INSPIRE-5Gplus

White Paper
Intelligent Security Architecture for 5G and Beyond Networks

Version 2.0

October 2022

Table of Contents

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

White Paper: Intelligent Security Architecture for 5G and Beyond, version 2.0

List of Contributors

Editor in Chief
Chafika Benzaid, University of Oulu, Finland

Section Contributors

Pol Alemany, Centre Tecnològic de Telecomunicacions de Catalunya, Spain

Rafał Artych, ORANGE Polska S.A.

Rodrigo Asensio, University of Murcia, Spain

Geoffroy Chollon, Thales SIX GTS France SAS, France

Charalampos Kalalas, Centre Tecnologic de Telecomunicacions de Catalunya, Spain

Edgardo Montes de Oca, MONTIMAGE EURL, France

Noelia Pérez Palma, University of Murcia, Spain

Alejandro Molina Zarca, University of Murcia, Spain

Hugo Ramon Pascual, Telefonica I+D, Spain

Wissem Soussi, Zurich University of Applied Sciences

Tarik Taleb, University of Oulu, Finland

Antonio Pastor, Telefoncia I+D, Spain

Final editing
Uwe Herzog, Ellen Tallås, Eurescom

Please cite:

C. Benzaid, P. Alemany, R. Artych, R. Asensio, G. Chollon, C. Kalalas, E. Montes de Oca, N. Pérez Palma, A. M. Zarca, H. R. Pascual, W. Soussi, T. Taleb, A. Pastor. **White Paper: Intelligent Security Architecture for 5G and Beyond Networks, version 2.0**. INSPIRE-5Gplus, Oct. 2022.

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.

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

Executive Summary

5G and the future 6G networks are recognized as key enablers to facilitate the digital transformation, thanks to their capabilities to enable highly reliable and extremely fast connectivity. Nevertheless, the promising capabilities of 5G and beyond (B5G) networks come at the cost of complex and ever-evolving cyber-threat landscape. Thus, appropriate mechanisms to enforce and manage security in such a challenging environment are vital to reap their benefits in accelerating the society's digitalization.

Motivated by this need, INSPIRE-5Gplus, a 5G-PPP phase 3 project, is promoting the shift towards fully automated and smart security management of B5G at both the platforms and verticals levels. To this end, INSPIRE-5Gplus devises and implements a fully automated end-to-end smart and service security management framework that fosters protection, trustworthiness, as well as liability in managing 5G network infrastructures across multiple domains, owned and managed by the same legal entity. INSPIRE-5Gplus seeks to guarantee that the delivered security fulfils the expected Security Service Level Agreement (SSLA) requirements. The advanced B5G security management vision enabled by INSPIRE-5Gplus framework is realized through the adoption of a set of emerging concepts and technologies, including: Zero-touch network and Service Management (ZSM), Software-Defined Security (SD-SEC) models, Artificial Intelligence/Machine Learning (AI/ML) techniques, Distributed Ledger Technologies (DLT), and Trusted Execution Environments (TEE).

This white paper introduces the evolved version of the overall INSPIRE-5Gplus framework's High-Level Architecture, describing its main functional blocks, the key security management services provided by the functional blocks and their role in empowering 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 new set of advanced security use cases. The presented use cases cover different advanced security problems that will be demonstrated through INSPIRE-5Gplus demonstrators, namely: Demo1 – Security Management Closed Loop; Demo2 – Trust and Liability Management; and Demo3 – Moving Target Defense (MTD). The security issues covered by the described UCs include attack detection over encrypted traffic, prevention of introspection attacks, automated assessment of SSLA fulfilment, misbehaviour detection in self-driving vehicular networks, on-demand and verifiable isolation of critical virtualized network functions, and proactive defence for End-to-End (E2E) network slices. The presented UCs promote different emerging technologies that can be leveraged to solve the security issues under consideration. This includes the use of advanced ML techniques such as Reinforcement Learning, TEE, MTD, and the new concept of "Deep Attestation" proposed by INSPIRE-5Gplus as a mean to measure in a verifiable way specific security properties. It is worth mentioning that Demo1 is now accepted as an ETSI ZSM proof of concept (PoC), named "PoC #6: Security SLA assurance in 5G network slices". The accepted INSPIRE-5Gplus ETSI ZSM PoC has recently been publicly demonstrated in the last ETSI Security Conference 2022[1].

[1] https://www.etsi.org/events/2068-etsi-security-conference

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

1 Introduction

One key lesson learned from the COVID-19 crisis is the imperative need to accelerate the digital transformation, allowing to empower inclusive, sustainable, and resilient society. However, without a limitless and reliable connectivity that can provide communication "anytime", "anywhere", and for "anything", such society's digitalization will be difficult to achieve. 5G and the future 6G networks are recognized as key enablers to facilitate the digital transformation, thanks to their capabilities to enable highly reliable and extremely fast connectivity [1][2].

The promising capabilities of 5G and beyond (B5G) networks come at the expense of an increased cyber-threat surface [3]. Thus, appropriate mechanisms to enforce and manage security in such a challenging environment are paramount to reap their benefits in accelerating the society's digitalization. In this vein, INSPIRE-5Gplus[2] project is promoting the shift towards fully automated and smart security management of B5G at both the platforms and verticals levels. To achieve this goal, INSPIRE-5Gplus devises and implements a fully automated end-to-end smart network and service security management framework that fosters protection, trustworthiness, as well as liability in managing 5G network infrastructures across multiple technological domains (e.g., radio access network (RAN), core network (CN), and mobile edge computing (MEC)). INSPIRE-5Gplus strives to guarantee that the delivered security meets the desired Security Service Level Agreement (SSLA) requirements. The advanced B5G security management vision enabled by the INSPIRE-5Gplus framework is achieved by leveraging a set of emerging concepts and technologies, including: Zero-touch network and Service Management (ZSM[3]), Software-Defined Security (SD-SEC) models, Artificial Intelligence/Machine Learning (AI/ML) techniques, Distributed Ledger Technologies (DLT), and Trusted Execution Environments (TEE).

In [2], INSPIRE-5Gplus project released a first version of the smart, trustworthy, and liable 5G security framework the project is designing and developing. In this white paper, we present an updated version of INSPIRE-5Gplus framework, elaborating further on the security management services offered by the different functional blocks of the framework, and describing a new set of use cases illustrating the applicability of the proposed framework. The white paper is organized as follows. In Section 2, the overall INSPIRE-5Gplus framework architecture is presented, highlighting the main functional blocks, their roles, and the provided services. Section 3 describes a set of advanced security use cases, illustrating how the INSPIRE-5Gplus framework can be applied as a security management solution for the identified security problems. Section 4 concludes the white paper.

[2] https://www.inspire-5gplus.eu
[3] https://www.etsi.org/technologies/zero-touch-network-service-management

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

2 INSPIRE-5Gplus Framework High-Level Architecture

2.1 Architecture Overview

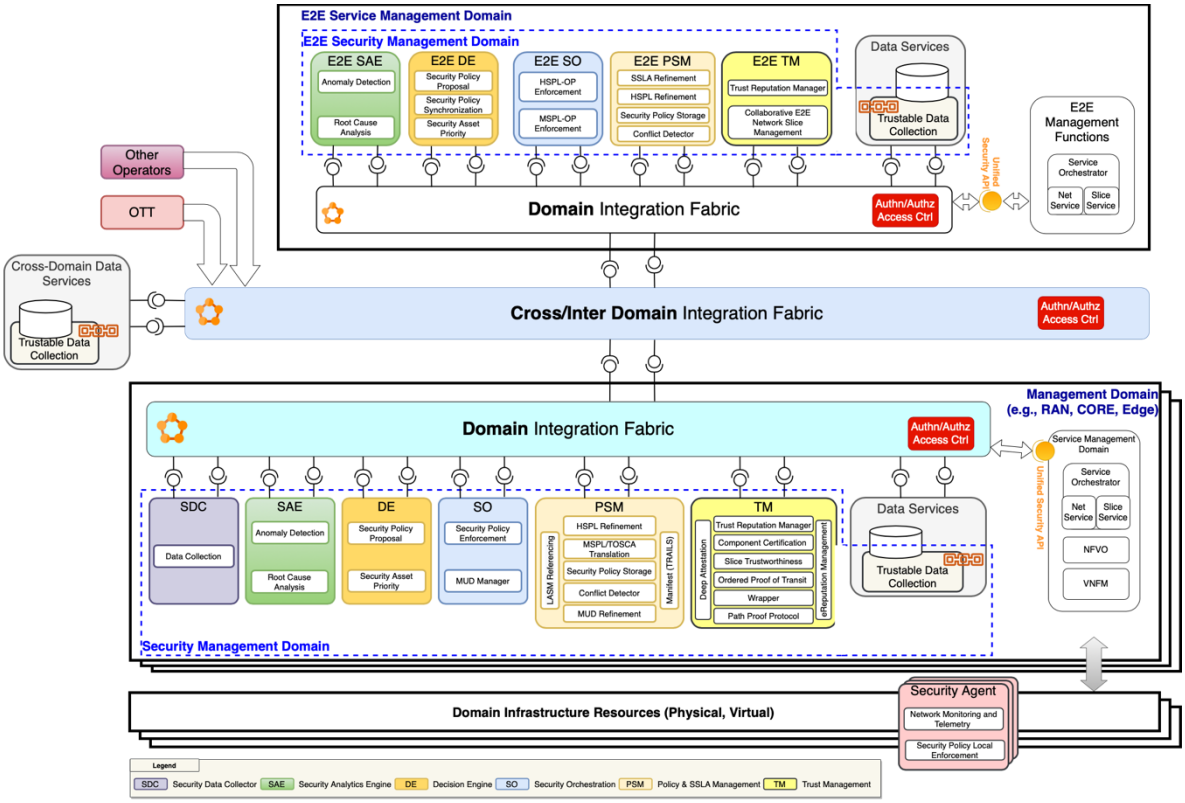

Figure 1 - The INSPIRE-5Gplus Framework HLA.

INSPIRE-5Gplus framework is devised to support fully automated E2E network and service security management in 5G environments across multiple technological domains (e.g., RAN, CN, and MEC) owned by the same legal entity. The framework enables not only protection but also trustworthiness and liability in managing virtualized network infrastructures across multi-domains.

The high-level architecture (HLA) of the INSPIRE-5Gplus framework follows the key design principles of the ETSI ZSM reference architecture [4] by supporting the separation of security management concerns per domain, enabling AI-based software-defined security management closed loops, and adopting a service-based architecture whereby the provided security management services are exposed and dynamically consumed through an integration fabric as needed. As portrayed in Figure 1, INSPIRE-5Gplus HLA consists of several security management domains (SMDs), each of them overseeing the intelligent security automation of resources and services within its scope. The E2E SMD is a special SMD that coordinates between domains to manage security of E2E services (e.g., E2E network slice). It is worth mentioning that the separation of security management concerns per domain and the adoption of service-based and software-defined security models allow to build robust and sustainable security measures that can adapt to dynamic changes in threat landscape and security requirements in future mobile networks.

Although the INSPIRE-5Gplus framework is developed with a focus on single operator environment requirements, the inter-domain integration fabric provides an inherent capability to extend security management to multi-operator and Over-The-Top (OTT) environments in the near future.

In what follows, we describe the core functional modules composing the INSPIRE-5Gplus framework HLA at both domain and E2E levels.

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

2.2 Domain-Level Functional Blocks

2.2.1 Security Data Collector

The main function of the Security Data Collector (SDC) is to collect all the data reported by the security agents and enablers at the domain level, and which are required by the security management functions (e.g., Security Analytics Engine). The types of data collected by the SDC may include, among other, performance monitoring data (e.g., counter data and statistics); security monitoring data (e.g., traffic meta-data, packet capture); event/alarm data (e.g., system logs, application traces, system traces); machine learning reference datasets; and external data (e.g., Cyber Threat Intelligence, external datasets).

Table 1 summarizes the services provided by SDC.

Table 1 - Services provided by SDC.

Service Name	Service Description	Potential Consumers
Data Collection Service	This service sets up and launches the mechanisms for collecting data from the different security agents, security enablers and network devices.	SAE, PSM

2.2.2 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 potential cause of the observed security incidents by analysing and correlating data from other services (e.g., Anomaly Detection service). The RCA 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.

Table 2 summarizes the services provided by SAE.

Table 2 - Services provided by SAE.

Service Name	Service Description	Potential Consumers
Anomaly Detection Service	This service has the capabilities of detecting and/or predicting anomalous behaviours due to malicious or unintentional actions.	DE, Domain Data Services, Operators
Root Cause Analysis Service	This service identifies the cause of the observed security incidents by analysing and correlating data from other services (e.g., Anomaly Detection Service) and learning from past experience.	DE, Domain Data Services, Operators

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

2.2.3 Decision Engine

The Decision Engine (DE) manages the security mitigation by creating the possible security reactions in the scope of a SMD. It fits between the events and notifications emitters, as for example the SAE and the Security Orchestrator (SO). These respective communications take place through the integration fabric for decoupling each component with their deployment details. The DE can initiate the security mitigation in proactive or reactive fashion in its Security Policy Proposal Service. The possible proactive actions can be static, such as SSLA enforcement templates, or dynamic, such as MTD operations that could neutralize undetected infections and help reducing attackers' success probability. The possible reactions are orders understandable by the SO and they stretch from network reactions, such as filtering a device, to services reactions, like the redeployment of a virtual network security function (VSF). Moreover, DE interacts with the E2E DE to share state, mitigation taken locally in a SMD or to receive orders from the global E2E DE oversee. The DE also provides a Security Asset Priority Service to help with ordering mitigations when multiple proposals are found, or when a mitigation might negate a previous reaction.

Table 3 summarizes the services provided by DE.

Table 3 - Services provided by DE.

Service Name	Service Description	Potential Consumers
Security Policy Proposal Service	This service creates and proposes security mitigation policy for enforcement in a local SMD to submit them to the local SO.	SAE
Security Asset Priority Service	This service manages the associated priority of reactions raised during conflict detection and concurrent mitigations in a local SMD containing multiple local reaction loops running in parallel.	Operator, DE, E2E DE

2.2.4 Security Orchestration

The Security Orchestrator (SO) is the security enabler in charge of enforcing among the system the security requirements specified in the security policies or dynamically generated by DE. The SO has two different entry points to initiate the orchestration process, proactive and reactive, which will use the Integration Fabric to communicate with the different SDN Controllers, NFV MANO and Security Management Services in order to allocate, chain and (re)configure different VSF as standalone services or as a 5G Network Slice. These VFS provide the system with the security capabilities required by the policy (e.g., deploy agents for monitoring the network or establish channel protection). The SO requires the support from different modules of the HLA's entities; in particular, the Trust Management (TM) Component will provide trust and reputation indicators of assets, the Policy Framework provides the translation from the security policy into final asset configuration, Data Services provide the entry points of the different assets of the infrastructure (e.g., through a SDN controller or an API) and DE provides insights and evolved plans inferred. This cognitive behaviour grants self-healing, self-repairing, self-protection, and self-configuration, transforming the managed system into an autonomous and intelligent system, capable to react locally in an autonomous way to ongoing attacks or foreseen threats, generating mitigation countermeasures that maintain the security capabilities enforced [5][6]. Potential reactions encompass, among others, filtering at different levels a DDoS attacker (via RAN or vFirewall), or redeploy, reconfigure, migrate or decommission VSFs with more trustable versionsIn addition, when a new device is connected to the system, the Security Orchestrator can retrieve from the device manufacturer the Manufacturer Usage Description (MUD) file, as well as the associated signature file. From MUD file the security requirements required by the specific device and its vulnerabilities can be extracted, thus enforcing security capabilities to mitigate vulnerabilities

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

and enforcing security requirements required from the specification of the device that has recently connected.

Table 4 summarizes the main services provided by SO.

Table 4 - Services provided by SO.

Service Name	Service Description	Potential Consumers
Security Policy Enforcement Service	This service allows requesting policies enforcement (including 5G security slice policies) in a management domain.	DE, E2E SO
MUD manager service	This service enables the management of the MUD within the system when a new device is connected to it, performing the retrieving of the MUD file with control and deploying related policy within the system.	DE

2.2.5 Policy and SSLA Management

The Policy and SSLA Management (PSM) component transforms the abstract Protection Level and Security Level requirements and constraints expressed by the medium abstraction policy level (MSPL-OP) into specific parameters that indicate, to the SO, the security services to configure, deploy and manage. The specified security services could form part of a 5G security sub-slice that form part of an E2E 5G Security Slice.

Table 5 summarizes the main services provided by PSM.

Table 5 - Services provided by the PSM.

Service Name	Service Description	Potential Consumers
HSPL Refinement Service	This service refines HSPL policies into MSPL policies	SO
MSPL/TOSCA Translation Service	This service refines MSPL policies into precise configurations, API calls, specific low-level configurations needed to interact with the enablers. It could also translate MSPL to TOSCA[4] to be compatible with some orchestrators (e.g., OSM, ONAP) that support TOSCA.	SO
Security Policy Storage Service	This service stores policies enforced by other domain entities to keep track of them. It could be implemented using Distributed Ledge Technologies (DLT) to assure liability.	DE, SO
Conflict Detector	This service performs the conflict detection at the SMD level. A conflict is considered when the enforcement of a policy contradicts a previously enforced policy or when it is impossible to enforce for other reasons (e.g., lack of resources, or lack of capacity in the domain).	DE, SO
MUD refinement service	This service is in charge of performing the translation from the MUD file to MSPL-OP.	SO

[4] http://docs.oasis-open.org/tosca/TOSCA/v1.0/os/TOSCA-v1.0-os.html

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

LASM Referencing Service	When a new component is added, this service retrieves data from the Manifest, also called TRAILS, and stores them in an ontology.	SO, DE, SAE
Manifest (TRAILS)	This descriptor contains SSLA.	NA

2.2.6 Trust Management

The Trust Management (TM) contains various internal services for the trust related functions in the INSPIRE-5Gplus security framework. Among other services, this block provides trust and reputation calculation (at the component and domain level) as well certification based on trust metrics. For trust in how data flows traverse a network and how they are processed spatially, its Ordered Proof of Transit (oPoT) service verifies the correct order of nodes on the network path followed by a flow. 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. A metadata file or data structure is enclosed in the protected VNF package and describes the various security functions applied with their parameters.

Table 6 summarizes the main services provided by TM.

Table 6 - Services provided by the TM.

Service Name	Service Description	Potential Consumers
Trust Reputation Manager	This service assigns trust and reputation values to monitored 5G entities and provides this information to security management entities and end users in 5G virtualized networks. The service is endowed with capabilities to improve the received data processing and the score accuracy.	SO
Component Certification Service	This service works at the component level and provides a static evaluation of different 5G network components by measuring trust metrics.	SO
Slice Trustworthiness Service	This service 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.	SO
Ordered Proof of Transit Service	This 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.	SO
eReputation-Management	This service computes some components reputation (assimilable to some Trust level) metrics over a VNF infrastructure.	SO, SAE (for RCA services)
Wrapper Service	This service produces the modifications on the protected binaries with the aim of hardening the code against confidentiality, integrity, illicit usage and vulnerability exploits risks. Specifically, Systemic wrapper hardens executable files (programs and library functions) against confidentiality and integrity violation risks, leveraging the potential of Trusted Execution Environments (TEE) and offering deep monitoring	SO

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

	capabilities.	
Path Proof Protocol	This service allows to prevent deviating the traffic on a given route (hijacking attacks). The PPP enabler addresses the issue (application-layer approach) thanks to a two-party cryptographic-based anomaly detection protocol.	DE, SO.
Deep Attestation Service	This service could be deployed as a resident service for each virtualized infrastructure. It allows to collect evidence of security properties (thank to cryptography).	DE, SAE

2.3 E2E-Level Functional Blocks

2.3.1 E2E Security Analytics Engine

The E2E Security Analytics Engine (E2E SAE) 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) or to make the detections more effective and precise (e.g., reduce the number of false positives and improve the number of detected incidents). It generates notifications that will be used by E2E Decision Engine to trigger the necessary remediation or prevention procedures.

Table 7 summarizes the main services provided by E2E SAE.

Table 7 - Services provided by E2E SAE.

Service Name	Service Description	Potential Consumers
Anomaly Detection Service	This service analyses the data provided by the different domain SDCs or stored in the E2E Data Service to detect anomalies that can only be detected using information from more than one domain. Similar to a SIEM (Security Information Management System).	E2E DE
Root Cause Analysis	Similar to the RCA service defined in DE but operates at E2E level to identify cascading effects between different domains.	E2E DE, E2E Data Services, Operators

2.3.2 E2E Decision Engine

The E2E Decision Engine (E2E DE) is first, an augmented SMD DE and shares the same features described in Section 2.2.3. As, in some deployments, services might be also instantiated at the E2E level, they increase the attack surface. Then, it dictates for running a local E2E mitigation loop. Thus, the E2E DE contains the same Security Policy Proposal Service and the same Security Asset Priority Service as in a SMD domain. Second, the E2E DE acts as a hierarchical controller. It gathers notifications from the underlying SMD domains and manages the overall mitigations spanning across multiple SMDs. Those mitigations are enacted by the E2E Security Orchestrator. Using this holistic point of view, the E2E DE can select and propagate escalated reactions from a targeted domains to all other domains. To do so, the E2E DE is equipped with

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

an additional service, namely the Security Policy Synchronization Service. This service allows to synchronize the state and the reactions taken locally by an SMD back to the E2E DE for a possible escalation.

Table 8 summarizes the main services provided by E2E DE.

Table 8 - Services provided by the E2E DE.

Service Name	Service Description	Potential Consumers
Security Policy Proposal service	This service creates and proposes security mitigation policies for enforcement at the E2E level and all SMDs.	E2E SAE
Security Asset Priority Service	This service manages the associated priority of reactions raised during conflict and concurrent mitigations at the E2E level.	Operator, E2E DE
Security Policy Synchronization Service	This service allows the SMD DEs to escalate reactions and to receive new reactions manifest from the E2E DE.	DE

2.3.3 E2E Security Orchestration

The E2E Security Orchestrator is responsible for orchestrating and managing the various security enablers from multiple domains, in order to meet the security capabilities requirements outlined by the defined E2E security policy which, in the event that a 5G service is included, will be known as an E2E 5G Security Slice policy. The E2E SO maps the E2E security policy into the domain-specific policy and interacts with the SOs to deploy and manage the lifecycle of the necessary security enablers at domain level, which could be a sub-slice of an E2E 5G Security Slice.

Table 9 summarizes the main services provided by E2E SO.

Table 9 - Services provided by E2E SO.

Service Name	Service Description	Potential Consumers
MSPL-OP Enforcement Service	This service enforces and controls MSPL-OP cross-domain through interaction with SOs at domain level. Capable of enforcing 5G Security Slices.	E2E DE, PSM
HSPL-OP Enforcement Service	This service enforces and controls High-level Security Policy Language - Orchestration Policy (HSPL-OP) cross-domain through interaction with SOs at domain level.	Other Operators

2.3.4 E2E Policy and SSLA Management

The E2E policy and SSLA management (E2E PSM) block provides the required functions over the different levels of abstraction of security policies to the E2E SO for refining High level of abstraction (SSLA, HSPL-OP) into medium level of abstraction (MSPL-OP) and storing the E2E policies in a secured way. The Policy Conflict module provides the tool for avoidance conflicts at E2E level (e.g., detect inconsistencies between the policy capabilities and domain capabilities). 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 5G slice deployment-ready representations. These

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

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.

Table 10 summarizes the main services provided by E2E PSM.

Table 10 - Services provided by the E2E PSM.

Service Name	Service Description	Potential Consumers
Security SLA Refinement Service	This service refines SSLAs into HSPL/MSPL-OP policies for orchestration	E2E SAE, User/System operator, Other ISPs
HSPL Refinement Service	This service refines HSPL policies into HSPL policies intended for the domains underneath or MSPL policies.	E2E SO
Security Policy Storage Service	This service stores policies enforced by other domain entities and relates them to specific tenant & slice to keep track of them. It could be implemented using DTL to assure liability.	E2E SO, E2E DE
Conflict Detector	This service performs the conflict detection at the E2E level considering the E2E slice capabilities and its different sub-slices.	E2E SO, E2E DE

2.3.5 E2E Trust Management

The E2E Trust Management (E2E TM) facilitates E2E trust services across multiple domains, relying on the domain-resident TMs. It has the capability to compute, based on information aggregation and domain's Trust and Reputation Manager (TRM) outputs, final trust scores of the involved domains. Additionally, it allows any security management entity to request the needed cross-domain trust scores. For instance, the trust score of a given domain can be requested by E2E SO to operate in compliance with E2E security requirements, policies and SSLAs. Additionally, the E2E TM offers the collaborative E2E Network Slice Management for scenarios in which multiple domains and operators interact among them in a transparent and collaborative way.

Table 11 summarizes the main services provided by E2E TM.

Table 11 - Services provided by E2E TM.

Service Name	Service Description	Potential Consumers
Trust Reputation Manager Service	This service computes the resulting trust score of a given domain based not only on the output of the TRMs at domain level but also including historical information and cross-domain data.	TM (TRM service), SO
Collaborative E2E Network Slice Management	This service aims to allow a cooperative and collaborative management of Network Slices with the use of Blockchain technology.	E2E Management Function (Network Slice Managers)

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

2.4 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 several domains, being accessed only by authorized consumers. By introducing this service, the data persistence and data processing are separated, allowing to enable stateless management functions and eliminate the need for per-function data persistence and per-function processing.

The Data types are those collected by the SDC (see the examples listed in Sec. 2.2.1). Standard formats should be used, such as PCAP for network traffic, JSON with schema for data interchange, STIX for sharing Cyber Threat Intelligence. The collected data can be either real- time data or historical data required for security-related analysis (e.g., analysis of risk, liability and root cause, and detection of vulnerabilities and intrusions). The data should be normalised either by the SDC or by an adaptor so that the consumers of the data can use them. They should be handled either within the domain where they were generated 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 can pertain to one domain or can be shared between domains for cross-domain security analysis and control. They can be stored and used by different security management functions, such as the SAE, DE, and SO. The Data Services should support different types of storage techniques (e.g., DBMS, DLT, persistent data bus) that can be dynamically selected depending on the requirements.

Table 12 summarizes the main services provided by the domain-level and cross-domain Data Services.

Table 12 - Services provided by the Data Services.

Service Name	Service Description	Potential Consumers
Data Access Service	This service allows retrieving, updating and removing information concerning the status of the infrastructure provided by the different security agents and enablers.	All

2.5 Integration Fabric

ZSM reference architecture designed the Integration Fabric (IF) to provide communication services intra and inter SMD. In addition, IF has security by design, performing registration with authentication and discovering services deployed under the same infrastructure. Also, IF has been designed to enable communication-related security features in a service mesh like authorisation/access control.

Table 13 summarizes the main services provided by IF.

Table 13 - Services provided by IF.

Service Name	**Service Description**	**Potential Consumers**
Management services registration service	This service enables the registration/deregistration 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.	All
Management services discovery	This service allows the discovery of registered security management services and their capabilities.	All

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

service		
Management communication service	This service allows the communication between security management services via dedicated communication channels.	All
Management service invocation routing service	This service allows the authorized service consumer to invoke a discovered security management service.	All

2.6 Unified Security API

The Unified Security API is a set of commands/rules that define the interfaces that allow the exchange of information between the Management Functions (e.g., Network Slices or Network Services Managers) and the HLA components designed in the INSPIRE-5G-plus project.

The main interaction between the Management Functions and the HLA components is done through the E2E SO/SMD's SO; as it is the key component to control and manage the security aspects around the Network Slices/Services deployed. Despite the main interaction being with the E2E SO/SMD's SO, other HLA components may be accessible, such as the E2E PSM/SMD's PSM, as they contain the security complementary information to the Network Slices/Services to be deployed.

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.

Table 14 summarizes the main services provided by the Unified Security API.

Table 14 - Services provided by the Unified Security API.

Service Name	Service Description	Potential Consumers
Network Slice/Service Actions	This API defines the format/structure (i.e., syntax and semantics) of the requests or list of requests that the INSPIRE-5Gplus framework offers to the E2E/SMD Management Functions (i.e., Network Slice Manager, Network Service Orchestrator, etc.).	INSPIRE-5Gplus modules (essentially, the E2E/SMD SOs). Different services managers (e.g., Network Slice Managers and Service Orchestrators).

2.7 Security Agent

The Security Agent (SA) is a security asset for monitoring and managing security at a local observation point (e.g., network interfaces of electronic circuit cards or virtual machines, switch port mirroring - SPAN, Terminal Access Point - TAP). It is able to capture data needed by other security functions and/or perform actionable behaviour decided locally but managed by other security functions (e.g., SOs). 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. In fact, 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

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

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.

Table 15 summarizes the main services provided by SA.

Table 15 - Services provided by SA.

Service	Service Update	Potential Consumers
Security Policy Local Enforcement Service	This service receives a security rule, SSLA or security policy (e.g., MSPL), in a standard format and translates it to the security enablers' format to be able to process it (e.g., real-time assessment by a deployed monitoring probe).	DE, SO
Network Monitoring and Telemetry Service	This service is in charge of generating on-demand data (logs, alerts, network telemetry, network datasets, statistics, trends). Acting as passive or active probe.	SAE, SDC

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

3 HLA Instantiation Examples

This section describes a representative set of five advanced security use cases (UC) defined in the INSPIRE-5Gplus project, and which will be demonstrated as part of INSPIRE-5Gplus three demonstrators, namely: Demo1 – Security Management Closed Loop (UC1, UC2 and UC3); Demo2 – Trust and Liability Management (UC4); and Demo3 – Moving Target Defense (UC5). The five UCs focus, respectively, on the following advanced security issues: attack detection over encrypted traffic, automated assessment of SSLA fulfilment, misbehaviour detection in self-driving vehicular networks, on-demand and verifiable isolation SSLA of critical virtualized network functions, and proactive defence for E2E network slices. For each UC, we illustrate how the proposed INSPIRE-5Gplus framework can be applied as a security management solution for dealing with the identified security problems. The described UCs advocate different emerging technologies that can be leveraged to solve the security issues under consideration. This includes the use of advanced ML techniques such as Reinforcement Learning, TEE, MTD, and the new concept of "Deep Attestation" proposed by INSPIRE-5Gplus as a mean to provide to measure in a verifiable way specific security properties.

3.1 UC 1: Network Attacks over Encrypted Traffic in SBA

3.1.1 Problem Description & Aim

Network operators depend on network traffic monitoring capacity to increase operational efficiency and security in their platforms. 4G and previous generations use massively a set of management tools, including network probes, to operate and control the communication services. The general recent trend is to encrypt all type of traffic on internet, impacting the existing mechanisms for management and security5. In 5G, data plane traffic between the RAN and the Core, which relies upon the use of GPRS Tunnelling Protocol (GTP), is not always encrypted, but the trend is to provide this security requirement with IPsec, increasing the security by mobile operators. Ciphering adoption in 5G also applies to control plane. 5G Core includes the concept of Service Based Architecture (SBA) using HTTP/2 as the protocol base to leverage all signalling traffic, instead of legacy DIAMETER protocol. Starting with Release 15, 3GPP mandates TLSv1.2 for RESTful APIs.

The reasoning behind is that cloud environment and microservices in data centers and hyper-scalers, are the new commodity to deploy network functions. These environments demand application level E2E encryption over Internet services based on TLS (e.g., REST API channels and DNS over HTTP), QUIC (HTTPS over UDP). Consequently, current cybersecurity network monitoring tools, for example deep packet inspection (DPI), become ineffective in these environments, making it extremely difficult to detect some common attacks based on botnets, application layer attacks, DDoS or cryptomining. As a result, cybercriminals are adopting TLS encryption as part of their attack channels making their activity indistinguishable from real traffic found in the SBA interfaces. Additionally, the massive adoption of microservices, NFV and Cloud approach in the deployment of 5G Core components and monitoring tools, will open the door for introspection attack (i.e., direct access on the software) that can be exploited by a malicious attacker. In this way, attackers can reverse engineer or modify the monitoring software, adding the necessary modifications to directly affect the performance of the monitoring functions, making it unable to detect and react against a potential attack.

This use case proposes the evolution of the security monitoring tools to be capable of analysing encrypted traffic, so it can detect and mitigate attacks. Multiple probes could be allocated in different 5G network elements, to analyse the characteristics of the traffic and generate alerts to be addressed later, by the management and orchestrations systems. Additionally, this use case leverages TEE techniques (e.g., Intel's SGX) to prevent unauthorized access and modifications that could affect the behaviour and characteristics of the monitoring software.

[5] IETF RFC 8404: "Effects of Pervasive Encryption on Operators" - https://www.rfc-editor.org/rfc/rfc8404.html

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

3.1.2 Actors and Roles

- 5G Network administrator: such as Network/Security Operation Centres (NOC/SOC). It covers the role of the responsible of the administrative domain. Also, he is capable to enforce specific policies in the network (e.g., using a NFV MANO to re-instantiate a component).
- Malicious party: role represented by the attacker who wants to compromise a component of the network materializing a threat. In this case, it will hide the attacks using encrypted traffic by compromising directly 5G Core components.
- Security monitoring probes: integrated in the INSPIRE-5Gplus framework, they will be used to extract the relevant information from the different network flows to then push them to the analytics engines which can infer relevant information to detect the attacks.
- INSPIRE-5Gplus Security Management Domain (SMD) services that provide INSPIRE-5Gplus functionalities, including security analytics, decisions, visualization, report of the attacks and enforcement of corrective actions. It will receive the alerts generated by the security monitoring probes to visualize, report, and take the necessary actions against a potential attack to counteract. Figure 2 shows the actors and the INSPIRE-5Gplus HLA elements that are involved in the UC and their interactions.

3.1.3 Operational Flow of Actions

Before an attacker can start the attack, the following conditions need to be satisfied:

- 5G network based on SBA 5G Core in normal operation (No attacks or no awareness of an on-going malicious activity).
- The attacker has the capacity to access and compromise some 5G Core components, or the platform where they are deployed; this could be the case of the cloud or NFVI administrator.

Having the above-mentioned conditions satisfied, the operational flow goes as follows:

1. The attacker initiates actions on the network to compromise some component resources on NFV for its own benefit. At this stage, the administrator detects service performance impact, caused by degradation of some instances of the 5G Network Functions (e.g., a DoS attack, a cryptomining malware) generated by the malicious party, but the source of the problem and the remediation are not known.
2. To determine the source of the problem, he deploys the monitoring AI agents (Smart Traffic Analyzer or STA) in the network, so the agents can be activated in order to monitor the encrypted control or data plane traffic. Then, the administrator asks to increase the protection of the network probes on an untrusted environment such as 3rd party IaaS, for example a hyper-scaler datacenter.
3. To avoid Introspection attacks and reverse engineering, it is necessary to harden the integrity of the monitoring images leveraging the TEE. The runtime integrity verification needs to be backed by a TEE embedded routine, so the monitoring function cannot be compromised. The STA engine is capable of detecting the malicious ciphered traffic generated in the compromised function, reporting the resultant values, and providing the origin of the threat.
4. Identified malicious activity reports the threat to the Trust Reputation Manager (TRM) updating the trust of the involved entities and the Decision Engine (DE). The latest will generate a security policy to re-deploy the compromised function (e.g., an infected container or virtual machine of the 5G core network function).
5. The new policy will be forwarded to the Security Orchestrator (SO) to re-deploy the image, mitigating the attack.
6. The SO redeploys the compromised 5G function.

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

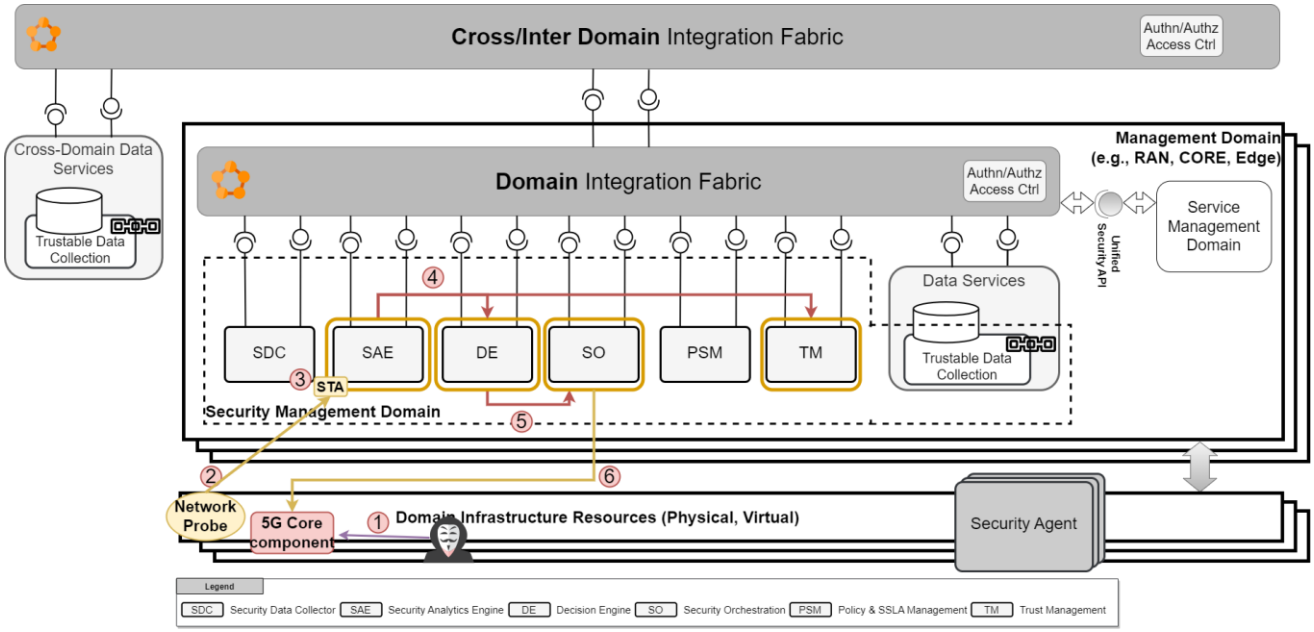

Figure 2 - UC1 operational actions flow within the HLA architecture.

3.2 UC 2: Definition and Assessment of Security and Service Level Agreements

3.2.1 Problem Description & Aim

This UC2 use case is about defining SSLAs to assess and control that security features are properly implemented, security properties are not violated, and violations are triggering self-healing and self-protection strategies. Thus, it includes security monitoring and analysis to remedy and prevent security breaches and vulnerabilities in a fully automated way.

The main objective is to define how SSLAs can be defined and applied, and how they facilitate agreements between different stakeholders regarding the expected level of cybersecurity and remediation strategies.

SSLAs can be defined to formalize requirements related to a wide variety of cybersecurity issues and concerns. They go well beyond current rules used by intrusion detection and prevention systems, as well as policy control systems, in that:

They are based on real-time metrics that allow a detailed or more abstract assessment of the security requirements of the various stakeholders involved.

They detect security breaches as well as the malfunctioning of security functions (e.g., due to evasion attacks).

They incorporate remediation strategies that can be automatically triggered to enforce the specified SSLAs.

The ability to define and manage SSLAs is essential for operators offering managed services. Similar to quality-oriented SLAs, SSLAs are a contract between two stakeholders that defines the services and levels of security expected by both parties. In other words, SSLAs are necessary for operators, service providers and end users to “contract” the requirements related to the security capabilities of the networks, slices and services provided. The SSLAs defined allow to control that the functions of security are correctly implemented and that security properties are not violated.

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

To further automate the process of defining and enforcing SSLAs, real-time monitoring of network, application, and system activity based on distributed probes is required. Probes, or security agents, capture data, metadata, and statistics that measure the parameters involved in specified SSLAs. Then, complex event processing and machine learning can be used to analyse and detect breaches at the local level by security officers or at the domain or cross-domain level by the Security Analytics Engine. Finally, when flaws are detected, corrective actions (e.g., self-healing or self-protection techniques) must be taken. These actions can be triggered manually by operators or automatically by the Decision Engine which interacts with Orchestrators and Controllers to perform the necessary actions.

SSLAs are defined to assess and control that: security functions are correctly implemented, security properties are not violated, violations trigger self-healing and self-protection strategies

Examples of SSLA metrics are Availability of data and services, Geolocation of data/services, Frequency of security scans, Number of GTP per subscriber, Access to insulation from other slices.

Security enforcement techniques include, for instance: Deployment time of new policies, Delay in applying patches, Delay in reconfiguration, Delay in revoking users/operators, and Delay in the replication of services and switching instances.

3.2.2 Actors and Roles

The actors and roles involved in UC2 are:

- Stakeholder organizations:
    - Network operators: that define the SSLAs and use the tools and applications to monitor and manage them, and use them to establish agreements with other stakeholders.
    - Slice managers: that define and provide the resources and functions required by specific SSLAs.
    - Service providers: that offer services that adhere to the user required SSLAs
    - End-users: that define their requirements that are translated to actionable SSLAs.
    - Cyber security experts/managers: that define and select the SSLAs that need to be considered in the network environment by the operators and service providers.
- Involved elements:
    - Probes: distributed and remote-controlled lightweight Security Agents implementing different analysis and detection techniques.
    - Security Function: enablers that translate, generate, process and/or use the SSLAs as a formalism to define the security requirements. These include, for instance, the Decision Engine, the Security Analytics Engine, the Policy and SSLA Management, the Security Orchestrator and Controllers, etc.

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

3.2.3 Operational Flow of Actions

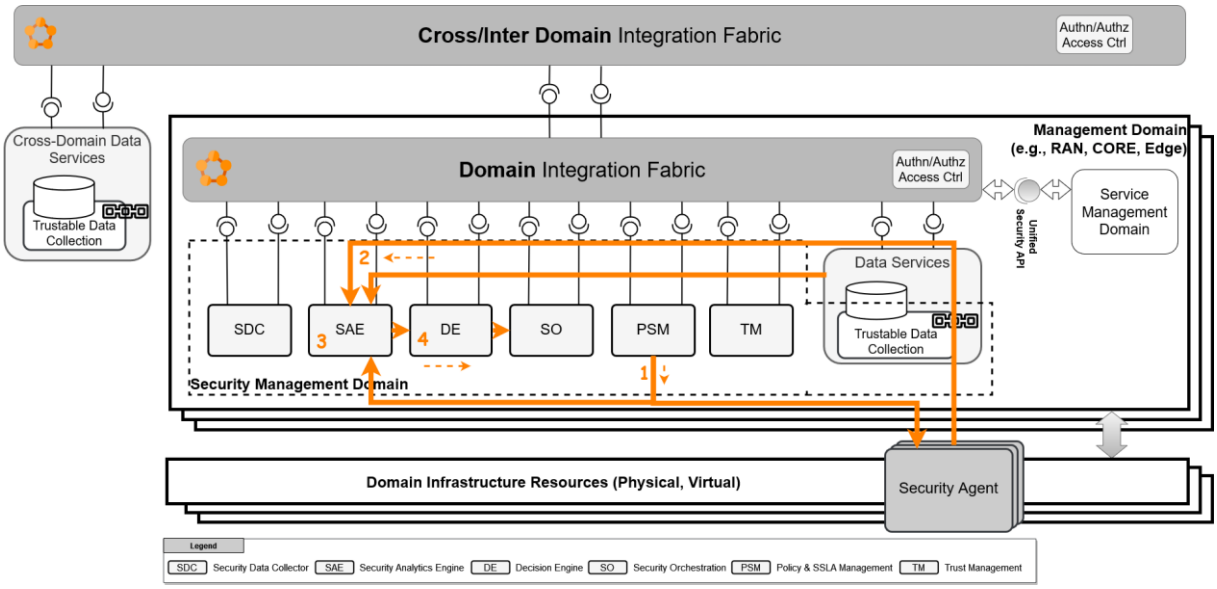

Figure 3 - UC2 operational actions flow within the HLA architecture.

The HLA enablers involved are represented in the Figure 3 above. The sequence of actions are as follows:

1. The SSLAs are defined by the operators using the PSM function and deployed in the appropriate enablers (i.e., Security Analytics Engines - SAEs and Security Agents - SAs).
2. The SAE obtains the required data from the SAs deployed in the physical or virtual machines (e.g., Probes that can capture and compute the features required by the machine learning or other techniques implemented by the SAE) and/or the Data Collector (e.g., a database containing historical data and Cyber Threat Intelligence data).
3. The SAE will perform the assessment of the SSLAs deployed either in real-time or not depending on the requirements and the techniques used.
4. The SAE will communicate the results in the form of alarms or notifications to the Decision Engine for performing the appropriate countermeasures in conjunction with the Security Orchestrator.

3.3 UC 3: Remotely Controlled Manoeuvring Manipulation

3.3.1 Problem Description & Aim

The remotely controlled manoeuvring manipulation UC is associated with security vulnerabilities that may arise in tele-operated driving scenarios, which involve remote control of automated vehicles over the mobile radio network. UC3 considers an automated driving scenario where an unexpected blockage is encountered on the planned trajectory of a vehicle. The obstacle needs to be overpassed through tele-operated driving commands received by a public transport control centre which handles tele-operation sessions. In particular, the vehicle transmits environment sensor data and/or video streaming information to the control centre, which, in turn, provides the visual representation of the altered vehicular environment and sends relevant control commands, e.g., appropriate speed level or steering wheel angle, to the automated vehicles.

In UC3, an attacker may gain access to autonomous-drive functions by exploiting the vulnerability of on-board units, e.g., sensor spoofing, or by manipulating the transmitted information, e.g., jamming the wireless channel. In both cases, the intruder may have the potential to undertake the control of safety-critical vehicular components, such as engine control and brakes, and perform manipulation to

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

vehicular data, e.g., inject falsified information and fabricate sensor readings, by gaining access to on-board diagnostics. Trajectory alteration via Global Positioning System (GPS) jamming/spoofing could be also a realization of this kind of attacks.

False data injection threats associated to UC3 are often difficult to detect and contain, particularly when attackers behave intelligently while conforming to normal system behaviour. In addition, tele-operated driving is associated with safety-critical driving situations; thus, timely and highly reliable prediction and detection of such attacks become crucial. In this context, data-driven misbehaviour detection empowered by reinforcement learning (RL) can be efficiently applied for real-time attack mitigation (e.g., detection of anomalous sensor readings, trajectory alteration identification) from authenticated users (i.e., *insiders*) who already possess valid credentials to interact with other legitimate entities in the system. RL provides a highly effective mean to consistently improve detection experience over time while interacting with unknown environments without relying on security threshold values. RL-based misbehaviour detection leverages the processing of streaming vehicular information at the transport control centre, to ensure accurate detection of manipulated manoeuvring information which may violate the semantic correctness of exchanged vehicular data [7].

3.3.2 Actors and Roles

The actors and roles involved in UC3 are:

- Mobile network operator: Responsible for providing and maintaining the communication infrastructure.
- Vehicle control centre user: Responsible for the bidirectional vehicular interaction via tele-operation sessions and provider of the remote-control commands to the automated vehicles.
- A set of legitimate vehicles: Genuine vehicles which periodically transmit beacon messages with information on each vehicle's position, speed, acceleration and heading angle.
- Malicious party: Represented by a malicious vehicle which intentionally transmits falsified manoeuvring information.
- Service provider: Responsible for delivering the end-to-end vehicular communication service.
- INSPIRE-5Gplus's HLA security modules: Security Data Collector, Security Analytics Engine, Decision Engine, and Security Orchestration.

3.3.3 Operational Flow of Actions

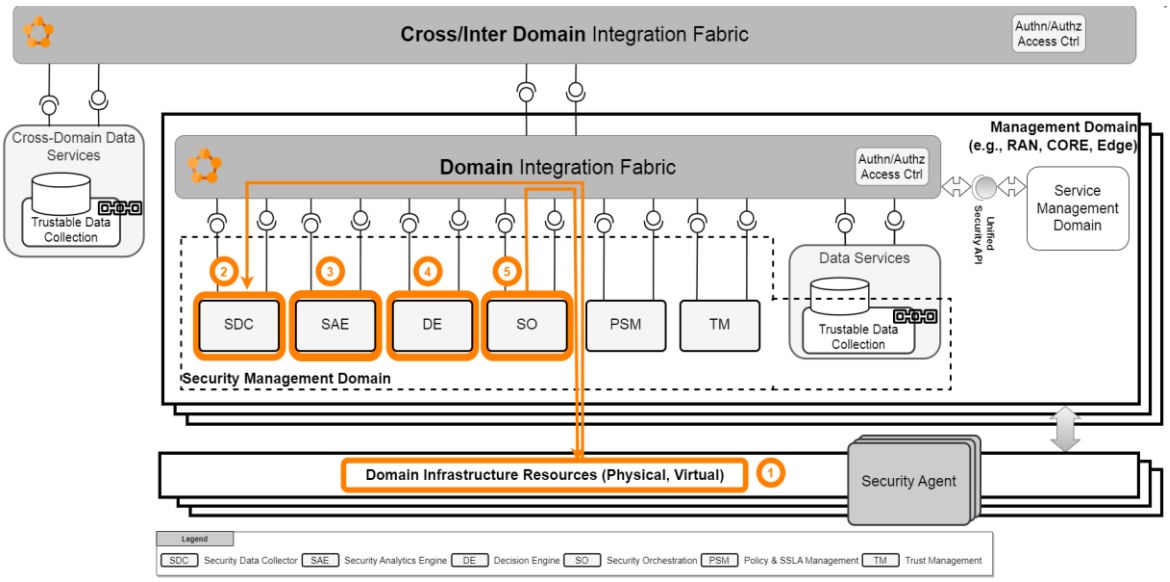

Figure 4 - UC3 operational actions flow within the HLA architecture.

The operational flow of actions for UC3 is illustrated in Figure 4 on top of the INSPIRE-5Gplus HLA for a specific management domain. UC3 includes the following sequence of actions:

1. Legitimate vehicles periodically transmit environment sensor data to the control centre for remotely controlled manoeuvring. When the manipulation attack takes place, the malicious vehicle injects falsified manoeuvring information with the aim to deceive the control centre to respond with incorrect and misleading commands to the legitimate vehicles.
2. Data collector performs the fusion of the vehicular network traces at the transport control centre.
3. Security analytics engine sequentially analyses the incoming streaming basic safety message reports based on the mobility parameters such as position, velocity, and acceleration, to instruct an RL algorithm for the detection of manoeuvring information manipulation. The algorithm exploits the intrinsic temporal and spatial inter-dependencies of the messages to detect the anomalous patterns due to the manipulation attack.
5. Upon detection of the manipulation attack, the decision engine provides the verdict to the security orchestrator to apply the pre-determined reactive security policy, i.e., manipulation data originated from the malicious vehicle to be filtered.
6. Security orchestrator enforces the appropriate security measure, i.e., filtering of the falsified manoeuvring information. The malicious vehicle is isolated and legitimate commands are sent back to the vehicles by the control centre.

3.4 UC 4: Isolation of Components over Virtualized Infrastructure

3.4.1 Problem Description & Aim

5G and B5G infrastructures will have to meet heterogeneous cybersecurity requirements (e.g., Cybersecurity Act[6], NIS directive[7] and regulations or standards related to 5G verticals like eHealth, Transport, Energy, Vehicular, industry under Seveso directive[8], etc.), and be able to dynamically (almost in real time) adapt. The simplest (state-of-the-art) strategy to implement everywhere the highest level of security is unrealistic. Some requirements may be even contradictory. Most vertical 5G use cases do not need the strongest possible security level. Thus, verticals will be reluctant to pay for services that they do not need and do not use. And maintaining such a security level for all network and service components requires enormous effort that increases the cost of service platforms in an unbearable manner.

The use case objective is to demonstrate an on-demand isolation service over the virtualized infrastructure and the delivery of evidence that the committed isolation is achieved for the critical components, under conditions agreed between parties. This use case resolves 2 major security issues:

- In a virtualized environment, under the state of the art, the requirement of isolation of critical services from basic services is not resolved and generally ends with the request to put in production dedicated physical infrastructure for these critical services (for instance a dedicated physical infrastructure to operate virtualised Lawful Interception services in communication networks). Formalizing these security requirements in terms of collocation constraints or level of criticality allows to support them using the placement optimization algorithm - the new way of orchestration of physical resources to serve the needs of deployed services (both critical and basic). This placement algorithm takes into account multiple

[6] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[7] https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[8] https://eur-lex.europa.eu/eli/dir/2012/18/oj

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

constraints including latency (e.g., for end-to-end slices) or energy consumption to compute the optimal orchestration over multi-site infrastructures.

- The commitment to isolate the critical services from the basic ones needs to be verifiable by users without direct physical access to the infrastructure. The Deep Attestation framework proposes an elegant way to resolve this issue using the method to measure this isolation agreed with the Client. In this specific use case, the Operator claims the services are isolated between each other regarding their affinity or criticality constraints and delivers the tool to collect on each physical server the information about placement of active services and their criticality level. The Deep Attestation framework collects this security properties on each requested server and protects each property (by digital signature) using the attestation scheme, the evidence that the affinity and anti-affinity conflicts have been resolved in the right way on each targeted server is delivered directly to the Client.

3.4.2 Actors and Roles

The actors and their roles involved in this UC are:

- Operator of Virtualized Infrastructure.
- Client / Vertical customer which requests isolation of its critical services.
- Trust Management with Deep Attestation Service which operates measurements to deliver evidence.
- Policy and SSLA Management with Placement Optimization System coupled with infrastructure Orchestration System.

3.4.3 Operational Flow of Actions

In the preliminary phase:

- Client has defined its network slice or chain of components to be deployed over the infrastructure.
- Client and Infrastructure Operator agree on the subset of Client's critical components, which need to be isolated from other components (third party) operated by Operator as stated in SSLA (Security Service Level Agreement).
- Client and Infrastructure Operator agree on the way to measure effectiveness of components isolation, based on tools proposed by Operator.

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

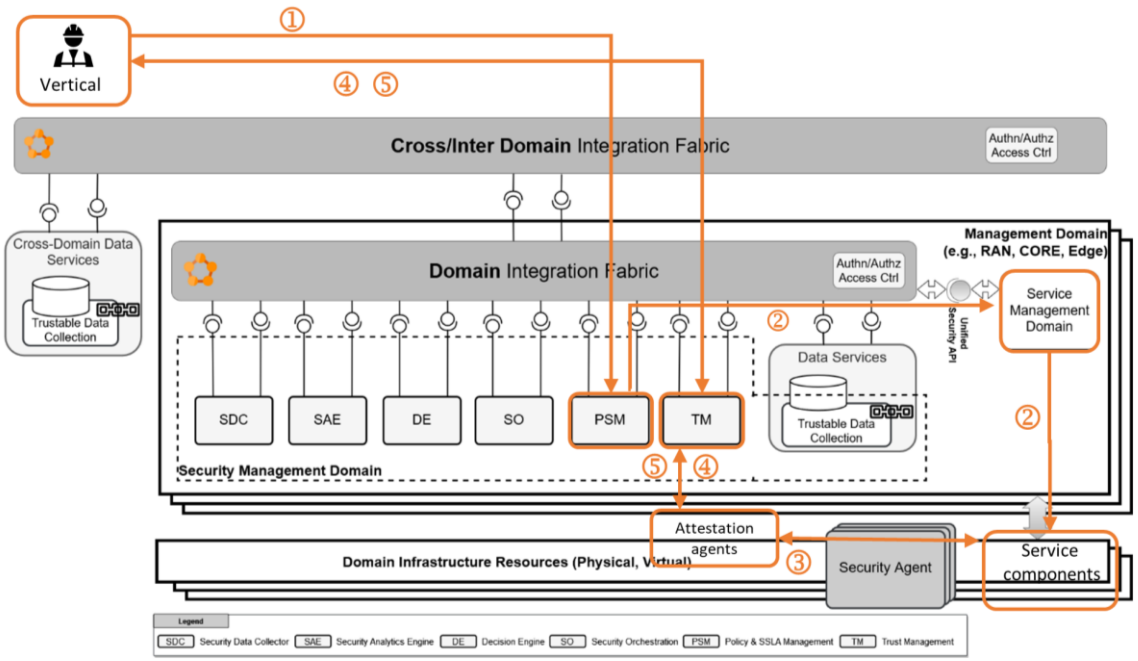

Figure 5 - UC4 operational flow of actions and HLA mapping.

As illustrated in Figure 5, UC4 includes the following sequence of actions:

1. Client issues a request to deploy its network slice or chain of components according to SSLA that is processed by PSM module.
2. PSM triggers deployment of components according to isolation request included in SSLA - in Service Management Domain, it performs components placement optimization with security constraints.
3. The isolation is measured by Attestation agents according to the agreed measurement method.
4. In the component operation phase Client may request delivery of evidence of isolation in an on-demand manner.
5. On each request the isolation is measured according to the agreed measurement method and the evidence of isolation is delivered to Client.

3.5 UC 5: End-to-End Slice Protection based on Moving Target Defense and Anomaly Detection

3.5.1 Problem Description & Aim

As mobile network operators (MNOs) go more decentralized with Multi-access Edge Computing (MEC) and virtualized with container-based and VM-based network functions, 5G and Beyond telecom networks are growing in complexity. Network slices become critical and challenging systems to protect due to their considerable attack surface. They can be attacked at the physical layer, starting with the infrastructure they are hosted in, or at the virtualization layer, targeting the virtual resources composing them, such as Network Services (NS), VNFs and Virtualisation Deployment Units (VDU). In order to protect all the different running network slices in large-scale infrastructures from the above-mentioned threats, the security management has to be automated, responsive, and adaptive to the various incidents.

UC 5 aims to improve the proactive and reactive protection of network slices. Firstly, the use case aims at collecting resource usage and network metrics through multiple points of the 5G network to assess

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

the network state in real-time and detect anomalies or security incidents such as intrusion and network attacks. Secondly, the use case aims at using MTD mechanism, which is to shift the NFV network components, for proactive and reactive protection. Proactively, this reduces the time window attackers have to collect intelligence on the network, organize an attack plan, and perform the attack. Ideally, it would become impossible to conclude such steps in the allowed time window. Reactively, MTD operations could be used to mitigate ongoing detected attacks such as Command and Control (C&C), DDoS, VNF tampering, and network slice compromises.

3.5.2 Actors and Roles

The actors and roles involved in this UC are:

- SDC: It provides an overview of the network state using probes and security functions dispersed over the infrastructure to collect monitoring data.
- SAE: It processes incoming data collected by the SDC to detect attacks, abnormal traffic flows, and to perform risks and threat assessments.
- DE: The Decision Engine provides the proactive and reactive security policies and operations to enforce, based on incoming security alerts and threat intelligence of the SAE.
- SO: It enforces the policies and operations of the DE in coordination with the SMD
- SMD: it deploys/updates the network slices following the enforced security policies and Network Slice Templates.

3.5.3 Operational Flow of Actions

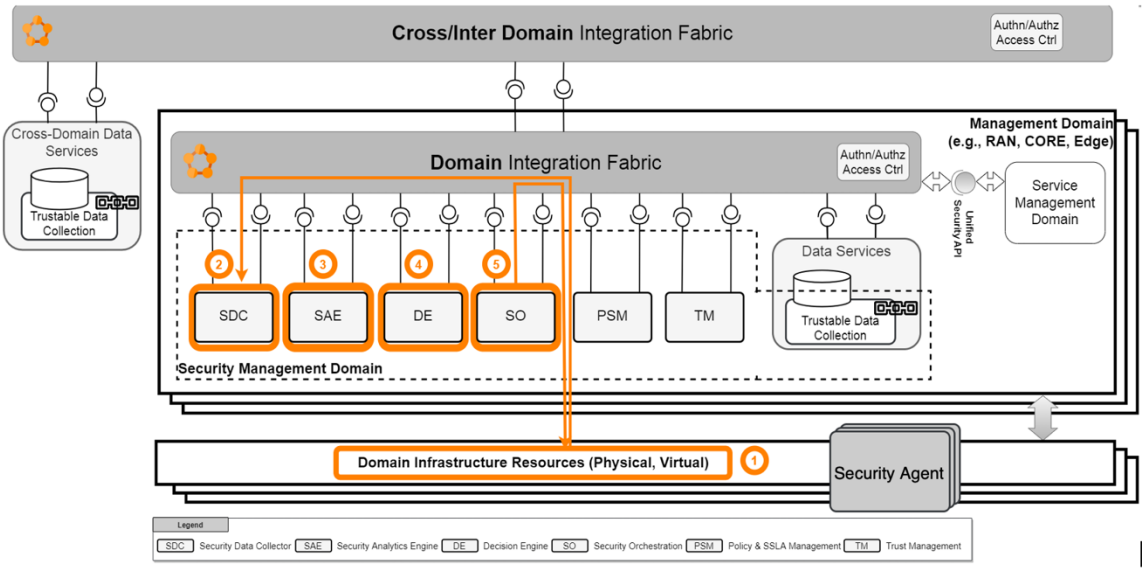

Figure 6 - UC5 operational flow of actions and HLA mapping.

The operational flow of actions of this security mechanism comprises five consecutive phases:

1. The probes at different locations of the Domain Infrastructure Resources level (as defined in the INSPIRE-5Gplus HLA architecture depicted in **Error! Reference source not found.**) collect monitoring data and send them to the SDC.
2. The SDC parses and processes the raw data, feeding them to the SAE.
3. Risk and threat models, as well as attack alerts from different anomaly and attack detection services in the SAE are generated from the SDC monitoring data and fed to the DE.

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

4. The DE decides a mitigation or a prevention MTD action, forwarded to the SO's MTD controller for enforcement.
5. The SO, using the MTD controller, coordinates at the SMD level the management and orchestration operations to enforce the MTD action in the relevant slice(s).

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

4 Conclusions

The acceleration of digital transformation is contingent not only on the fast and reliable connectivity promised by 5G and beyond networks, but also on making those networks secure and trustworthy. In this vein, INSPIRE-5Gplus project is delivering an innovative software-defined security orchestration and management framework that promotes the shift towards fully automated and smart security management for future connected systems and pervasive services. The framework's architecture enables zero-touch security services that provide protection, trustworthiness, and liability capabilities in managing 5G systems across multiple technological domains. The advanced security management vision enabled by INSPIRE-5Gplus framework is realized by leveraging on emerging technologies, including ZSM, AI/ML, DLT and TEE. The separation of security management concerns per domain and the adoption of service-based and SD-SEC models, allow INSPIRE-5Gplus framework to enable robust and sustainable security measures that can adapt to dynamic changes in threat landscape and security requirements in future mobile networks.

This white paper presented the evolved version of the overall INSPIRE-5Gplus framework's High-Level Architecture, describing its main functional blocks, the key security management services provided by the functional blocks and their role in enabling intelligent closed-loop security operations. Moreover, the white paper introduced a set of advanced security use cases to show how INSPIRE-5Gplus framework can be applied as a zero-touch security management solution for 5G systems. The security issues covered by the described UCs include attack detection over encrypted traffic, prevention of introspection attacks, automated assessment of SSLA fulfilment, misbehaviour detection in self-driving vehicular networks, on-demand and verifiable isolation of critical virtualized network functions, and proactive defence for E2E network slices. The described UCs promote different emerging technologies that can be leveraged to solve the security issues under consideration, namely the use of advanced ML techniques, TEE, MTD, and the new concept of "Deep Attestation" developed by INSPIRE-5Gplus as a mean to deliver verifiable security property measures.

INSPIRE-5Gplus is currently preparing three demonstrators to validate the proposed HLA through a set of representative 5G and beyond security UCs, including the ones described in this white paper. The three demonstrators Demo1, Demo2, and Demo3 aim at showcasing the automated instantiation of security management closed loops based on agreed SSLAs, the trust and liability management, and the use of MTD for proactive protection of network slices, respectively. To achieve this goal, the three demonstrators will integrate several security enablers developed in INSPIRE-5Gplus project, each of them providing the capabilities to implement one or several of the different identified HLA's services. It is worth mentioning that Demo1 is now accepted as an ETSI ZSM proof of concept (PoC), named "PoC #6: Security SLA assurance in 5G network slices"[9]. The accepted INSPIRE-5Gplus ETSI ZSM PoC has recently been publicly demonstrated in the last ETSI Security Conference 2022[10].

[9] https://zsmwiki.etsi.org/index.php?title=PoC_6_Security_SLA_assurance_in_5G_network_slices.
[10] https://docbox.etsi.org/Workshop/2022/10ETSISECURITYCONFERENCE/10_SECURITY_RESEARCH/

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

5 References

[1] 5G IA. *European Vision for the 6G Network Ecosystem*. White Paper, Version 1.0, June 2021.

[2] 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.

[3] R. Asensio, C. Benzaid, P. Alemany, D. Ayed, M. Christopoulou, C. Dangerville, G. Gür, V. Hoa La, V. Lefebvre, E. Montes de Oca, R. Muñoz, H. Nguyen, M. Nguyen, J. Ortiz, A. Pastor, P. Porambage, G. Santinelli, W. Soussi, T. Taleb, R. Vilalta, A. Zarca. *White Paper: Evolution of 5G Cyber Threats and Security Solutions*. INSPIRE-5Gplus, Mar. 2022.

[4] ETSI GS ZSM 002. *Zero-touch Network and Service Management (ZSM); Reference Architecture*. August 2019.

[5] A. M. Zarca, J. B. Bernabe, R. Trapero, D. Rivera, J. Villalobos, A. Skarmeta, S. Bianchi, A. Zafeiropoulos, P. Gouvas. Security management architecture for NFV/SDN-aware IoT systems. *IEEE Internet of Things Journal*, *6*(5): 8005-8020, 2019.

[6] C. Benzaid and T. Taleb. AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?. IEEE Network Magazine, Vol. 34, No. 6, Nov. 2020, pp. 140 - 147.

[7] R. Sedar, C. Kalalas, F. Vázquez-Gallego and J. Alonso-Zarate, "*Reinforcement Learning Based Misbehavior Detection in Vehicular Networks*. In Proc. of IEEE International Conference on Communications (ICC), May 2022, pp. 3550-3555.

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

6 List of Abbreviations

5G-PPP	The 5G Infrastructure Public Private Partnership
ACID	Atomicity, Control, Isolation, Durability
AI	Artificial Intelligence
API	Application Programming Interface
B5G	5G and Beyond
C&C	Command and Control
CN	Core Network
CRUD	Create, Read, Update and Delete
DBMS	Database Management System
DE	Decision Engine
DLT	Distributed Ledger Technology
DNS	Domain Name System
DPI	Deep Packet Inspection
E2E	End-to-End
GPS	Global Positioning System
GTP	GPRS Tunnelling Protocol
HLA	High Level Architecture
HSPL	High-Level Security Policy Language
IF	Integration Fabric
JSON	JavaScript Object Notation
LASM	Liability-aware Security Manager
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
MUD	Manufacturer Usage Description
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
NOC	Network Operations Center
NS	Network Service
ONAP	Open Network Automation Platform
oPoT	ordered Proof of Transit
OSM	Open Source MANO

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties

OTT	Over the Top
PoC	Proof of Concept
PSM	Policy and SSLA Management
RAN	Radio Access Network
RCA	Root Cause Analysis
RL	Reinforcement Learning
SA	Security Agent
SAE	Security Analytics Engine
SBA	Service-Based Architecture
SD-SEC	Software Defined Security
SDC	Security Data Collector
SDN	Software Defined Network
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMD	Security Management Domain
SO	Security Orchestrator
SOC	Security Operations Center
SPAN	Switched Port Analyzer
SSLA	Security Service Level Agreement
STA	Smart Traffic Analyzer
STIX	Structured Threat Information eXpression
TAP	Terminal Access Point
TEE	Trusted Execution Environments
TLS	Transport Layer Security
TM	Trust Management
TOSCA	Topology and Orchestration Specification for Cloud Applications
TRAILS	sTakeholder Responsibility, Accountability and Liability deScriptor
TRM	Trust and Reputation Manager
UC	Use Case
UDP	User Datagram Protocol
VDU	Virtualization Deployment Unit
VNF	Virtualized Network Function
VSF	Virtual network Security Function
ZSM	Zero-touch network and Service Management

© 2019 - 2022 INSPIRE-5Gplus Consortium Parties