INSPIRE-5Gplus

White Paper

Intelligent Security Architecture for 5G and Beyond Networks

November 2020

Table of Contents

White Paper: Intelligent Security Architecture for 5G and Beyond

List of Contributors

Editor in Chief

Chafika Benzaid, Aalto University, Finland

Section Contributors

Pol Alemany, Centre Tecnologic de Telecomunicacions de Catalunya, Spain

Dhouha Ayed, Thales SIX GTS France SAS, France

Geoffroy Chollon, Thales SIX GTS France SAS, France

Maria Christopoulou, National Centre for Scientific Research Demokritos, Greece

Gürkan Gür, Zurich University of Applied Sciences, Switzerland

Vincent Lefebvre, TAGES, France

Edgardo Montes de Oca, MONTIMAGE EURL, France

Raul Muñoz, Centre Tecnologic de Telecomunicacions de Catalunya, Spain

Jordi Ortiz, University of Murcia, Spain

Antonio Pastor, Telefonica I+D, Spain

Ramon Sanchez-Iborra, University of Murcia, Spain

Tarik Taleb, Aalto University, Finland

Ricard Vilalta, Centre Tecnologic de Telecomunicacions de Catalunya, Spain

George Xilouris, National Centre for Scientific Research Demokritos, Greece

Please cite:

C. Benzaid, P. Alemany, D. Ayed, G. Chollon, M. Christopoulou, G. Gür, V. Lefebvre, E. Montes de Oca, R. Muñoz, J. Ortiz, A. Pastor, R. Sanchez-Iborra, T. Taleb, R. Vilalta, G. Xilouris. **White Paper: Intelligent Security Architecture for 5G and Beyond Networks**. INSPIRE-5Gplus, Nov. 2020.

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.

Executive Summary

5G's capabilities and flexibility hold the promise of further facilitating the society's digitalization by enabling new services (e.g. remote surgery, advanced industrial applications) and communication modes (e.g. gestures, facial expressions and haptics). Current wireless communication systems do not meet the performance requirements of these new services, such as bandwidth, latency and reliability. Furthermore, the current COVID-19 crisis has fundamentally changed the way the world communicates and operates, accelerating the shift towards a more digital world. Such shift and the new requirements make the need of reliable and high-quality digital services promised by 5G more crucial than ever.

To fulfil 5G promises, a shift towards full automation of network and service management and operation is a necessity. However, a major challenge facing full automation is the protection of the network and system assets – services, data and network infrastructure – against potential cybersecurity risks introduced by the unprecedented evolution of the 5G threat landscape.

INSPIRE-5Gplus, a 5G-PPP phase 3 project, aims to address these cybersecurity risks by introducing innovative concepts for security management of 5G networks and beyond at the level of platforms and vertical applications and services. To meet this goal, INSPIRE-5Gplus will devise and implement a fully automated end-to-end smart network and service security management framework that empowers not only protection but also trustworthiness and liability in managing 5G network infrastructures across multi-domains. INSPIRE-5Gplus will allow the advancement of the security vision for 5G and beyond through the adoption of a set of emerging trends and technologies; namely, Zero-touch network and Service Management (ZSM), Software-Defined Security (D-SEC) models, Artificial Intelligence/Machine Learning (AI/ML) techniques, Distributed Ledger Technologies (DLT), and Trusted Execution Environments (TEE). INSPIRE-5Gplus will ensure that the provided security is compliant with the expected Security Service Level Agreement (SSLA) and regulatory requirements.

This White Paper introduces the overall INSPIRE-5Gplus framework's High-Level Architecture, its main functional blocks and their role in enabling intelligent closed-loop security operations. To illustrate how the INSPIRE-5Gplus framework can be applied as a zero-touch security management solution for 5G systems, the White Paper presents a representative set of advanced security use cases. The presented use cases cover different advanced security problems, including: (i) trustworthy composition of network slices using Blockchains (DLT) and secure deployment of E2E network slices in compliance with agreed SSLAs for automotive verticals; (ii) detection of network attacks over encrypted traffic in Service-Based Architectures; (iii) enforcement of E2E encryption policies while leveraging TEE to enable trustworthy execution of encryption-decryption operations; (iv) reactive and proactive protection of E2E network slices using, respectively, anomaly detection and Moving Target Defense mechanisms.

The INSPIRE-5Gplus project is currently evolving the architecture, defining the specific set of services to be provided by each functional block and devising the corresponding enablers. As the project's work progresses, we will release new White Papers to share our achievements with the community.

1 Introduction

The current COVID-19 pandemic has corroborated the key role of communication systems and connected services in empowering resilient societies. Essentially, the COVID-19 crisis has fundamentally changed the way the world communicates and operates, accelerating the digital transformation on an unprecedented scale. In fact, the restrictive measures enforced on people's movement and socializing have led to an upsurge in the use of digital services (e.g. video conferencing and collaboration tools) to enable remote working, online learning, virtual healthcare and even online socializing. 5G, with its capabilities and flexibility, is expected to further facilitate the society's digitalization. 5G holds the promise of enabling agile and dynamic integration of high quality and reliable services, such as real-time remote surgery, and supporting new communication modes, such as gestures, facial expressions, and haptics.

To fulfil 5G's promises, a shift towards full automation of network and service management and operation is a necessity. However, a major challenge facing full automation is the protection of the network and system assets – services, data and network infrastructure – against potential cybersecurity risks introduced by the unprecedented evolution of the 5G threat landscape. The main risk of full automation is the ability to replicate a small isolated error or attack broadly and rapidly, endangering the entire critical ecosystem.

The INSPIRE-5Gplus[1] project aims to address these cybersecurity risks by introducing innovative concepts for improving the security management of 5G networks and beyond at the level of platforms and vertical applications and services. To meet this goal, INSPIRE-5Gplus will devise and implement a **fully automated end-to-end smart network and service security management framework** that empowers not only **protection** but also **trustworthiness and liability** in managing 5G network infrastructures across multi-domains. INSPIRE-5Gplus will allow the advancement of the security vision for 5G and beyond through the adoption of a set of emerging trends and technologies, namely: **Zero-touch network and Service Management (ZSM[2])**, **Software-Defined Security (SD-SEC) models**, **Artificial Intelligence/Machine Learning (AI/ML) techniques**, **Distributed Ledger Technologies (DLT)**, and **Trusted Execution Environments (TEE)**. INSPIRE-5Gplus will ensure that the provided security is **compliant with** the expected Security Service Level Agreement (SSLA) and regulatory requirements.

This White Paper, the first in a series to be released in the course of the INSPIRE-5Gplus project, presents the smart, trustworthy and liable 5G security framework being designed and developed. It is organized as follows. In Section 2, the overall INSPIRE-5Gplus framework architecture is presented, highlighting the main functional blocks and their role. Section 3 describes a set of advanced security use cases, illustrating how the INSPIRE-5Gplus

[1] https://www.inspire-5gplus.eu

[2] https://www.etsi.org/technologies/zero-touch-network-service-management

framework can be applied as a security management solution for the identified security problems. Section 4 concludes the White Paper and provides an outlook for the future.

2 INSPIRE-5Gplus Framework High-Level Architecture

2.1 Architecture Overview

INSPIRE-5Gplus framework is designed to support fully automated End-to-End (E2E) network and service security management in multi-domain 5G environments. The framework empowers not only protection but also trustworthiness and liability in managing virtualized 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), and mobile edge computing (MEC).

The high-level architecture (HLA) of the INSPIRE-5Gplus framework, 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. E2E network slice) that span multiple domains. The E2E SMD coordinates between domains using security 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 intelligence 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. Although it is developed with a focus on single operator environment needs, the inter-domain fabric provides an inherent capability for security management among disparate networks as shown in Figure 1. In fact, the security-aware services available from the operator are **made accessible to third parties**, such as other operators or OTT services, via the inter-domain integration fabric exposed services. In the same way, this same operator may reach other operators' inter-domain fabric to accomplish an E2E service request originated locally.

In what follows, we provide a concise description of the key functional modules constituting the INSPIRE-5Gplus framework HLA at both domain and E2E levels.

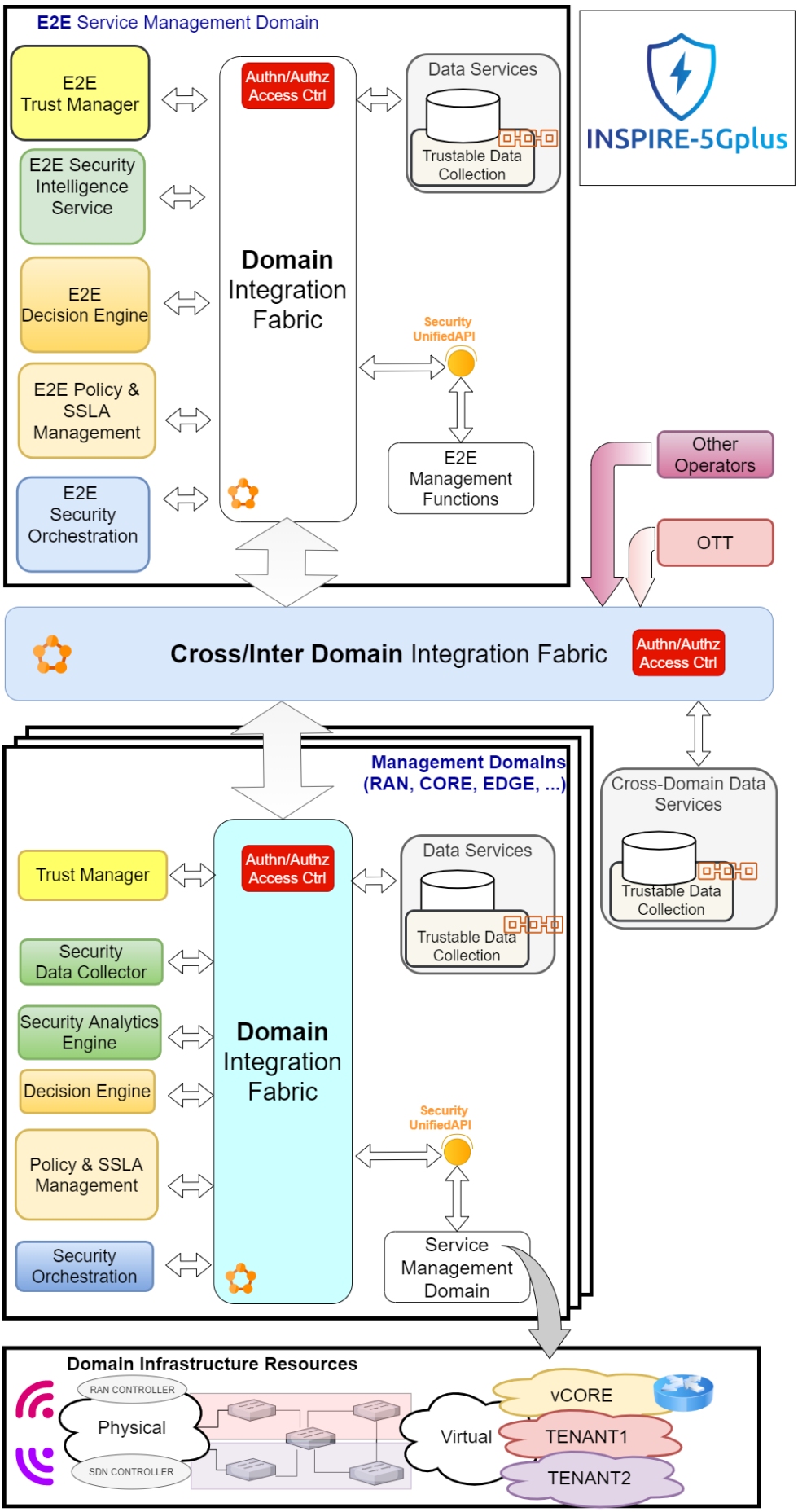

Figure 1 - The INSPIRE-5Gplus Framework HLA.

2.2 Terminology

– **Security Asset**

A security asset is any component that supports security related activities (protection, detection and/or mitigation). It can represent a hardware, a software or a virtualized function.

– **Security Enabler**

INSPIRE-5Gplus Security Enablers are the major building blocks to achieve a fully automated End-to-End security management in multi-domain 5G environments. They are all the security features, products or services developed within the project. These enablers can leverage on one or more security assets, their configuration and logic of operation to empower the Security as a Service paradigm.

– **Security Management & Orchestration Functions**

The security management and orchestration functions are the set of functional modules (e.g. security decision engine, security orchestrator, trust manager) that operate in an intelligent closed-loop way to enable SD-SEC orchestration and management that enforces and controls security policies of network resources and services in real-time. These functions leverage several security enablers to implement their services.

2.3 Domain-Level Functional Blocks

2.3.1 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, external data sets).

2.3.2 Security Analytics Engine

The main function of the Security Analytics Engine (SAE) is to derive insights and predictions on a domain's security conditions based on data collected in that specific domain or even from other domains. In the context of INSPIRE-5Gplus, the SAE provides Anomaly Detection and 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 do not conform to the expected normal behaviour. It 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 determines the origin of the anomaly and the location in the network where a corrective action should be applied to prevent the problem from occurring. As a result, the RCA service may provide recommended actions to correct or prevent the security incidents in a 5G environment.

2.3.3 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 which can be applied for securing a running targeted service. This central component acts as an arbitrator between security assets and the rest of the platform that manages domains.

The DE delegates the creation of actual mitigation actions to **Cognitive Long-Term** and **Reactive Short-Term** assets. These 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 historical data from several sources to internally deduce correlations, potential forecasts and propose elaborated mitigation plans to the DE.
- The Reactive Short-Term assets will rely on simple rules to provide quick and mundane reactions to specific events. These rules will be akin to what a human operator would do in the given a situation. Due to their simple and streamlined structure, the mitigations resulting from these assets can be rapidly computed and enacted.

The DE relies on multiple “third-party” assets running concurrently and waits for them to emit a mitigation proposal. These proposals can then be transmitted to the Decision Engine without following any given order and sometimes may even be conflicting. For example, a Reactive Short-Term asset may evaluate a device as legitimate and thus authorise its traffic. On the contrary, a Cognitive Long-Term asset may later identify that this same device as a potential DDoS source. In such situation, the DE has to arbitrate the conflicting reactions either by using a confidence level and/or by looking at a statistically built priority list. Finally, as a mitigation may take time to be applied by the underlying Security Orchestrator, the DE has to track selected reactions and may ignore newly received mitigation proposals to let the protected system stabilize.

2.3.4 Security Orchestration

The Security Orchestrator (SO) oversees the different security enablers to enforce the security requirements specified by the adopted security policies. The SO drives the security management by interacting, through the integration fabric, with different SDN controllers, NFV MANO and 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 with the evolving system model, that is derived from the structural information coming from the network administrators the monitors that inspect the deployment for any changes, 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 other, 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.

2.3.5 Policy and SSLA Management

The Policy and SSLA Management (PSM) component transforms the abstract Protection Level and Security Level requirements and constraints expressed by consumers and providers into specific parameters that indicate, to the Security Orchestrator, the security services to configure, deploy and manage. The PSM provides a framework defining the language and semantics to define Security Service Level Agreement (SSLAs) based on policies. These policies will be refined from a high abstraction level description to deployment-ready representations. These values will finally be enforced in real time in cooperation with other INSPIRE-5Gplus functions. The SSLAs provide the means to specify the security requirements or policies and the means for assessing or enforcing their fulfilment to obtain the desired security level.

2.3.6 Trust Management

The Trust Management (TM) contains various internal services for the trust related functions in the security framework. As a key building block, the Trust and Reputation Manager (TRM) service in the TM assigns trust and reputation values to monitored 5G entities and provides this information to security management entities and end users in 5G virtualized networks. In this respect, the Component Certification Service (CCS) works at the component level and provides a static evaluation of the different 5G network components by measuring trust 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 the slice, based on parameters, that can be used by the end-users or other system components.

For trust in how data flows traverse a network and how they are processed spatially, Ordered Proof of Transit (oPoT) service verifies the correct order of nodes on the network path followed by a flow. It provides trust in the guaranteed confinement of flows in a specific slice or slices, or for inter-domain trust. For the 5G networked services themselves, the Service Trust Manager (STM) service is designed for implementing smart contracts and

calculating 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 STM can be devised (each with different smart contracts), depending on the element for which the trust is being calculated.

The TM also provides a wrapper service that produces the modifications on the binaries (executable files) delivered by an obfuscation-based protected security routine embedded and added on the protected program. The output 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 exploits. A metadata file or data structure is enclosed in the protected VNF package and describes the various security functions applied with their parameters.

2.4 E2E-Level Functional Blocks

The E2E SMD is a special SMD that manages security of E2E services that span multiple domains. The E2E SMD coordinates between domains using security orchestration. Within the E2E SMD, the following functional modules are provided:

- **E2E Security Intelligence Engine**

  The E2E Security Intelligence Engine (E2E SIE) derives cross-domain insights and predictions based on data collected from different domains. It has a role similar to the SAE but at the cross-domain level. This function is necessary for analysing the data provided by the SDCs from different domains or stored in the Cross-Domain 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.

- **E2E Decision Engine**

  The E2E Decision Engine (E2E DE) manages the high-level security at the E2E level. This component consumes events from the E2E SIE or from the underlying domain-level DE to adapt and propagate the security decisions across multiple domains.

- **E2E Security Orchestration**

  The E2E Security Orchestrator (E2E SO) is responsible of orchestrating and managing the different security enablers from multiple domains to cover the security configuration requirements specified by the defined E2E security policy. The E2E SO 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.

- **E2E Policy and SSLA Management**

  The E2E policy and SSLA management (E2E PSM) block provides multi-level SSLA, HSPL, MSPL and final enabler configuration translations. Policy conflict avoidance is enforced

by this block to prevent contradicting policies or requirements of previously deployed security services.

– **E2E Trust Management**

  The E2E Trust Management (E2E TM) facilitates E2E trust services across multiple domains, relying on the domain-resident TMs. It can provide across-domain versions of trust functions by aggregating trust outputs of TMs in different domains and enriching them with inter-domain parameters. For this, it interacts with the E2E PSM and E2E SO to operate in compliance with E2E security requirements, policies and SSLAs.

2.5 Domain-Level and Cross-Domain Data Services

The Data Services allow the different functions to persist data that can be shared by functions in one or more domains. They need to manage the access to allow only authorized consumers. By introducing this service, the data persistence and data processing are separated, i.e. enabling stateless management functions and eliminating the need for per-function data persistence and per-function processing.

The Data Services should support different types of storage techniques (e.g. 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 normalised either by the SDC or by an adaptor so that the consumers of the data can use it. It 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 to assure ACID properties (Atomicity, Consistency, Isolation, Durability), particularly if multiple producers and consumers are involved.

The Data types are those collected by the SDC (see the examples list in Sec. 2.3.1). Standard formats should be used, e.g. PCAP for network traffic, JSON with schema for data interchange, STIX for sharing Cyber Threat Intelligence. The captured data can be either real-time data or historical data needed for security-related analysis (e.g. analysis of risk, liability and root cause, and detection of vulnerabilities and intrusions).

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

2.6 Integration Fabric

The integration fabric facilitates 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 registration service enables the registration/de-registration of security management services into/from the service registry (catalogue). For each registered security management service, the list of

supported capabilities is included as part of the registration. The discovery service allows the discovery of registered security management services and their capabilities. The invocation service allows the authorized service consumer to invoke a discovered security management service. The integration fabric allows the communication between the security management services via dedicated communication channels.

2.7 Unified Security API

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

2.8 Security Agent

The Security Agent (SA) is a security asset for monitoring and managing security at a local point. It is able to capture data needed by other security functions and/or perform actionable behaviour decided locally but managed by other security functions. The SAs communicate with the INSPIRE-5Gplus management plane in their security domain based on configurable security policies. An SA may provide security data to the analysis and management functions from the traffic plane, acting for instance as an active or passive probe.

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

3 HLA Instantiation Examples

This section describes a representative set of advanced security use cases (UC) defined in the INSPIRE-5Gplus project, illustrating how the proposed framework can be applied as a security management solution for dealing with the identified security problems.

3.1 UC 1: Secured Anticipated Cooperative Collision Avoidance

3.1.1 Problem Description & Aim

This UC is focused on looking into how to manage and control some security aspects affecting the virtual elements composing a deployed network slice for an automotive vertical. Using the experience gained during the development of the Anticipated Cooperative Collision Avoidance Test Case (TC) belonging to the EC 5GCroco project, this UC aims defining and addressing a set of situations in which the security of vehicular communications might be compromised.

Due to the fact that vehicular communications are a wide topic with different situations to study, in the current UC two specific scenarios are studied with the objective to show how the security around the management and orchestration of network slices and their virtual elements might be increased and implemented. The two scenarios investigate the following aspects:

1) The first scenario aims to study how Security Service Level Agreements (SSLAs) may be applied over Network Slices. While the use of SLAs is widely studied in order to ensure a defined network performance, by using SSLAs this use case aims to demonstrate how to re-configure a network slice during run-time. To do so, this first scenario will solve the situation in which an evil vehicle generates fake information and, based on different metrics defined in an SSLA, this will be detected and blocked by updating a set of firewalls within the deployed network slice.
2) The second scenario aims to add trustworthiness on the elements composing a network slice, i.e. network services and virtual network functions. To do so, a Blockchain network composed of Network Slice Managers and a certification service tool will be used. This scenario aims to add security before a service is deployed by allowing to only share resources that were validated and verified previously, and their results are known publicly. When a service provider wants to deploy a network slice for a specific service, if the descriptors (e.g. slice template) defining the network slice are not previously certified in the Blockchain, the service provider will not be able to use and offer them to the other network slicing domains.

3.1.2 Actors and Roles

The actors and roles involved in UC1 are:

– Network domains: The domains involved in this UC are the Edge, Transport and Core domains with data centers placed in the edge and in the core domains.

- Service Provider (SP): The owner of the entire vehicle communications service.
- A set of vehicles: Each vehicle will have its own ID and personal parameters in order to be identified.
- A malicious vehicle: This single vehicle will have the same characteristics as any vehicle, but its objective is to generate information describing fake situations such as an accident or traffic jam.
- Mobile Network Operator (MNO): The owner of the infrastructure in which an SP might deploy and offer their services through the use of a network slice and the virtual elements composing it.
- INSPIRE-5Gplus's HLA security modules: SAE, SO, PSM, E2E SIE, E2E SO, E2E PSM and Data Services
- Network Slice Manager: In charge of managing the deployment of the network slices and any related action affecting them.

3.1.3 Operational Flow of Actions

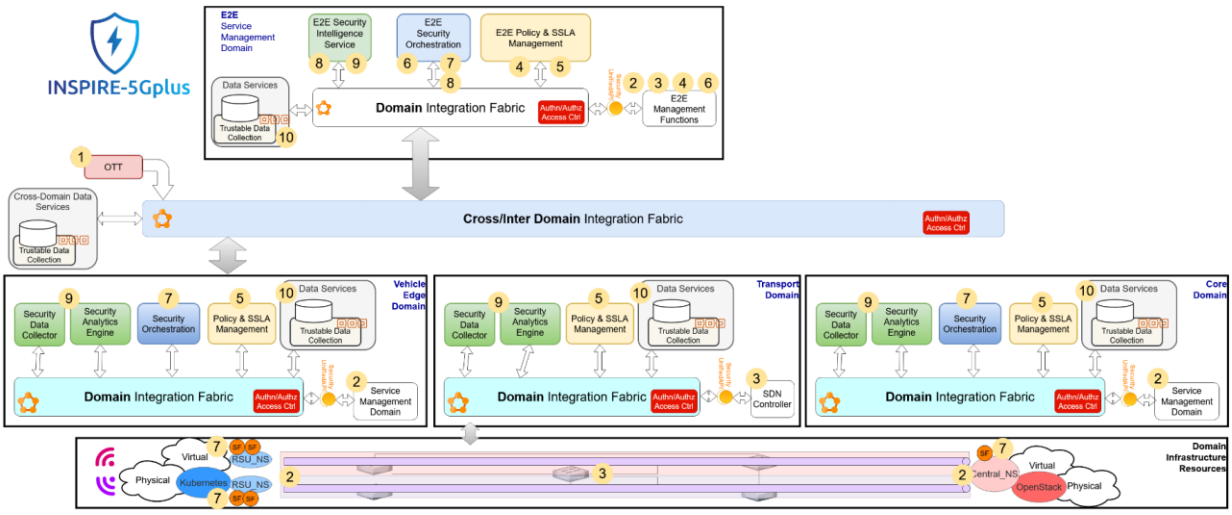

Figure 2 - UC1 operational actions flow within the HLA architecture.

Figure 2 presents the E2E Network Slice Deployment procedure for the UC involving the aforementioned HLA modules:

1) The vertical requests an E2E Network Slice with an associated SSLA to the E2E Network Slice Manager.
2) The E2E Network Slice Manager allocates each Network Service (NS) to the correct domain and requests its deployment to the specific Domain Slicer.
3) The E2E Network Slice Manager requests to the SDN Controller to configure the inter-domain paths between NSs.
4) The E2E Network Slice manager requests the associated SSLA to the E2E PSM.
5) The E2E PSM requests to each domain's PSM to configure and associate the SSLA to the deployed NSs.

6) The E2E Network Slice Manager requests to the E2E SO the Security Functions (SF) deployment next to the NSs composing the E2E Network Slice
7) The E2E SO forwards the request to each domain's SO the specific SF deployment
8) The E2E SO requests the E2E SIE to monitor the E2E Network Slice
9) The E2E SIE configures each domain's SAE to monitor the NS's security performance
10) Finally, when all the elements are deployed and configured, the data is saved. From this moment, if a vehicle generates any fake information, the domain SAE will detect it and inform the E2E SIE. This last element will pass the action request to solve the problem to the E2E SO, and this to the corresponding domain SO, so the last one may update the SF in order to solve the problematic situation.

The operational action flow for the second scenario is not presented in Figure 2, but the procedure follows the next steps: a) a certification service (provided by the Trust Management module) tests a set of descriptors (Network Slice and/or Services) and publishes the results to the other Blockchain nodes; b) a Domain Network Slice Manager aims to upload the same descriptors; c) all the other Domain Network Slice Managers (i.e. Blockchain peers) must validate and accept these descriptors; and, d) if validated, the descriptors are accepted and shared across all domains. From this moment, any domain may request the domains with those descriptors to deploy them and so avoid duplication of resources across domains while keeping trust among them.

3.2 UC 2: Network Attacks over Encrypted Traffic in SBA

3.2.1 Problem Description & Aim

5G networks will expand the use of encrypted communications. 5G Core follows a Service Based Architecture (SBA) using HTTP/2 as the protocol base to leverage all signalling traffic, instead of using the legacy DIAMETER protocol. Starting with Release 15, 3GPP specifies the use of TLSv1.2 as the base protocol implementation for RESTful APIs. On the contrary, the data plane between the RAN and the Core relies upon the use of GTP-U that is not usually encrypted. Mainly because at the application level the current tendency is the adoption of E2E encryption for internet applications and services based on the use of TLS, e.g. DoH (DNS over HTTPS) and QUIC (HTTPS over UDP). As a consequence, current cybersecurity network tools based on network monitoring will be ineffective in this environment, making it very difficult to detect some common attacks exploiting botnets, application layer attacks or DDoS. The detection is particularly challenging since these threats are also evolving to support TLS as a channel of communication.

To be able to detect these attacks, this use case proposes extending the security monitoring tools to be capable of analysing encrypted traffic. Basically, this means defining efficient mechanisms to collect network related data and introducing Machine Learning techniques to detect abnormal behaviour in the communications.

Furthermore, the use case brings trust to the traffic anomaly detection security function by leveraging TEE for enabling security-hardened execution and guaranteeing full confidentiality and integrity of its inference rules and detection results.

3.2.2 Actors and Roles

The actors and roles involved in UC2 are:

- 5G network administrator, such as the Network Operation Center / Security Operation Center (NOC/SOC) operatives: This actor is usually responsible for a specific administrative domain. But in this use case, several domains can be involved, e.g. Transport, 5G Core, NFV data centres, and it should be possible to enforce specific policies in the network, e.g. using the NFV MANO.
- Malicious party: Usually represented by the attacker or the botnet infrastructure.
- Security Agents: Probes integrated or adapted to the INSPIRE-5Gplus framework.
- INSPIRE-5Gplus's HLA security modules in the Management domain: SDC, SAE.

3.2.3 Operational Flow of Actions

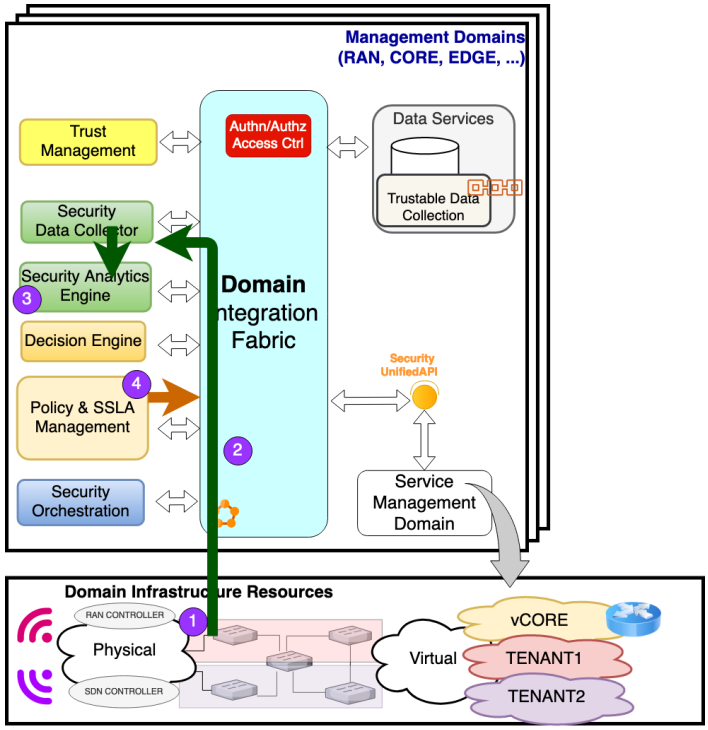

Figure 3 - UC2 operational actions flow within the HLA architecture.

The action flows of UC2 are shown in Figure 3 over the general architecture of the INSPIRE-5Gplus architecture for a specific management domain. UC2 includes the following sequence of actions:

1) Probes (Security Agents or enablers) deployed at different points in the network generate metrics.
2) The generated metrics are delivered to an SDC as a source of data and meta-data,

leveraging the domain integration fabric.

3) The SDC aggregates and transforms the metrics into a suitable format, fed to the inference engines in the SAE trained using AI/ML for identifying malicious behaviour patterns in the encrypted traffic. In this way, Service-Based Interface traffic can be classified (e.g. separating signalling from other types of traffic, such as attacks, machine-generated from user generated traffic).

4) Identified malicious flows and activity are reported to the administrator who will take appropriate actions to mitigate the attack, using the specified security policies. Mitigation actions will be done enforcing the policies on existing security agents or deploying new security agents (e.g. IPS, firewalls, active probes) or, alternatively, the affected functions (e.g. an infected container or virtual machine of the 5G core) can be cleaned and re-instantiated (with a certificated-by-vendor version) to remove the problem.

3.3 UC 3: Orchestration of Cryptomaterial for Connections

3.3.1 Problem Description & Aim

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. Also, confidentiality and protection in different 5G domains of the infrastructure, e.g. access, transport, or Core, is not always properly managed. Static keys or very long key and certificate refreshment periods open the opportunity to malicious data-access by attackers. In this context, the two requirements that need to be fulfilled are: endpoint authentication and data encryption. To provide these functions, 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.

As an extra secure communication layer, VNFs acting as proxies can be deployed dynamically to protect E2E communications. This is the case for IPSec and also for DTLS when protecting UDP communications, which is often used in IoT environments. The basis of both encryption schemes is the key derivation which in turn can be done in a centralized way or on the hosts. Following the former approach, IETF proposes I2NSF (based on IKE) and Thales proposes SD-SEC, both having important security similarities but different way of integration at network layer to provide more alternatives. While E2E communications may be encrypted, it is also true that memory introspection attacks are more likely to happen at MEC or end-point isolated locations. In fact, they can be carried out by a malicious operator with root access on the machine or via VM or Container-escape attacks in order to identify and get access to the secure link keys (such as AES). In this line, the proposal is to profit from TEE (e.g. SGX enclaves) to perform encryption-decryption operations transferring native code to the TEE, and in this way protecting the delegated VNF security from other VMs located on the same MEC node.

Therefore, the objective of this use case is to produce a Zero Touch solution based on the definition of policies and SSLAs that can be triggered automatically based on system state and data collection inputs. Specifically, it will define Zero Touch policies for encryption and related enforcement interfaces, to provide confidentiality between different domains in a 5G environment to reduce risks or as a mitigation response. Also, centralized policies governing the key management (e.g. cryptographic algorithms, key renewal) will improve the communications security.

3.3.2 Actors and Roles

The actors and roles identified for this UC include:

- System Administrator: is usually represented by the NOC or SOC, in charge of the management and monitoring of the network.
- The User Equipment (UE): end-point used by the end-users that needs to benefit from the protection level provided by the system.
- Security Intelligence Service: based on events collected from the network, will provide the Decision Engine with the information needed for reacting to security breaches.
- Long Term Cognitive Decision Engine: makes long-term decisions based on the information received from E2E Security Intelligence Service or the system's history of events.
- Network management domains: these domains depend on the deployment done by the operator and how administratively or technologically the network is organised. Administration domains might refer to regional or national management while the technical domains may correspond to the core, transport, RAN, data centre, or MEC.
- Security enablers: integrated or adapted to work within the Inspire-5GPlus framework. For this particular use case, one has: the virtual IPSec, proxyTLS, IETF NSF SDN application for key distribution, among others.

3.3.3 Operational Flow of Actions

The administrator/NOC/SOC, Security Intelligence Service or Cognitive Decision Engine decides whether there is a need for protecting traffic between two devices or between a device and the cloud. As a consequence, a policy (expressed using HSPL or as an SSLA) is specified that defines the E2E security requirement. Then, a translation and conflict detection process is needed. If there is no conflict, subsequent definitions are generated for each Management domain. At the very least, two virtual Domains, the transport network and the RAN will divert traffic to the domain's vIPSec enabler. This enabler will rely on a TEE (e.g. Intel SGX) where it will be initialized, and the E2E connectivity and configuration will be established from the centralized management entity (e.g. SDN Controller). In this way, the traffic will be protected E2E.

Figure 4 shows the action flows of UC3 over the general architecture of the INSPIRE-5Gplus

architecture. UC3 includes the following sequence of actions:

1) Three different entry points corresponding to a decision to protect the traffic E2E made by the NOC or SOC (1a), the E2E DE (1b) or as a reaction to an event generated by one of the management domains (1c) reacting to changes in the data plane and escalated to the E2E Domain that in turn may produce a new decision.

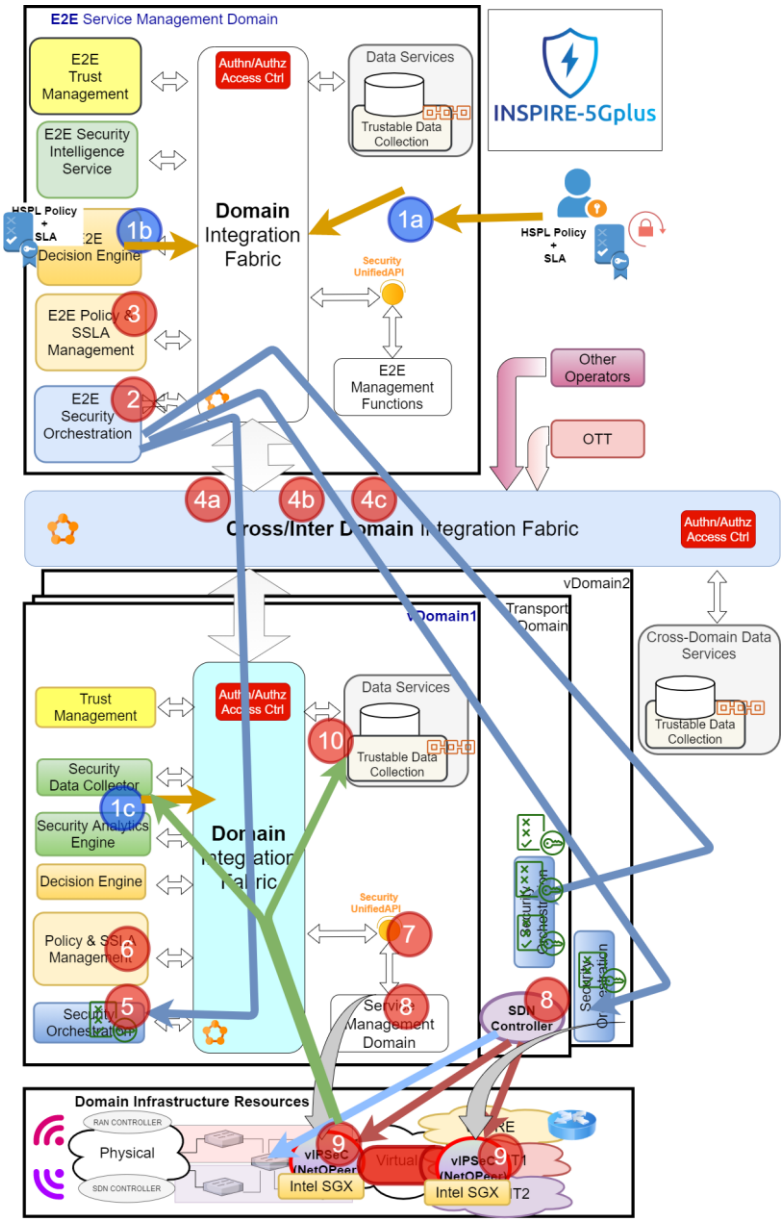

Figure 4 - UC3 operational actions flow within the HLA architecture.

2) The E2E SO receives the request specified using the High Level Abstraction Language independent from the deployment.

3) The E2E SO requests a refinement to the E2E PSM that will produce a lower level interpretation of the request incorporating specificities of the system.

4) The E2E SO analyses the refined request and enforces the final solution through the affected management domains. In this example 4a and 4c are intended for VNF and TEE management on the virtual domains, and 4b is intended for the management of the

connectivity through the backbone and the key distribution.

5) On each Management Domain, the SO in charge of that domain will receive a High Level abstraction request. This step will happen on each affected Management Domain.

6) The SO will request a refinement of the request similarly to what was done in the E2E domain but limited to the scope of the precise management domain. This step will happen on each affected Management Domain.

7) The SO will enforce the final decision via the Unified Security API to the MANO or to the SDN controller, following the current deployment example.

8) The crypto material is distributed and the tunnel is established. This crypto material can be updated periodically or on demand, to increase the security.

9) The traffic from the UE is protected E2E. The data protection operations are enclosed within the TEE enclave.

10) Usage data, events and service provisioning information are stored in the Trustable Data Collector which will later be used for Liability analysis or as input to other processes such as the E2E DE cognitive Long-Term Cognitive Decision Engine.

3.4 UC 4: End-to-End Slice Protection based on Moving Target Defense and Anomaly Detection

3.4.1 Problem Description & Aim

This UC aims at protecting network slices, one of the fundamental building blocks of 5G, that will allow the realization of advanced use cases in several Verticals not feasible with legacy mobile networks. However, such new capabilities enabled by 5G advancements come with various side effects, including the increased attack surface due to new flavours of technologies introduced, such as software-defined infrastructures, slicing with multi-tenancy, multi-actor service paradigms and complex/multi-tier architecture. Under certain circumstances, these could constitute potential sources of vulnerabilities, increasing the likelihood of security incidents.

This UC will investigate both proactive and reactive security mechanisms for E2E slice protection. 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 and their subsequent resolution by INSPIRE-5Gplus security enablers and related actors. 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. The infrastructure is part of the Athens Testbed hosted by NCSR "Demokritos", in the context of 5GENESIS. An important consideration of this UC will be to strike a balance between security effectiveness of MTD and the cost of reconfiguring the protected network.

The cooperation between the MTD mechanism and the Slice Manager is mainly based on network slice monitoring, especially of critical slices, that will trigger their reconfiguration

based on a defined threat and cost model. This chain will be supported by additional enablers, including an Anomaly Detection Framework, a Security Orchestrator and a Monitoring Framework, provided by INSPIRE-5Gplus. In addition, MTD will provide protection of the security functions themselves in a slice to increase their robustness against reconnaissance and attacks, while maintaining their configuration integrity. All these actions will form a unified and closed-loop scheme based on a data-driven approach for E2E network slice protection.

3.4.2 Actors and Roles

The actors of UC4 are the following:

- Mobile Network Operator (MNO): The owner of the infrastructure.
- Service Provider (SP): A Service Provider that deploys its services over the MNO infrastructure.
- Network Domains: They refer to the RAN, Core, Transport and Edge domains.
- Network Operations Center (NOC): The Operator's NOC Department is responsible for the monitoring and management of the network.
- Monitoring Framework: It provides an E2E overview of the network's status to the NOC.
- Security Agents: Probes deployed at different points in the network to collect incoming data from the infrastructure.
- Security Analytics Engine: It deploys the Anomaly Detection Service that processes incoming data and detects abnormal traffic flows.
- Decision Engine: It provides the mitigation actions (like slice re-configuration) based on incoming data and alerts.
- Security Orchestrator: It deploys, configures or activates security functions over the network slices.
- Slice Manager: It deploys network slices based on defined Network Slice Templates.

3.4.3 Operational Flow of Actions

Figure 5 depicts the operational flow of actions for UC4 in a specific management domain, using the annotated blue arrows. All interactions between the building blocks of the INSPIRE-5Gplus HLA take place through the Integration Fabric. The UC includes six steps of subsequent actions:

1) The Security Agents collect data from several points of the network and deliver them to the Security Data Collector.
2) The Security Data Collector ingests the collected data, transforming them to appropriate data formats for further processing and feeds them to the Security Analytics Engine.

3) The Anomaly Detection Service provided by the Security Analytics Engine performs all necessary data pre-processing and ML inference to detect abnormal traffic resulting from potential security incidents. In case of detected anomalies, the SAE provides trigger alerts to the administrator and other building blocks through the Integration Fabric.
4) The Decision Engine, which refers to the MTD mechanism for the specific UC, decides the mitigation actions based on the received data. It is important to note that the Decision Engine (i.e., the MTD mechanism) does not necessarily get triggered by an alert from the SAE, in order to proceed to network re-configurations. It can also act in a self-driven manner to improve defense standing (particularly to minimize attack surface and evade attacks) and to protect the 5G system proactively. However, these steps are numbered sequentially to provide a clear explanation of the action flow.
5) The Security Orchestrator proceeds with the deployment of the appropriate Security Functions over the network slices to enforce the mitigation policy.
6) The Slice Manager deploys the updated Network Slice Template, by communicating with the components of the Management and Orchestration Layer (MANO), namely the NFV Orchestrator (NFVO), the Virtual Infrastructure Manager (VIM), the Element Management System (EMS) and the WAN Infrastructure Management (WIM), in order to manage the functions in the network and perform CRUD operations on network slices.

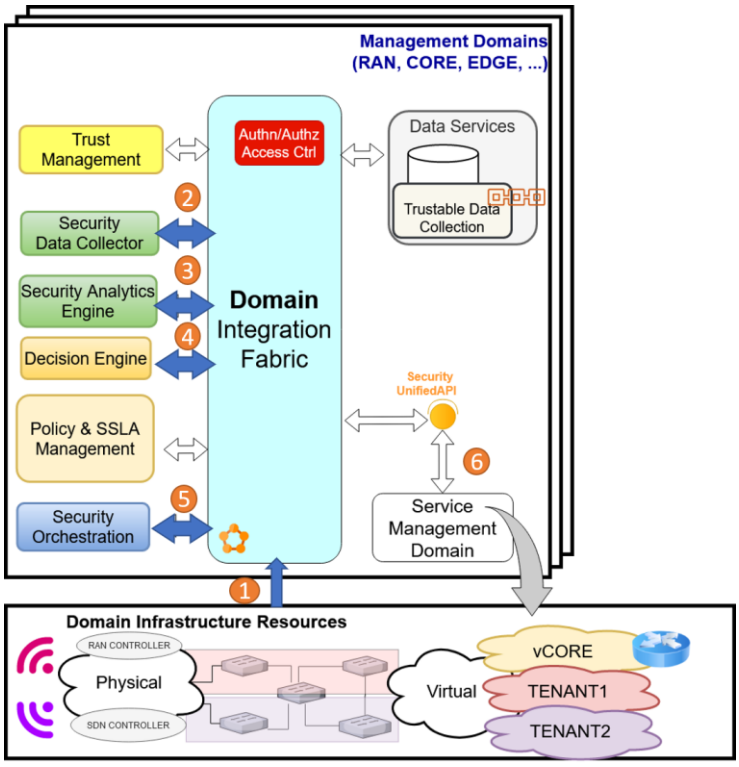

Figure 5 - UC4 operational flow of actions and HLA mapping.

4 Conclusions and Next Steps

Fostering digital transformation hinges not only on the connectivity and high quality of services provided by 5G, but also on the realization of secure and trustworthy 5G systems. To this end, the INSPIRE-5Gplus project is committed to deliver an innovative Software-Defined security orchestration and management framework for future connected systems and pervasive services. The framework's architecture empowers zero-touch security services for protection, trustworthiness and liability in managing 5G systems across multiple domains leveraging on emerging techniques, including ZSM, AI/ML, DLT and TEE.

This White Paper introduced the overall INSPIRE-5Gplus framework High Level Architecture (HLA), its main functional blocks and their role in enabling intelligent closed-loop security operations. To illustrate how the INSPIRE-5Gplus framework can be applied as a Zero-Touch security management solution for 5G systems, the White Paper presented a representative set of advanced security use cases defined in the INSPIRE-5Gplus project. The presented use cases cover different advanced security problems, namely: (i) trustworthy composition of network slices using blockchains (DLT) and secure deployment of E2E network slices in compliance with agreed SSLAs for the automotive vertical application domain; (ii) detection of network attacks over encrypted traffic in Software-Based Architectures; (iii) enforcement of on-demand E2E encryption policies while leveraging TEE to enable trustworthy execution of encryption-decryption operations; and, (iv) reactive and proactive protection of E2E network slices respectively using anomaly detection and MTD mechanisms.

The INSPIRE-5Gplus project is currently evolving the architecture, defining the specific set of services to be provided by each functional block and devising the corresponding enablers. As the project work moves forward, we will release other White Papers to share our achievements with the community.

5 List of Abbreviations

ACID	Atomicity, Control, Isolation, Durability
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
CCS	Component Certification Service
CN	Core Network
CRUD	Create, Read, Update and Delete
DBMS	Database Management System
DE	Decision Engine
DLT	Distributed Ledger Technology
E2E	End-to-End
EMS	Element Management System
HLA	High Level Architecture
HSPL	High-Level Security Policy Language
I2NSF	Interface to Network Security Function
IKE	Internet Key Exchange
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
MANO	Management and Orchestration
MEC	Mobile Edge Computing
ML	Machine Learning
MNO	Mobile Network Operator
MSPL	Medium-Level Security Policy Language
MTD	Moving Target Defence
NFV	Network Function Virtualization
NFVO	NFV Orchestrator
NOC	Network Operations Center
oPoT	ordered Proof of Transit
OTT	Over the Top
PSM	Policy and SSLA Management
RAN	Radio Access Network
RCA	Root Cause Analysis
SA	Security Agent
SAE	Security Analytics Engine

SBA	Service-Based Architecture
SD-SEC	Software Defined Security
SDC	Security Data Collector
SDN	Software Defined Network
SIE	Security Intelligence Engine
SIEM	Security Information and Event Management
SMD	Security Management Domain
SO	Security Orchestrator
SOC	Security Operations Center
SP	Service Provider
SSLA	Security Service Level Agreement
STIX	Structured Threat Information eXpression
STM	Service Trust Manager
STS	Slice Trustworthiness Service
TEE	Trusted Execution Environments
TM	Trust Management
TRM	Trust and Reputation Manager
UC	Use Case
UE	User Equipment
vAAA	virtual Authentication, Authorization and Accounting
vIDS	virtual Intrusion Detection System
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
VSF	Virtual network Security Function
ZSM	Zero-touch network and Service Management