacks: unauthorised access to data on the one side and detection of software characteristics and behaviour the other side. A holistic security survey will be made to identify the attack surface, the security threats and the remediation that are deemed appropriate.

3.2.3.1 Problem Description and Objective

5G networks will expand the use of encrypted communications that can be used for cyberattacks. 5G Core defines Service Based Architecture (SBA) using HTTPS encryption, and data plane traffic will be encrypted. Also, the current tendency to pervasive E2E encryption over internet applications and services, e.g. DoH (DNS over HTTPS), QUIC (HTTPS over UDP) are also based on TLS adoption. Therefore, current cybersecurity network tools based on network monitoring will not be effective in this environment, making it very difficult to detect some common attacks based on botnets, application layer attacks or DDoS.

To be able to detect these attacks, the security monitoring needs to be capable of analysing encrypted traffic, and it also needs to be protected from introspection attacks and evasions.

Introspection attack (direct access on the software) can be exploited by a malicious attacker and, in this way, access the Software Defined code, reverse engineer it and find a way to disable the detection.

[3] https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html

Evasions will prevent the monitoring function from working correctly. This can be done by making it crash, by reducing its performance resulting in partial traffic analysis, or by introducing unknown attack techniques that remain undetected.

In the following we give more details on the environments this test case can adopt data plane SBA, and control plane IPX-SEPP.

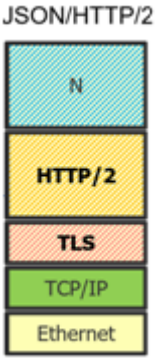

Figure 10: SBA protocol layers

Software-Based Architecture

SBA uses HTTP/2 over TLS (as represented in Figure 10). This introduces vulnerabilities related to attack based on REST APIs that are hidden inside TLS. Possible attacks are the following: malicious vulnerability scans, DDoS, application layer attacks on SBA microservices, IPX SEPP, interfering with SB Interfaces such as Naf, etc.

Figure 11 represent the SBA 5G architecture reference points and service-based representation.

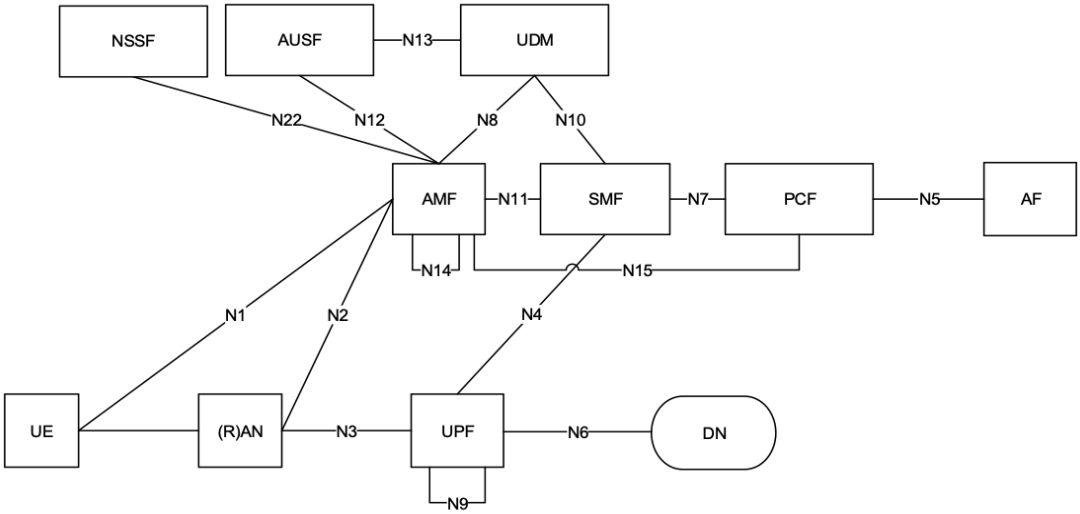

Figure 11: Release 15 SBA blocs and reference points. Source 3GPP TS 23.501 V1.2.0

The reference point representation shows the interaction that exist between the NF services in the network functions described by point-to-point reference point (e.g. N11) between any two network functions (e.g. AMF and SMF).

Service-based representation shows the network functions (e.g. AMF) within the control plane that enables other authorized network functions to access their services. 5G Control Plane only uses the service-based interfaces for their interactions.

IPX-SEPP

Internetwork Packet Exchange (IPX) is a network layer protocol that provides connectionless datagram services for Ethernet, Token Ring, and other common data-link layer protocols. Security

Edge Protection Proxy (SEPP) enables secure interconnect between 5G networks. The SEPP ensures end-to-end confidentiality and/or integrity between source and destination network for all 5G interconnect roaming messages (depicted in Figure 12).

According to the 3GPP 5G security specifications TS 33.501 and TS 29.573, SEPP provides:

- A separate security negotiation interface (N32-c) and an end-to-end encrypted application interface (N32-f);
- Encapsulation of HTTP/2 core signalling messages using JOSE (JSON Object Signing and Encryption) protection for N32-f transmission;
- Operator control of security per roaming partner (via a key library);
- Trusted intermediary IPX nodes to read and possibly modify specific IEs in the HTTP message, while completely protecting all sensitive information end to end.

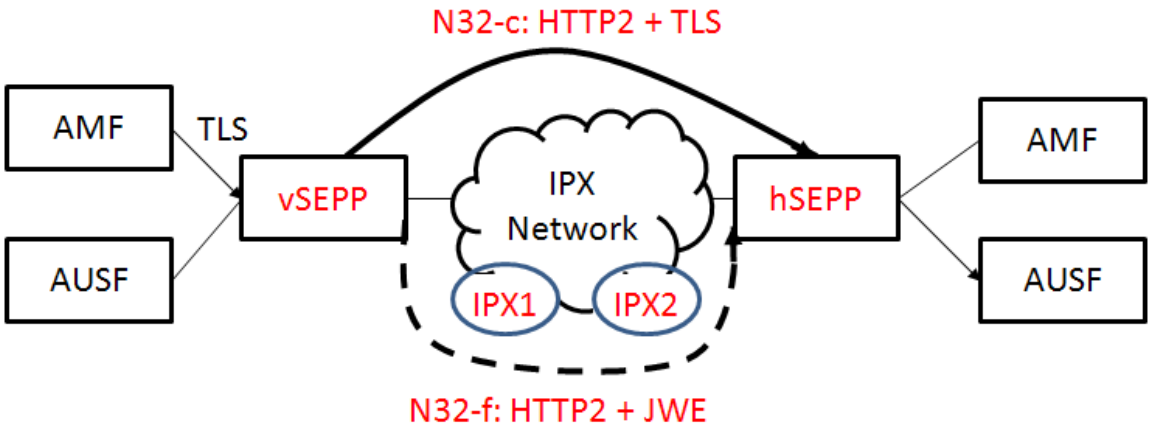

Figure 12: IPX-SEPP end-to-end security

3.2.3.2 Functional Architecture

To detect network attacks and security function evasion techniques it is necessary to perform real-time monitoring of traffic, based on probes (Security Agents) deployed at different points in the network (Figure 13, Component 1) for capturing and feeding data and meta-data, through the Security Data Collector (Component 2), to inference engines trained using AI/ML (Component 3) to identify malicious behaviour patterns in the encrypted traffic. In this way, Software-Based Interface traffic can be classified (e.g. separating signalling from other types of traffic, machine from user generated traffic). Identified malicious flows and activity will be mitigated using specific security policies (Component 4), that will be blocked by security agents (e.g. IPS, firewalls, active probes).

Analysing protocol exchanges is a first step in the detection of anomalies.

To avoid Introspection attacks and reverse engineering, it is necessary to harden the integrity monitoring of the network functions using Trusted Execution Environments (TEE, Component 5). The runtime integrity verification needs to be backed by a TEE embedded routine.

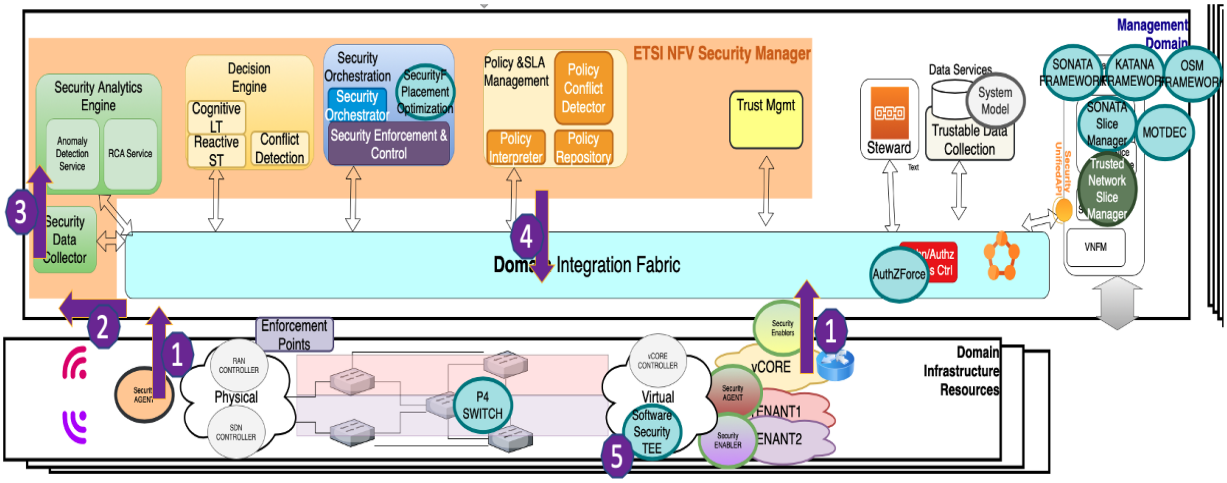

Figure 13: Components in Inspire-5Gplus' beyond 5G architecture

3.2.3.3 Target KPI

Target KPIs			
SLR Title	SLR Unit	SLR Value	Explanation/Reasoning/Background
Number of false positives	Number	Ratio of FP < 1%	Determine the ration of FP with respect to the number of supposed attacks
Number of false negatives	Number	Ratio of FN < 1%	Determine the ration of FN with respect to the number of simulated attacks. This needs to be done under controlled conditions (i.e. using generated traffic that contains different types of attacks)
Detection delay	Time in sec.	< 10 sec.	The detection rules and algorithms should perform so that the attack is detected and blocked before it has the possibility of impacting the services

Table 9: Target KPIs for TC3

3.2.3.4 Requirements for deployment, preconditions

The generation of datasets is needed to train the ML algorithms (supervised or semi-supervised ML). For obtaining these datasets, the 5G-VINNI 5TONIC facility (illustrated in Figure 14) provides a NFV infrastructure to deploy 5G core VNFs, plus MEC capacity to different verticals, but is not yet supporting 5G SA. VNFs for Stand Alone 5G Core will be needed. On the other hand, MI's EPC-in-a-Box based on Software Defined Radio (SDR) will be ready for experimenting and generating datasets on 5G SA.

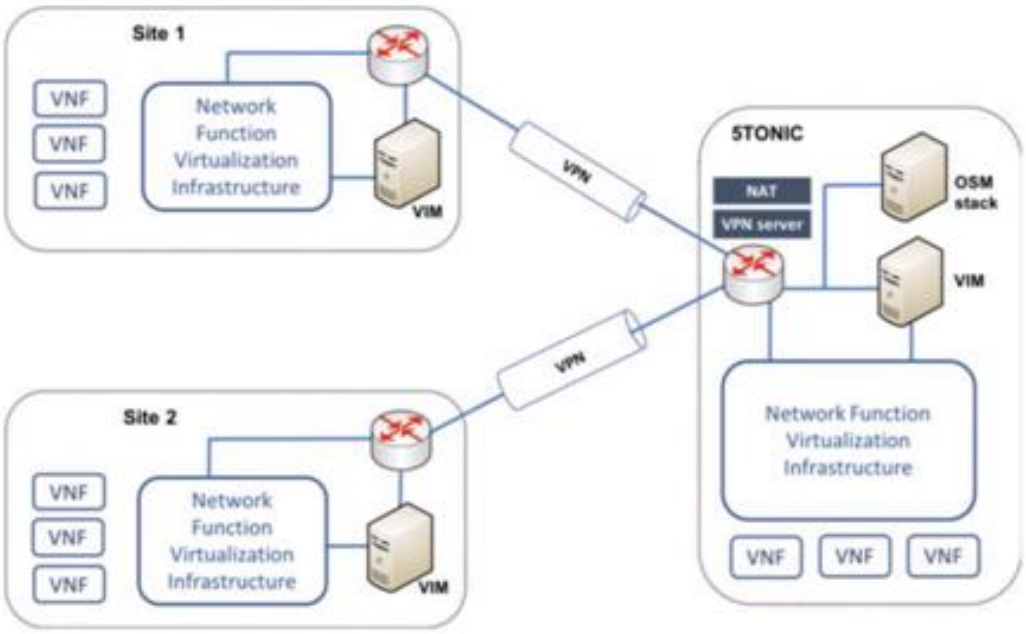

Figure 14: 5G-VINNI 5TONIC facilities

The monitoring function (consisting of data collection and aggregation probes) needs to be deployed and tested to determine its effectiveness in detecting and protecting traffic from attacks intra/inter site. The probes act as Security Agents that capture network traffic, extract the required meta-data (per packet and per flow) and eventually block certain traffic using the IP addresses and port numbers. The meta-data from the deployed probes is made available to the security analysis functions. The results of this analysis can be used to change the configuration of the security functions (via the orchestrators and controllers, or directly by the active probes).

Another identified pre-condition for implementation is to perform a thorough security survey to identify how data and code used for the AI/ML processing are exposed to various threats (e.g. adversarial ML and evasion attacks) and how leveraging Intel SGX enclave can elevate security and prevent these identified threats (i.e. providing a secure execution environment that protects both the data and executables). This initial survey will be worked out with detailed information on the architecture, protocols, collected data structures, ML processing algorithms used, as well as the operating system and running hardware used.

3.2.3.5 WP3/WP4 enablers

The following enablers are involved:

- MMT monitoring framework: composed of a centralised security management application and distributed probes. The probes can be deployed as passive (for detection only) or active (for detection and blocking specific IPs or flows).
- Software trust (integrity) leveraging TEE.
- Software protection (confidentiality and execution control) techniques
- Smart Traffic analysis: consists of an AI inference model for encrypted traffic for detecting cryptomining attacks.
- Data collector and aggregator (semantic): based on GrPC protocols

- Mouseworld[4]: system that allows testing new AI models by generating a mix of real traffic over HTTPS, traffic produced by commercial generators, web browsing clients, and attacks.
- EPC-in-a-Box: 5G SA experimental platform based on SDR, open-source or proprietary EPC and integrating the MMT security monitoring framework.

3.2.3.6 Methodology and expected outputs

The methodology followed includes the following steps:

1. Definition and setup of the 5G SA test platform in the5G-VINNI 5TONIC facilities.
2. Initial security analysis identifying the attack surface in the different activities (data collection, data transit, data pre-processing and detection)
3. Extension of existing enablers:
    i. The monitoring function needs to be extended with the following modules:
        - Protocol plug-ins that can parse the implicated protocols (e.g. IPX, HTTP2) and analyse the initial non-encrypted message exchanges that establish the connections or sessions.
        - ML algorithms adapted for behaviour analysis of the targeted protocols.
        - Possible extensions of the Software-oriented anti-tampering enabler (leveraging Intel SGX) for offering data protection of both Software and data.
        - Software protections mechanism (integrity, confidentiality and execution control). Possible support extensions to meet the considered implementations (OS, code type, ML algorithms, and structure, …)
4. Integration of existing components:
    i. Smart Traffic analysis.
    ii. Security Data Collect (SDC) and Security Analytics Engine (aggregator).
    iii. Traffic generator for training and testing the ML algorithms.
    iv. Software protection mechanisms (which are levelled-up by Intel SGX during the Inspire-5Gplus project).
5. Experiments to evaluate the solution and measure the KPIs.

Expected Outputs

The main outputs will be the description of the solution and experiments, the KPI measures obtained, and the conclusions (e.g. positive and negative aspects, future developments needed). The security enhancements of the platform will be demonstrated and challenged. Statements for future works for security enhancements will also be provided.

[4] Pastor, Antonio & Mozo, Alberto & Lopez, Diego & Folgueira, Jesus & Kapodistria, Angeliki. (2018). The Mouseworld, a security traffic analysis lab based on NFV/SDN. ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security. 1-6. 10.1145/3230833.3233283.

3.2.3.7 Timeline and risks

Phase	Time	Description	Risks
Set up of platform	M18	Deploy the existing components in the testing facilities.	Unavailability of bug free 5G SA platform. Mitigation: simulate the traffic and the attacks using some gNodeb emulators and traffic generators.
Extensions	M20	Extend the enablers	Lack of resources (underestimated the effort needed) Mitigation: reduce the scope of the test case to focus on some important aspect. Give provisional values only.
Integration	M26	Integrate the different elements	
Experiments	M30	Test and evaluate the solution	Security survey by its conclusions, challenges the benefits of using the considered security techniques for any types of reasons including (performance impact, efficiency of the global security design. Hardware-Software compatibility issues when considering Intel SGX or software-based techniques.

Table 10: Timeline and risks for TC3

3.2.4 Test Case 4: E2E Encryption TEE secured SECaaS

5G verticals use slices across multiple domains to exchange sensitive data. E2E slices provide, to some degree, the privacy needed; but E2E cryptographic protection is also needed to provide extra privacy and origin authentication (e.g. actual end-user or end-entity sending the data). In this context, two requirements to be fulfilled are: endpoint authentication and data encryption. Therefore, Zero Touch VNF-based E2E encryption over 5G MECs is proposed following the centralized SDN control paradigm for key distribution and, at the same time, hardware-based enclaves on the MEC to protect cryptographic material usage.

3.2.4.1 Problem Description and Objective

As an extra secure communications layer, VNFs acting as proxies can be deployed dynamically to protect communications end-to-end. It is the case for IPSec and for DTLS in case of UDP communications as is usually seen in IoT environments. The basis of both cryptosystems for the data encryption part is key derivation which in turn can be done centralized or on the hosts. For the authentication part, it may rely on Pre-Shared Key mechanism; or public key credentials (e.g. X.509 certificates) if the use case requires stronger authentication and/or non-repudiation of the data origin. Following the former approach, IETF proposes I2NSF (based on IKE) and Thales proposes SD-SEC, both having important similarities.

While end-to-end communication may be encrypted, it is also true that latest computer processor vulnerabilities open the door to memory introspection to extract keys (such as AES). The idea here is to take profit of SGX enclaves to perform encryption-decryption operations transferring native code to the TEE, therefore protecting the delegated VNF security from other MEC node's neighbouring VMs. As the current version of Thales SD-SEC is developed using a Java language and as it is not considered to insert the complete Java virtual machine inside the Intel SGX enclave (in order to run in extenso the Java cryptography class and methods), some engineering work will be produced to

consider a transcription of the Java code into x86 native code (1:1 iso-functional) and most likely the use of Java Native Interface (JNI) to call the SGX-embedded “transcripted” code. On the other hand, when considering the I2NSF (IKE based) concurrent implementation, this language transfer will not be needed as the code is already in the X86 64-bit native form.

The Objective is to produce a Zero Touch solution based on Policy and SSLA definition that can be triggered automatically based on system state and data collection inputs.

3.2.4.2 Functional Architecture

The policy hierarchy for the aforementioned test case is shown in Figure 15. The initial point is an Orchestration HSPL arriving at the E2E security Orchestrator that will in turn generate multiple MSPLs that need to be provided through the integration fabric to the multiple domains. Then a provisioning is triggered to provide with the VMs and the configuration needed.

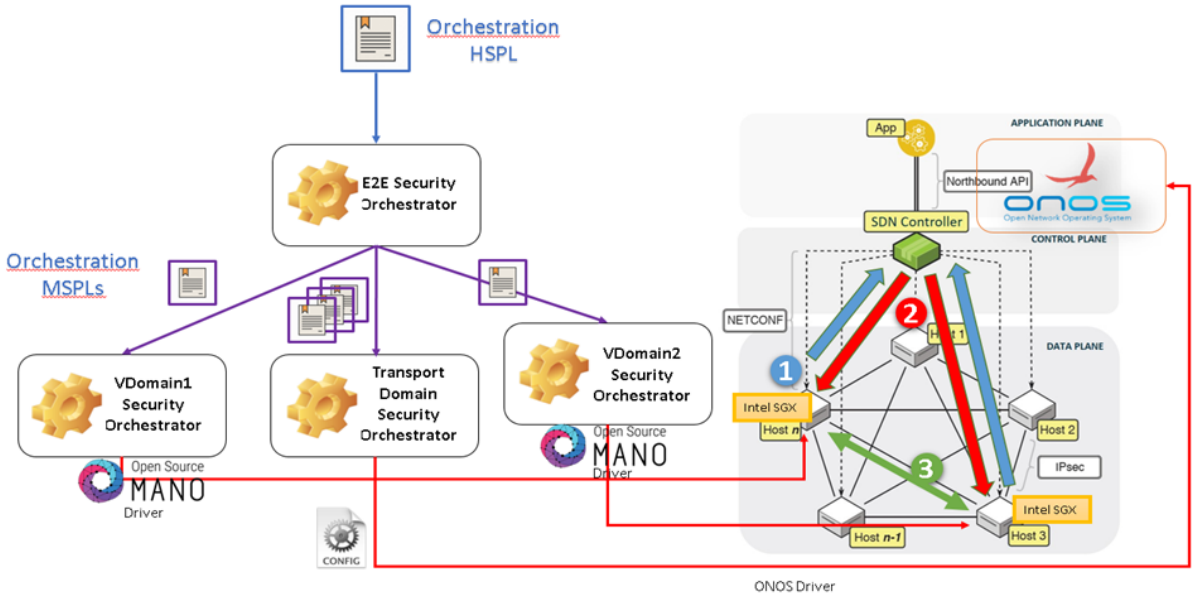

Figure 15: Policy hierarchy Test Case 4

Figure 16 shows the concept and how 5G Slicing can be used to provide yet an extra level of protection. The approach proposes a central entity to coordinate the provision of cryptographic configuration and material.

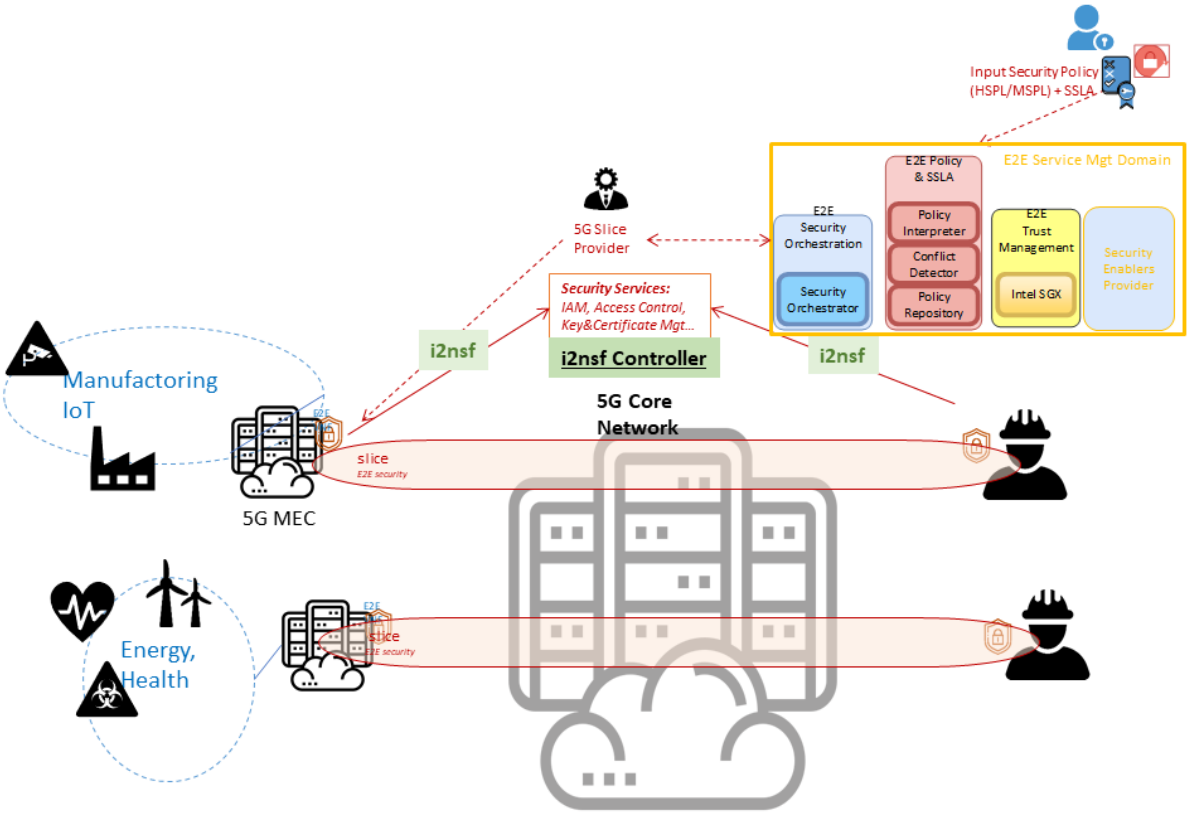

Figure 16: Initial proposal on how HSPL-MSPL policy framework and Security Orchestrator would integrate an i2nsf controller to provide slicing capabilities

While the initial approach for this test case relies on an HSPL for orchestration provided to the E2E Security Orchestrator, the reactive scenario shown in Figure 17 relies on an event on the data plane to trigger the full process. Figure 17 also describes the sequence of interactions with the components involved that will provide the final objective of the test case.

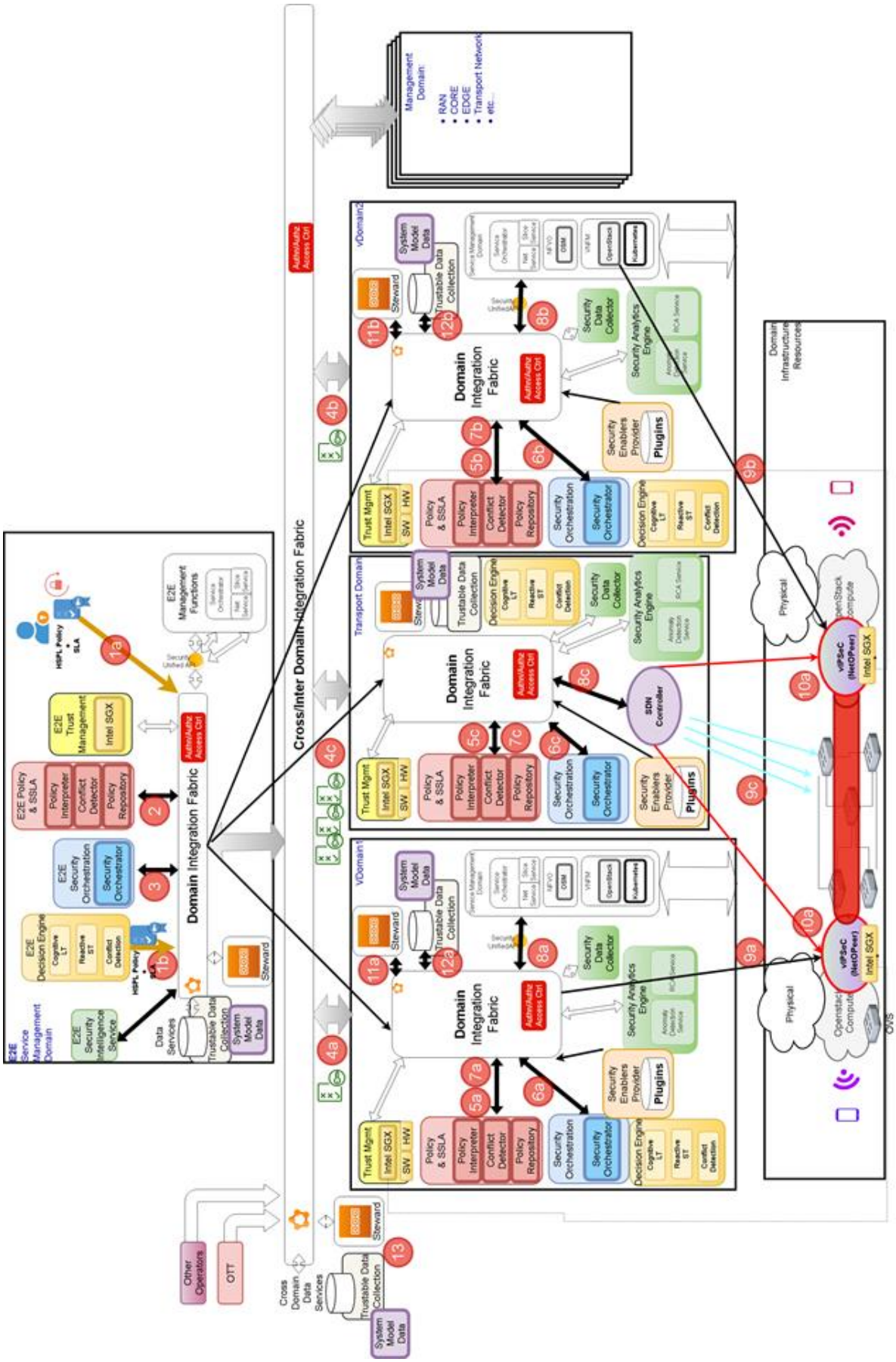

Figure 17: Test Case 4 Step by Step Reactive Scenario

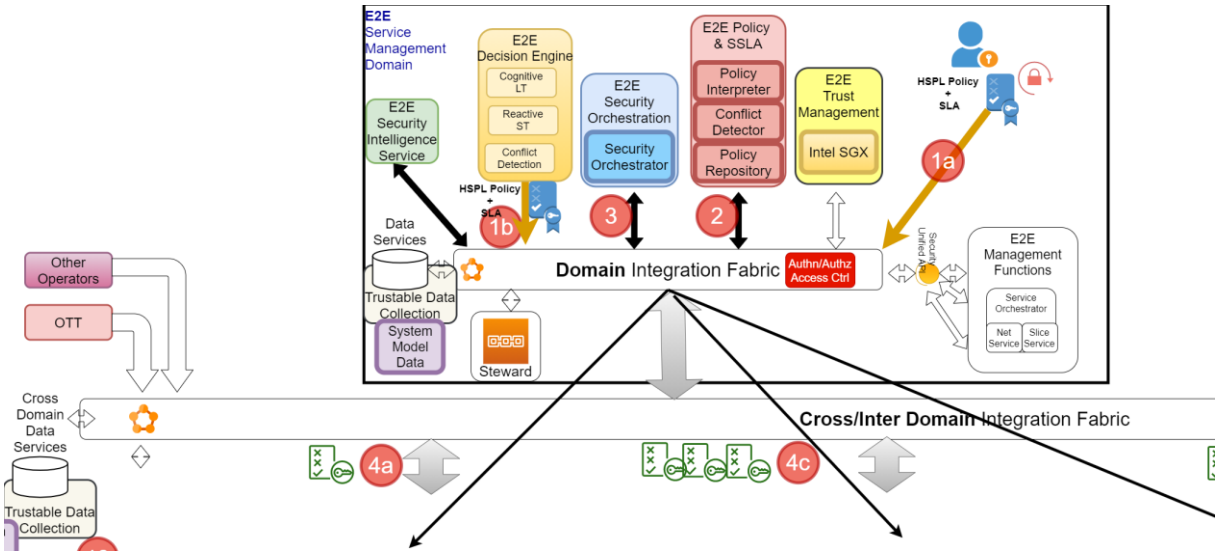

Figure 18: Initial steps detail. Test case bootstrapping

The test case is initiated (Figure 18) either via a request from system administrators installing new SSLAs and/or security policies, either via the E2E Long-Term/Short-Term Decision Engine as a self-protecting countermeasure.

At that point a full SSLA/Policy translation (HSPL->MSPL) is performed generating medium level orchestration policies for each specific domain. In this Test Case in particular, an orchestration HSPL is refined in multiple orchestration MSPLs (3 IPSeC MSPLs and 2 Forwarding traffic MSPLs, the later may contain slicing properties) by the Policy Interpreter that relies on the Policy Repository and the Conflict Detector to determine the translations from the higher level policies agnostic of the underlying technology to the medium level policies that take into account information about the scenario and the technologies available.

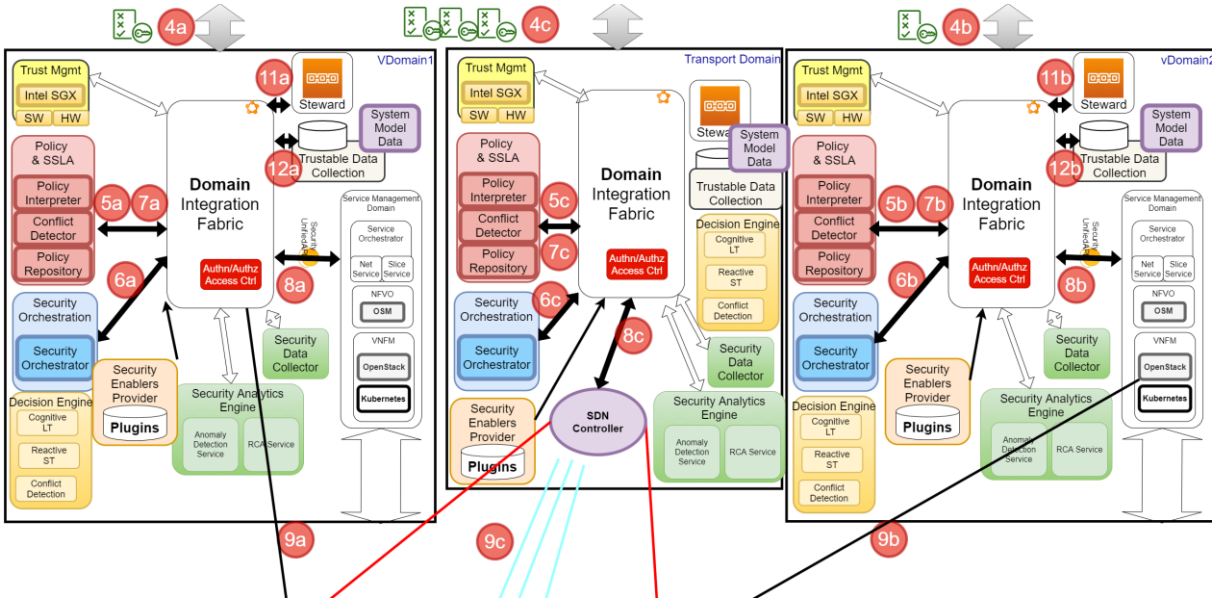

Figure 19: Steps for refinement of the MSPL orchestration policies for each domain

Steps 5 to 8 represent the refinement of the MSPL orchestration policies for each domain (Transport, vDomain1 and vDomain2) into the specific actions/configurations needed, MANO instantiation of VNFs, that implement the IPSeC tunnelling function, or configurations deployment through SDN, that redirect the selected traffic into those VNFs, or TEE enablement, that ensure that the cryptographic

material is not exploited by third parties, among others. Finally steps 11 and 12 represent the storage of meaningful information about the process for further usage by the system, e.g, as entries for decision taking.

3.2.4.3 Target KPI

Target KPIs			
SLR Title	**SLR Unit**	**SLR Value**	**Explanation/Reasoning/Background**
CryptoDeploymentTime	ms	Mean Value < 1 ms	Time spent onto deploying the NetConf devices to create the IPSec Tunnels and receive the cryptographic material and configuration
RekeyPacket Delay	ms	Mean Value < 200 ms	Packet delay introduced in data path cause by periodic key refreshment of encryption tunnel
TEEOverload	%	20	In average compare the time spent into a measured communication E2E with and without TEE to measure the cost of that enablement
Mean Time to Resolve (MTTR)	ms	Mean Value < 40 ms	Establish the cost of the reactive scenario where events from a certain domain will trigger the channel protection mechanisms, This is important to know if this mechanism can be used for short communication bursts or not
E2EE Policy Orchestration Lifecycle - Initial deployment time	ms	Mean value < 100 ms	Total duration of the initial orchestration of a new End-to-end data encryption (and/or MAC/signature) policy to take place, from the time of reception of the end-user's Security Policy by the Security Orchestrator to the time when the deployment reaches the status of fully operational (enforcing the policy). Time depends pretty much on the deployment and the RTT between E2E domain and other domains.
E2EE Policy Orchestration Lifecycle - Update time	ms	Mean value < 100 ms	Total duration of the orchestration of an update of a previously deployed E2EE policy to take place, from the time of reception of the end-user's policy update, to the time when the deployment and/or reconfiguration thereof reaches the status of fully operational (enforcing the new policy). We will consider the worst-case scenario in which the policy

			update triggers the revocation/update of all data encryption keys. Time depends pretty much on the deployment and the RTT between E2E domain and other domains.

Table 11: Target KPIs for TC4

3.2.4.4 Complementary measurements

Complementary KPIs			
SLR Title	**SLR Unit**	**SLR Value**	**Explanation/Reasoning/Background**
InterDomain FabricTime	ms	Mean Value < X ms	Time spent into communication between the different Fabrics and processing time of each Fabric. The relevance of this is capital. If the fabric is too slow, we might just have to skip multi-domain fabrics

Table 12: Complementary KPIS for TC4

3.2.4.5 Requirements for deployment, preconditions

- Multi-Device Synchronized Time monitoring
- Multi-Compute NFV system
- Programmable SDN network (optional) - might work with vxlan
- Kubernetes VIM for at least one of the two domains (MECs) in Thales SD-SEC case

3.2.4.6 WP3/WP4 enablers

- Security Orchestrator: the piece in charge of orchestrating received policies into the different Domains at end to end level or in precise actions at each Domain
- SliceManager/ProviderProvides slicing capabilities
- IAM
    - For managing and enforcing dynamic authentication and authorization policies, especially in the DTLS proxies (see below)
- i2NSFController as SDN Controller APPThis controller is in charge of deploying the coordinated cryptographic material into the IPSeC Tunneling VNFs(vIPsec)
- i2NSF agent/ vIPsecVNF in charge of encapsulating the unprotected traffic into the tunnel
- DTLS ProxyProxies enforcing the E2EE policies on UDP communications, possibly interacting with the IAM enabler.
- VNFM (OSM)
    - MANO system in charge of management and orchestration of the virtualization infrastructure and in some cases the SDN network.
- TEE - Intel SGXTrusted Execution Environment techniques to protect unauthorised access to the cryptographic material by third parties, such as neighboring VMs.

- Policy Repository
    - Repository containing already enforced policies, providing a historical that allows the conflict detection.
- Conflict Detector Entity able to detect policy conflicts within policies and inter-policies
- Cognitive Long-Term Planning
    - AI based enabler from Inspire capable of taking decisions for long term planning.
- Data Collectors (Optional - Only if reactive approach)

3.2.4.7 Methodology and expected outputs

Methodology

1. Evaluation of existing software elements/enablers to be used.
2. Extension of existing enablers to follow the ZSM/Fabric communication scheme.
3. Definition of Policies that trigger the Test Case, implementation and integration onto Inspire Architecture, which needs to be deployed onto UMU and 5TONIC testbed
4. Implementation, deployment and integration iterative procedure
5. Extraction of KPIs

Expected Outputs

The outputs are the KPIs defined in previous section and the recommendations on thresholds where the proposal is interesting or how it can adapt to different security flaws scenarios.

3.2.4.8 Timeline and risks

Phase	Time	Description	Risks
0 - Basic scenario	M12	First Demo for EC Review. Fully Virtual. UEs VMs. Prepared to run on a laptop if needed	Enabler integration complexity MultiDomain Fabric difficulties
1 - Integration on Testbed	M14	Integrate into final testbed	No risks are foreseen
1- SGX integration Engineering	M 20	On THALES's SD-SEC java-based solution. The feasibility of the code transcript from Java to SGX embedded native code and the use of the JNI interface must be tested.	The crypto class of Java cannot be easily transcripted into native
2 - UE Integration	M20	Integrate 5G UEs	Need for 5G SA UEs and 5G SA core Need of LBO MEC
3 - Reactive Scenario	M24	Allow Reactive provisioning	Possible limitations on events provided by 5G network

Table 13: Timeline and risks

3.2.5 Test Case 5: End-to-End Slice Protection based on Moving Target Defense and Anomaly Detection

3.2.5.1 Problem Description and Objective

5G comes with extensive features and capabilities, allowing the realization of advanced Use Cases, not feasible with legacy mobile networks. However, this advancement comes with various side effects, including the increased attack surface due to new flavours of technologies introduced in 5G, such as:

- Software-defined infrastructures
- Slicing and multi-tenancy
- Multi-actor service paradigms
- Complex, multi-tier architectures

Under certain circumstances, these could constitute potential sources of vulnerabilities, increasing the probability of security incidents.

On the other hand, an interesting opportunity stems from the fact that 5G network components are highly heterogeneous and distributed across the network, thus creating an enormous amount of diverse data (mostly logs and monitoring information), whose analysis can lead to effective inference of security incidents.

The objective of this test case is the protection of network slices through proactive and reactive security mechanisms. One aspect includes the collection and joint analysis of heterogeneous data from multiple points of the 5G infrastructure for integrated monitoring, with specific focus on detecting and classifying anomalies associated with security incidents. Another aspect is the provision of Moving Target Defense (MTD) approach to dynamically reconfigure parts of the infrastructure, in order to increase the attacker's effort and cost. An important consideration of this Test Case will be to strike a balance between security effectiveness of MTD and the cost of reconfiguring the network.

Figure 20 depicts a high-level mechanism for end-to-end slice protection, based on the security assets introduced in INSPIRE-5Gplus. The Moving Target Defense Mechanisms deployed inside this Test Case should be adapted corresponding to the faced threat. The level of MTD applied could range from no action to simple indirection and even to multiple stacked indirections. The end goal is to avoid penalizing legitimate users and progressively make the path to the protected resources more and more complex for malicious users.

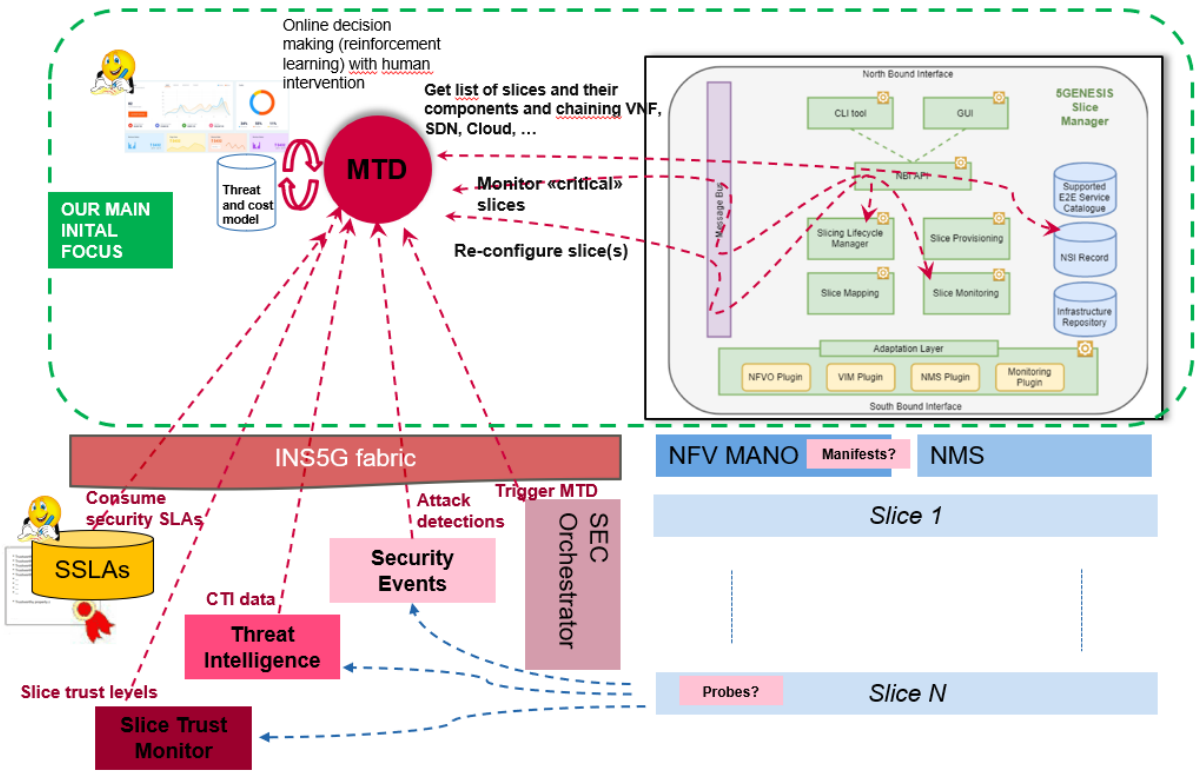

Figure 20: Moving Target Defence and Slice Management

This Test Case provides the opportunity to explore several scenarios for protecting the network slices, summarized below:

Scenario 1 - Dynamic Service IP mutation

An example of an MTD strategy could be to hide the true IP of a service to its "potentially" malicious users using a programmable MTD-ready DNS server, as depicted in Figure 21. During a DNS name request, the DNS server can return a "fake" IP to the user instead of the true IP. Then, when the user communicates with the fake IP, the MTD intercepts and redirects the traffic to the true IP while translating all the answers to correctly hide the service. If the level of maliciousness bound to a user keeps increasing, the MTD can stack this true/fake IP mechanism to fuzzy the location of the protected resources.

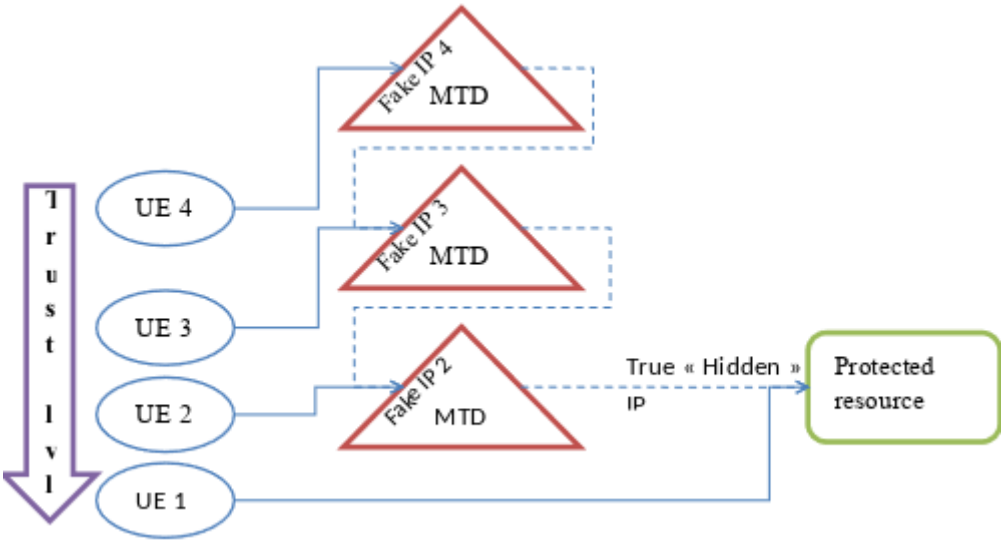

Figure 21: MTD Mechanism

Scenario 2 - Optimized Security Function Mutation

Another interesting scenario is the MTD based protection of the security functions themselves in a slice to increase their robustness against reconnaissance and attacks. In this case, the premise of this MTD is to change the attack surface of security management framework for malicious entities while optimizing the cost versus protection trade-off. A specific scenario is the optimized protection of Security Agents in NFV environment against attacks on availability (i.e. DDoS) [https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58648].

Here is how it works:

- MTD policy is a composite of potential actions for changing attack surface. Here we will implement the IP and port mutation MTD action.
- The MTD controller implements the necessary actions to realize an MTD action in 5G environment for Security Agents (through I5G+ security framework).
- Defence Optimization Engine (OptSFC) optimizes the policy, i.e. when and which security agents are mutated based on
- The security “ambiance” (e.g. the activity level of hostiles, e.g. a global botnet threat),
- Resource availability
- Security SLAs (e.g., for stringent security policies, it is more likely to accept the overhead of extra Security Agent protection)
- Domain (e.g. edge domain is potentially more prone to infiltration as the steppingstone by malicious devices) and
- Specific security events in the network.
- Reinforcement Learning and rule-based schemes are used in to evaluate the solution space and pick optimal decisions.

Future directions and next steps

The Test Case provides the opportunity of investigating additional extensions, as the Project’s milestones keep progressing.

Such an extension is protecting the Slice Manager from imminent attacks, since it is a critical building block in virtualized multi-domain 5G infrastructure. Therefore, another application is the protection of the Slice Manager against scanning and reconnaissance using IP and port mutations.

3.2.5.2 Functional Architecture

The functional Architecture of the Test Case is depicted in Figure 22. The testbed will realize an end-to-end 5G network comprising of multiple domains (RAN, Core, Edge, Transport). In the context of this test case, we will deploy network slices for different services (e.g. eMBB, URLLC) and will collect monitoring logs through probes dispersed over the domains.

The Network and Service Management Platform includes the E2E Monitoring Framework, the Anomaly Detection Engine, the MTD module and part of the 5GENESIS Experimentation Suite, comprising the Experiment Lifecycle Manager (ELCM), the KATANA Slice Manager and OSM (NFVO and VNFM).

Based on the Telemetry received by the probes, the Anomaly Detection Engine will track potential security incidents, while MTD in cooperation with the Slice Manager will be responsible for the dynamic reconfiguration of the network to minimize the probability of attacks.

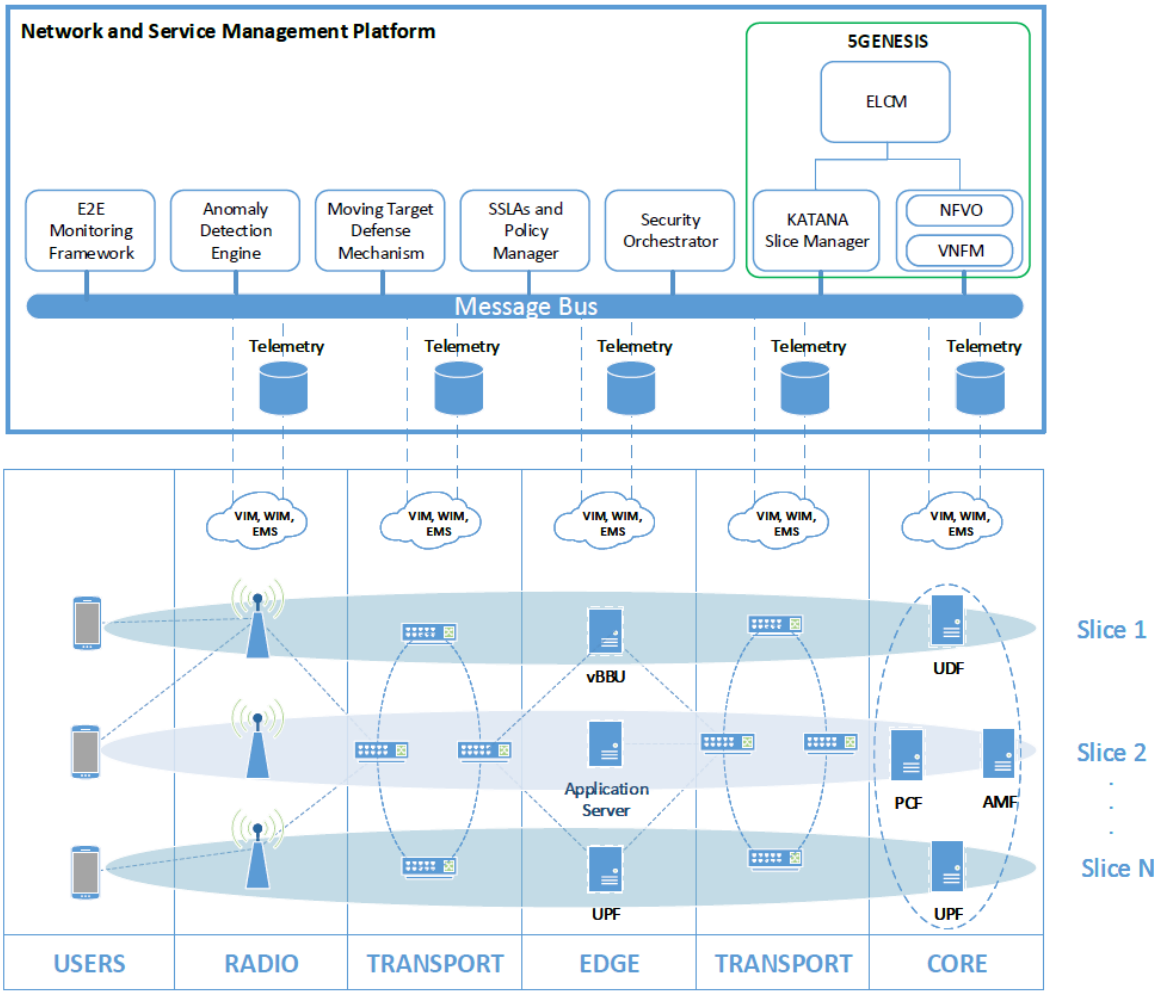

Figure 22: TC5 Functional Architecture.

3.2.5.3 Target KPI

Target KPIs			
SLR Title	**SLR Unit**	**SLR Value**	**Explanation/Reasoning/Background**
Mean Time to implement the MTD action (MTID)	[s]	MTID < 5 s.	How long it takes an MTD action (e.g., IP change) to be relayed to the action enforcer
MTD action cost a. Worst-case (C_w) b. Mean (C_m)	[percent]	C_w< 50% increase C_m< 20% increase	A comparative value showing the overhead of MTD action (example metrics to monitor change in CPU load, change in response time for the protected function)
Protection gain of an MTD policy a. Worst-case (P_w) b. Mean (P_m)	[percent]	P_w > 5% increase P_m > 10% increase	A comparative value showing the gain in protection terms for a performed MTD action
Mean decision time for MTD action (MDTA)	[ms]	MDTA < 500 ms.	The mean time it takes for the optimization engine to come up with a new MTD policy

Table 14: TC5 Target KPIs

3.2.5.4 Complementary measurements

The complementary measurements will consist of Radio and Core related KPIs, as well as infrastructure-related measurements, providing an end-to-end overview of the platform state. These measurements will accompany the primary KPIs, allowing the investigation of possible correlations during testing. The following list provides a representative overview of such complementary measurements that can be further populated in the course of development, if deemed necessary:

Radio:

- Radio conditions report per UE (RSRP, RSRQ, RSSI, SINR)
- Signalling events per UE and Base Station
- Type of service delivered per UE (eMBB, URLLC)
- Throughput per UE

Core:

- Usage Data Records (including User and Services information)
- Aggregated traffic per service
- Success and Failure rates
- Bearer information
- Network utilization KPIs (e.g. total bytes received/delivered)

Infrastructure:

- CPU utilization
- Memory Load
- Disk utilization per Device
- Network Traffic (bytes received/bytes delivered)

3.2.5.5 Requirements for deployment, preconditions

The requirements and pre-conditions to properly develop this TC are:

1. Interoperability of enablers: The TC will utilize multiple enablers from partners that either will be developed or upgraded in the context of INSPIRE-5Gplus. It will be imperative to define their communication interfaces over the Integration Fabric, as it will be defined in the context of INSPIRE-5Gplus. Further requirements regarding enablers will be evaluated as the Test Case evolves in the context of INSPIRE5Gplus.
2. Appropriate data models: New data models are needed to properly handle data generated by the RAN and CN networks. Multiple solutions provide different data formats that need to be processed by the Security Analytics Framework in order to detect possible threats.
3. Multi-domain Network Slicing: The testbed will comprise multiple domains (RAN, CN, Transport, Edge) in order to fulfil the INSPIRE-5Gplus High Level Architecture.
4. Light weight configurable probes to extract meta-data, SSLA metrics and statistics from diverse structured information (e.g. network traffic, logs).

3.2.5.6 WP3/WP4 enablers

- Katana Slice Manager (NCSRD)
- Security Analytics Framework (NCSRD)
- Moving Target Defence Controller (ZHAW)
- MMT probes and monitoring framework (MI)

- Defence Optimization Engine (OptSFC) (ZHAW)
- Security Orchestrator (THALES)

3.2.5.7 Methodology and expected outputs

Methodology

The Methodology consists of several basic operations and workflows that need to be realized, in order to provide a complete end-to-end testing platform. The first step is specifying the requirements of each enabler, proceed with the required upgrades and validating their function through appropriate testing. The next step includes integration of the enablers and interoperability testing. The final step is integrating the enablers with the infrastructure components and validating the end-to-end system operation before demonstrating the Test Case.

In summary, the Methodology consists of the following operations:

- Requirements analysis for the components to be employed in the Test Case
- Evaluation of enablers
- Implementation of appropriate extensions on the selected enablers (functional verification)
- Integration of enablers, deployment and evaluation (unit testing, interface API testing)
- Integration of the enablers with the infrastructure (system level testing)
- Test Case demonstration

Expected Outputs

The expected outputs will consist of successful functional verification results both on component and system level, as well as measurements of Security KPIs that should be below/above the thresholds specified under different attack scenarios.

3.2.5.8 Timeline and risks

This Test Case will be deployed over the Athens Testbed on the NCSRD Campus, which is supported by 5GENESIS and 5G!Drones. As a result, the anticipated technical support will last until the end of 5G!Drones in 2022. After completion of 5G!Drones, the designated Lab Personnel of INSPIRE-5Gplus will keep supporting the testbed. Table 15 provides the timeline for the deployment of this Test Case:

Phase	Time	Description	Risks
0 – Requirements Analysis and initial enablers' advancements	M14	This phase includes analysis of the requirements for integrating the involved enablers and initial implementation of their extensions.	Enablers integration complexity: There are multiple enablers that need to be integrated, increasing the complexity of the project. A mitigation action is to consider different scenarios involving only a subset of the enablers and dedicate future integration in these cases.

1 – Enablers integration	M24	During this phase, we will proceed with additional advancements on the enablers and begin their integration on the Athens testbed. This Phase will include component development, unit testing and interface API testing, as well as synthetic data generation for functional verification. The objective of this Phase is to complete the integration testing of the enablers and begin their integration with the infrastructure layer components.	Synthetic data generation poses a risk regarding the volume of data needed to effectively use ML. This is mostly related to the number of available 5G UEs, since the laboratory provides limited physical devices. Testing is required in order to determine whether this limited number will be efficient for a ML approach. A mitigation action is the emulation of multiple devices using specialized software. Delays in development during the enablers' integration process are an additional risk.
2 – Test Case Demonstration	M36	The objectives of this Phase are to complete the end-to-end validation and testing of the platform environment, demonstrate the proper functionality of the enablers and validate the defined KPIs for this Test Case.	5GENESIS infrastructure availability End-to-end system proper operation. Availability of 5G specific data, especially radio and core related.

Table 15: Timeline and risks for TC5

3.2.6 Test Case 6: GDPR aware counterparts for cross-border movement

The rationale of this test case is the enforcement of law and directives on cross-border scenarios for connected cars, even if it could be applied to other environments such as eHealth and IoT in general.

The test case proposes the use of virtual counterparts as a point of law-enforcement independent from UE/Cars manufacturers, taking profit of the ISP network relation with geographical attachment and, in particular, the 5G EDGE nodes to apply local laws to visiting users. Connected cars contain a small computer in charge of data processing and communications management named OBU (On-Board Unit). This test case inherits from the projects SURROGATE and MIGRATE that were presented as part of 5GINFIRE the idea of a virtual OBU (vOBU) as a counterpart for each hardware OBU to which delegate processing functions among other possibilities.

3.2.6.1 Problem Description and Objective

Each country in the EU has its own laws in terms of data privacy and the EU itself defined the GDPR as a mean to control data leakage and data transfer on third parties, making special distinction for cloud providers. There is a need to ensure that data uploaded while users are in roaming complies with country laws and when that fails allocate liability to whom might be responsible.

- With that in mind vOBUs with specific analysis of GDPR functions might be stored on each operator depending on the country and offered as a VNF.
- These vOBUs also register their operations on the DLT.
- These vOBUs also may provide with different channel protection mechanisms to ensure confidentiality between the UE/car and the cloud. Actually, these schemes might be also applicable to wearables, where more sensitive data can be located.

3.2.6.2 Functional Architecture

The rationale of the Test Case is shown in Figure 23. Even if it is shown as a multi-operator scenario, it can be also thought as an international single operator deployment. It is important to highlight the difference in legislation between countries and how to ensure that the legislation is enforced when the devices move between them, therefore avoiding the need of relying in third parties such as cloud providers and their (usually less restrictive) local legislations.

The Smart Contracts and Blockchain is envisioned to provide with liability to the system and therefore the Trust Management services within the INSPIRE-5Gplus architecture.

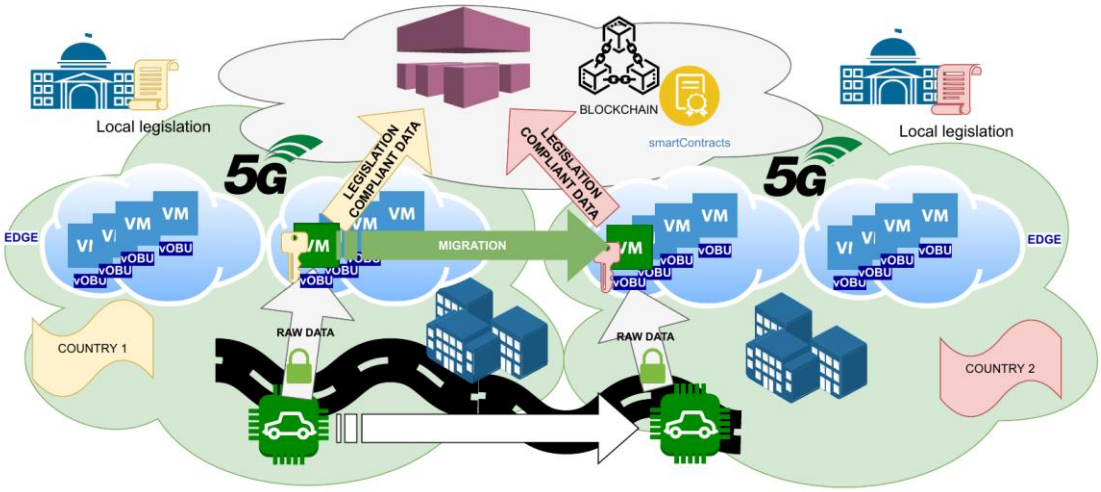

Figure 23: Test Case 6 Functional Architecture

Figure 24 shows the sequence diagram on the process of migration. It is important to highlight the need for data migration unless a full key exchange process is desired. This part of the exchange is open to benefit to TEE and other technologies to ensure that the data migration remains secure.

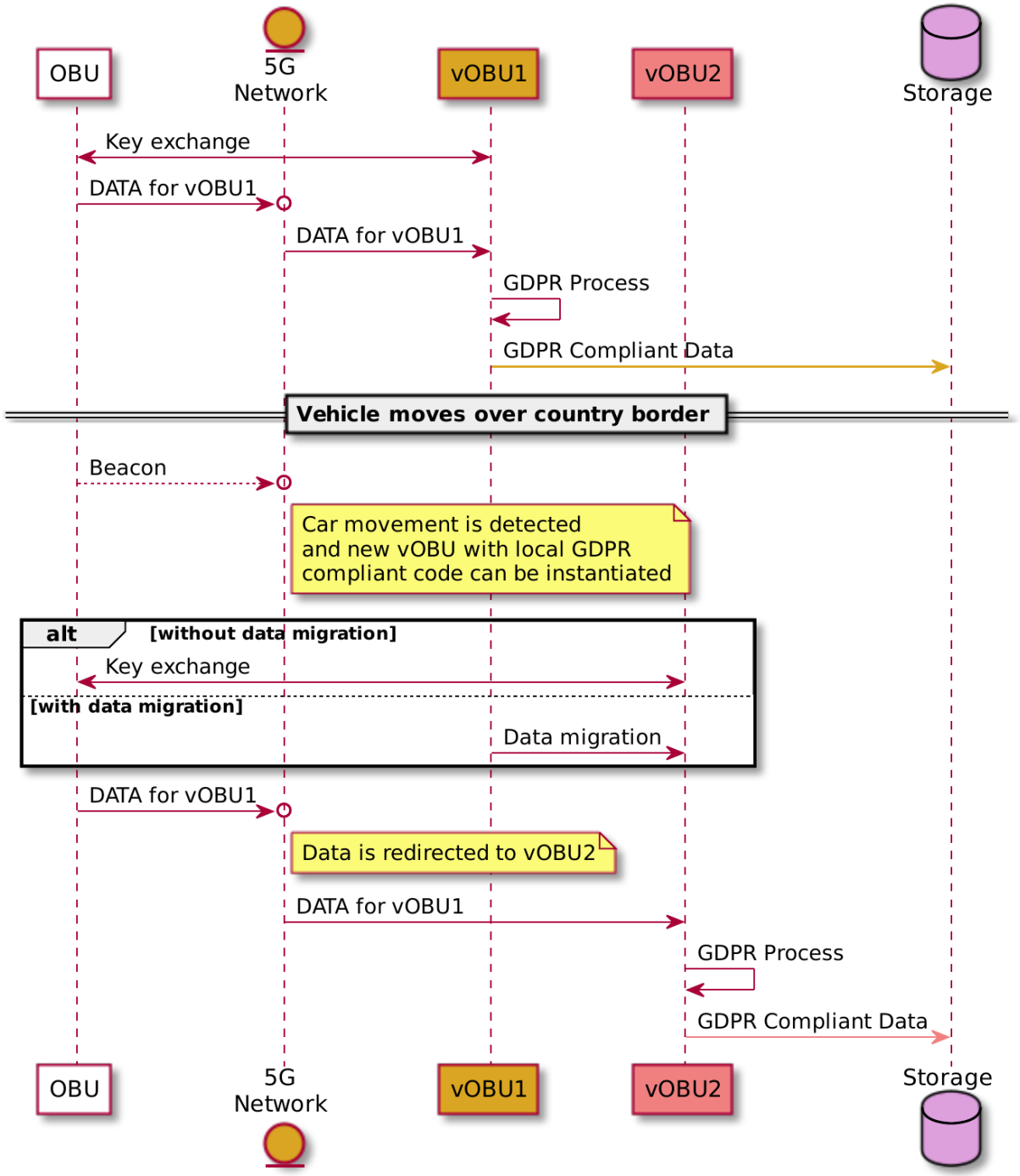

Figure 24: Sequence Diagram

Figure 25 shows the scenario and the interactions between the different parts of the architecture. The NOC or the system administrator needs to enable the GDPR enforcement service. After that, every single OBU connecting is forced to go through the vOBUs in charge of checking the legislation. It is important to highlight the need of providing liability not only on the data generated and stored but also on the vOBUs version themselves in order to find responsibilities if the system is deceived.

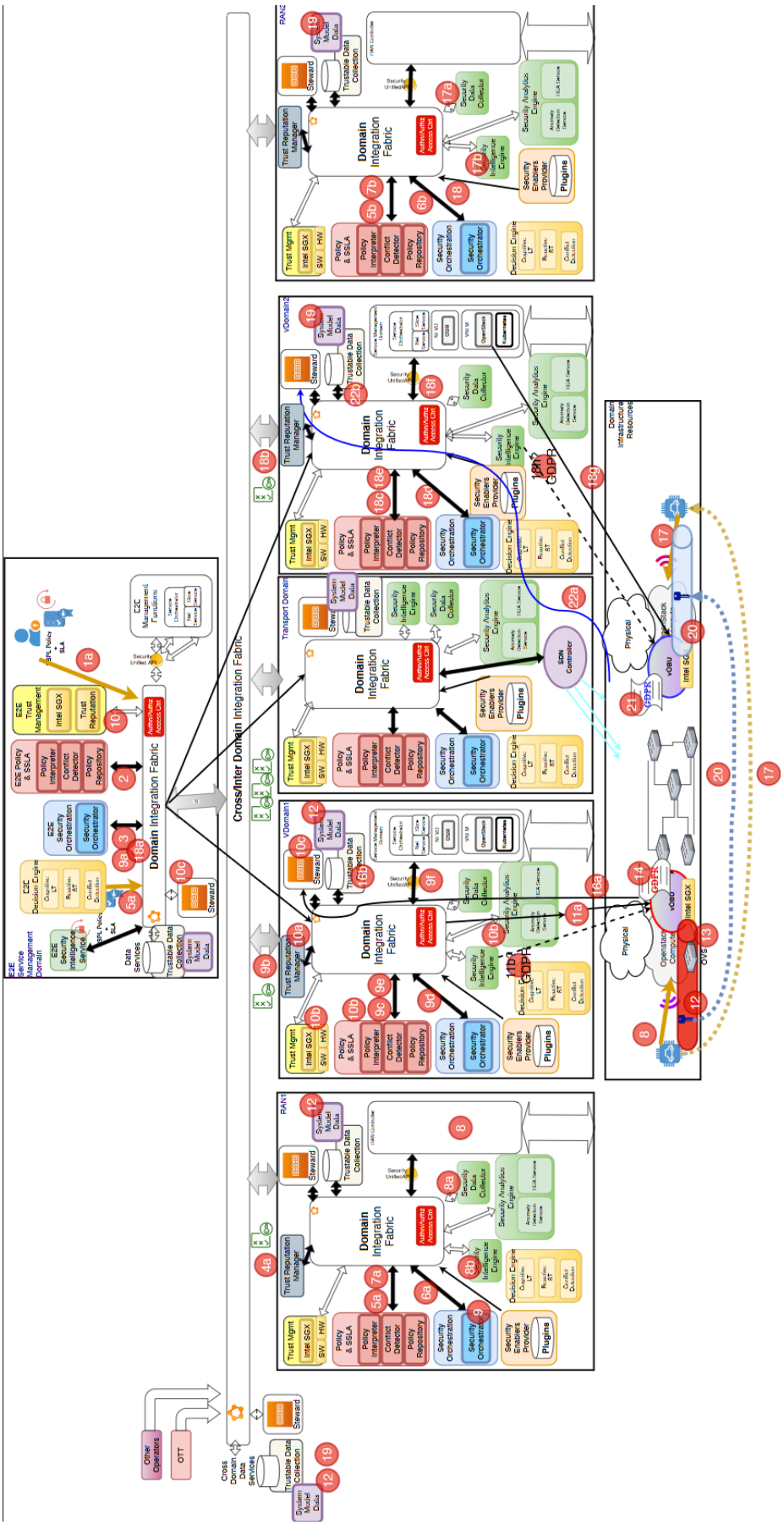

Figure 25: Scenario

This test case implies a multi-operator scenario or an international operator context, one from which the car is leaving (source context) and one to which the car is arriving (destination context), therefore, two RAN domains are defined, two virtual domains collocated with the g-NodeB of each RAN and a transport domain interconnecting everything.

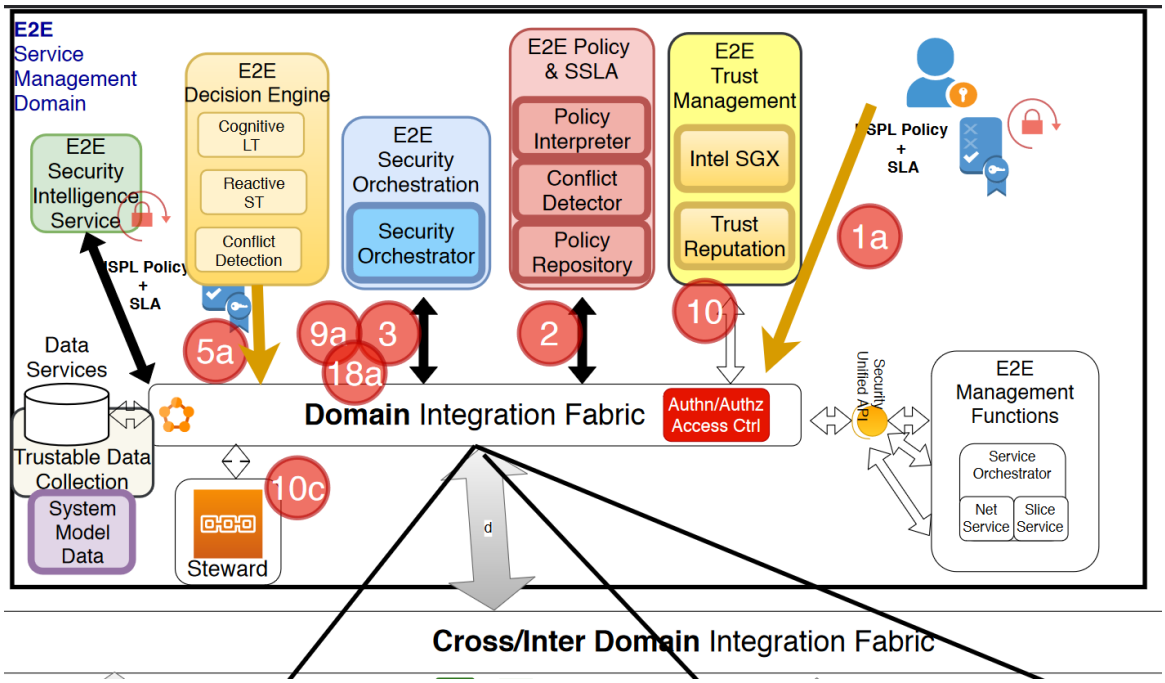

Figure 26: Test Case Bootstrapping

The test case is initiated (Figure 26) via a request from system administrators installing new sSLAs and/or security policies that enforce the GDPR compliance for moving/roaming devices. Therefore, when a car starts its engine, automatically the vOBU is in place to start a security association and start receiving data.

At that point a full sSLA/Policy translation (HSPL->MSPL) is performed generating medium level orchestration policies for each specific domain. In this Test Case in particular, an orchestration HSPL is refined in multiple orchestration MSPLs, apart from the ones needed to have the virtual counterparts, an orchestration policy for movement detection and a specific GDPR policy are envisioned.

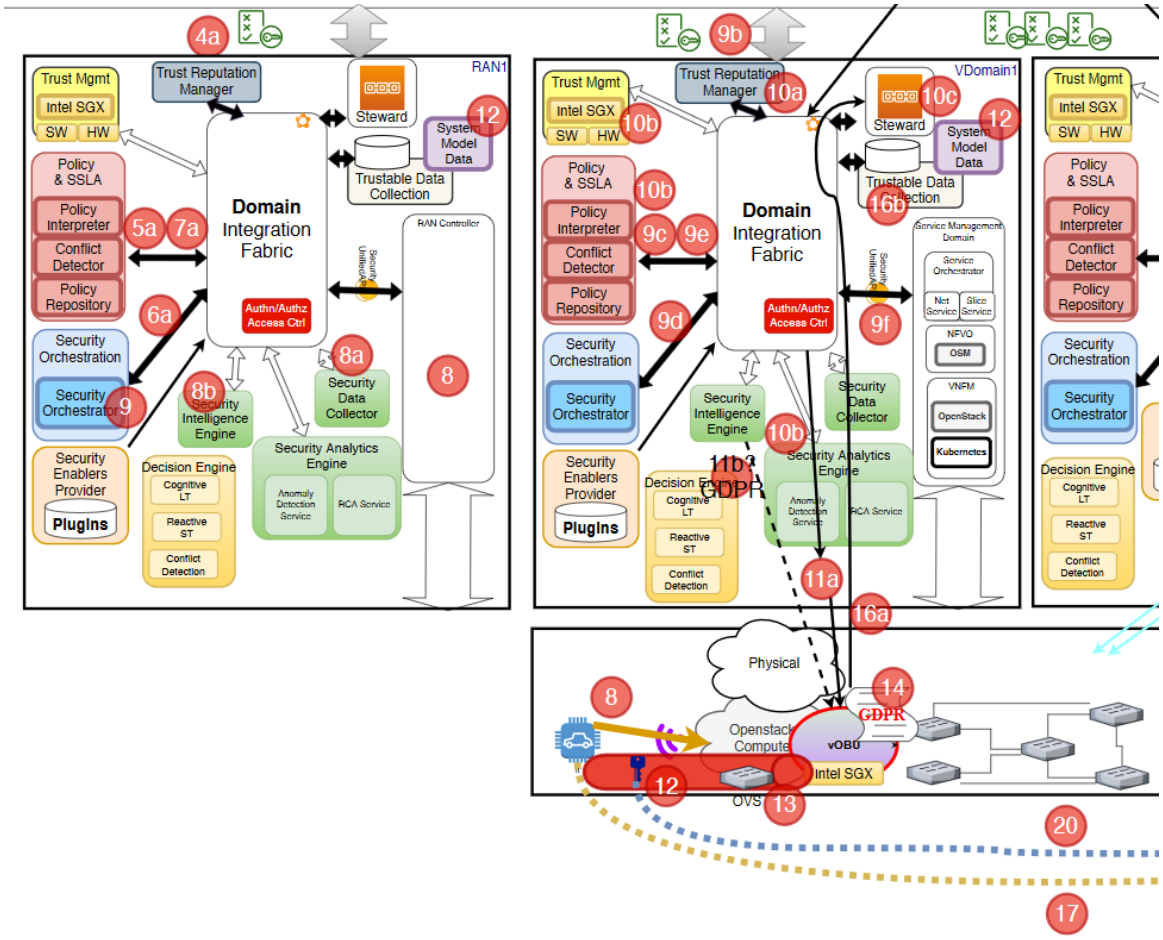

Figure 27: Source context GDPR protection

Figure 27 shows the interactions that enable RAN connectivity from the car to the vOBU, the need for a transparent redirection mechanism (13) and the integration of Intel SGX to protect keying material and ensuring that the instantiated vOBU is trustable.

As shown in the previous figures, prior to the deployment of the vOBU, E2E Trust Manager asks the selected domain (vDomain1 in this case) Trust Manager to calculate the domain's trust value. It calculates the trust score using as inputs the results of previously performed transactions, the monitoring data obtained by the agents deployed in both VNFs and network, the Trust (TEE) values, and the compliance with the previously defined policies and SSLAs. If the obtained value is valid (it is above the previously defined threshold), the deployment will occur. If not, a different domain will be selected. Regardless of the score, the result of the transaction will be stored in both chains (the local-domain one and the one located on the E2E domain).

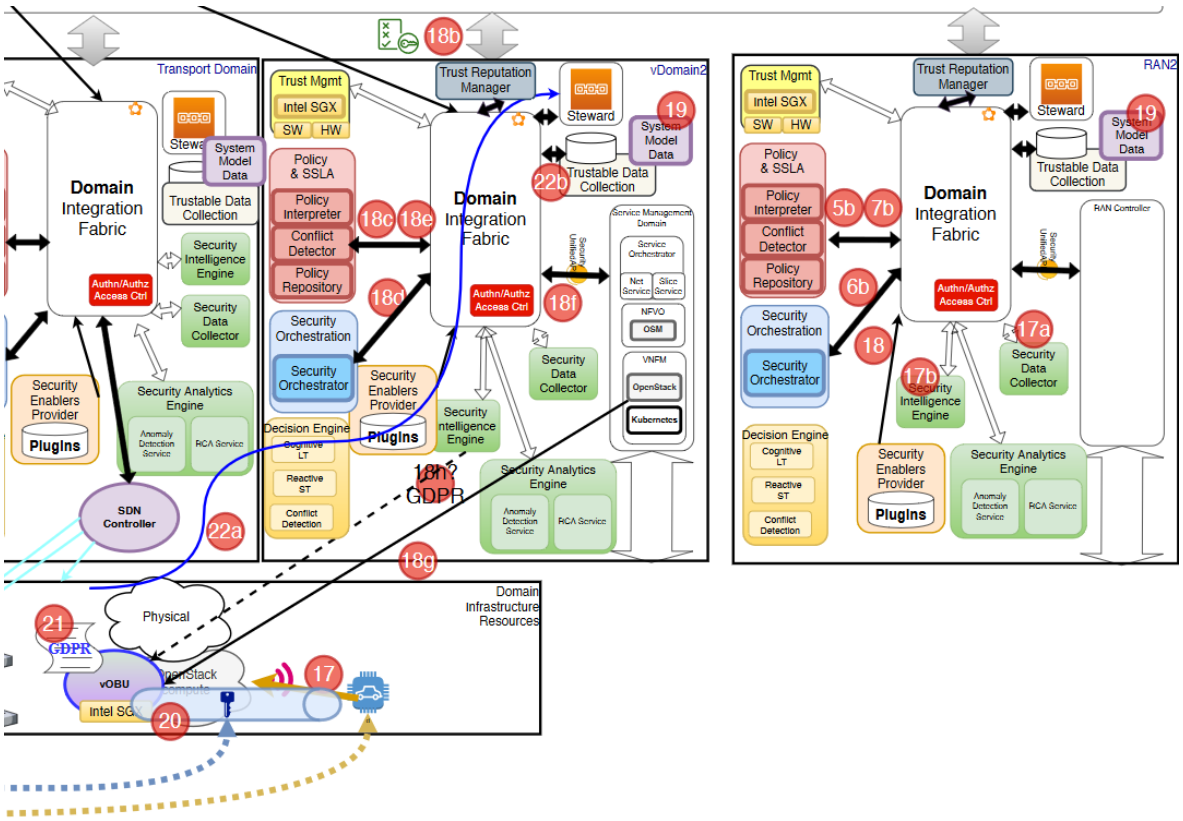

Figure 28: Detection of movement, migration and reporting

Figure 28 details the process in which the car moves to another location with other law regulations, therefore a new version of vOBU ensuring law fulfilment is instantiated and keying material is migrated to provide transparent handover to the OBU. In addition, the fulfilment of laws and actions taken by vOBU are sent to the DLT system so that its trustiness can be measured and taken into consideration.

3.2.6.3 Target KPI

Target KPIs			
SLR Title	**SLR Unit**	**SLR Value**	**Explanation/Reasoning/Background**
Initial Time	ms	Mean Value < 200 ms	When the device is turned on and depending on the solution adopted there might be an initial delay until messages can be processed by the network.
Message Overload	ms	Mean Value < 10 ms	Each message sent from a OBU needs to be redirected to the vOBU and to be analysed for GDPR compliance. The measurement of the overload produced by this process is needed.
Migration time	ms	Mean Value < 50 ms	Time needed since the last message sent on the original network is processed and the first message on the visited network is processed.

Table 16: Target KPIs for TC6

3.2.6.4 Requirements for deployment, preconditions

- Multi-RAN deployment. Multi-operator/roaming environment desirable
- Programmable SDN network. If transparent counterpart is desired
- Multi-compute NFV system with geographical resource allocation system.
- DLT deployment

3.2.6.5 WP3/WP4 enablers

- Security Orchestrator
    - The piece in charge of orchestrating received policies into the different Domains at end to end level or in precise actions at each Domain
- Migrate (UMU)
    - Migration VNF system from 5GINFIRE might need some adaptation
- DLT
    - DLT system to maintain coherency and provide
- Policy Repository
    - Repository containing already enforced policies, providing a historical that allows the conflict detection
- Conflict Detector Entity able to detect policy conflicts within policies and inter-policiesData Collectors
    - Entities in charge of inspecting the network usage.
- Behavioural Profiles- vOBU certification
    - Profiles defined as a register of the “behaviour” of a device, in terms to be able to anticipate to a possible attack. This is needed as the number of connected devices grows, it is more difficult to reduce the surface of the attacks. For that purpose, Manufacturer Usage Description (MUD) is an IETF standard aimed to define the intended behaviour of the devices through Access Control Lists. These “profiles” could be adapted and extended to certify the proper behaviour of the deployed vOBU, among other deployed services.
- Trust Manager
    - The element, which is able to calculate from both historical and current data, how reliable a cloud (or a service) is. This is relevant as a client will be able to know how reliable the architecture on which its services are deployed is, and a Cloud Service Provider (CSP) will be able to know the reliability of the services that will deploy. To improve the usefulness of this mechanism, it could be interesting implementing it as a Smart Contract, to provide the obtained trust values in a non-repudiate and auditable way.
- TEE
    - Trusted Execution Environment techniques to protect the cryptographic material

3.2.6.6 Methodology and expected outputs

Methodology

Evaluation of existing software elements/enablers to be used.

Extension of existing enablers to adapt communications to the Integration Fabric, evolving to a service mesh communication scheme.

Definition of Policies that trigger the Test Case, implementation and integration onto Inspire-5Gplus Architecture, which needs to be deployed onto the testbed

Implementation, deployment and integration iterative procedure

Extraction of KPIs

Expected Outputs

The outputs are the KPIs defined in previous section and the recommendations on thresholds where the proposal is interesting or how it can adapt to different security flaws scenarios.

3.2.6.7 Timeline and risks

Phase	Time	Description	Risks
0 - Basic scenario	M12	First requirements definition and adaptations based on deployment	No risks are foreseen.
1 - Integration on Testbed	M14	Integrate into final testbed	No risks are foreseen
2 - UE Integration	M20	Integrate 5G UEs	No risks are foreseen
3 - Reactive Scenario	M24	Allow Reactive provisioning	Possible limitations on events provided by 5G network

Table 17: Timeline and risks for TC6

3.2.7 Test Case 7: Intelligent and Secure Management of Shared Resources to Prevent (D)DoS

This Test Case's main goal is to protect shared resources within slices under un-mitigated DDoS attack. In addition, it provides a damage control mechanism to avoid resource starvation during undetected and unmitigated attacks.

3.2.7.1 Problem Description and Objective

Dealing with security threats is a never-ending task where attackers continuously renew their strategies. The security provider needs to always find and adapt to new threats. This cat-and-mouse game leads to moments where attackers have the upper hand with pristine offensives that thwart deployed defences. For instance, the contemporary (Distributed) Denial of Service ((D)DoS) attacks are getting stealthier, having the ability to mimic genuine behaviour with low-bandwidth usage, which allows them to evade the detection mechanisms. The goal of the TC7 is to demonstrate the ability to do damage control when a situation in a slice escapes direct threat detection and mitigation. In fact, the interdependence between slices due to virtual network functions and infrastructure resources sharing increases the risk of *indirect (D)DoS*; that is, the direct (D)DoS

exhausts the resources of one slice, which may influence the resources shared with other slices, affecting the availability and performance of provided services. A potential attack scenario, as illustrated in Figure 29, is as follows:

1. An attacker creates a botnet army by infecting many mobile devices. The botnet is used to launch a DDoS attack against a VNF in slice 1;
2. The INSPIRE-5G+ security assets eventually deployed on the targeted slice are unable to detect the attack;
3. Noticing the degradation in performance, the system triggers a scale up (i.e. increasing the resources for the VNF) or a scale out (i.e. increasing the number of VMs serving the VNF);
4. If this scaling up/scaling out is performed in an uncontrolled way, it may lead to exhausting physical resources shared with slice 2.

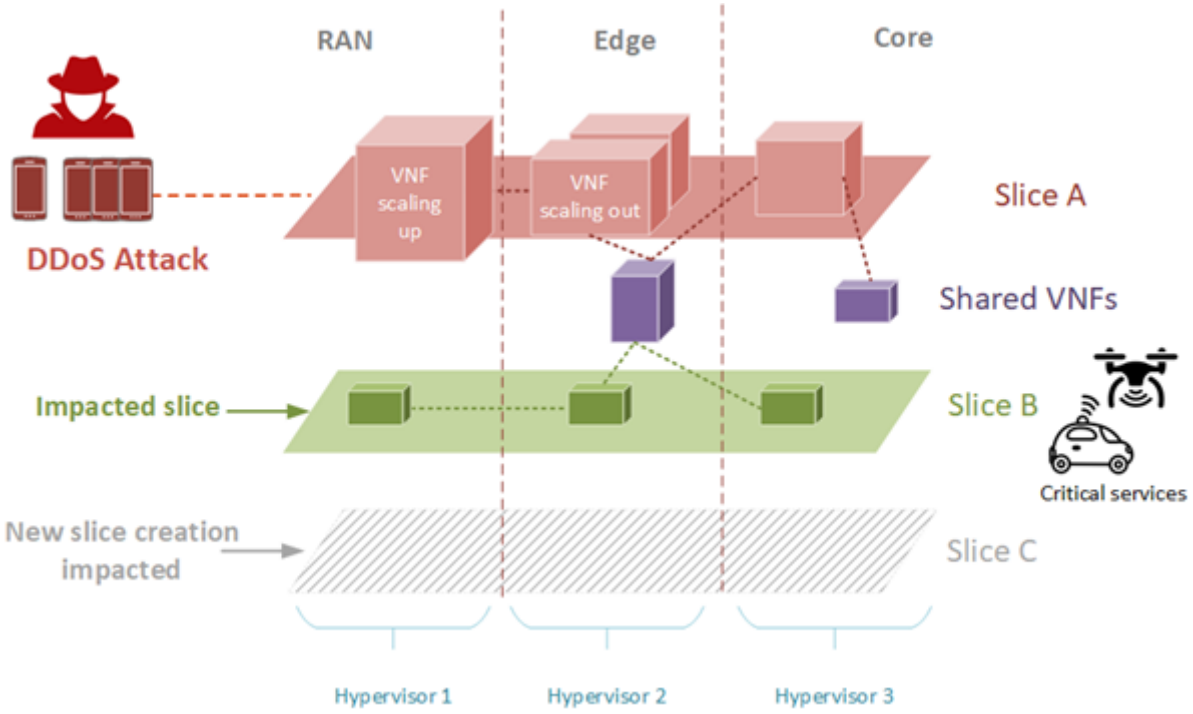

Figure 29: DDoS against Shared Resources

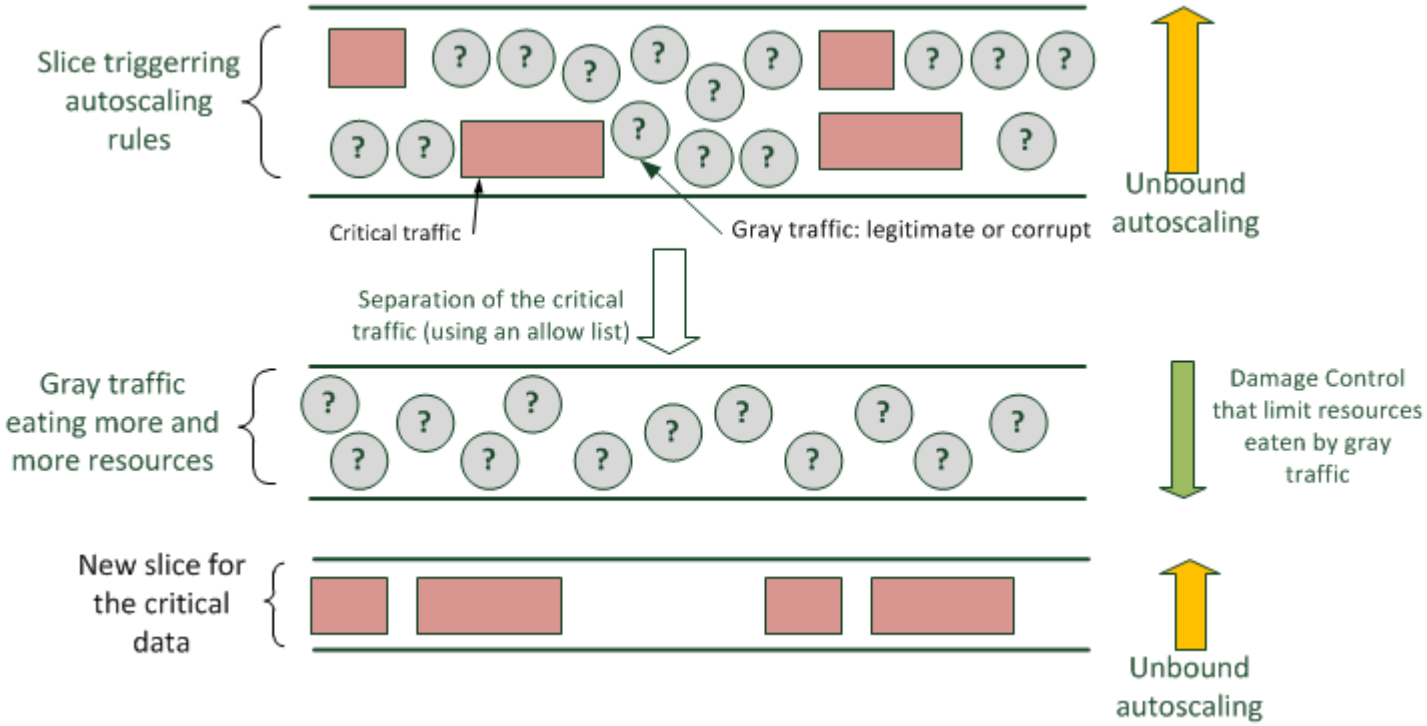

Figure 30: Potential (D)DoS Mitigation Strategy

In this TC, we focus on how to detect and prevent (D)DoS against shared resources using Machine Learning (ML). The goal is to develop an ML-based solution that allocates resources to slices in a way to prevent the (D)DoS from negatively impacting the services while fulfilling the required SLA of each slice.

The ML will help find the best strategy for mitigating the (D)DoS attack. This could imply (as depicted in Figure 30): allocating more resources for given slices, creating a new slice to separate the traffic that is considered legitimate (e.g. using white lists) from traffic that could be considered suspicious or less critical. The suspicious traffic can be sent to a slice that will perform more thorough security analyses. The aim is to maintain the minimum required SLA for the applications and users of the slices.

The ML techniques have been proven vulnerable to adversarial attacks, which may fool the ML model to take wrong decisions regarding the resource allocation. To mitigate this issue, the ML model will be made robust to adversarial attacks.

3.2.7.2 Functional Architecture

Figure 31 depicts the different components that are involved in a given domain and the cross-domain. The numbers in Figure 31 indicate the main steps of the procedure to mitigate the attacks:

1. E2E/Domain SSLA requests a scaling up/out to ensuring the KPIs;
2. E2E Security Intelligence Service/Domain Security Analytics Engine or E2E/Domain Decision Engine (where the damage control resides) foresees an impact on the other slice's resources. The Domain-level Decision Engine l validates or refuses the autoscaling request;
3. The auto-scaling receives stricter scaling rules;
4. The Domain-level Decision Engine may trigger the creation of a new slice to ensure that critical services / traffic will not be affected.

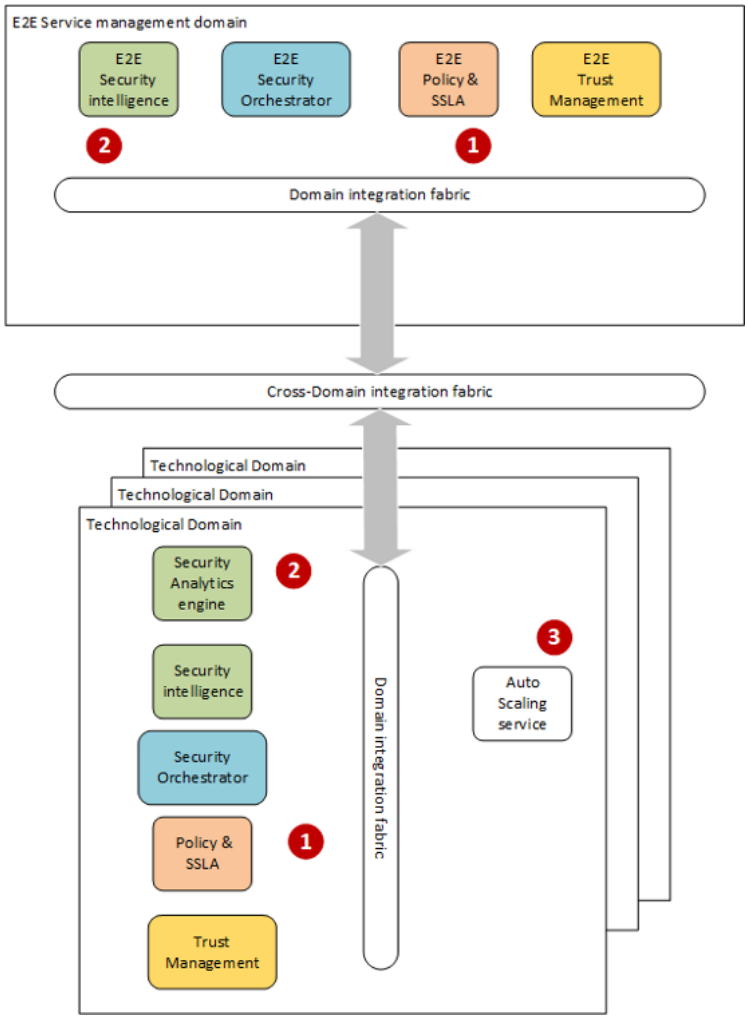

Figure 31: Mapping of TC7 to INSPIRE-5Gplus HLA

3.2.7.3 Target KPIs

The success of the TC in meeting its objectives will be assessed against the following Key Performance Indicators (KPIs)

KPI Title	KPI Unit	KPI Value	Explanation/Reasoning/Background
Service response time	%	>60%	Improvement ratio compared to the case without our solution
Service downtime	%	>60%	Improvement ratio compared to the case without our solution
SLA enforcement	%	>99%	SLAs of slices are practically always respected for critical services or slice
New slice acceptance	T/F		Ability the create new slices using free resources preserved by the damage control component
Blocked adv. examples rate	%	>95%	The percentage of adversarial examples successfully detected

Table 18: Target KPIs for TC7

3.2.7.4 Complementary measurements

KPI Title	KPI Unit	KPI Value	Explanation/Reasoning/Background
Ratio of allowed malicious scale-up	%	<5%	The percentage of scale-up due to (D)DoS that have escaped the damage control mechanism. A lower value means that our system is able to protect resources by refusing some scaling requests (optional). This needs to be determined through a controlled experiment where network traffic containing DDoS attacks is generated.

Table 19: Complementary KPIs for TC7

3.2.7.5 WP3/WP4 enablers

- Network slice manager
- Analytics Engine:
    - PunchPlatform: a generic engine to process monitoring logs and events for computing services behaviour across time.
    - MMT (Montimage Monitoring Tool) framework to analyse the meta-data provided by the monitoring agents.
    - Legitimate traffic detector (rules that allow determining what part of the traffic is reliable, e.g. white list of IP source addresses or well-established behaviour patterns).
- SLAs manager
    - MMT SSLA metrics, assessment and enforcement
- Active/Passive Probes (adapted to SLAs monitoring)
    - MMT-Probes to extract meta-data
    - Separating traffic using active probes that are orchestrated to load balance the traffic or the slice controller that load balances the traffic
- Auto-scaling tools
- Damage control component
- ML models robust to adversarial attacks

Optional enablers

- Standalone (D)DoS detection asset based on classical statistics (Spider);
- (D)DoS detection asset that computes flows' fingerprints to build frequency distributions of protocol uses, for classification using DBSCAN. For now, it uses batch training but there is work in progress to support online analysis (to be verified);
- EPC-in-a-Box: 5G SA experimental platform integrating the MMT security monitoring framework.

3.2.7.6 Methodology and expected outputs

Methodology

- Investigation of existing software tools/enablers to be used in the TC and identification of required extensions and new developments to be made;
- Implementation, deployment and integration through an iterative procedure;
- Demonstration and measurement of defined KPIs.

Expected outputs

- Avoid resources starvation during an un-mitigated attack;
- Ability to distinguish known good traffic from unknown (potentially malicious) traffic;

3.2.7.7 Timeline and risks

Phase	Time	Description	Risks
0 -	M12	Identify the test case requirements.	No risks are foreseen
1 -	M18	Deploying network slices with auto-scaling and monitoring capabilities enabled and conducting stealthy DDoS attack.	No risks are foreseen
2 -	M24	Design and implementation of DDoS-aware auto-scaling solution (i.e., Damage Control Component).	No risks are foreseen
3 -	M30	Integration in the test infrastructure.	Possible complexity in integrating the developed enablers
4 -	M36	Demonstrate and evaluate the defined KPIs.	Availability and possible limitations on services provided by 5G testbed (X-Network)

Table 20: Timeline and risks for TC7

3.2.8 Test Case 8: Security posture assessment and threat visualization of 5G networks

5G infrastructure, services and assets result in complex multi-domain networks. The complexity and multi-domain nature of such networks increases the difficulty of assessing their security posture. Furthermore, the security posture of 5G networks is affected by human actors, policies and existing mitigation mechanisms. In this test case, we present a software-aided process to facilitate the security assessment process of 5G network using the open source tool DiscØvery. This test case was derived from the 5G-CARMEN project[5]. 5G-CARMEN is focused on the Bologna-Munich corridor. The objective of 5G-CARMEN is to leverage 5G advances to provide a multi-tenant platform than can support the automotive sector. The aim is to deliver safer, greener, and more intelligent transportation with the ultimate goal of enabling self-driving cars. The test case is based on the Back-Situation Awareness use case of 5G-CARMEN. In the Back-Situation Awareness, the 5G-CARMEN

[5] https://5gcarmen.eu

promotes extended situation awareness by enabling vehicles and infrastructure to share the perception of the environment.

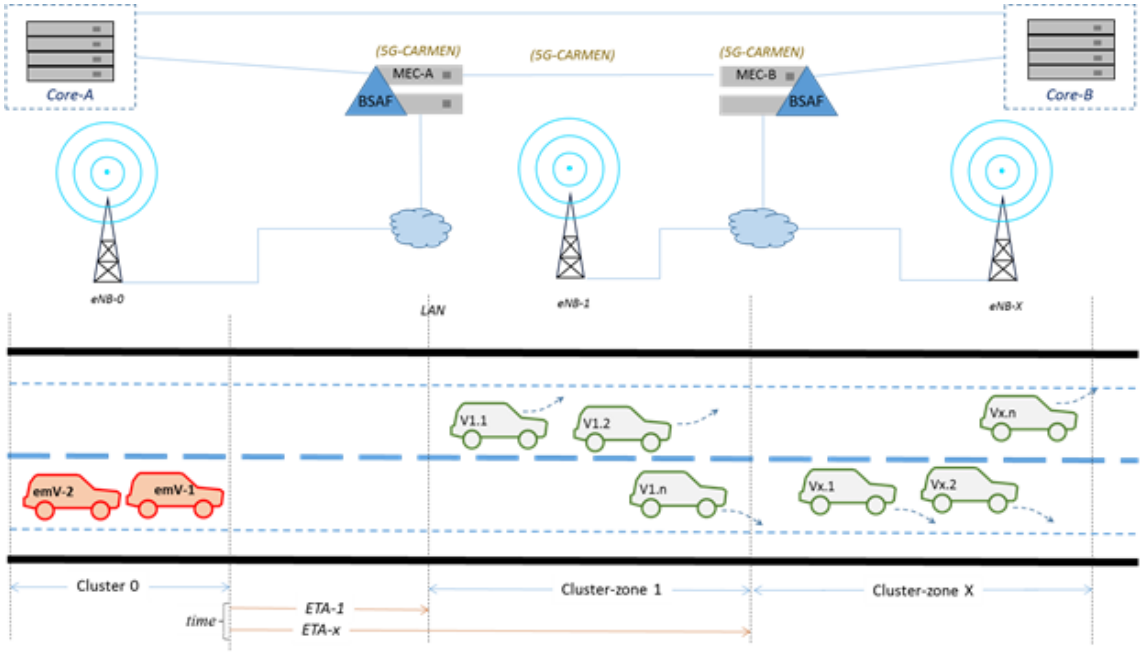

Figure 32: Back Situation Awareness in 5G-CARMEN6

Figure 32 provides an overview of the Back-Situation awareness scenario as described in 5G-CARMEN. The scenario involves two emVs that have been dispatched. Their Estimated Time of Arrival (ETA) and other relevant information (e.g. Type of emVs) is being communicated by the infrastructure to the vehicles at the front of the emVs which travel on route as the emVs. Based on the ETAs notification, the other vehicles will then negotiate between themselves and cooperatively manoeuvre to clear corridor for the emVs to pass through un-hindered. Additionally, the infrastructure can provide manoeuvre actions to the vehicles to assist in the formation of a clear corridor. The ETA along with other relevant information, such manoeuvre recommendations, can either be calculated at the infrastructure, or it can be derived by the vehicles' on on board unit using by processing the information such as the emVs' location, speed, direction provided periodically by the infrastructure. An example manoeuvre recommendation could be to notify the vehicles to increase the gap between each other and/or turn towards the road shoulder of their respective lane.

3.2.8.1 Problem Description and Objective

This test case focuses on reducing the complexity of assessing the security posture of 5G networks. 5G networks are composed by several virtualized assets that provide services to end users and other service consumers. The virtual nature of 5G assets means that they are highly dynamic and flexible. The dynamic nature of such assets introduces significant complexity to process of security analysis. Depending on the deployed assets, the security considerations of the network can be different. A 5G network will need to be able to deploy a different security mechanism or update the configuration of its deployed assets. A security analyst needs to not only have a view of high-level of the different 5G network configurations, but also the low-level deployment information.

In this test case, we will provide a modelling language to express the assets of 5G networks to facilitate security assessment. The modelling language will provide concepts to express users, service

[6] https://5gcarmen.eu/wp-content/uploads/2020/03/5G_CARMEN_D2.1_FINAL.pdf

providers, policies and other concepts to describe the necessary components of a network that affect its security. The concepts of the modelling language will allow security analysts to better design the different configurations of 5G networks. Once a 5G network has been modelled, a security analyst will be able to deploy functions for automated security assessment. Examples of such automated functions are threat and vulnerability identification, suggestions for security policies and insights for security mechanisms.

3.2.8.2 Functional Architecture

The functional architecture of the test case is divided into the following components:

- The desktop application DiscØvery: is the application that will be used to perform security analysis on the 5G network. DiscØvery supports several algorithms and features for facilitating the assessment of a 5G network's security posture.
- DiscØvery's model generation algorithms: the algorithms that be used to automatically generate the components of a 5G network.
- DiscØvery's cyber-security insights: a list of custom suggestions and insights that are result of DiscØvery's automated security analysis processes. The insights are based on the unique characteristics of a network.
- A description of the 5G network under analysis: the description will include a detailed enumeration of the components of the 5G network, its assets, its security mechanisms and policies. The list will be used to create the components model of the 5G network that cannot be detected with the DiscØvery's automated algorithms. This information includes high-level policies, actors and assets.
- Network information from the 5G network under analysis: the networks information is manually collected and imported to DicsØvery. Network capture files contain crucial information that can be used by DiscØvery's algorithms to automatically create network models.

DiscØvery is part of the Policy & SLA Management component of the High-level architecture of the INSPIRE-5Gplus, which is shown in Figure 33.

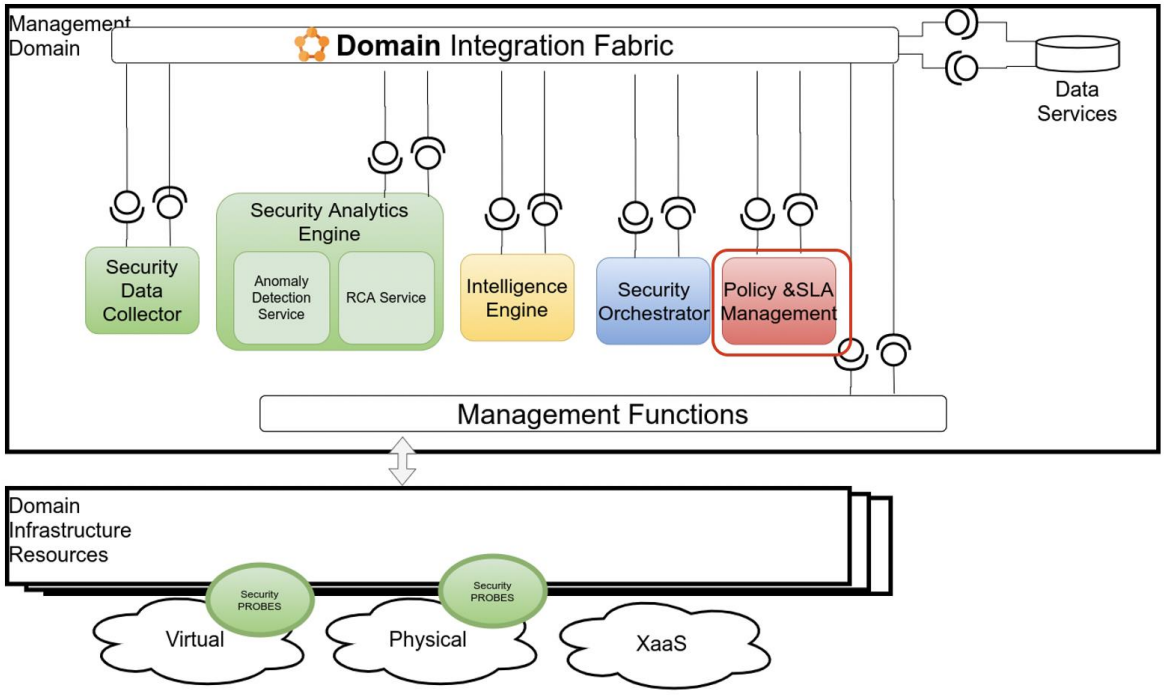

Figure 33: DiscØvery in the High-Level Architecture of INSPIRE-5Gplus

3.2.8.3 Target KPI

The evaluation of the outcomes of the test case will be based performance indicators against the following SLRs:

Target KPIs			
SLR Title	SLR Unit	SLR Value	Explanation/Reasoning/Background
Automated model generation	[%]	>75%	DiscOØvery's automated model generation algorithms are able to model only the network layer of a 5G network. Security policies or certain security mechanisms cannot be elicited by network information. For that reason, models automatically generated by network data will not represent all the components of the network. The aim of this SLR is to identify the percentage of the actual network that can be modelled automatically.
Automated Vulnerability assessment	[%]	>70%	The automated assessment of network's vulnerabilities can result to vulnerabilities that cannot impact the system. For example, the attack vector for a vulnerability is not materialized in the network and the vulnerability cannot be exploited. This SLR will measure the percentage of identified vulnerabilities that can be to used exploit the network.
Threat identification	[%]	>70%	The automated identification of threats can result to threats that are may be out of scope of the network's security requirements. This SLR will measure the percentage of the threats that are necessary for the networks to be protected.
Cyber-security Insights assessment	[%]	>65%	The derived cyber-insights may be addressed by existing security mechanisms or may be considered out of scope. This SLR will measure the percentage of the cyber-insights that were used to improve the security posture of a 5G network.

Table 21: Target ACCA KPIs of Test Case 8

3.2.8.4 Requirements for deployment, preconditions

The test case will evaluate the features and functions of the software tool DiscØvery. DiscØvery is cross-platform desktop tool. It can be installed in the form of an application on Windows, macOS and most Linux-bases distros. The compile the tool from its open source code, it requires the node.js[7] tool installed on the host system.

3.2.8.5 WP3/WP4 enablers

In this test case we demonstrate the DiscØvery enabler for network system modelling and security assessment. DiscØvery has multiple functions covering the objectives of WP3 and WP4.

The network system modelling enabler is used to automate the model generation of 5G networks using network information, such as network capture files. This enabler allows a security analyst to accurately capture and design a 5G network.

The following enablers will be demonstrated:

- Model Generation of 5G networks through network capture files
- The cyber-security insights assessment that will provide a security analyst a list of recommendations on how to improve the security posture of the network. The recommendations will be divided into high-level recommendations that cover policies and process, and low-level recommendations that cover security mechanisms
- The automated identification of threats based on the attributes of the network
- The automated assessment of vulnerabilities of the network's components

3.2.8.6 Methodology and expected outputs

The data and assets that will be analysed in the TC will be provided by the outputs of the 5G-CARMEN project. Since DiscØvery is an open source tool, all the data and developed features will be made available through its GitHub repository[8]. The repository will include the necessary technical documentation and developed models that resulted from the analysis of the test case.

The expected outputs of the test case are to demonstrate the use of software-aided security analysis of complex and dynamic 5G networks. The test case is focussed on the security issues that derive from connected vehicles in cross-border scenarios as described in the Back-Situation Awareness. Additionally, the test case will validate the analysis processes of DiscØvery in the context of security analysis of 5G networks.

3.2.8.7 Timeline and risks

The test case is based on the 5G-CARMEN EU project. 5G-CARMEN is an ICT-18 project that started in November 2018 and it will finish in October 2021. 5G-CARMEN is currently in the initial demonstration phase. The security analysis of the use cases took place during the first year of the project. As result, all the necessary data to develop the test case for the INSPIRE-5Gplus project are available at the time of writing this document.

The timeline of the test case is divided in three phase evolution until the end of the INSPIRE-5Gplus project. In Table 22 we show the phases of the case.

[7] https://nodejs.org/en/

[8] https://github.com/CyberLens/Discovery

Phase	Month to be finished	Description	Risks
0 - Modelling of the test case	M12	Develop the graph models that represent the different stages of the test case for analysis using DiscØvery.	No risks are foreseen.
1 - Security analysis and development	M24	Perform security analysis using DiscØvery's features and algorithms. This phase will improve the current features of DiscØvery and will refine or develop additional features to facility the security analysis.	No risks are foreseen.
2 - Results validation and demonstration	M36	This phase will demonstrate the results of the security analysis and evaluate the defined KPIs of the test case.	No risks are foreseen

Table 22: Test Case 8 timeline and risks

3.2.9 Test Case 9: Secure and privacy enabled local 5G infrastructure

This test case is originated from the consideration that multiple local 5G network operators, mobile network operators and computational resource providers (e.g., cloud service providers) are running on a common platform to cater 5G services and computational resources to end users in a secure and privacy enabled manner. In this test case, we intend to demonstrate how to use smart contracts for security-oriented service level agreements (SSLAs) for local 5G operators and infrastructure providers running on a common platform. As a decentralized infrastructure and distributed general ledger agreement, the blockchain presents a great opportunity to establish data security, privacy and trust for automation and intelligence development in multi-tenant multi-operator environment and it creates a new decentralized programmable smart ecosystem.

3.2.9.1 Problem Description and Objective

Local 5G network operators may deploy their network infrastructure including both radio access and backhaul networks. We consider a scenario where a network slice is formed with multiple local 5G network operators. Initially, the notion of the 5G Network Slice Broker has been introduced, which resides inside the infrastructure provider, detailing the required interfaces and functional enhancements for supporting on-demand multi-tenant mobile networks based on the latest 3GPP network sharing management architectures. However, in this test case, we consider the role of network slice broker will be more advanced and operate as a separate entity that perform as mediator between the network operators and the end users. As the slice broker, we use the security enabler, which we develop for INSPIRE-5Gplus project, called SFSBroker (Secure and Federated Slice Broker) mechanism. SFSBroker may allow orchestrating the life cycle of the network slice with multiple local 5G network operators and resource providers in an automated and secured process. Here, federation refers to the orchestration of services (i.e., network functions, computational resources, etc.) offered by multiple local 5G operators. The objective is to use smart contracts with SFSBroker for security-oriented service level agreements (SSLAs) for local 5G operators and infrastructure providers running on a common platform.

3.2.9.2 Functional Architecture

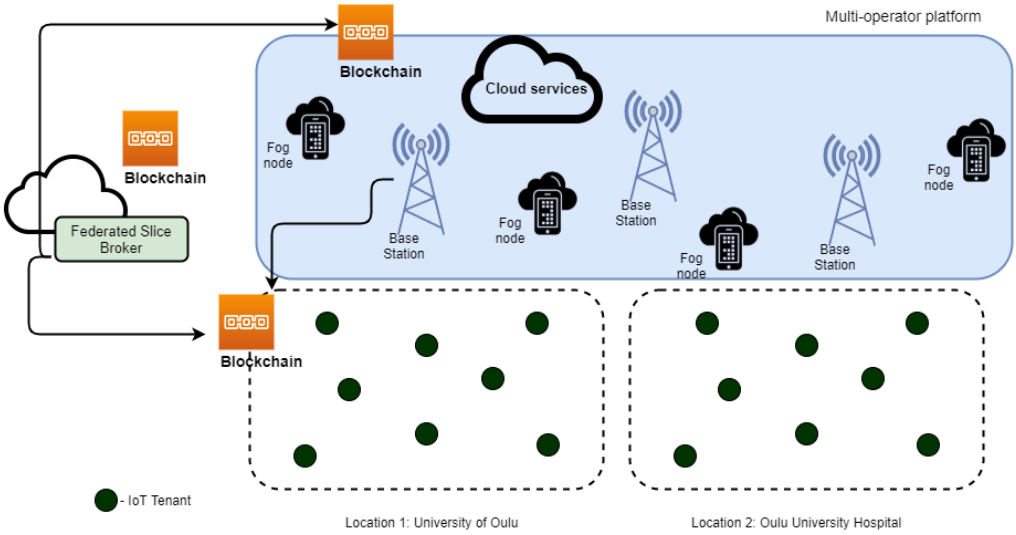

Figure 34: Initial proposal for Test Case 9

The functional architecture of the test case is mainly divided into three segments by incorporating interoperable hierarchical Blockchain networks.

IoT tenant cluster: Represents a collection of IoT nodes and edge computing nodes that are restricted to a limited geographical area. In our case we consider two localized sites including IoT tenants may lease the networking and computational resources, and data processing services from multiple service providers/operators. The internal blockchain network of the tenant cluster publicly holds the attributes to be evaluated when a particular slice broker is required to select. The smart contracts automatically select the particular slice broker as per the requirement.

Brokering mechanism: This maintains a common queue to store the past and anticipated service/resource requests emerging from the clients, the possible E2E slice formation that fulfils their requests, availability of networking and computing resources at the providers, traffic status, etc. The slicing service also maintains attributes to assess the physical infrastructure in the selection process. These attributes derived by evaluating the service delivery standards along with the corresponding SSLAs. The SSLAs defined as smart contracts and the SSLA assignment happens using the assignment smart contract.

Operator/Service provider cluster (Infrastructure cluster): This denotes the local 5G network operators, mobile network operators as well as the cloud service providers. The infrastructure cluster holds the predefined smart contracts for each SSLA to be agreed by slice broker.

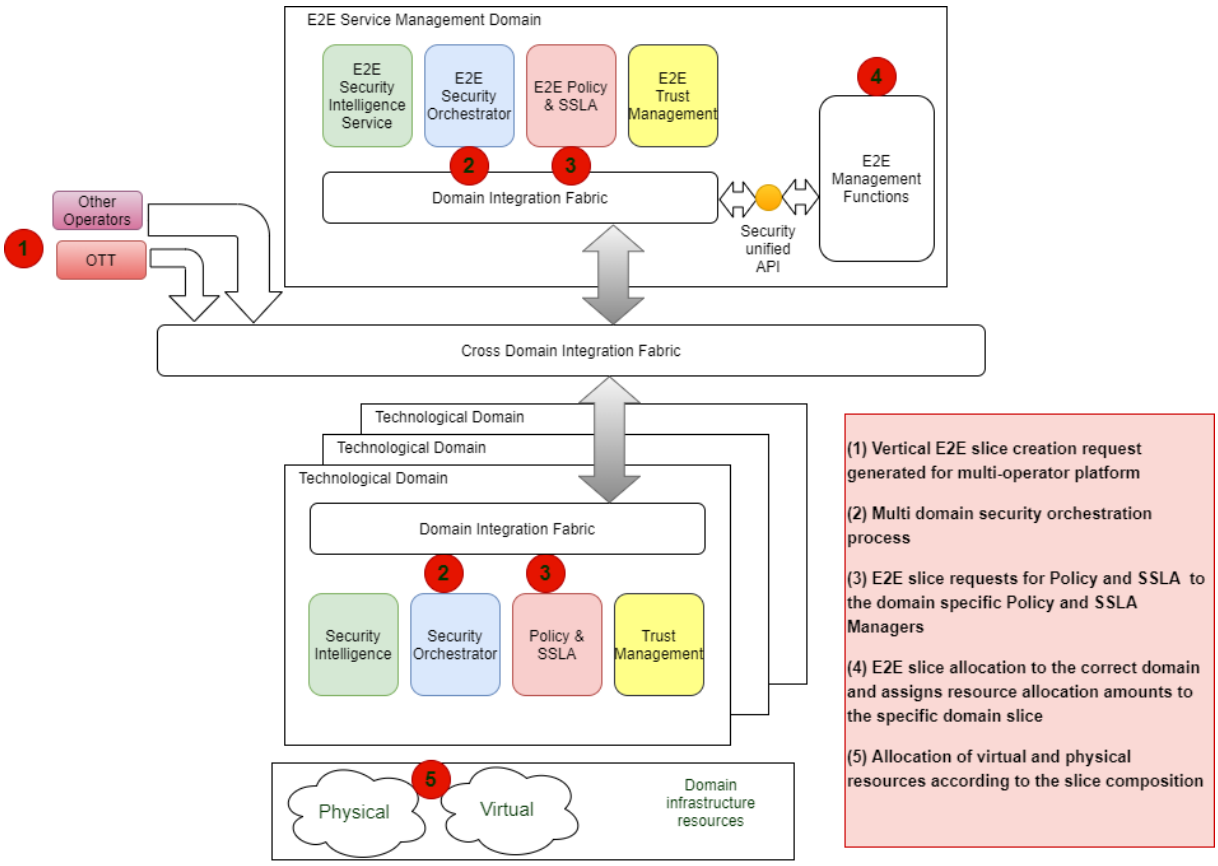

Figure 35: Mapping of TC9 on the INSPIRE-5Gplus High Level Architecture

3.2.9.3 Target KPI

Target KPIs			
SLR Title	SLR Unit	SLR Value	Explanation/Reasoning/Background
Latency	sec	<15sec	Time to serve one user request. This denotes E2E slice creation based on a resource request occurred from an IoT tenant.
Scalability/ Throughput	tps	> 50-100	Number of transactions that tenant blockchain can process in a given second

Table 23 Target KPI for TC9

3.2.9.4 Requirements for deployment, preconditions

Secured E2E Network Slicing: The E2E Network Slices need to be offered by network operators and resource providers. Therefore, the testbed needs to be composed (i.e., the local operator should offer) of different domains including RAN, backhaul and core network functionalities.

Distributed Ledger Technologies (DLTs) - Private permissioned Blockchains are maintained separately at three clusters including IoT tenants, Slice brokers and local operators.

3.2.9.5 WP3/WP4 enablers

SFSBroker: Secured and federated slice brokering mechanism

3.2.9.6 Methodology and expected outputs

Methodology

Investigation of state-of-the-art slice brokering mechanisms and identification of key limitations.

Identification of the key requirements for the secured and federated slice brokering mechanism.

Investigate the capabilities of distributed ledger technology to overcome the limitations identified and the applicability of identified requirements.

Design and development of SFSBroker mechanism.

Implementation, deployment and integration of the proposed system.

Evaluation of the KPIs upon the deployment on testbed.

Expected outputs

Secure and federated network slice brokering mechanism with smart SSLAs that enable multiple local operators and resource providers to offer their network service and resources to IoT tenants in an automated and scalable manner.

3.2.9.7 Timeline and risks

Phase	Time	Description	Risks
0 - Basic scenario	M18	First requirements definition and design of the SFSBroker security enabler.	No risks are foreseen.
1 - Integration on Testbed	M24	Complete the design and implementation of SFSBroker security enabler and apply it in the given test case.	Low maturity of the enabler.
2 - Results validation and demonstration	M36	This phase will evaluate the defined KPIs of the test case.	Possible limitations on services provided by 5G testbed (5GTN)

Table 24: Description of timeline and risks for TC9

4 5G security testing infrastructure environment

4.1 Overview

One of the main objectives of WP5 is to specify the appropriate testing environment for the integration & experimentation of the 5G security test cases. In this section, we describe the envisioned testing infrastructure and how it relates to the previously detailed test cases.

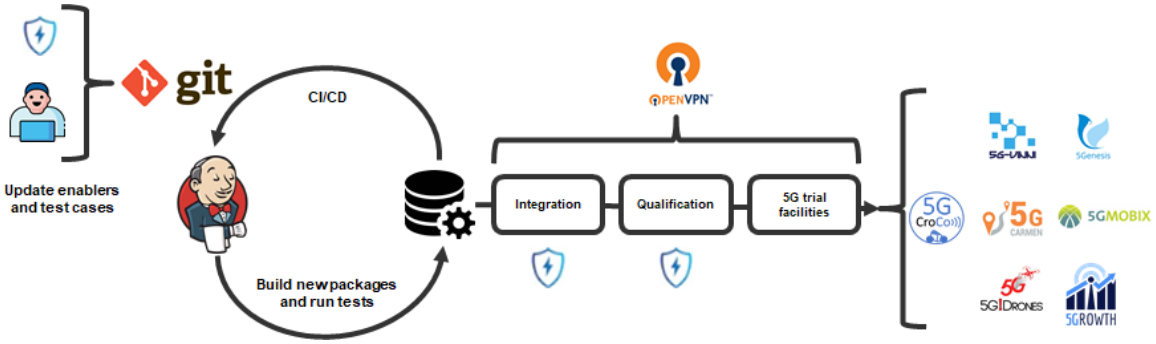

Figure 36: Overview of INSPIRE-5Gplus security testing infrastructure environment

In Figure 36 the overview of the Security Testing Infrastructure is shown. It can be observed that the origin of the proposed infrastructure is the INSPIRE-5Gplus developer contributions towards enablers and test case scripts. These contributions are stored in INSPIRE-5Gplus repository (git based), and each update triggers a continuous integration/continuous deployment (CI/CD) cycle. Packages for enablers and test case are (re-)built and unit tests are run using CI/CD tools, such as Jenkins. Test Cases can be deployed and run in the following platforms: Integration platform (common for INSPIRE-5Gplus test cases), Qualification platform (common for INSPIRE-5Gplus test cases) and dedicated 5G trial facility (specific per test case, based on ICT-17, ICT-18 and ICT-19 5GPPP projects).

Integration and Qualification Platforms will be able to run both enablers and test cases as single network services. These network services will be dynamically deployed and tested, thus providing a first validation towards final deployment in dedicated 5G trial facilities.

4.2 Repository

We have created an institution account in Github for INSPIRE-5Gplus (github.com/inspire-5gplus). This account will serve as public repository of the project and it will be linked to CI/CD tools for the deployment and run of automated tests.

Figure 37: Github repository for INSPIRE-5Gplus

Each enabler and test case will have its repository, including unit tests for enablers and test scripts for each of the test cases. These test scripts will allow the deployment of system level tests for operational validation of the 5G security test cases, with specific pre-defined sequences and success criteria. Well-known test automation frameworks can be considered for the implementation of the different tests to allow re-usability of already defined test sequences and provide easy-to-read result reports that follow a common format for all implemented tests.

4.3 Integration Platform

Integration platform(s) is a stripped-down infrastructure version exploited for continuous integration activities and verification tests of developed 5G security assets, containing the minimum required hardware and software components or mock-up versions of real ones.

A vanilla OSM R8, OpenStack and Kubernetes platforms have been deployed as integration platform and are available for all enablers and test cases.

4.4 Qualification Platform

Qualification platform(s) is a medium-scale laboratory deployed infrastructure comprising hardware and software components, where the 5G security assets having succeeded in the integration and verification tests will be deployed for validation activities.

A vanilla OSM R8, OpenStack and Kubernetes platforms have been deployed as qualification platform and are available for all enablers and test cases.

4.5 Available 5G trial facilities

This section presents the main characteristics of all testbed facilities that will be used to carry out the multiple TCs previously presented. Table 25 provides the relationship between test cases and 5G trial facilies.

Facility	Lead Partner	Test Cases
Athens	NCSRD	TC5
Murcia	UMU	TC4, TC6
AALTO	AALTO	TC7
Barcelona	CTTC	TC1
Oulu	UOULU	TC9
5TONIC(MouseWorld)	TID	TC3, TC4
EPC-in-a-box	MI	TC2, TC3, TC7
CLS Testbed	CLS	TC8

Table 25: Test Case and 5G trial facilities

4.5.1 Athens Testbed

4.5.1.1 Architecture and Components of the Facility

The Athens Testbed is hosted by NCSR "Demokritos" (NCSRD) one of the most significant research centers in Greece, located in north-east Athens. NCSRD comprises an extended campus of 150-acre area, combining indoor and outdoor environments, dispersed around the campus and interconnected by an optical fiber backbone. NCSRD is directly connected to the Greek Educational, Academic and Research Network (GRNET), providing access to Internet and GEANT (pan-European data network for the research and education community).

The Athens Testbed contains 5G and 4G indoor and outdoor infrastructure based on commercial and open source solutions by Amarisoft, Athonet, Nokia and Openair Interface. The Amarisoft Callbox Classic solution provides a compact 5G and 4G deployment in NSA and SA options (gNB, eNB, EPC Rel. 15 and 5GC included) with NR operating on 3.5GHz. Amarisoft's radio access network has also been connected with Athonet's EPC Rel. 15, forming an alternative setup.

In addition, the Laboratory owns NI USRPs N310 and B210 along with suitable servers for operating Openair Interface 5G implementation. The USRPs are synchronized by the Octoclock Clock Synchronization Unit. The infrastructure also contains 4G legacy solutions, including NOKIA's Flexizone Pico BTS and an additional Amarisoft 4G Radio Access and Core Networks.

Figure 38: Amarisoft Callbox Classic 5G (Left) and Main Data Center (Right) in NCSRD

The main Data Center of the Athens Testbed is located in the Media Networks Laboratory in NCSRD and hosts the Katana Slice Manager and all MANO layer components (NMS, EMS, NFVO, etc). In addition, the Data Center includes an NFV infrastructure (NFVI) that is orchestrated by the NFVO (OSM). Currently, the main Data Center comprises 3 compute nodes, operating with OpenStack release "Queens", providing multiple tenants for the Virtual Infrastructure Manager (VIM) and 5GENESIS software components deployment.

The Slice Manager is the component that mediates between the Coordination layer components of the 5GENESIS architecture and the MANO layer. The 5GENESIS Slice Manager is responsible for the lifecycle of network slices, i.e. it manages the creation and provision of network slices over the infrastructure. The Slice Manager provides an API in order to communicate with the Coordination Layer and receive requests for network slices in the form of Generic Slice Template (GST). The GST is

mapped to the Network Slice Template (NEST) by filling in the technical specification of the GST according to the slice requirements.

Katana is already configured to operate on top of the NFV Orchestrator instance, WIM and multiple edge and core NFVIs. In addition, specific interfaces have been developed to allow the provision of resources in the RAN and Core via the supported EMS. The WAN backbone network on the NCSRD site is composed by several physical SDN Switches forming a spine –leaf architecture. All switches are OpenFlow enabled and are controlled by a centralized OpenDayLight (ODL) SDN controller, which is responsible for installing forwarding rules (flows) on each switch. The SDN backbone network can offer isolation and QoS policies for each network slice instantiated on the platform.

An Integrated Services Router (ISR) by Cisco, alongside a Firewall (i.e. Cisco ASA 5510) are used for the realization of the core network gateway on the NCSRD site. Through these nodes the NCSRD core network is connected to the Internet, via the access provided by GRNET. Finally, there is a WAN emulator implemented by Mininet, running on a physical server on the NCSRD site, providing realistic network topologies for multiple experiments.

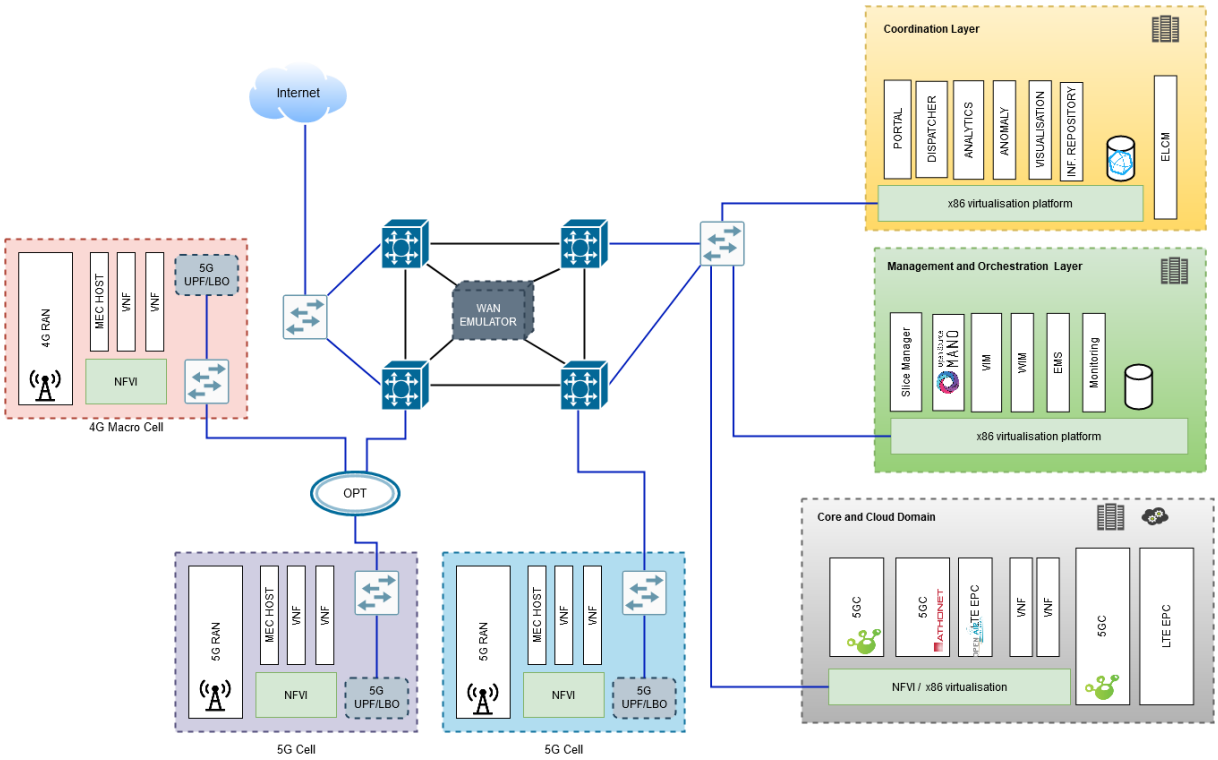

Figure 39: High Level Overview of the Athens Testbed

4.5.1.2 Test Cases

Test Case 5: End-to-end Slice Protection based on Moving Target Defence and Anomaly Detection

4.5.1.3 Capabilities

- Network Slicing based on the Katana Slice Manager[9]
- Commercial and Open Source 5G Infrastructure (Amarisoft gNB & EPC/5GC, Openair Interface, 5G COTS UEs)
- OSM as NFV Orchestrator

[9] https://github.com/medianetlab/katana-slice_manager

- Virtualization Infrastructure Management (Openstack, Kubernetes)
- WAN Infrastructure Manager
- Infrastructure Monitoring (Prometheus, Grafana, InfluxdB)
- Experiments coordination based on the Open5GENESIS Suite (Access Portal, Experiment Life Cycle Management, Results Repository, Analytics)
- IXIA's IxChariot Traffic Generator
- Security Analytics Framework[10]

4.5.1.4 Required building blocks for security test cases

- Analysis of WP3/WP4 enablers integration

Test Case 5 will utilize existing enablers developed in separate projects, which are going to be extended or developed from scratch in the context of INSPIRE-5Gplus. Enablers include:

  - Katana Slice Manager (NCSRD)
  - Security Analytics Framework (NCSRD)
  - Moving Target Defence Controller (ZHAW)
  - MMT probes and monitoring framework (MI)
  - Defence Optimization Engine (DOE) (ZHAW)
  - Security Orchestrator (THALES)

4.5.1.5 Facility Limitations

- Test case risks

Test case risks are defined per phase in the respective TC5 Section. These include enablers' integration complexity, limited number of 5G COTS UEs that could impact the selection of ML approach, as well as the availability of the infrastructure in NCSRD campus, which is used by other projects concurrently.

4.5.1.6 Enhancements Required

- Test case requirement analysis
  - 5G SA
  - Concurrent Slices
  - Integration and end-to-end operation validation of participating enablers
  - Support of data generated by the Radio Access and Core Networks.
- Provide necessary enhancements
  - Upgrade to 5G SA
  - APIs for WP3/WP4 enablers inter-communication
  - New data models and enhanced visualization of data generated in the Radio Access and Core Network Domains
  - Investigation of ML algorithms in the context of anomaly detection and MTD in order to provide an intrusion detection system with an acceptable threat detection accuracy

[10] 5GENESIS Consortium, "Deliverable D3.13 Security Framework," 2019. [Online]. Available: http://5genesis.eu/wp-content/uploads/2019/10/5GENESIS_D3.13_v1.0.pdf. [Accessed October 2020].

4.5.1.7 Timeline and risks

NCSRD is the host of the Athens Facility which is currently used in the context of 5GENESIS and 5G!Drones. As a result, the anticipated technical support will last until the end of 5G!Drones in 2022. After completion of 5G!Drones, then the designated Lab Personnel of INSPIRE-5Gplus will keep supporting the testbed.

Since the Athens Testbed is used in other ICT Projects, an apparent risk is temporary unavailability of the facility due to other events, including demonstrations, project reviews and measurement trials. The mitigation action is proper planning ahead to avoid scheduling conflicts with INSPIRE-5Gplus activities.

4.5.2 Murcia Testbed

4.5.2.1 Architecture and Components of the Facility

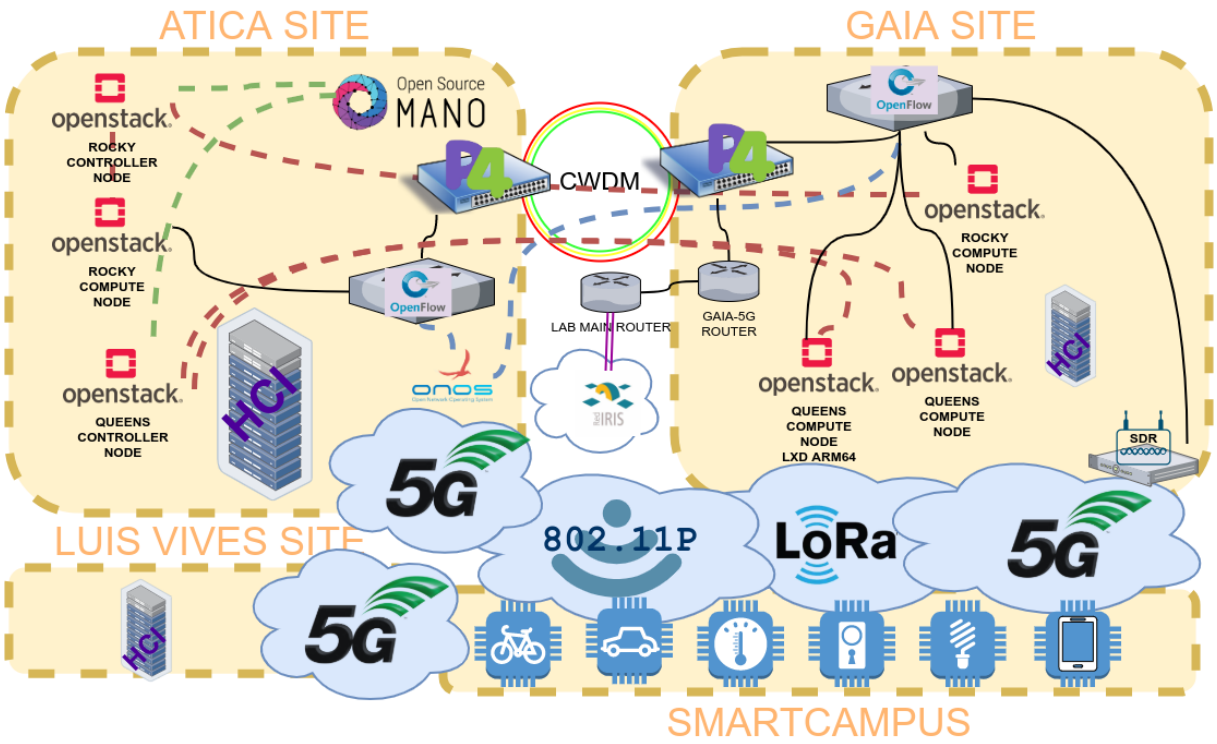

Figure 40: Architecture of the Murcia Testbed

4.5.2.2 Test Cases

- Test Case 4: E2E Encryption TEE secured SECaaS
- Test Case 6: GDPR aware counterparts for cross-border movement

4.5.2.3 Capabilities

- Security - OpenVPN connectivity
- Slicing, Edge, …
- Multi-Access Edge Computing (802.11p + LoRA + 5G)
- OpenFlow (Delta PicOs)
- Dataplane programmability (Stordis and Edgecore Tofino powered switches)
- Commercial (Amarisoft + AW2S) and OpenSource 5G (ETTUS SDR + OpenAirInterface)

- VNFM (OSM + OpenStack), also RPI Drone EDGE available.

4.5.2.4 Required building blocks for security test cases

- Analysis of WP3/WP4 enablers integration

This testbed already served as ANASTACIA's testbed, therefore Policy framework is already deployed and tested as well as Security Orchestrator.

Integration Fabric is being deployed at the time this document is being written.

Indy DLT is deployed and available for the integration with Trust reputation manager.

4.5.2.5 Facility Limitations

- InterOperator roaming handover is long term capability to be obtained.

4.5.2.6 Enhancements Required

- Test case requirement analysis
  - TC4
    - At least two VIM (OpenStack) and SDN between the compute nodes
    - 5G (might be NSA)
    - May nee P4 equipment for GTP tunnelling diversion
  - TC6
    - At least two VIM (OpenStack), SDN between compute nodes and two different RAN (to simulate country change)
- Necessary enhancements
  - Integration Fabric deployment
  - Kubernetes deployment upgrade for Inspire-5GPlus architectural components

4.5.2.7 Timeline and risks

P4 equipment needs to be shared. The testbed is in continuous upgrade and an upgrade on inter-building connectivity is scheduled shortly.

Open source core is not yet available. Commercial cores are also not a possibility at this moment. The existing 5G deployment does not accept roaming. Unless a open source core becomes available there is no roaming possibility foreseen.

4.5.3 Aalto Testbed

4.5.3.1 Architecture and Components of the Facility

The testbed provided by Aalto University, X-Network, is part of the Finnish national project 5GTNF (5G Test Network Finland). It is located at the Otaniemi campus of Aalto University, covering an area of 25 km2. As depicted in Figure 41, the facility integrates different components, including 4G LTE eNBs, 5G NR gNBs, MEC/edge platforms, EPC and experimental 5G cores.

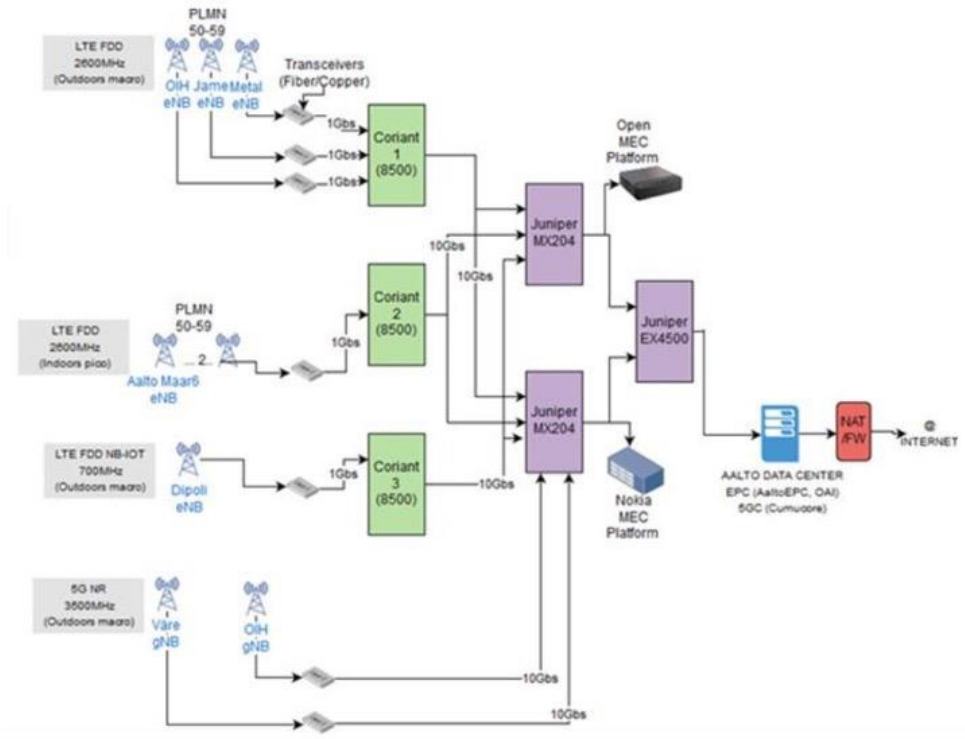

Figure 41: Overview of the Network Deployment in Aalto University

The facility is incrementally building a solution for the management and orchestration of the virtual resources. It is a supporting site to the ICT-17 trial facilities (5GEVE and 5Genesis) and ICT-19 trial facility (5G!Drones).

4.5.3.2 Test Cases

TC7 – Intelligent and Secure Management of Shared Resources to Prevent (D)DoS

4.5.3.3 Capabilities

- **Radio Access Network (RAN)**
  X-Network operates different types of RAN. This includes LTE and NB-IoT networks. Furthermore, the facility operates a NR gNB as described in Table 26 (the gNB is currently operating in NSA mode). In order to perform 5G tests, Aalto University has been granted by national regulatory authority, TRAFICOM, the license to 3.5 GHz. Two commercial UEs (Huawei Mate 20 5G and Samsung A90 5G) have been tested with the current NR gNB.

Component	Details
eNB (4G)	• Ericsson NB-IoT (3.6 – 3.8 GHz) • Nokia LTE (FDD 2.6 GHz (band 7))
gNB (5G)	• Nokia AiScale gNB • Functional split (RRU, DU, CU) support

	• Frequency bands: 3.6 – 3.8 GHz
RAN controller	• X-Network makes use of commercial RAN. The controller of the RAN is currently based on WEM (Web Element Manager)

Table 26: RAN components of X-Network

- **Core Network**
  The core network (CN) includes three different virtualized EPC core network implementations which are Nokia core, Aalto core and CMC core (Cumucore). The later implements a prototype of 5G core architecture including AMF, SMF, UPF, NSSF and NRF. The CN will be running in a datacentre located at the campus. An overview of the CMC CN is shown in Figure 42. It is worth noting that other CNs can also be considered during the project.

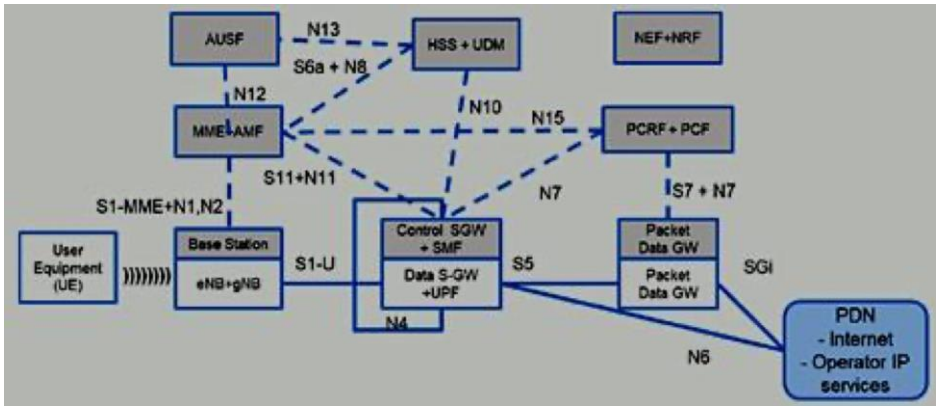

Figure 42: Overview of the EPC/5GC architecture

- **Cloud and MEC**
  The computing infrastructure deployment at Aalto facility consists of both cloud and MEC deployments. The data centre (DC) is physically located in the premises of the campus (Otakaari building) and hosts the different cloud-based 4G/5G network functions.
  Different MEC/edge solutions are available which are deployed between the DC and the RANs. This includes Nokia MEC, Nokia edge and Aalto MEC. The latter is not ETSI compliant and consists of VMs hosting the UPF and the vertical applications. The connections between eNB/gNB is based on fibre converge in SDN-ready Juniper MX204 edge routing platform with capacity up to 400 Gbs (an overview is provided in Figure 41).
- **Orchestration and Management**
  In order to manage the different VNFs and their lifecycles, Aalto University is building a home-made orchestration solution. An overview is shown in Figure 43. While the NFVO is responsible for managing the different VNFs on the top of the virtualized environment, the RAN controller is used to control gNB. Aalto University facility makes use of a commercial gNB (Nokia AirScale gNB). Currently, the gNB can be managed only via a Web Element Manager (WEM).

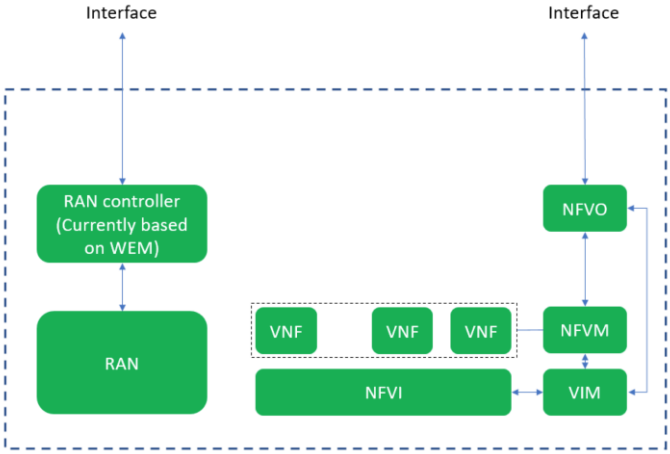

Figure 43: Overview of the current/planned orchestration solution at X-Network

- **Network Slicing**
  The deployment of a network slice is based on a Network Slice Template (NST). An example of an NST used in X-Network is shown in Figure 44. Different information is considered, including the set of VNFs, the service category, the start and the end dates, etc.

```
--data-raw '{
        "blueprint": 33,
        "vnfs": [
            5
        ],
        "name": "slice21",
        "type": "controlplan",
        "startDate":"2021-08-12",
        "endDate":"2023-08-14",
        "domainName": "dd.example.com",
        "description": "sdfdsf sfdf sf sf",
        "startDate": "2021-08-12",
        "endDate": "2023-08-14",
        "type": "controlplan"

    }'
```

Figure 44: An example of an NST used in X-Network

- **KPIs**
  A number of KPIs can be measured in the facility. This can be captured from different levels which are summarized in Table 27.

KPI	Level	Details
Cell availability	RAN	Cell availability
Cell throughput	RAN	Cell throughput
Average connected UEs	RAN	Average connected UEs
Latency	RAN	Latency related to F1-U interface
CPU usage	NFVO	CPU utilization per VNF
Memory usage	NFVO	Memory utilization per VNF
Slice deployment duration	NFVO	Time required to create a slice
Slice decommissioning duration	NFVO	Time required to release a slice

Table 27: KPIs measured in Aalto's Facility.

4.5.3.4 Required building blocks for security test cases

- Analysis of WP3/WP4 enablers integration

TC7 will rely on existing enablers developed in separate projects (which can be extended if required) as well as new enablers that will be developed in the context of INSPIRE-5Gplus project. The enablers include:

- Network Slice Manager;
- Analytics Engine (PunchPlatform, MMT);
- SLA Manager (MMT SSLA);
- Active/Passive Probes (MMT-Probes);
- Auto-scaling service;
- Damage Control Component;
- ML model robust to adversarial attacks.

4.5.3.5 Facility Limitations

- Test case risks

TC7 risks are defined per phase in Table 20. The potential risks include: (i) the complexity of integrating the enablers; (ii) the limitation of services provided by the facility. In fact, the facility does not yet have a final orchestration solution allowing to manage network slices. We are incrementally building a home-made orchestrator to deploy and manage network slices; and (iii) the unavailability of X-Network facility as other projects may need to use it for higher priority tests.

4.5.3.6 Enhancements Required

- Test case requirement analysis
  - Slices sharing virtual/physical resources.
  - Auto-scaling service.
- Necessary enhancements
  - Network slicing management capabilities in X-Network.
  - APIs for enablers' inter-communication.
  - Integration Fabric deployment.

4.5.3.7 Timeline and risks

X-Network facility is still evolving its capabilities and enhancing its services through several research projects. A key risk is the limitation of the required services (e.g., slice management capabilities) by the time of testing. Moreover, X-Network is used in other ICT projects (e.g., 5G!Drones). Thus, a potential risk is the unavailability of the facility due to its use for demonstrations related to other projects.

4.5.4 Barcelona Testbed

4.5.4.1 Architecture and Components of the Facility

CTTC will use part of its ADRENALINE Testbed to develop the previously defined TC1 - (ACCA). Figure 45, presents the ADRENALINE testbed architecture. As it can be seen, this testbed is composed by a set of edge domains, three transport domains (optical and packet-based) and a core domain.

The management of the computing resources available in the multiple domains is done using either Kubernetes -i.e. containers- or OpenStack -i.e. Kernel-Virtual Machine (KVM)-. Regarding the networking resources -e.g. the configuration of optical or packet flows-, this is done through a set of OpenDayLight controllers deployed in all switches.

As defined in Section 3.2.1, it is planned to create two vehicular scenarios. Both of them will use the architecture elements within the red area in Figure 45. Among them, there are 2 computing resources nodes: The Core Domain with a multi-node OpenStack and the Vehicle Edge Domain with two MEC nodes based on Kubernetes. In addition, the transport domains involved on both scenarios makes us of the optical path.

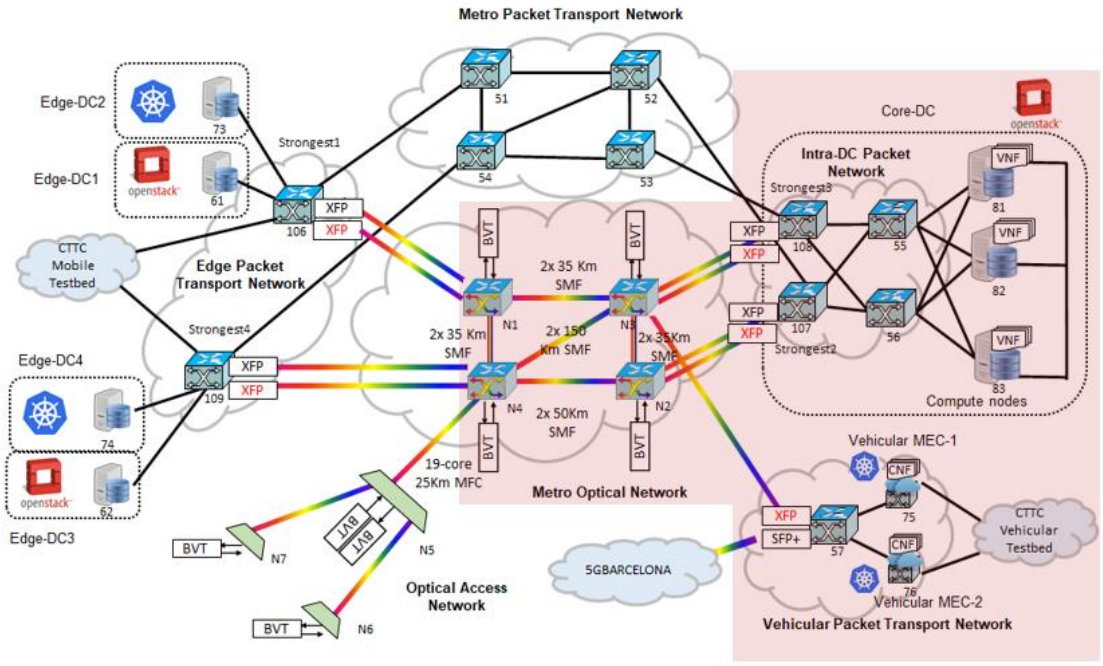

Figure 45: ADRENALINE Testbed Architecture

4.5.4.2 Test Cases

The TC to be deployed in the ADRENALINE testbed is the TC1 - ACCA. On the first of the two planned scenarios, the objective is to deploy a Network Slice that once an SSLA violation rises, the Network Slice is updated by changing the configuration of the Network Services deployed in the RSU nodes. Regarding the second scenario to be demonstrated in this testbed, the objective is to make use of Blockchain in order to add trust in the deployment of Network Slices when a new RSU is added into the network.

4.5.4.3 Capabilities

- Security

The current security capabilities available focus on the use of the SONATA Verification and Validation (V&V) tool to verify and apply tests on Virtual Network Functions (VNFs) and Network Services (NSs) in order to check and confirm that they do the functionality and the service they are thought to do.

- Slicing, Edge, ...

The control plane of the ADRENALINE testbed allows deploying End-to-End Network Slices in the in mutli-domain and using any of the computing technologies currently available -i.e. Kubernetes and OpenStack-. The Network Slice Manager deployed is the one within the SONATA Service Platform (SP).

Together with the capability of managing network slices, within the ADRENALINE testbed it is possible to deploy single NSs through the use of two NFV Orchestrators (NFVOs): SONATA SP and Open Source MANO (OSM).

Finally and as already introduced, the ADRENALINE testbed has multiple transport domains interconnecting the different Virtual Infrastructure Manager (VIM) available. The set of VIMs make use of Kubernets and OpenStack to manage container-based and KVM-based deployments respectively.

4.5.4.4 Required building blocks for security test cases

- Analysis of WP3/WP4 enablers integration

The enablers to carry out the whole TC (and the two scenarios) are on one side the management of SSLAs for Network Slicing and the use of Blockchain on Network Slices. Both enablers are not operative yet and will be developed during the WP3 and WP4 development phase respectively.

4.5.4.5 Facility Limitations

- Test case risks

The ADRENALINE testbed is used by the whole CTTC Optical Network & Systems department, so different project may be using it. Some risks may appear due to the unavailability of the testbed as other projects may need to use it for higher priority tests (-i.e. final review, conference demonstrations, etc.).

As the TC1 aims to look the security aspects based on the Use Case coming from the EUC 5GCroco project, some of the resources such RSUs or vehicles units may be unavailable to be used. A precise planning will be necessary.

4.5.4.6 Enhancements Required

- Test case requirement analysis

Currently the implemented TC in 5GCroco does not focus on security of the information exchange between the elements in the network. This information exchange is done through the use of MQTT messages (http://mqtt.org/) using the publish/subscribe architecture.

- Necessary enhancements

In order to enforce the security within the TC, an objective is to enhance the original TC by adding or improving some security aspect of the MQTT such as Client Authentication, Client IDs, x509 Client Certificates or the restriction to topics among other possibilities.

4.5.4.7 Timeline and risks

The Barcelona testbed is currently used with other projects, so the main risks about it is the coincidence of two projects being tested in it. Although this is already managed and there has never been the issue of having two projects in testing phase, we must keep it in mind.

4.5.5 Oulu Testbed

4.5.5.1 Architecture and Components of the Facility

5GTN represents 5G test network developed and deployed in Oulu, Finland, together with different partners that are closely involved in the development and specification of the 5G technology. The test network targets to serve various application developers by providing extensive test facilities in a carrier-grade state-of-the-art network. 5GTN includes the University of Oulu campus, VTT and the technology village together with several distant locations around Oulu, for example, Oulu University Hospital Test Lab and Nokia factory.

Additionally, outside Oulu Region, Ylivieska test network with approximately 15 base stations was connected to 5GTN at the end of 2017. Another two distant locations are Ii Micropolis and Sodankylä airport, where 5GTN is utilised for testing vehicles in winter conditions and in general, for future self-driving technology. The locations 5GTN covers can be seen in Figure 46. Overall, 5GTN has close to 50 on-air base stations around northern Finland in an area with 450km distance between the two farthest remote locations.

The network architecture depicted in Figure 46 includes the currently existing assets (green and white) as well as during 2018 upcoming assets (orange). The current 5GTN uses technologies including 3GPP specified evolved packet core elements and LTE radio access technology, with a special emphasis on small cell-based solutions. The first 5G proof-of-concept (5G-PoC) devices are also an integral part of the network.

The network is controlled by operator grade EPC (Evolved Packet Core) and which makes the University of Oulu in practice a network operator. The network within the campus is being complemented by a wireless sensor network (IoT, internet of things) extension with estimated 1000 small form factor IoT platforms with different kinds of sensors and wireless connectivity. Furthermore, big data computing servers for network data analytics purposes complement the network. Some of these servers are distributed within the network thus allowing mobile edge computing as well as caching services.

The Nokia EPC runs in a virtualised environment connected to application creation environment with open application programming interfaces, which make it possible to integrate new services to e.g. network management and IoT applications, which thus can be integrated as a part of the whole network offering the experimental environment for research also in data acquisition, cloudification, and analytics.

The test network architecture is highly heterogeneous including in addition to LTE and 5G PoC technologies wireless technologies such as IEEE 802.11, Bluetooth Low energy, LoRa, NB-IoT, UWB and LTE evolutions like LTE-M and LTE-U.

Virtual Multi-access Edge Computing (MEC) deployed in the test network enables service creation environment for low latency services complemented with location and privacy awareness. It also provides mobility and streaming data analytics with real time applications. Edge computing supports heterogeneity. Furthermore, the EPC core of 5GTN controls a licensed shared access (LSA) environment (CORNET network) included in the environment.

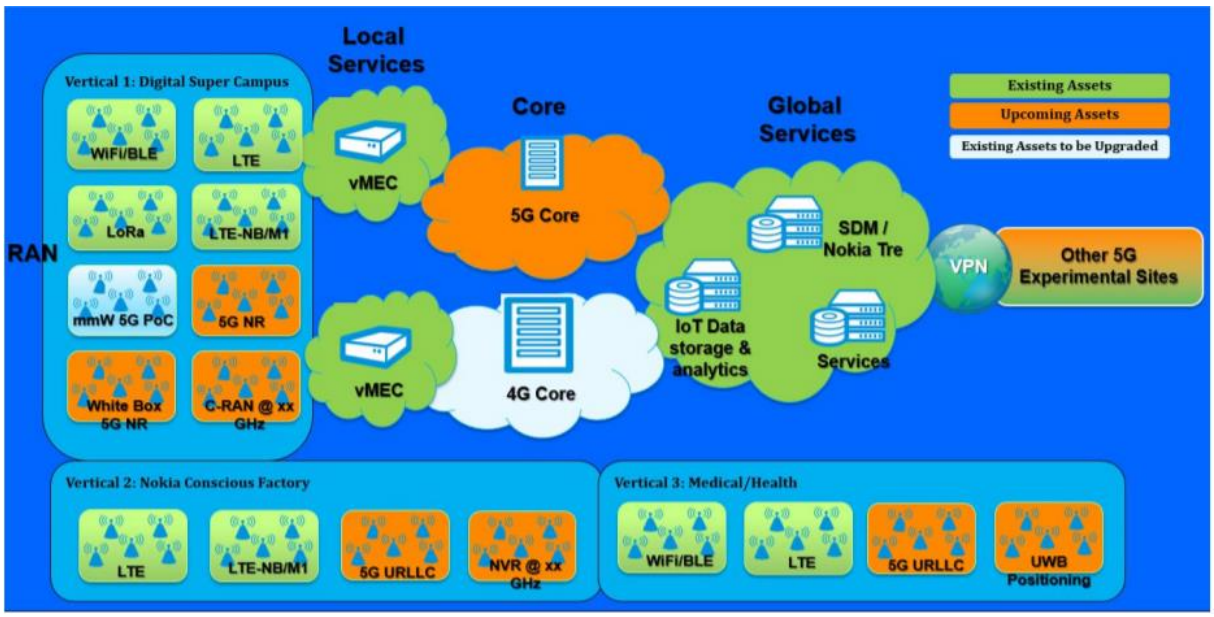

Figure 46: 5GTN architecture including existing and upcoming assets

4.5.5.2 Test Cases

Test Case 9: Secure and privacy enabled local 5G infrastructure

4.5.5.3 Capabilities

- Radio Access Networks

Both test sites of the 5GTN currently deploy one macrocell and six small cell eNodeBs (eNB). The macrocells are installed outdoors, while the small cells are indoor installed. The eNBs operate in an LTE band 7 (2.6 GHz) and are based on the Frequency Division Duplexing (FDD) scheme. The near future plans are to deploy 3.5 GHz equipment and bring first proof of concept 5G radio equipment to the network.

Interoperability with WLAN networks was specified to 3GPP standards already in Release 8. Integrating WLAN networks both as trusted and un-trusted access into the 5G test network according to the 3GPP specifications are in near future plans. However, the transmission resources of WLAN networks can already be exploited in the test network through Layer-3 mobility protocols, such as Mobile IP (MIP), and multi-path protocols, like Multi-Path TCP (MPTCP).

Currently, the test network implements a pre-commercial 2 LTE-M capability (Category-0). Some LTE-M features are already standardized, while some other are still work in progress. However, the overall aim of LTE-M is to connect constrained IoT devices by exploiting the existing LTE infrastructure. Lower resource consumption of LTE-M compared with regular communications is obtained through a narrower bandwidth (1.4 MHz/200 kHz) and advanced power save modes. LTE-M provides also enhanced coverage, reduced hardware costs, and simplified signaling.

- Cloud Core

The core network entities run on an OpenStack cloud environment. In the first phase of the test network development, System Architecture Evolution Gateway (SAE-GW) and Mobility Management Entity (MME) are installed. The rest of the core network functionality runs from a remote core network, located at Nokia's premises in Tampere, Finland. The remote core network is connected over a Virtual Private Network (VPN) tunnel. However, as SAE-GW and MME run locally in the test network, all data traffic and most of the control traffic stays within the local network, in both VTT's and CWC's test sites separately.

- MEC capabilities

The MEC functionality in the test network will be based on Nokia's MEC solution. The MEC concept is one of the key services in 5G. It allows third-party service providers to bring their services and service-specific functions close to users through standardized interfaces and an open architecture. As the services can be brought to RANs, MEC can result in lower delays and more efficient exploitation of network capacity. Being based on the cloud concept, MEC capabilities can be made dynamic and scalable.

MEC enables a lot more possibilities for application developers in mobile networks. When a service or, for example, a service-specific feedback system is very close to the users, control of service quality can be made efficient. Also, transmission resources for the end users' wireless links, that typically act as bottlenecks in terms of capacity, can be controlled better on application requirement basis. One example could be over the-top video content providers with CDNs. Instead of using CDN edge servers physically located in a remote cloud system, edge servers could be deployed in a MEC system with a cache containing the most used content in the area covered by base stations driven by the MEC system.

- IoT Integration

The testbed provides also access points to Machine Type of Communication (MTC) systems and support the testing of different IoT scenarios and concepts. One of the key components in the integration of IoT systems to 5GTN is an IoT Gateway (IoT-GW) solution. It enables utilizing different radio technologies used in different IoT systems, unifying the very heterogeneous IoT device set. The gateway software provides a plug-and-play style of integration for the southbound information collection interfaces (toward IoT devices) as well for the northbound interfaces for distributing the information to other entities and cloud systems.

Both IPv4 and IPv6 routing are supported in the gateway together with various data transfer protocols such as HTTP and Constrained Application Protocol (CoAP). The gateway supports a number of different radio technologies including Bluetooth, IEEE 802.15.4 ZigBee, LTE and LTE-M, IEEE 802.11 WLAN, and also the 868 MHz radio used, for example, by Enocean sensors. The proof of concept implementation and scenario realization of IoT-GW have also been done with VTT's Tiny Node sensors. IoT-GW acts as a point-of-attachment between the 4G/5G access network and various sensor networks beyond the gateway. The gateway software enables virtualization of its different components. In addition, the gateway software can take advantage of MEC technologies with regards to data processing carried out at the gateway. The gateway filters unnecessary data at the edge of the wireless core network and sends only necessary and/or processed data to the network. MEC technologies enable also creating dedicated services where data does not go further than a respective MEC module in order to improve data privacy, e.g. in factory environments.

4.5.5.4 Required building blocks for security test cases

The test case should be integrated with WP3 security enabler Secure and Federated Slice Broker (SFSB) framework.

4.5.5.5 Facility Limitations

Oulu 5GTN is still lacking a fully functional softwarized 5G core. The testing is not yet supported for all 5G network functions. And also, some risks may appear due to the unavailability of the testbed as other projects may need to use it for higher priority tests.

4.5.5.6 Enhancements Required

Test case may require a fully functional sotwarized 5G core to measure the latency values. Moreover, the network slicing capabilities in 5GTN needs to be also enhanced.

4.5.5.7 Timeline and risks

Oulu 5GTN is still evolving its capabilities and enhancing the services with the development of other projects. One key risk is that the unavailability of required 5G services in 5GTN by the time of testing this particular test case with the given hardware and software compatibilities.

4.5.6 MouseWorld/5TONIC Testbed

5TONIC

The global 5G Telefonica Open Network Innovation Centre (5TONIC) was created in 2015 by Telefonica I+D and IMDEA Networks Institute as a leading European hub for knowledge sharing and industry collaboration in the area of 5G technologies. The laboratory provides an open research and innovation ecosystem for industry and academia that will promote joint project development, joint entrepreneurial ventures, discussion fora, and a site for events and conferences, all in an international environment of the highest impact. 5TONIC will also serve to evaluate and demonstrate the capabilities and interoperation of pre-commercial 5G equipment, services and applications. Currently, 5TONIC is a key infrastructure part of the Infrastructure projects in the 5G PPP phase 3, 5GVINNI and 5GEVE, and for advance verticals, such as 5GROWTH. The site already has a deployed network infrastructure for supporting pre-5G trials and a number of use-cases detailed in www.5tonic.org.

The 5TONIC site is located at IMDEA Networks premises in Leganés, but it has access to other locations for the support of different network functions and use-cases: UC3M campus both at Leganés and Madrid City Centre, Telefónica I+D lab at Almagro Central Office (includes Mouseworld Lab), Telefónica headquarters campus Distrito C, 5G IFEMA Lab at Feria de Madrid and connection with Telefónica Spain lab at Alcobendas.

A general schema of this infrastructure is schematized in Figure 47, that illustrates the architecture of an initial set-up (to be further extended according to the needs and interests of the Laboratory members).

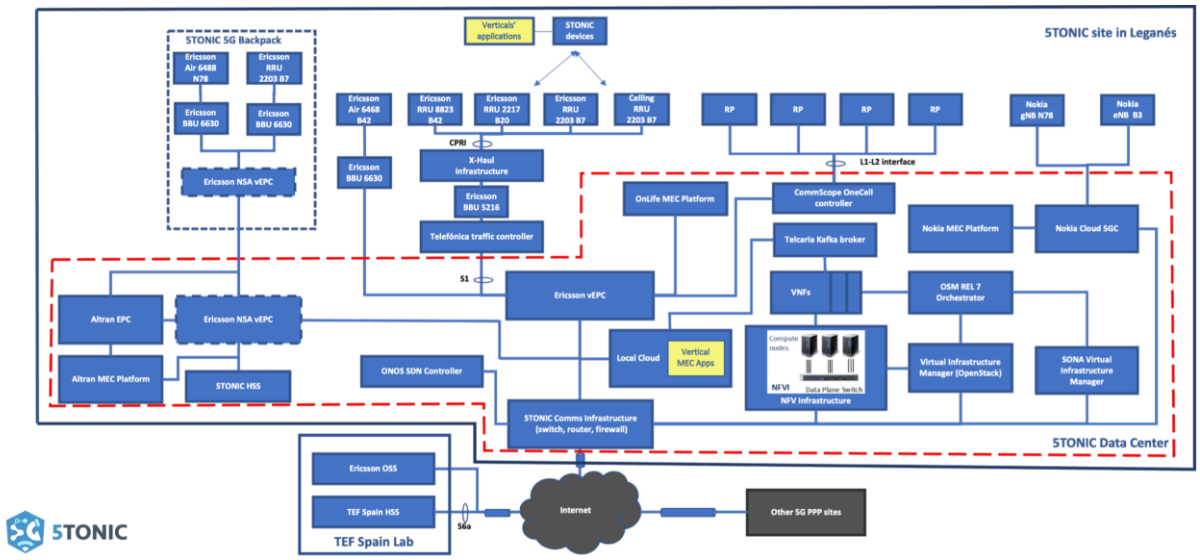

Figure 47: 5TONIC testbed main site

The 5TONIC laboratory, as a multi-purpose environment, counts with multiple racks, in a Data Center infrastructure, which may be flexibly interconnected according to any experimentation requirements, along with a common infrastructure to aid experimentation, trials and demonstrations with 5G products and services. In particular, secure external access may be provided via VPN gateways, allowing different solutions to support management, control and data operations from remote network locations, depending on specific requirements. To support the operation of all the components, the 5TONIC infrastructure provides a common infrastructure of 7 high-performance servers, which are used for different purposes: storage and backup of 5G experimental data, execution of NFV management software, deployment of SDN controllers, performing intensive computing simulations (e.g., using distributed computing or NS-3 simulator) and baseband processing of frequency signals, among others. The testbed is completed with a heterogeneous set of end-user equipment for experimentation purposes, including 20 laptops/workstations (these may also be used as mobile nodes) and a pool of smartphones; a set of VPN gateways, to support the remote access to the 5TONIC laboratory; and different wireless measurement equipment, e.g., supporting equipment to generate baseband signals for transmission in the 60 GHz band, as well as 2 signal analysers to inspect baseband and/or intermediate frequency 60 GHz signals.

Mouseworld

The emulation network traffic digital twin (internally called Mouseworld Lab) is part of the 5TONIC testbed, acting as an additional location from Telefonica, where is possible to make some dedicated experiments related with AI aspects, before or in parallel with the 5TONIC testbed in Leganés.

Mouseworld is the solution in charge of emulating a specific network configuration and generating the required traffic to be used subsequently by the machine learning algorithms. Mouseworld Lab is an emulation environment setup in Telefonica premises that allows deploying network scenarios in a controlled way. To this end, Mouseworld Lab provides a way to launch clients and servers and collect the traffic generated by them even if they interact with clients and servers outside the Mouseworld in the Internet.

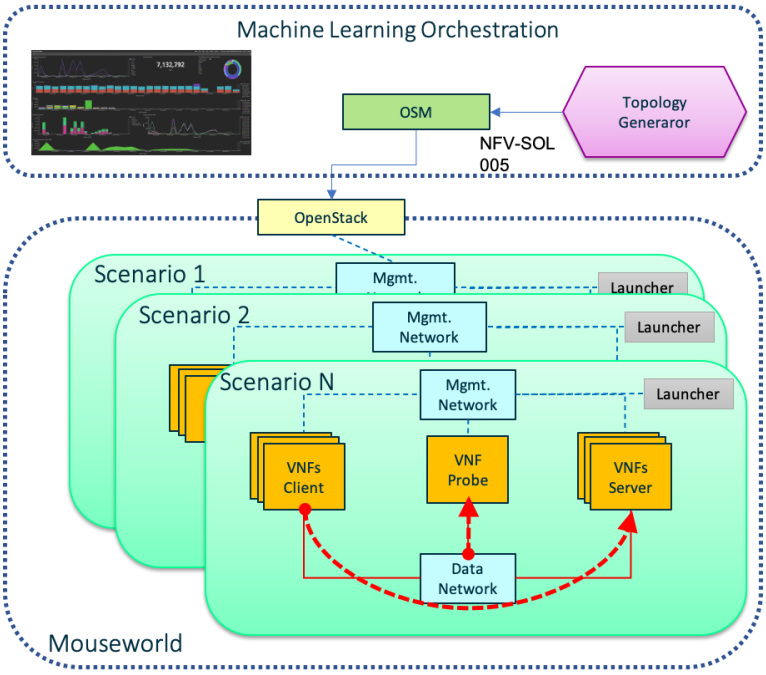

Figure 48: Mouseworld Lab (Telefonica) conceptual framework

The Mouseworld environment is composed of several modules interacting in a pipeline: Topology Generator, Launcher, Collector and Tagger (as different types of VNF Probes). The Topology generator is in charge of deploy different scenarios, using OSM, based on predefined templates created during the experimentation design. The Launcher uses as input a traffic network specification

for VNFs clients and servers and runs experiments that generate real network traffic that cross not only the Mouseworld network but also the Internet. Additionally, and with the aim of mimicking the statistical distribution of the Internet traffic patterns, the Launcher runs synthetic sessions that generate network traffic of a collection of complementary Internet protocols using Keysight Breaking Point, a commercial traffic generator, that allows to generate complex patterns of synthetic traffic. The injection of these packets is made in parallel with the traffic generated by the real experiments. The Collector module capture all the packets generated by a concrete experiment. Optionally it can group them in flows based on the five-tuple of source and destination ip-address/port number and transport protocol with the Tagger.

4.5.6.1 Test Cases

Test Case 3: Network attacks over encrypted traffic in SBA.

Test Case 4: E2E Encryption TEE secured SECaaS.

4.5.6.2 Capabilities

5TONIC

- Transport Network

The 5TONIC laboratory includes a metro-core network, which can be connected to the components described before in several ways. The metro-core network setup is composed by IP/MPLS and optical devices. The experimental setup is built with emulated nodes, which run in an Ubuntu server Linux distribution. Each emulated node implements a GMPLS stack (including RSVP, OSPFv2 and PCEP) and a Flexible Node emulator.

- 5G RAN and Core

On the 5G air interface and other radio aspects, 5TONIC infrastructure includes different scenarios provided by commercial, opensource or legacy research purpose solutions to support advanced experimentation with Software Defined Radio (SDR) systems. LTE and 5G NR-capable radio are provided by Ericsson, several scalable SDR platforms, along with a set of 60 GHz down/up-converters, supporting the generation and reception of arbitrary signals in the frequency bands under consideration and several commercial and opensource solutions currently under evaluation (LimeNetSDR and OpenAirInterface). In the case of the core architecture, Ericsson 5G-EPC and EPC-in-a-box deployment are used, and additional ones are under consideration.

- MANO and NFVI

5TONIC use as a MANO solution the ETSI OSM (Open Source MANO). This solution is aligned with the architecture and interfaces proposed by the ETSI NFV team, providing several services and a good performance. It runs in a virtual machine using a server computer with 16 cores, 128 GB RAM, 2 TB NLSAS hard drive and a network card with 4 GbE ports and DPDK support. Several VIM instances based on OpenStack are supported. 5TONIC is providing this NFV infrastructure to several projects in 5GPPP. Due to the necessity to manage and orchestrate network functions in different sites, this MANO can manage other NFV infrastructures controlled by the local VIM available at each site. The connectivity between sites require a VPN connection, a service offered by the 5TONIC too depending on the agreements with the other sites.

- Edge/MEC

Multiples Edge providers are evaluated in 5TONIC for Edge/MEC use cases in several 5GPPP projects. Some relevant solutions are Intel/Saguna, Intel or OpenNESS.

- Security

This setup allows the deployment and/or testing of different NFV/SDN domains, multi-layer control & orchestration, multi-tenancy NFV/SDN and multi-vendor NFV/SDN. Secure external access, both for control and for distributed inter-site connection is also provided via VPN gateways. Access and communications are protected with a commercial Fortinet Firewall.

Mouseworld

- MANO and NFVI

Mouseworld use ETSI OSM and NFV SOL-005 API for the NFV/SDN architecture. It has the capability to create virtual scenarios instances (slices), isolate the traffic between scenarios in the experiments, generate network traffic on demand and captures (using VNF probes).

- Machine Learning

The main property of Mouseworld Lab is the capacity to create/destroy different simultaneous scenarios, to launch different test to generate traffic to be used for experimentation in a controlled environment. This functionality allows two different activities. First, data set generation in order to create machine learning models (some postprocessing could be done optionally, such as grouping packets in flows, a label is attached to each flow representing the type of traffic that the flow contains). Second, the repeatability capacity: Same environment conditions allow evaluating different Machine Learning tools response and different versions, based on the similar statistical patterns.

- Security

Mouseworld infrastructure access for experiments execution, data gathering, and test are done using VPNs gateways and controlled by firewall. The use of IPSec-based tunnels is supported. In terms of capacity to deliver security traffic, Mouseworld allows generating malicious traffic, and different types of attacks (DDoS, vulnerability scans, etc.) based on Keysight Breaking Point security commercial traffic generator.

4.5.6.3 Required building blocks for security test cases

Several enablers are envisioned in this facility. The use of different WP3/WP4 enablers, such as VNFs and probes, need to be integrated into Mouseworld and 5TONIC, including virtualization format, interfaces, etc. Also, in order to demonstrate the viability of the test case specific attack and traffic patterns will be created and machine learning models trained. In addition, some enablers need to be adapted to run in the environment such as Proof of transit or IPSec agents for I2NSF. Finally, developments in INSPIRE-5Gplus Security Orchestrator, Policy Engine and Trust Manager need to be integrated with 5TONIC/Mouseworld orchestrators and managers to add the security capacity expected.

4.5.6.4 Facility Limitations

Due to its collaborative nature, 5TONIC common infrastructure and services (e.g., connectivity), can be used in the project. However, there are network elements that are the property of companies that are not partners of the projects (e.g. commercial NR and 5G Core from Ericsson). The use of these platforms by 5TONIC members and collaborators will require an agreement in a case by case basis. In case of lack of agreement, or 5G Stand Alone components availability, alternative plans will be put in place, such as the use of open source solutions and/or traffic simulation tools, already in study.

4.5.6.5 Enhancements Required

Planned enhancements include:

- Test case requirement analysis to study needs not covered currently:
  - Connectivity with other facilities
  - Integration capacity with orchestration and management plane and interfaces
  - Technical availability such as Stand Alone 5G Core, user terminals

4.5.6.6 Timeline and risks

5TONIC/Mouseworld is a shared infrastructure. 5TONIC Board, a members committee, should approve the experiments, and other 5GPPP projects need to be informed (5GVINNI, 5GEVE, etc.). Nonetheless, INSPIRE-5Gplus is part of the 5G PPP program, and should avoid any conflict.

4.5.7 EPC-in-a-Box Testbed

4.5.7.1 Architecture and Components of Facility

EPC-in-a-Box platform represents 4G LTE, and forthcoming 5G, network core commercialised by Montimage and Cumucore. It is a ready-to-use appliance allowing the creation of a full end-to-end 4G/5G network in 5 minutes. It can be used not only for experimentally testing but also to create a small-scale mobile network in order to provide mobile connection in white or gray zones.

The overall architecture of EPC-in-a-Box testbed platform is depicted in Figure 49. It basically consists of 3 main building blocks: Radio Access Network (RAN), Evolved Packet Core (EPC) and Montimage Monitoring Tool (MMT). Other IP Multimedia Subsystems (IMS) can be easily introduced in the Packet Data Network (PDN), such as VoLTE.

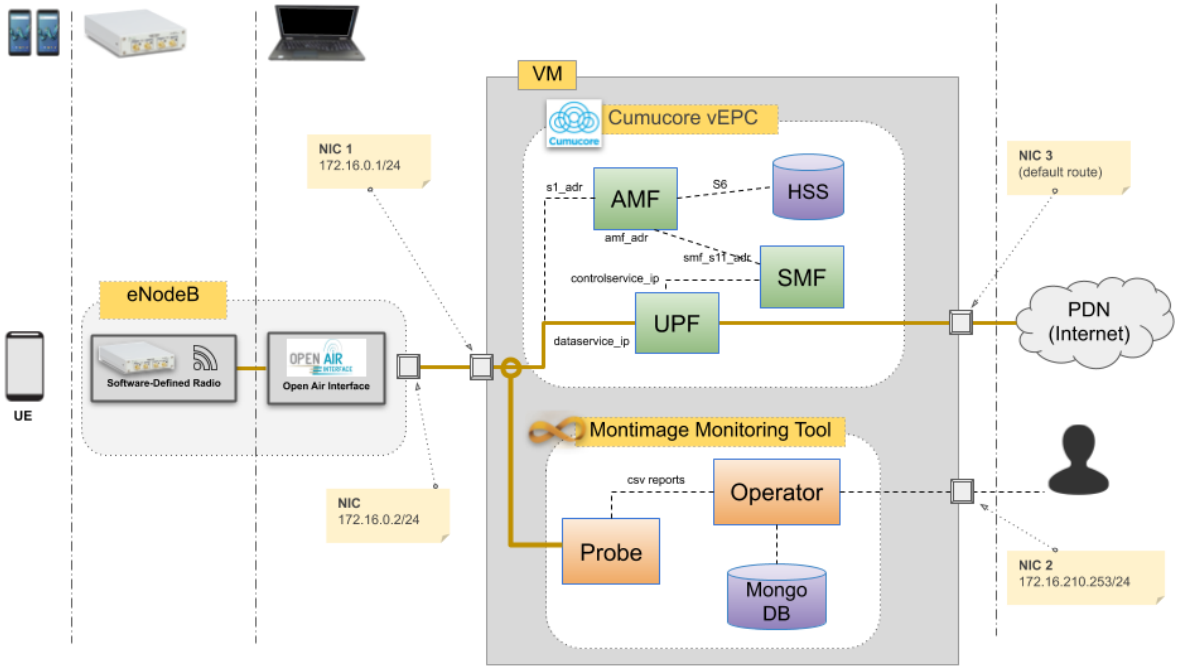

Figure 49: Architecture of EPC-in-a-Box Components

Once deployed, the testbed platform creates a 4G/5G network allowing commercial of the shelf (COTS) User Equipment (UEs) to connect. After being successfully attached, the UEs have access to the IP services in PDN or from the internet such as browsers, Web applications, VoIP video calls, etc. All the traffic between the RAN and the EPC is captured and analysed in real-time by MMT to ensure

that the defined security properties and SLAs are respected. MMT supports automated decision and reaction in the case an anomaly is detected.

4.5.7.2 Test Cases

- TC2: Definition and assessment of Security and Service Level Agreements and automated remediation
- TC3: Network attack detection over encrypted traffic in SBA
- TC7: Intelligent and Secure Management of Shared Resources to Prevent (D)DoS

4.5.7.3 Capabilities

- Opensource hardware and software

The RAN is constructed by using open-source Software-defined Radio. Currently we use 2 front ends: Ettus USRP B210 connecting via USB 3.0 and Ettus USRP X310 connecting via 10Gbps Ethernet; and two eNodeB softwares: OpenAireInterface (3GPP LTE Rel-10/12 PHY layer / 3GPP NR Rel-15 layer) and srsLTE (3GPP LTE Rel-10).

The EPC is initially installed using Cumucore's vEPC with whom Montimage has established a partnership. Many other EPC opensource solutions have also been installed and tested in the testbed, such as, openair-cn (3GPP Rel-10), nextEPC (3GPP Rel-13), free5Gc (3GPP Rel-15), and open5Gs (3GPP Rel-14).

- Portable, ready-to-use, zero-touch deployment and management for both experiementing and small-scale deployment of end-to-end 4G/5G networks

The testbed is available as a software package or appliance allowing to quickly deploy a mobile network. Figure 50 represents our plug-and-play appliance that creates a 4G LTE network. Its hardware consists of USRP B210 SDR and a Dell laptop. Once it is turned on, it creates a preconfigured LTE network that COTS UEs can connect to.

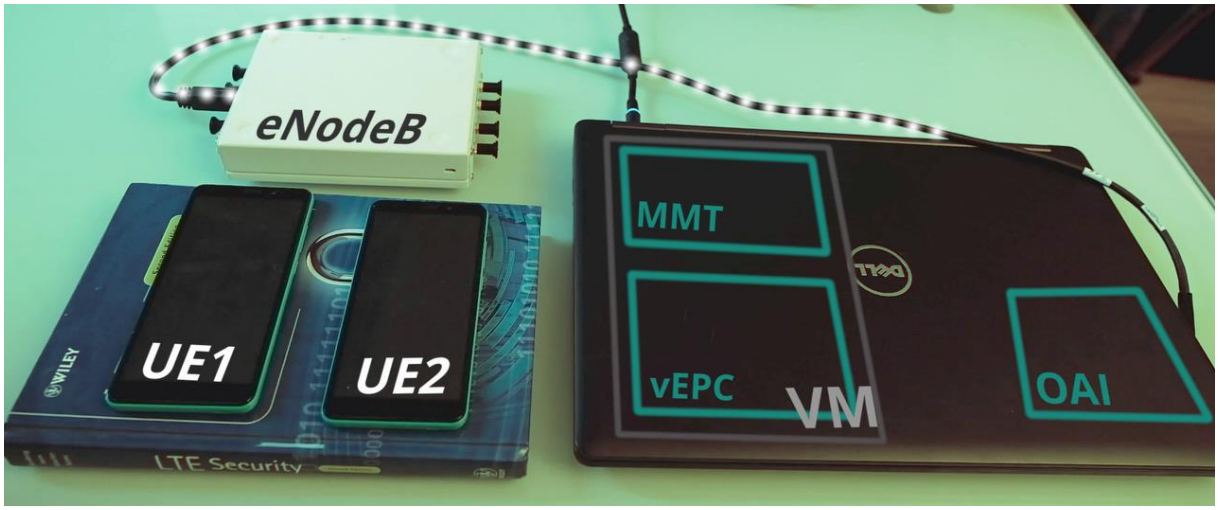

Figure 50: Rapid deployment of EPC-in-a-Box

- Integrated-security analysis and network visualisation in real time

The MMT is a network traffic monitoring and security analysis framework. It is located between the RAN and the EPC to monitor network traffic of both the data and control planes. It uses a combination of Deep Packet Inspection (DPI), statistics and Machine Learning techniques to decode S1AP traffic between RAN and EPC. Consequently, it is able to collect network statistics, such as, QoS Class Identifier, statistics per UE, dynamically updated the topology; and, information concerning the

configuration of eNodeBs, EPC's components, and UEs. It also integrates a security analysis engine using rule-based and Machine Learning to detect abnormal behaviour of the network. It allows easily experimenting attack scenarios to demonstrate the effectiveness of the security mechanisms. MMT also supports customised dashboards for defining and viewing new collected statistics and notifications.

- On-the-fly programmability of data plane

This capability will be developed during Inspire-5Gplus project and consists of introducing a programmable router supporting Programming Protocol-Independent Packet Processors (P4) between the RAN and the Core network. The router allows early detecting and preventing security issues, such as, (D)DoS attacks. It will contain also a lightweight mitigation mechanism, for example, acting as a firewall to block malicious traffic sources. The most important role of the router is to allow users to reroute data plane traffic on-the-fly, without restarting the router. This capability can be used to enable Mobile Edge Computing (MEC) to reroute traffic used by MEC services without passing through EPC core network, thus increasing the performance and reducing the latency.

4.5.7.4 Required building blocks for security test cases

WP2/WP3/WP4 enablers that can be used:

- Monitoring (necessary)
- Security optimisation techniques
- Security orchestrator
- Self_protection (necessary)
- SSLAs (TC2)
- Encrypted traffic analysis (TC3)
- DDoS prevention (TC7)

4.5.7.5 Facility Limitations

Radio emissions need to be limited to a few meters to avoid interferences with existing mobile networks.

4.5.7.6 Enhancements Required

The following enhancements are being planned to be developed during Inspire-5Gplus project:

- Support 5G Non-StandAlone/StandAlone configurations

EPC-in-a-Box testbed is currently ready for 4G LTE small-scale network. It is being updated to support 5G Non-Stand-alone configuration, and 5G Stand-alone as soon as possible. This should be available by Month 14 (January 2021).

- Support on-the-fly programmability of data plane using P4

At M24 (November 2021), we plan to have a programmable router using P4 between the RAN and the EPC in order to reconfigure the data plane on-the-fly.

- Enhancement of MMT to analyse encrypted traffic by M30 (May 2022). Several Machine Learning algorithms are being explored.

4.5.7.7 Timeline and risks

- Timeline

	Month	Description
Phase 1	M14	Support 5G Non-Stand-Alone/Stand-Alone configurations
Phase 2	M24	Support on-the-fly programmability of data plane using P4
Phase 3	M30	Enhancement MMT to analyse encrypted traffic

Table 28: EPC-in-a-Box timeline

- Risks

EPC-in-a-Box testbed deploys open-source or commercial RAN and EPC solutions, so the main risk is the dependency of the development on the roadmap of these solutions: the 5G SA configuration could be available later than the expected M14. However, the phases 2 and 3 can be performed independently with respect to phase 1. Thus, we can start phase 2 before M14 and meanwhile wait for the complete availability of 5G SA configuration.

4.5.8 CLS Testbed

4.5.8.1 Architecture and Components of the Facility

The CLS is hosted on cloud infrastructure of CyberLens B.V in the Netherlands. The infrastructure was developed in the context of the H2020 project 5G-CARMEN. CLS is involved in the 5G-CARMEN due to its cybersecurity expertise in the domain of 5G. In 5G-CARMEN, CLS is developing several security mechanisms to improve the security posture of the CCAM platform and edge components in the 5G network.

The infrastructure is focused on the assessment of security mechanisms, as well as the impact to overall security posture of a 5G network. As a result, the infrastructure can be used to model several different 5G network topologies that can be stress-tested through virtualized attacks. The resulting analysis of the attack and its patterns are then used to develop security mechanisms or ML algorithms. These outputs are then applied to the modelled network and evaluated based on the performance and impact.

4.5.8.2 Test Cases

Test Case 8: Security posture assessment and threat visualization of 5G networks

4.5.8.3 Capabilities

- Network traffic generation
- Generation of attack patterns
- Modelling of 5G network behaviour under stress
- Monitoring of simulated components
- Stress testing of components
- Modelling of malicious actors' behaviour

4.5.8.4 Required building blocks for security test cases

Test Case 8 will use the DiscØvery security analysis enabler which will be extended in WP3 and WP4.

4.5.8.5 Facility Limitations

The facilities are designed for modelling the behaviour of 5G systems in the context of security analysis. As result, they are not suitable for modelling process or performance related functions and operations of 5G networks.

4.5.8.6 Enhancements Required

The facilities will be extended with the ability to simulate additional 5G network components and malicious attacks. Specifically, the following functions will be developed:

- Modelling of malware propagation on 5G components
- Modelling of cross-border MEC communication
- Modelling of denial of service attacks against edge components
- Modelling of security mitigation mechanisms, such as intrusion detection

4.5.8.7 Timeline and risks

CLS has developed the facility and currently uses it to test and develop security mechanisms for the H2020 project 5G-CARMEN. After the completion of the 5G-CARMEN, CLS will continue improving their facility and related infrastructure.

One risk, since the facility is used for another H2020 project, the facility can be temporarily unavailable during demonstrations, and project reviews. The risk can be mitigated with proper planning to avoid conflict between the 5G-CARMEN and INSPIRE-5Gplus project.

5 Conclusions

In this deliverable were presented the set of test cases selected for validation on the INSPIRE-5Gplus project. This set of test cases where selected by performing an exhaustive requirements elicitation of 5G security use cases defined in WP2, stemming from the new and enhanced 5G security and trust/liability assets developed in WP3 and WP4.

For that purpose, in Section 2 are described the set of KPIs that will be taken in consideration for the validation of the different test cases. Moreover, an initial description of the INSPIRE-5Gplus Framework High-Level Architecture, being developed in WP2, is also presented.

In Section 3, the initial description of the selected test cases is presented by emphasizing on the list of enablers from WP3 and WP4 required for the validation, the relationship with the HLA, the required KPIs for validation, and the timeline and risks according to the timeline of the INSPIRE-5Gplus project and the facilities to be used.

In Section 4, the appropriate testing environment for the integration and experimentation of the 5G security test cases is discussed, and the envisioned testing infrastructure related to the test cases is presented by detailing the available capabilities and possible enhancements required for the successful testing.