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

INSPIRE-5Gplus

INtelligent Security and PervasIve tRust for 5G and Beyond

D2.3: Final Report on Advanced 5G Security Use Cases

Version: v1.0

Deliverable type	R (Document, report)
Dissemination level	PU (Public)
Due date	30/04/2022 (M30)
Submission date	06/05/2022
Lead editor	Rafał Artych(OPL)
Authors	Rafał Artych, Aleksandra Podlasek (OPL), Pawani Porambage, Suwani Jayasinghe, Nisita Weerasinghe, Tharaka Mawane Hewa, Yushan Siriwardhana, Madhusanka Liyanage, Mika Ylianttila, Chafika Benzaid, Tarik Taleb (UOULU), Pol Alemany, Ricard Vilalta, Raul Muñoz, Charalampos Kalalas, Roshan Sedar (CTTC), Ghada Arfaoui (ORA), Orestis Mavropoulos (CLS), Antonio Pastor, Hugo Ramon (TID), Rodrigo Asensio, Alejandro Molina, Noelia Perez (UMU), Maria Christopoulou (NCSRD), Wissem Soussi, Onur Kalinagac, Gürkan Gür (ZHAW), Edgardo Montes de Oca, Vinh Hoa La (MI)
Reviewers	Vincent Lefebvre, Antonio Pastor, Geoffroy Chollon,
Work package, Task	WP2, T2.4
Keywords	Security Enablement, 5G Security Use Cases, ZSM HLA

Abstract

This deliverable presents the final set of security use cases stemming from new and enhanced 5G security and trust/liability enablers developed in INSPIRE-5Gplus project. Described use cases were prepared with emphasis on presenting the cooperation of enablers delivered by different Project partners within proposed High-Level Architecture and were selected to cover the vast majority of targeted enablers. Finally, the set of use cases is analysed with respect to 5G security needs, emerging security enabling technologies and envisioned 5G security test cases.

Document revision history

Version	Date	Description of change	List of contributor(s)
v0.1	29/03/22	Initial version	All Authors
v0.2	07/04/22	New identificators and use case ordering, Section 2 updated, Chapter 3 completed	All Authors
v0.3	08/04/22	For internal review	Vincent Lefebvre, Antonio Pastor, Geoffroy Chollon,
v0.4	14/04/22	Updates according to reviewer remarks	All Authors
V0.9	27/04/22	Editorial corrections	Rafał Artych
V0.91	27/04/22	Final editing, version for GA approval	Uwe Herzog, Anja Köhler
V1.0	06/05/22	Executive Summary and list of abbreviations updated. Submitted.	Rafał Artych, Uwe Herzog

List of contributing partners, per section

Section number	Short name of partner organisations contributing
Section 1	OPL, UOULU
Section 2	AALTO, UOULU, OPL, CTTC, UMU, TID, MI, ORA, NCSRD, ZHAW, TAGES, TSG
Section 3	OPL, CLS, CTTC, UMU, TID, ORA, ZHAW
Section 4	OPL

Disclaimer

Acknowledgment

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

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

Executive Summary

This deliverable discusses the final set of security use cases that serve to demonstrate the potential of new and enhanced 5G security and trust/liability enablers developed in INSPIRE-5Gplus project. The set includes 23 use cases related to both generic 5G Platforms and specific verticals (investigated by other projects within 5G-PPP).

Whereas security use cases describe scenarios how specific security problems can be addressed using assets based on enabling technologies considered in the project, test cases will be devoted to integration and validation of selected use cases in real environment. Thus, use cases are focused rather on showing what enablers are needed and how they can cooperate to tackle identified security gaps or enhance the security and liability of 5G and beyond systems and services.

Use cases describe how current trends and enabling technologies like Automation and Zero-touch Service Management, Trusted Execution Environments, Artificial Intelligence and Machine Learning, Distributed Ledger Technologies, advanced cybersecurity techniques (security monitoring optimization, Cyber Threat Intelligence and data sharing, Security and Service Level Agreements), Dynamic Liability and Root Cause Analysis can be used and often combined together to address particular security problems.

For each use case the description includes:

- the presentation of the context and the relevant security problem addressed by the use case;
- the Identification of actors - the roles of the user, system or equipment;
- the sequence of events covering preparation, execution and closing of the use case with the diagram of the basic flow;
- achieved goals;
- the summary indicating how the use case fits into the architecture proposed in the INSPIRE-5Gplus.

Described use cases were prepared with emphasis on presenting the cooperation of enablers delivered by different Project partners within proposed High-Level Architecture of the INSPIRE-5Gplus security management framework and were selected to cover the vast majority of targeted security enablers. Enablers are presented in particular usage scenarios but often they may find the use in other application areas or domains of mobile systems. Details of enablers and security management framework are documented in other INSPIRE-5Gplus deliverables and publications.

In addition, use cases were analysed with respect to identified previously 5G security needs, emerging security enabling technologies considered in the project and the relation to 5G assets being the subject of security problems.

As the analysis shows presented uses cases cover most of the technology domains addressing the security gaps identified previously by INSPIRE-5Gplus.

Use cases included in the deliverable refer to various 5G usage scenarios and security problems occurring within entire system starting from mobile devices through network components and underlying technologies (like Network Slicing or virtualization) ending in end-to-end services and security assets needing protection. Since INPIRE-5GPlus security enablers and mechanisms can be applied to various domains, use case are often relevant to even more than one 5G asset group.

Finally, the references of use cases to demonstrations validating selected security assets in the real environment are pointed out. Considered demo scenarios are based on presented use cases and show possible integrations of enablers into comprehensive solutions.

Table of Contents

List of Figures

List of Tables

Abbreviations

5G-AKA	5G Authentication and Key Agreement
5G-PPP	5G Infrastructure Public Private Partnership
5G NSA	5G Non-Stand Alone
5G SA	5G Stand Alone
ACCA	Anticipated Cooperative Collision Avoidance
ACST	Advanced CyberSecurity Techniques
AF	Application Function
AI	Artificial Intelligence
AMF	Access and Mobility Management Function
B5G	Beyond 5G
BS	Base Station
C&C	Command and Control
CCAM	Cooperative, Connected, and Automated Mobility
CN	Central Node
CCT	Component Certification Tool
(D)DoS	(Distributed) Denial of Service
DL	Dynamic Liability
DLT	Distributed Ledger Technology
DPI	Deep Packet Inspection
DTwC	Digital Trustworthy Certificate
eMBB	enhanced Mobile Broadband
ETA	Estimated Time of Arrival
ENISA	European Union Agency for Cybersecurity
FL	Federated Learning
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
HSPL	High-level Security Policy Language
ICS	Information and Communication Systems
IDS	Intrusion Detection System
IoT	Internet of Things
KPI	Key Performance Indicators
LASM	Liability-Aware Service Manager
LOS	LASM Ontology Service
LRS	LASM Referecing Service
MANO	Management and orchestration
MEC	Multi-access Edge Computing
MIP	MEC Infrastructure Provider

ML	Machine Learning
MLP	Multi-Level Perceptron
mMTC	massive Machine Type Communications
MNO	Mobile Network Operator
MOTDEC	Moving Target Defense Controller
MPS	Mobile Positioning System
MSP	MEC Service Provider
MTD	Moving Target Defense
MMT	Montimage Security Monitoring Framework
MUD	Manufacturer Usage Description
NFV	Network Function Virtualisation
NFVI	NFV Infrastructure
NOC	Network Operation Centre
NSM	Network Slice Manager
NST	Network Slice Template
NWDAF	Network Data Analytics Function
OAM	Operations, Administration and Maintenance
OBU	On-Board Unit
oPoT	Ordered Proof of Transit
OptSFC	Optimizer for security functions
PoI	Policy Management
PNF	Physical Network Function
RA	Remote Attestation
RAN	Radio Access Network
RCA	Root Cause Analysis
RSU	Road-Side Units
RT-SSLA	Real-Time Security Service Level Agreement
SBA	Service Based Architecture
SD-SEC	Software Defined Security
SDN	Software Defined Networks
SDR	Software Defined Radio
SF	Security Functions
SFSB	Federated Slice Brokering
SLA	Service Level Agreement
SMD	Security Management Domain
SMF	Session Management Function
SOC	Security Operation Centre
SLA	Service Level Agreement
SLP	Slice Provider

SSLA	Security Service Level Agreement
STA	Smart Traffic Analyzer
TEE	Trusted Execution Environment
TC	Test Case
TRM	TrustManager
TRAILS	sTakeholder Responsibility, Accountability and Liability deScriptor
TSLA	Trust Service Level Agreement
UAV	Unmanned Aerial Vehicle
UC	Use Case
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
URLLC	Ultra-Reliable Low Latency Communication
V2X	Vehicle to Everything
V2XMisDet	Lightweight and Space-efficient vehicle authentication enhanced with misbehaviour detection
VNF	Virtual Network Function
vOBU	virtual On-Board Unit
VSF	Virtual Security Function
ZSM	Zero touch network & Service Management

1 Introduction

1.1 Scope

INSPIRE-5Gplus objective is the advancement of security vision for 5G and Beyond through the adoption of emerging trends and technologies, and providing assets and models to address some of remaining and newly arising security challenges for various 5G usage scenarios.

This deliverable discusses the final set of 5G security use cases (UCs) that serve to demonstrate the potential of targeted security assets and trust/liability mechanisms. The set includes use cases related to both generic 5G Platforms and specific verticals (investigated by other projects within 5G-PPP).

After description of each use case in one unified manner, the set of use cases is analysed with respect to 5G security needs, emerging security enabling technologies and envisioned 5G security test cases.

1.2 Target audience

The target audience of this deliverable are stakeholders, industry and academic working groups interested in security of 5G technologies and infrastructure especially how new assets and models can address various 5G security challenges. While use cases discussed hereafter present how specific security problems can be addressed using INSPIRE-5Gplus security assets and trust and liability mechanisms, details of employed enablers can be found in respective deliverables of Work Package 3 (WP3)[1] [2] [3] and Work Package 4 (WP4)[4] [5].

1.3 Methodology

The work on use cases has started in INSPIRE-5Gplus project's Work Package 2 (WP2) in parallel with the conceptualization of INSPIRE-5Gplus' High-Level Architecture and development of security assets and mechanisms in WP3 and WP4.

Security use case serve to demonstrate how specific security problems can be addressed using assets based on enabling technologies considered in the project, whereas test cases are devoted to integration and validation use cases in real environment. The deliverable D2.2 [6] provided the initial list of illustrative use cases and their relationship with the emerging enabling technologies. This initial set was also used to select the group of test cases described in D5.1[8]. With the progress of work in WP2, WP3 and WP4 the initial list was extended with new use cases in order to present the whole potential of envisaged security assets and trust and liability mechanisms.

Presented use cases were developed with emphasis on showing the cooperation of enablers delivered by different Project partners within proposed High-Level Architecture and were selected to cover the vast majority of targeted enablers. In consequence the broad set of use cases form the foundation for further validation and demonstration of selected security assets in the real environment.

Use cases refer to various 5G usage scenarios and security problems located in various domains of 5G System. In order to facilitate the reading, they are grouped together by 5G components they are related to.

1.4 Structure

The main part of the deliverable - Section 2 is devoted to description of use cases that demonstrate how INSPIRE-5Gplus enablers can be applied to solve security problems (threats) related to 5G assets.

Section 3 summarizes Use Cases with respect to security requirements, enablers and INSPIRE-5Gplus demonstrations under development.

Section 4 concludes this deliverable.

1.5 Reference Architecture - INPIRE-5Gplus HLA

To facilitate the understanding of the UCs description and their mapping to the HLA of the INSPIRE-5Gplus security management framework, we briefly describe the main components of the HLA in what follows. The interested readers may refer to D2.2 [6] and D5.1 [8] for more details on the HLA functional blocks.

As depicted in Figure 1, the INSPIRE-5Gplus framework HLA is split into Security Management Domains (SMDs) to support the separation of security management concerns (e.g., for the Radio Access Network RAN, Edge or Core Network). Each SMD is responsible for intelligent security automation of resources and services within its scope. The E2E SMD is a special SMD that manages security of E2E services (e.g., network slice) that span multiple domains. The E2E SMD coordinates between domains using orchestration. The decoupling of the E2E security management domain from the other domains allows to escape 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, including:

- **Security Data Collector (SDC)**, which aims 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).
- **Security Analytics Engine (SAE)**, which derives 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.
- **Decision Engine (DE)**, which 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.
- **Security Orchestration (SO)**, which 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.
- **Policy and SSLA Management (PSM)**, which transforms the abstract Protection Level and Security Level requirements and constraints expressed by consumers and providers into specific parameters that indicate, to the SO, the security services to configure, deploy and manage.
- **Trust Management (TM)**, which provides various services for the trust related functions, such as trust reputation calculation, component certification, and Ordered Proof of Transit (oPoT).

The various security management services provided by these modules are exposed within the same domain but also cross-domain, to the authorized consumers, through an integration fabric. Data Services allow the different security services to persist data that can be shared in one or more domains.

The functional modules operate in an intelligent closed-loop way to enable AI-driven software defined security (SD-SEC) orchestration and management in compliance with the expected Security Service Level Agreement (SSLA)[6] and regulatory requirements. By adopting service-based and SD-SEC models, INSPIRE-5Gplus framework allows to build up sustainable security measures that can adapt to dynamic changes in threats landscape and security requirements in next-generation mobile networks.

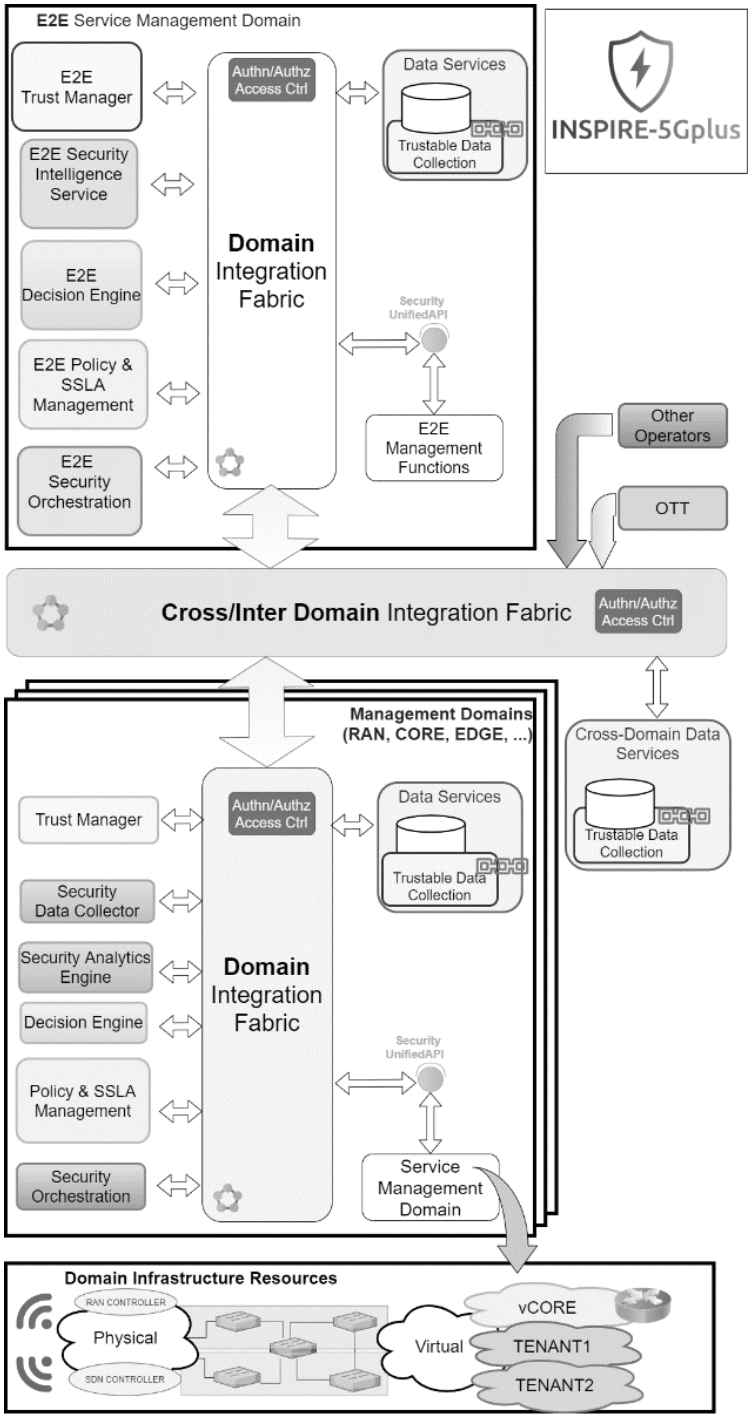

Figure 1: INSPIRE-5Gplus Framework HLA

2 INSPIRE-5Gplus Use Cases

2.1 UC A - Detection and Mitigation of GNSS (e.g., GPS) Spoofing Attack

2.1.1 Problem description

Network slicing and management rely on the characteristics of user equipment (UE) mobility pattern and UE density. Such systems need the UE to report its location information to allocate the communication resources to a certain area. Nowadays, the global navigation satellite system (GNSS), specifically GPS, is the primary location technology used by UE due to its global coverage and accuracy. However, the unencrypted civil GPS signals are inherently vulnerable to spoofing attacks. Indeed, an attacker can use low-cost software defined radio (SDR) tools, such as USRP, to generate fake GPS signals to fool the GPS receiver into calculating false positions. Thus, without an accurate verification of the position claimed by a UE in attack conditions, the network may be deceived into migrating services to a wrong place, which may prevent the UE to access the services they need timely and effectively. As illustrated in Figure 2, a GPS spoofer can mislead the target aerial UE (UAV or Drones) to deviate from the planned path by sending the fake GPS signals to UE, which leads to deploying the network services to the wrong place (e.g., edge server) and wasting network resources.

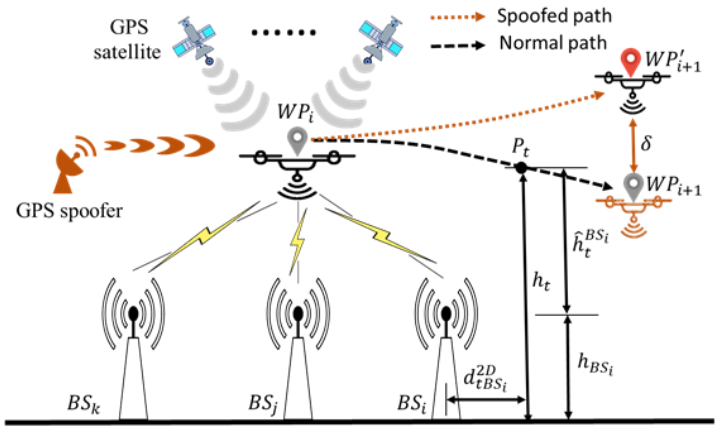

Figure 2: UC A scenario [3]

2.1.2 Goals

The goal of UC A is to introduce machine learning (ML) methods into the edge servers for checking the authenticity of the GPS position reported by a UE. Specifically, the proposed method leverages the theoretical path losses difference computed based on the GPS positions and the radio signal path losses collected by the BS to indicate the integrity and authenticity of the planned and real-time UE trajectory. In addition, a deep learning model, namely Multi-Level Perceptron (MLP), is introduced to the edge server in order to find the dynamic thresholds and verify the authenticity of the UE GPS information. If a GPS spoofing is detected, the edge server can contact the UAV ground control station to request to land the drone, and release network resources once spoofing confirmed. The goal is to make sure that the network resources are deployed into the needed area and avoid resources wasting.

2.1.3 Actors

The actors and roles involved in this UC are:

- A set of aerial UE (e.g., UAVs or drones)
- A GPS spoofer
- Mobile Network Operator (MNO)

- the Multi-access Edge Computing (MEC) servers and base stations

2.1.4 Preconditions

To demonstrate the anti-GPS spoofing use case, the Mobile Positioning System (MPS) service is required to be accessed in the edge server to provide the real time path loss between a base station and a UE. Additionally, the GPS location of UE needs to be also available in the edge server for computing the theoretical path loss.

2.1.5 Basic flow

The basic flow, using UAV as example of UE, consists of the following steps:

1. Service Deployment: The MNO, remotely controlling a set of drones, sends the flight missions to drones including the mission type and starting and ending GPS positions.

2. Service Running: Upon receiving the mission, UAV follows the flight route and periodically broadcast its telemetry data, including GPS position, over the air for collision avoidance and airspace enforcement.

3. Attack Begin: The GPS spoofer generates fake GPS signals to make UAV deviate from the planned trajectory.

4. Spoofing Detection: Collected by the nearby base stations, the position information is augmented with the uplink RSS measurements that enable the edge server to use ML learning models to cross-check that the GPS position provided by the UAV is not spoofed.

5. Attack Mitigation: When a GPS spoofing is detected, a warning is sent by edge server to the MNO that decide to redeploy or cancel the service.

2.1.5.1 Diagram

Figure 3 illustrates the basic flow of UC A.

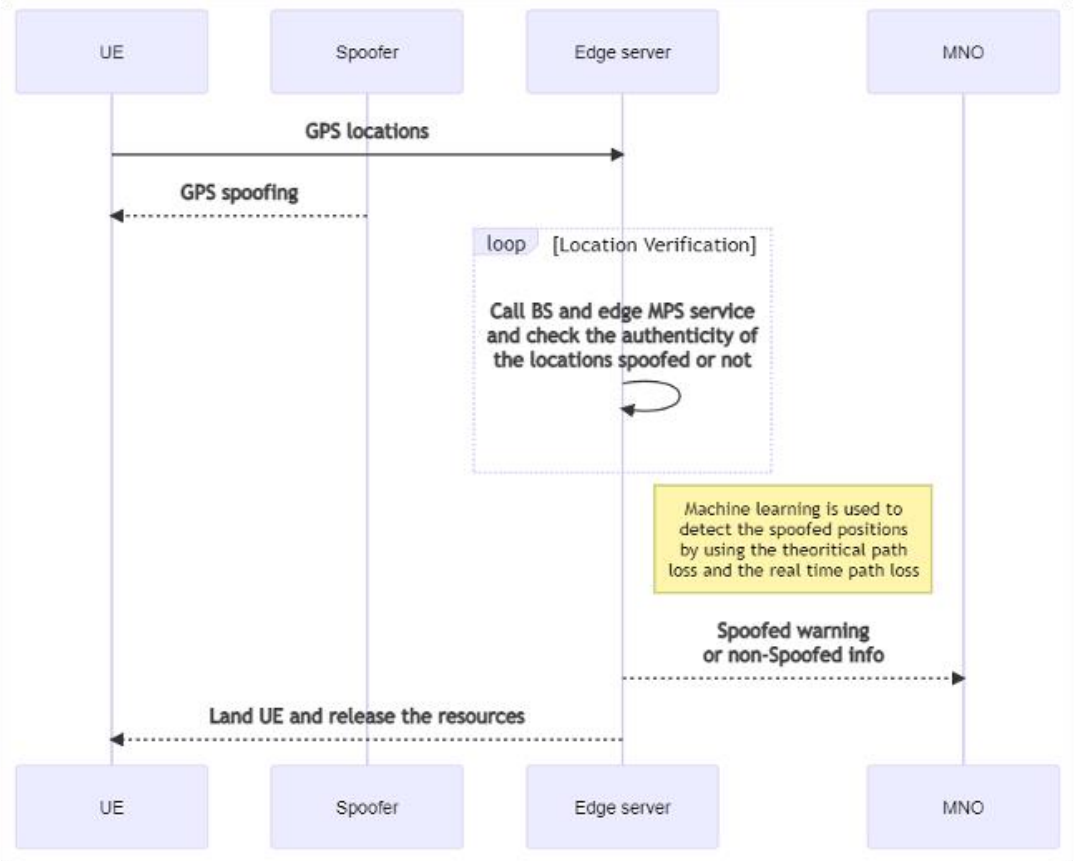

Figure 3: Basic flow of UC A

2.1.6 Post conditions

The spoofed GPS positions are effectively detected at the edge, allowing precise location of the radio network slice serving the UE.

2.1.7 Success criteria

The spoofed GPS positions are successfully detected using the theoretical path losses for the planned path and the real-time path losses obtained from BSs.

2.1.8 Use case summary

2.1.8.1 Mapping on INSPIRE-5Gplus architecture

As depicted in Figure 4, the UC involves the “Security Data Collector” to collect telemetry (including GPS positions) reported by the UE (e.g., UAV) and the path loss measurements reported by the base stations. The collected data are forwarded to the “Security Analytics Engine”, which uses ML techniques to detect the spoofed positions by using the theoretical path loss inferred from the reported positions and the real-time path losses received from the base stations. If a spoofing is detected, an alert is sent to the “Decision Engine” for further mitigation actions.

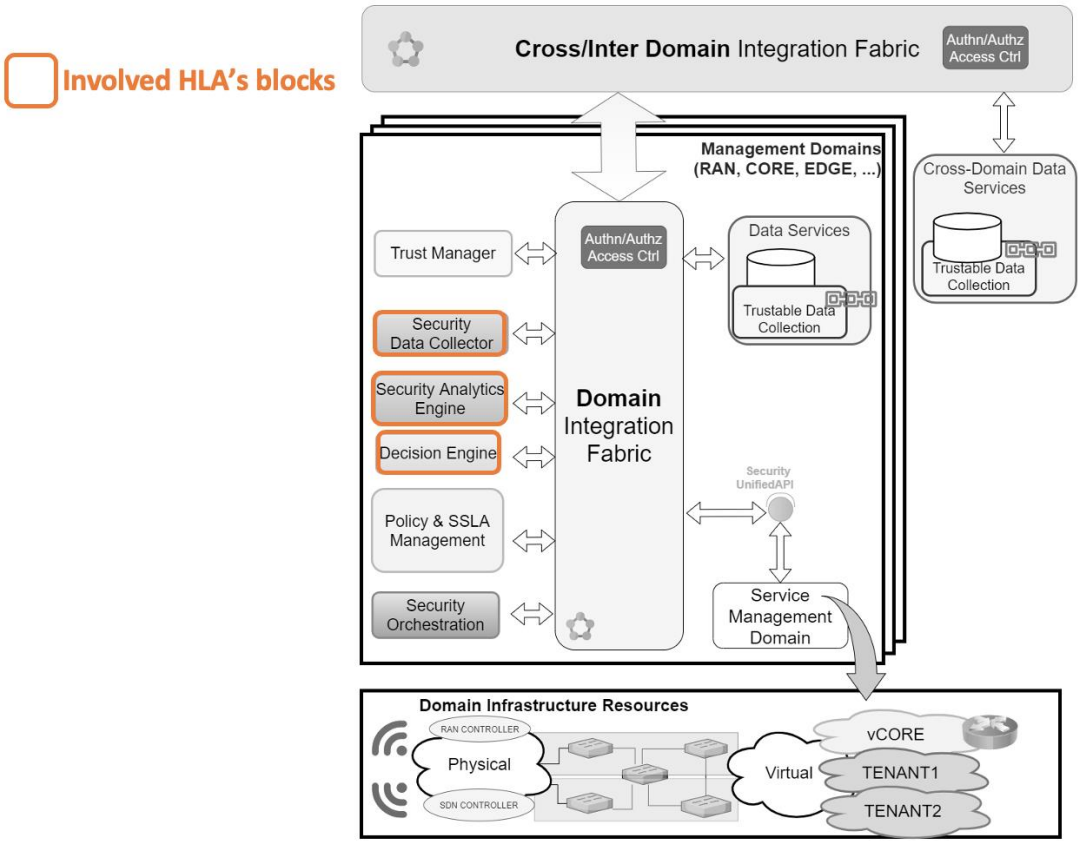

Figure 4: UC A mapping to INSPIRE-5Gplus HLA

2.1.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Anti-GPS Spoofing enabler
- Security Data Collector
- Security Analytics Engine
- Decision Engine

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.2 UC B - Federated Learning based Anomaly Detector for 5G networks

2.2.1 Problem description

It is possible to detect security threats by inspecting the network flows and has been used for applications such as firewalls and IDS. It is believed that better results can be gained by analysing the network flows using machine learning or artificial intelligence-enabled tools. But it should be done so that user privacy is preserved while adhering to many other operational constraints, such as privacy regulations and resource constraints.

Therefore, the proposed anomaly detector uses federated learning for training the model that is used for detection. Federated learning allows training models on local devices that can be aggregated on a server located elsewhere in the network without gathering network flows. The hierarchical system proposed here consists of two stages. The first stage consists of a set of anomaly detectors which are served by an aggregation server placed in the domain security service of each domain. Each anomaly detector consists of a model and a data base apart from the detector. The data marked as normal from the stage 1 anomaly detectors will be sent to the stage 2 anomaly detector. The stage 2 anomaly

detector is developed such that it has more functionalities and an ability to classify the data than stage 1. Only the network flow that is labelled as normal will be allowed to continue to its destination by the stage 2 anomaly detector. If any anomaly is undetected and interrupts the network operations, the models will be retrained to prevent similar incidents in the future.

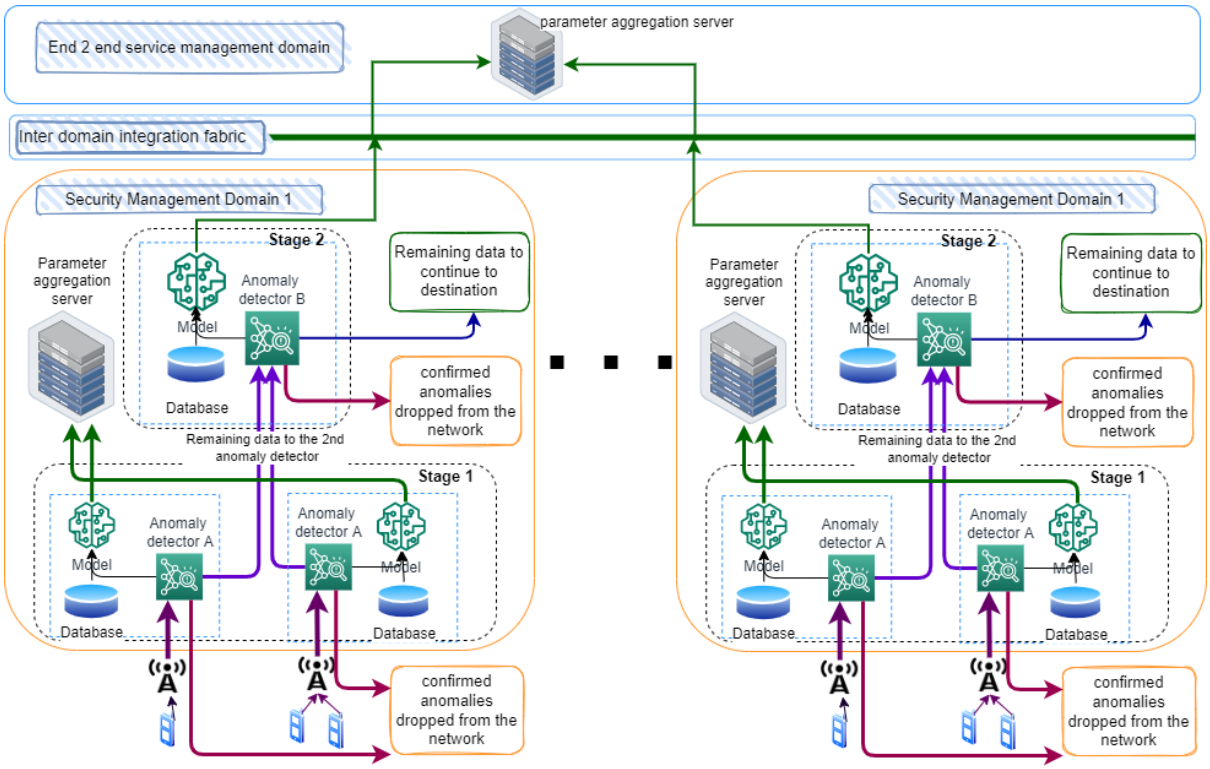

Figure 5: UC B - federated learning-based anomaly detector

2.2.2 Goals

The main objective of the proposed anomaly detector is to successfully defend the network against possible security attacks. The hierarchical system placed inside the network will analyze the network flow and categorize it as an anomaly or not in 2 stages. It is expected to defend the network with sufficient accuracy so that the performance expectations are fulfilled. While it is expected to fully defend against known attacks, the system should have the capability to respond to unprecedented events as well.

The proposed anomaly detectors train their detection models on the devices with local data. One significant problem with training the anomaly detectors with federated learning is that they are vulnerable to poisoning attacks. If an anomaly detector is trained using poisoned data or poisoned model supplied by the federated learning participants, the detector (in this case this can also be a security function) is not capable of functioning with a higher accuracy.

This arises the need of the anomaly detection models to be robust against the poisoning attacks. The robust FL algorithms should be able to remove the effect of the poisoning attacks from the system, keep only the model updates from legitimate users, and learn only from those updates, which are a must for proper functioning.

2.2.3 Actors

The actors and roles involved in this UC are:

- E2E domain orchestrator
- Security domain orchestrator
- security analytics service
- Anomaly detectors
- Aggregation servers

2.2.4 Preconditions

The anomaly detectors use federated learning-based models. In a federated learning life cycle, an engineer selects the model that suits the requirement. Therefore, it is expected that before starting the service, a suitable model will be selected by the responsible authorities. Also, the model should be trained with network flows that sufficiently cover possible scenarios expected in the network in both normal and abnormal events.

2.2.5 Basic flow

The basic mechanism can be divided into 2 types: a detection mechanism and a training mechanism. Both are described below, starting with the training mechanism. The training mechanism should take place at the beginning of the mechanism implementation and when the security threat or similar event that interrupts the service is undetected by the anomaly detectors.

- The aggregation server communicates the model to be trained to the model of each detector in stages 1 and 2.
- A model placed at each detector trains the given model with available data and communicates it back to the aggregation server.
- The servers aggregate the parameters with predefined criteria and send it to the model again for training.
- After training the model for several rounds, the aggregation server will send the parameters for detection to the anomaly detector.

The detection flow will take place as below.

- Network flow will be directed through the stage 1 anomaly detector where it will be classified as an anomaly or not. Anomaly traffic will be dropped and traffic classified as normal traffic will be directed to stage 2.
- Stage 2 detectors will classify network flow again, and network flow classified as normal will be directed to the destination, while others will be dropped from the network.

2.2.5.1 Diagram

While there are 2 flows in the basic flow section, the detection flow is simple and clearly depicted in Figure 5. Therefore, Figure 6 and Figure 7 show only how the training flow is taking place. When an anomaly is detected, the security analytic engine will inform the E2E orchestration engine and Stage 1 aggregation server. Figure 6 and Figure 7 depict the flow after the message from the security analytic engine is received by the aggregation server and E2E orchestration engine, respectively.

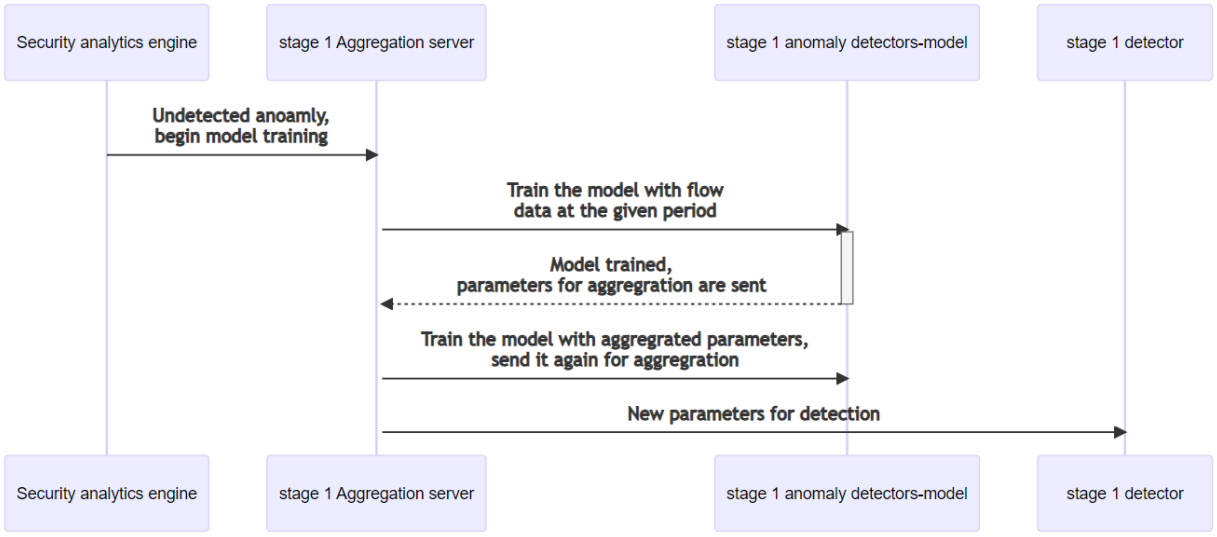

Figure 6: Flow for training-security analytic engine notifies stage 1 aggregation server

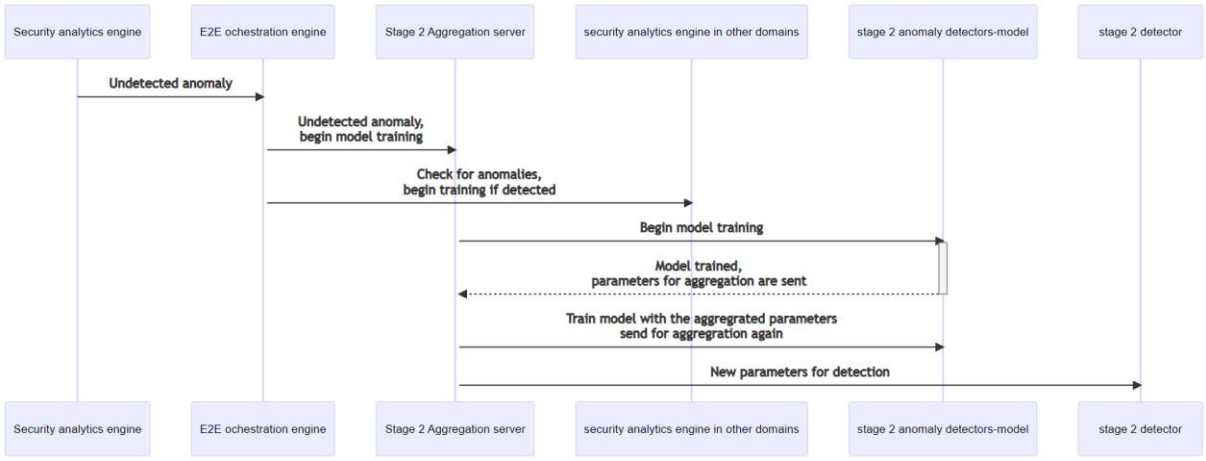

Figure 7: Flow for training-security analytic engine notifies E2E orchestration engine

2.2.6 Post conditions

All the detectors will be updated at the end of the training phase with the new model parameters. The database of each detector will be updated.

2.2.7 Success criteria

The anomaly detection mechanism is considered successful if almost all anomaly traffic is dropped from the network and no normal traffic is detected as anomalous. I.e., there are no false positives or false negatives in the output of the network. Also, if a new anomaly continues to travel to its destination undetected, all detector models, databases, and network flows need to be updated so that the event does not interrupt network operations. After deploying the proposed mechanism, the network should be able to continue operations without interruptions in the event of an anomaly or likely event.

2.2.8 Use case summary

A federated learning-based tool is proposed to detect anomalies in the ZSM architecture and it consists of 2 stages. The two main basic flows include training the model and detecting service. The proposed system uses components such as a security analytic engine and security data collection services to successfully operate.

2.2.8.1 Mapping on INSPIRE-5Gplus architecture

The proposed flows require artificial intelligence and network flow related data. Therefore, it is more associated with the security data collector and security analytic engines of each domain.

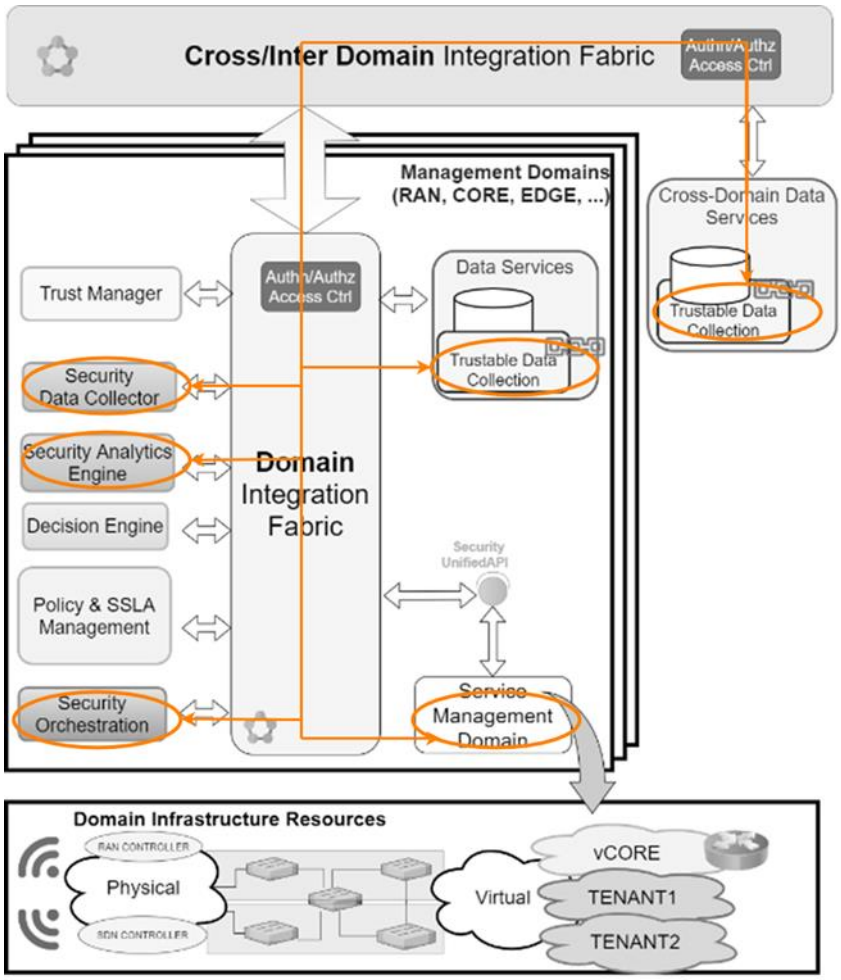

Figure 8: UC B mapping to INSPIRE-5Gplus HLA

2.2.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Robust Federated Learning Security
- Security Data Collector
- Security Analytics Engine
- Security Orchestrator

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.3 UC C - Root Cause Analysis based on similarity learning

2.3.1 Problem description

Generally, in Information and Communication Systems (ICS) and particularly in 5G-based systems, it is frequent that failures are recurrent. The system administrators, who have some experience dealing with failures, can react more quickly and efficiently against their recurrence. The mitigation actions (e.g., reset a particular server every night) can be thus taken promptly. However, this human-based troubleshooting task becomes a lot more challenging, time consuming or even impossible in complex systems. Especially due to the fact that failures usually propagate through causal chains and produce evolving fingerprints of noisy symptoms. This leads to the need of an automated tool helping humans troubleshoot a system to group events that are causally connected and keep unrelated events separated). Achieving this is often not straightforward since components of a system can exhibit similar symptoms of two unrelated failures.

2.3.2 Goals

In this section, we introduce the use case concerning the RCA tool based on machine learning that takes into account the highly granular monitoring indicators (e.g., statistics and data extracted from the logs, metrics, network traffic, and any data that could identify the system state) and the deep analysis to assess the similarity of a newly observed event reflecting the current status of the system and each learned one saved in the historical database. RCA enables systematizing the experience in dealing with incidents to build a historical database and verify whether a newly detected incident is similar enough to an observed one with known causes. Thanks to RCA's suggestions, remediation actions could be timely and wisely taken to prevent or mitigate the damage of the recurrence of problems.

More precisely, the partners will deploy an IoT network representing an Industrial Campus. MMT is used to monitor this network by analysing the traffic and different hardware-related indicators (e.g., CPU usage, memory usage, battery level, power consumption, CPU temperature, etc.) captured by one or several dedicated sniffers and offer two principal features:

- Anomaly detection (e.g., node failure, malformed packet, modified traffic, misbehaviour of compromised or intrusive devices, attacks, etc.)
- Machine Learning-based Root-cause Analysis to determine the cause of the detected anomalies

RCA allows making sure that the alarm is not a false positive and serves to identify what was the cause (e.g., device malfunction or attack), and also identify if there are attacks (e.g., DoS attacks) that could prevent the true positive (e.g., fire detection) from occurring. In case of doubt, additional slice and service can be deployed by the orchestrator to verify if it is a false positive or true negative (e.g., activate a video camera to obtain visual information).

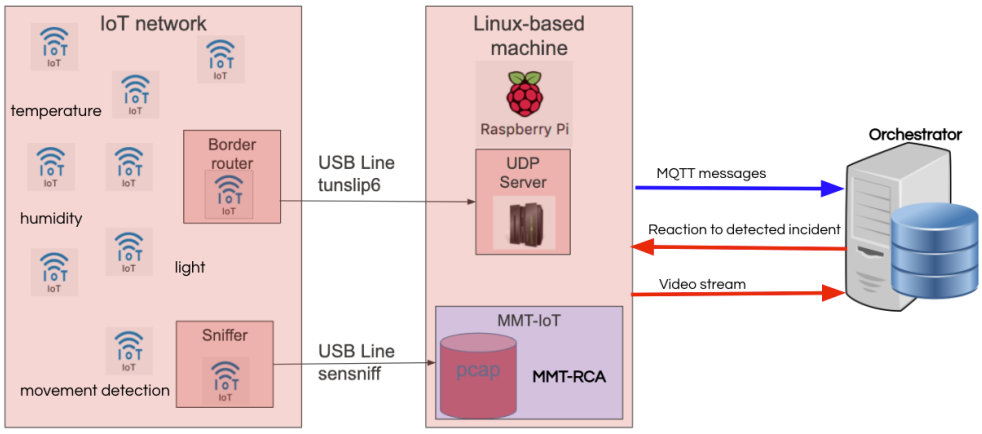

Figure 9: Industrial Campus use case architecture

Figure 9 represents the IoT network (left rectangle) where the Border router and Sniffer are deployed. The information captured by the IoT devices is transmitted to the application server, and the sniffer sends the network monitoring data to the MMT-RCA module that will analyse it to identify anomalous behaviour. Once an incident is detected, the MMT-RCA module will notify the Orchestrator indicating the potential root-causes based on its analysis. The reaction will be taken afterwards manually by a human or automatically based on a decision rule or algorithm.

2.3.3 Actors

The actors involved in this use case are the following:

- **IoT Campus** sends monitoring data to MMT-RCA. Several **IP cameras** can be activated and manipulated/rotated from distance to focus on the source of the anomaly (i.e., fire)
- **MMT monitoring framework with the MMT-RCA module** analyzes collected data and raises alerts if needed.
- **Security Orchestration** receives analysis results from MMT-RCA and displays on web-based dashboards
- **Technician Command Center** clicks the button on the web-based interface to activate the CRITICAL mode once receiving an alert from MMT-RCA.

2.3.4 Preconditions

As a knowledge-based tool, MMT-RCA needs training dataset to learn about the potential incidents taking place in the IoT Campus. That means we would need to perform malicious activities and generate the incidents so that MMT-RCA can save all relevant data features. More precisely, we have to create a real or “virtual” fire that MMT-RCA can learn from. Once the incident reoccurs, it will be detected and alerted by MMT-RCA with its corresponding potential root-cause, based on the calculation of similarity score.

2.3.5 Basic flow

2.3.5.1 Diagram

The following flow diagram depicts the main interactions between actors involved in the use case.

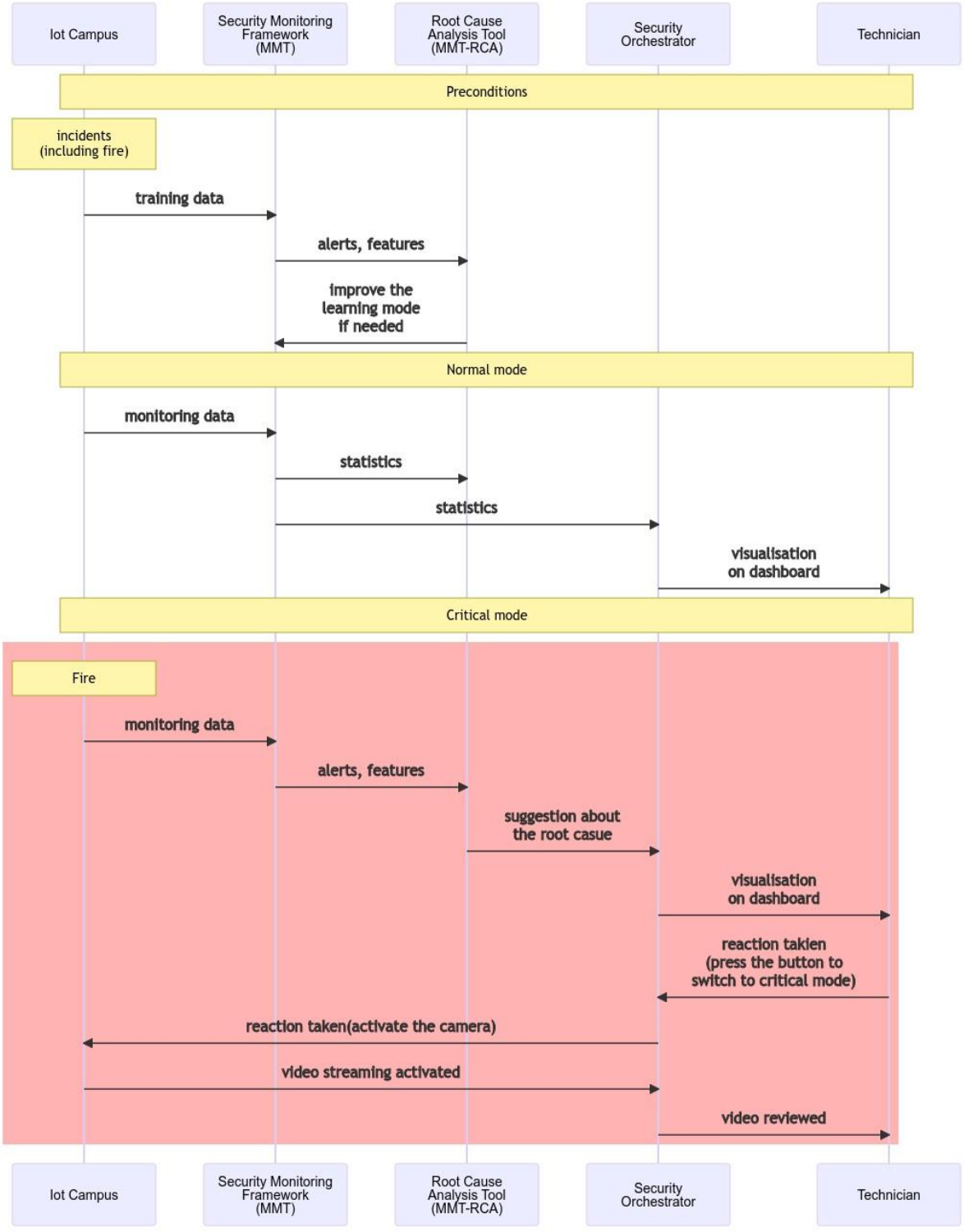

Figure 10: Use case C diagram

2.3.6 Post conditions

- The video streaming is activated properly
- The camera focuses on/ zooms in the zone of the fire
- The technician is able to view the live stream captured from the camera.

2.3.7 Success criteria

- MMT-RCA detects the anomaly (e.g., several IoT devices stop sending data or send data slower than a standard rate) and determines that the fire might be the root-cause in near real time.
- The technician can see an alarm message on his dashboards shortly after the fire is triggered.
- The live stream is displayed shortly after the technician clicks on the button to activate the camera.

2.3.8 Use case summary

2.3.8.1 Mapping on INSPIRE-5Gplus architecture

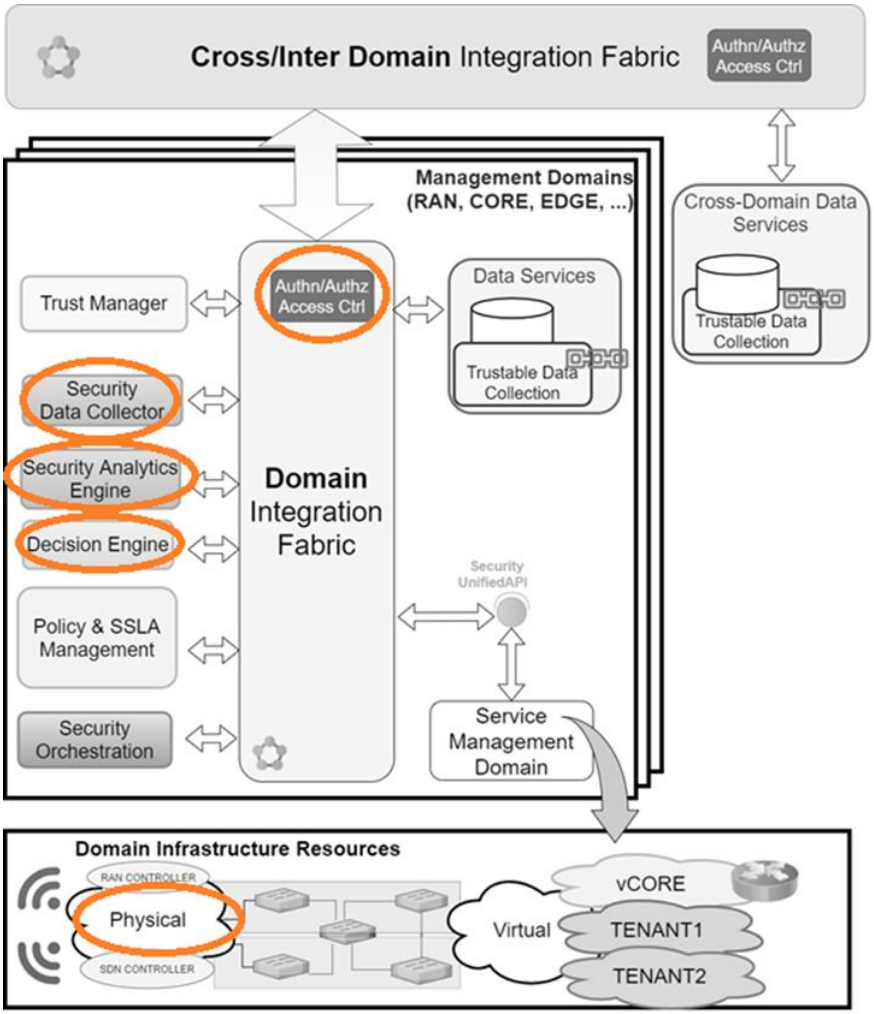

Figure 11: UC C mapping to INSPIRE-5Gplus HLA

2.3.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are the following:

- WP4 - RCA: Root Cause Analysis
- WP3 - Security Monitoring Framework (MMT)
- Security Data Collector
- Security Analytics Engine
- Decision Engine

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.4 UC D - Utilization of data provided by network analytics

2.4.1 Problem description

Compromising mobile devices can have serious implications on security and privacy of its users, it can also form the initial step of more advanced attacks on services or infrastructure. In order to detect these types of threats active or passive probes for the 5G Data plane (acting as Security Agents in INSPIRE-5Gplus framework) are often used. The collected data are delivered to security analytics functions that can identify malicious behaviour of end devices or network components.

The NWDAF (Network Data Analytics Function)[2] is a part of the Service Based Architecture (as specified in 3GPP TS 23.501) that can perform inference, derive analytics information (i.e. statistics and/or predictions) using data provided by other control plane functions and components. Since some of the derived information is related to security (analytics related to UE abnormal behaviour) it can be used within INPIRE-5Gplus framework both at the domain and E2E security management levels as additional source about current or potential attacks.

2.4.2 Goals

The main goal of this UC is to present how external cyber-security analytics data derived by dedicated standardized 5G core Network Function (NF) can be utilized in the INSPIRE-5Gplus security architecture and show how external management system can benefit from the data exposed by 5G System.

2.4.3 Actors

The actors and roles involved in this UC are:

- Mobile Network Operator (MNO) – operating 5G network with 5G Core equipped with NWDAF (Network Data Analytics Function)
- Mobile device users (Alice, Bob) – using 5G devices connected to MNO network
- Malicious party (Mallory) – performing attack on mobile devices (cyber-attack: device hijacking, physical attack: device theft)
- Security management framework for UE domain.

2.4.4 Preconditions

MNO 5G network is equipped with NWDAF (Network Data Analytics Function) configured to collect events provided by 5G Core functions (AMF, SMF, PCF, UDM, AF) and retrieve information from data repositories (e.g. UDR via UDM for subscriber-related information). NWDAF includes the Analytics logical function that can perform inference (using pre-trained ML models) to identify a group of UEs or a specific UE with abnormal behaviour.

Malicious party has performed attacks on user devices leading to abnormal behaviour (there are malicious applications running on the devices or devices have been stolen and misused).

Security framework is configured to consume information provided by NWDAF (Abnormal behaviour related network data analytics) and to apply respective security policy.

[2] 3GPP TS 23.288 V17.0.0 (2021-03) : Architecture enhancements for 5G System (5GS) to support network data analytics services (Release 17)

2.4.5 Basic flow

The UC includes the following sequence of actions:

1. NWDAF collects 5G Core events and information and produces analytics for user devices with abnormal behaviour. According to 3GPPP specification following exceptions can be distinguished:

Expected analytics type	Exception IDs matching the expected analytics type
mobility related	*Unexpected UE location, Ping-ponging across neighbouring cells, Unexpected wakeup, Unexpected radio link failures.*
communication related	*Unexpected long-live/large rate flows, Unexpected wakeup, Suspicion of DDoS attack, Wrong destination address, Too frequent Service Access.*

2. The generated analytics (exception events) are delivered to an Security Data Collector (SDC) leveraging the domain integration fabric using direct NWDAF API or NEF functionality.
3. The Security Data Collector aggregates and transforms the metrics into a suitable format.
4. Security Analytics Engine (SAE) performs analytics using other types of data (e.g. from monitoring probes in Data plane) and correlates results with NWDAF events.
5. Decision Engine applies relevant mitigation action related to detected events. For security related events (discovered by SAE) additional actions are defined by security policy.
6. The decision is implemented by Security Orchestration.

2.4.5.1 Diagram

Figure 12 illustrates the basic flow of UC D.

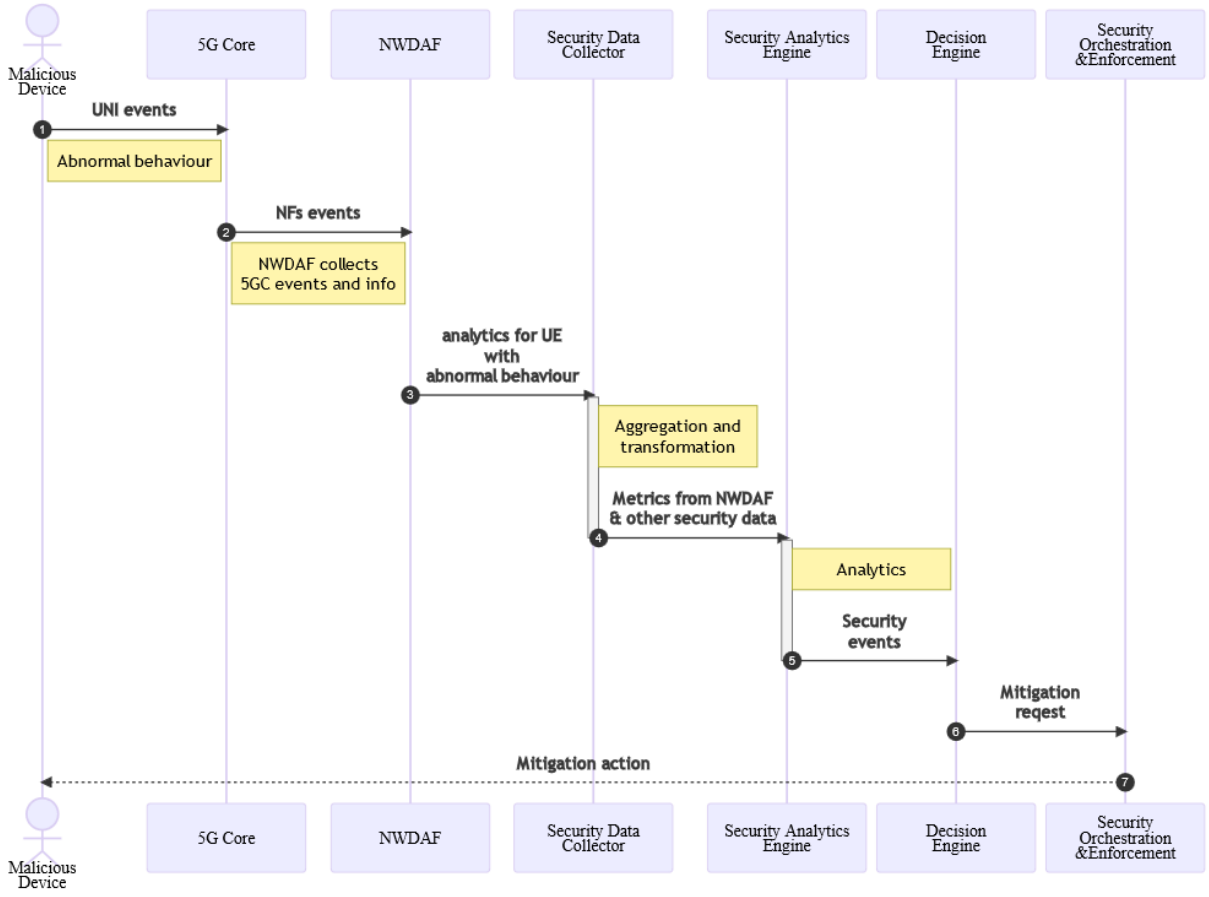

Figure 12: Use case D diagram

2.4.6 Post conditions

After implementing mitigation actions, the system should be monitored.

The detected security event should be reported to the relevant parties (device owners, service provider, other affected parties).

2.4.7 Success criteria

The main success criteria are:

- Events detected by NWDAF are correlated with other metric sources and used by SAE for detection
- The proper mitigation is selected and applied
- Parties affected by the detected incident are notified
- Gathered data are kept to be used for future preventions

2.4.8 Use case summary

This use case illustrates how dedicated 5G core analytics can be utilized in the INSPIRE-5Gplus security architecture as Security Agent to perform automated actions and shows how external management system (here related to security management) can benefit from the data exposed by 5G System.

2.4.8.1 Mapping on INSPIRE-5Gplus architecture

As depicted in Figure 13, the UC involves components of INSPIRE-5Gplus HLA for 5G Core domain.

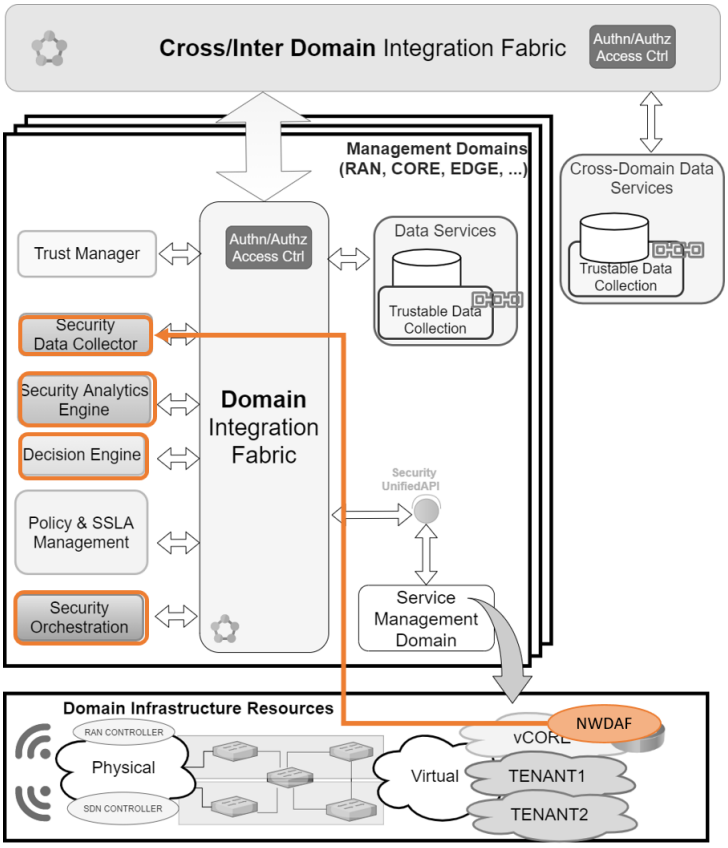

Figure 13: UC D mapping to INSPIRE-5Gplus HLA

2.4.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers involved in this use case are:

- Security Data Collector
- Security Analytics Engine
- Decision Engine
- Security Orchestration

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.5 UC E - Remotely controlled manoeuvring manipulation

2.5.1 Problem description

The remotely controlled manoeuvring manipulation use case is closely associated to the emerging cooperative, connected, and automated mobility (CCAM) services in 5G and beyond vehicular environments. In particular, as illustrated in Figure 14, this use case entails security vulnerabilities that may emerge in tele-operated driving scenarios, related to the remote control of automated vehicles by a human or by an artificial intelligence module over the mobile radio network. Figure 14 shows an automated driving scenario where an unexpected blockage is encountered on the desired route of a vehicle. The obstacle needs to be overpassed through tele-operated driving commands with direct control exchanged via a public transport control center which handles tele-operation sessions. Other examples of vehicular scenarios where tele-operated driving can be deployed include: remotely initiated lane change or speed adaptation on highway, not-responding driver and undefined traffic conditions.

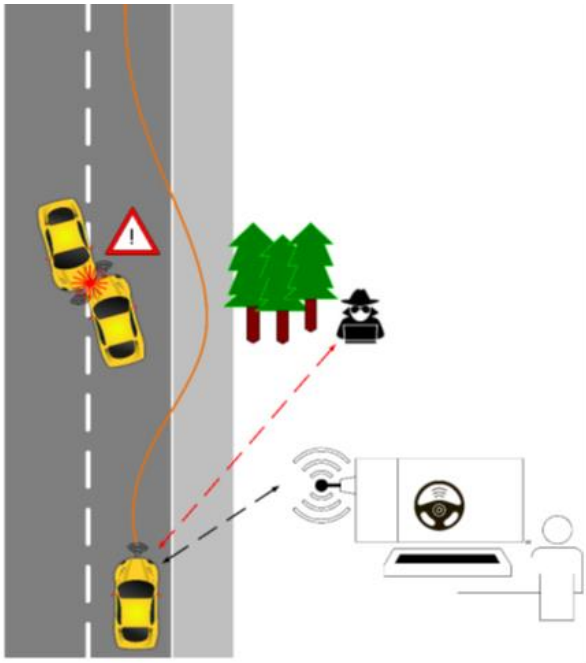

Figure 14: Remotely controlled manoeuvring manipulation use case

This use case involves real-time vehicle operation with stringent connectivity requirements. In particular, vehicles transmit environment sensor data and/or bandwidth-hungry video streaming data, in the uplink direction. The vehicle control center, upon reception and processing of the fused information, provides the visual representation of the vehicle environment to the remote driver, and sends back its control commands, e.g., desired speed or steering wheel angle, to the automated vehicles.

In this use case, an attacker may gain access to autonomous-drive functions due to 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 become capable of undertaking the control of safety-critical vehicle components, such as engine control and brakes, and perform alterations to vehicular data, e.g., inject falsified information and fabricate sensor readings, by gaining access to on-board diagnostics. Trajectory alteration via GPS jamming/spoofing could be also a realization of such type of attacks.

Threats associated to this use case can be efficiently mitigated by leveraging the security enforcement features of our INSPIRE-5Gplus enabler, coined "*Lightweight and Space-efficient vehicle authentication enhanced with misbehaviour detection*" (V2XMisDet), offering two layers of protection. In particular,

the enabler prevents unauthorized users (i.e., *outsiders*) from accessing the firmware and vehicle software through (over-the-air) online updates, exploiting the advanced features which enhance the 5G Authentication and Key Agreement (5G-AKA) procedure. In addition, the misbehaviour detection capabilities of our enabler allow the attack mitigation (e.g., detection of anomalous sensor readings, trajectory alteration identification, etc.) from authenticated users (i.e., *insiders*) who already possess valid credentials to interact with other legitimate entities in the system. This is achieved by processing streaming vehicular information at the transport control center, ensuring accurate detection of erroneous/falsified data which may violate the semantic correctness of exchanged V2X information.

2.5.2 Goals

The associated security enabler for this use case aims at successfully addressing threats and attacks related to the manipulation of manoeuvring information in tele-operated driving. Such attacks may either originate from malicious outsiders which are vehicles/users exogenous to the original system, or from insiders which are already authenticated and possess valid credentials to interact with other legitimate entities in the system. Since tele-operated driving is associated with safety-critical driving situations, the timely and highly reliable prediction and detection of such incidents is crucial. Besides detecting malicious actions, the enabler needs to guarantee that the security enhancements will not come at the expense of network performance.

2.5.3 Actors

The actors and roles involved in this UC are:

- Mobile Network Operator
  - RAN, 5GCore (CP + UP), Mobile Edge
- A set of vehicles (legitimate)
- Vehicle control center user
- Malicious party
- Service provider

2.5.4 Preconditions

In case of insider attack model, the malicious party is considered authenticated and possesses valid credentials to communicate with other legitimate members. In case of outsider attack model, the malicious party is able to inject falsified information to the exchanged data between legitimate vehicles and the control center.

2.5.5 Basic flow

The basic flow of actions of the actors and the system is as follows:

1. A vehicle periodically transmits environment sensor data to the control center for remotely controlled manoeuvring (normal operation);

2. The control center provides the visual representation of the vehicle environment to the remote driver and sends back its control commands (normal operation);

3. When the manipulation attack takes place, the attacker injects falsified manoeuvring information during step 1.

4. The control center responses with incorrect and misleading commands to the remotely controlled vehicle, being deceived by the falsified manoeuvring information in step 3.

5. With the aid of V2XMisDet enabler, false data injection is correctly detected, traffic originated from the malicious party is isolated, and legitimate commands are sent back to the vehicle by the control center.

2.5.5.1 Diagram

Figure 15 illustrates the basic flow of UC E.

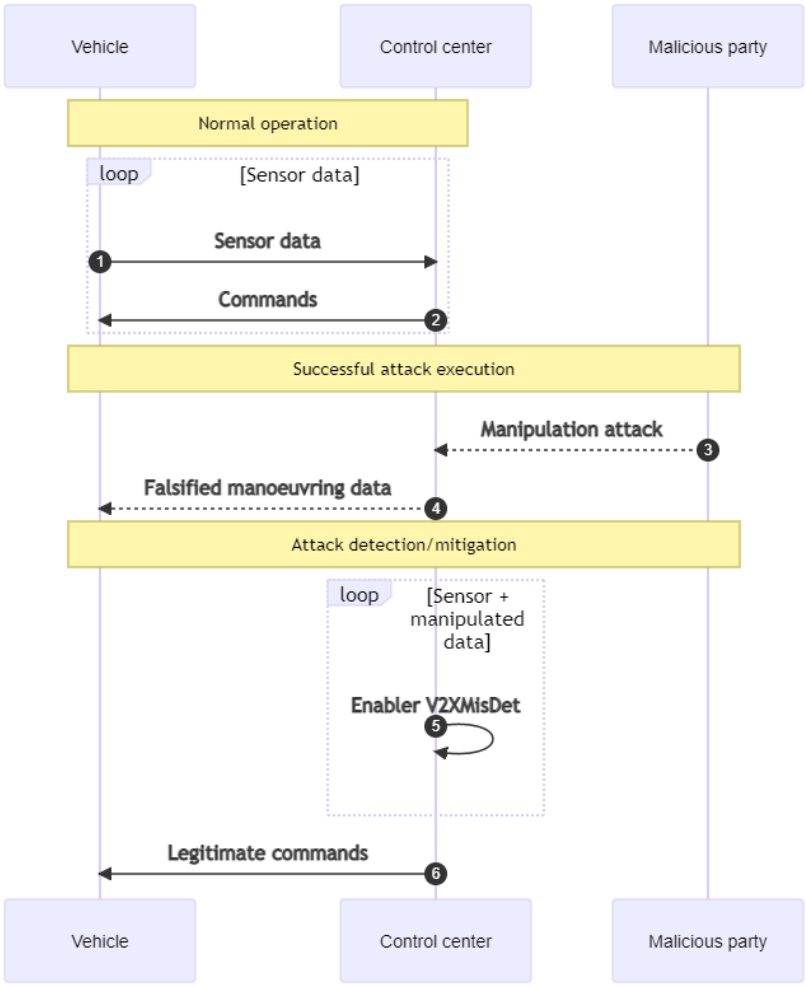

Figure 15: Basic flow of UC E

2.5.6 Post conditions

With the help of V2XMisDet enabler, attacks from outsiders can be efficiently prevented with controlled false positive rates. Otherwise, in the case of attacks from insiders, the misbehaviour detection capabilities of the enabler allow the accurate and timely detection of such false data injection in the manoeuvring information of the remotely controlled vehicle, by processing incoming data in the control center and detecting anomalous behaviour.

2.5.7 Success criteria

Authentication integrity is achieved when all exchanged V2X messages are protected from any alteration attempted by an outsider. Detection of manoeuvring manipulation by an insider should be highly accurate, timely and with very low false positive/negative rates due to the mission-critical nature of vehicular communication.

2.5.8 Use case summary

The remotely controlled manoeuvring manipulation use case entails false data injection attacks that may take place during tele-operated driving in vehicular environments. To this end, an INSPIRE-5Gplus

enabler, coined V2XMisDet, offers two layers of protection: i) enhanced authentication against outsider attacks; ii) detection of manipulated information (caused by an insider), in the exchanged messages between legitimate vehicles and the control center.

2.5.8.1 Mapping on INSPIRE-5Gplus architecture

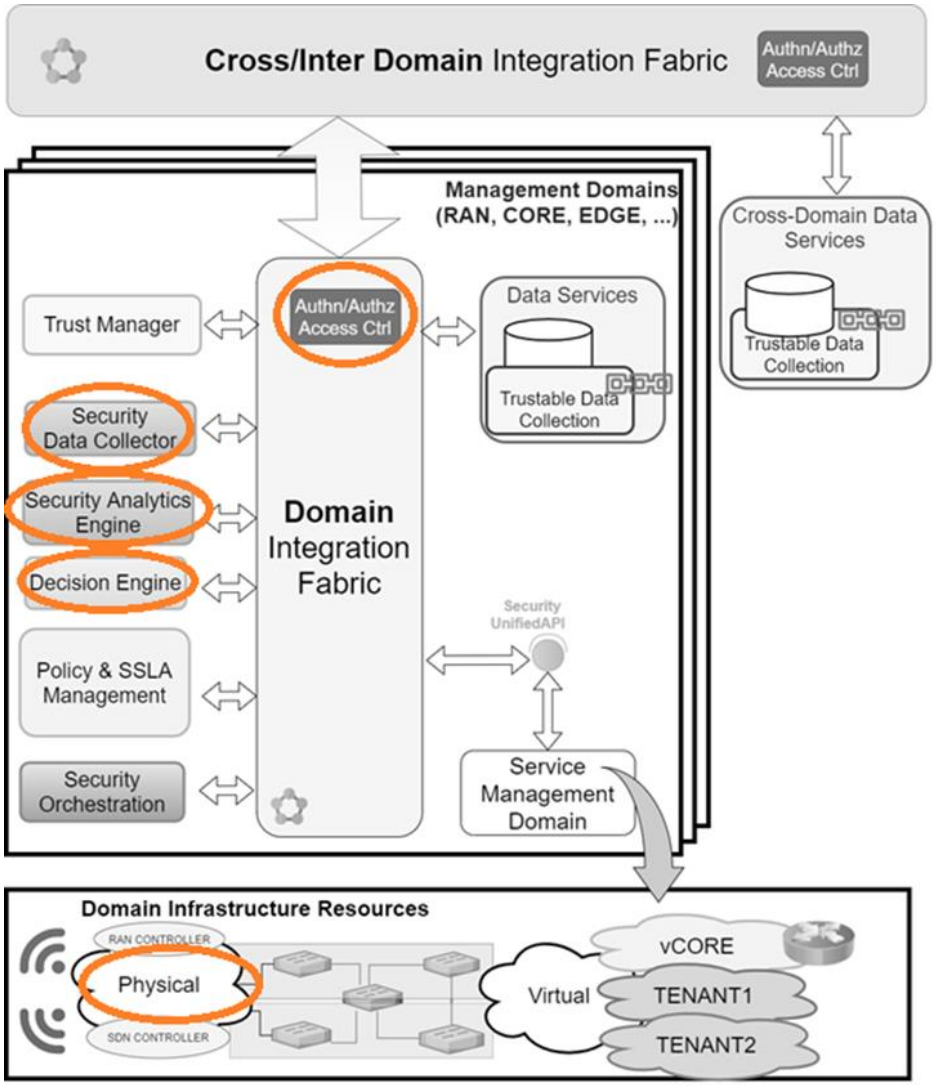

Figure 16: UC E mapping to INSPIRE-5Gplus HLA

2.5.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Lightweight and space-efficient vehicle authentication enhanced with misbehaviour detection (V2XMisDet)
- Security Data Collector
- Security Analytics Engine
- Decision Engine

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.5.8.3 Comments

This use case is closely associated to the ICT-18 5GCroCo[3] tele-operated driving use case requiring real-time operation (i.e., high reliability and low latency).

2.6 UC F - HD map update poisoning

2.6.1 Problem description

The high definition (HD) map update poisoning use case is closely associated to the emerging CCAM services in 5G and beyond vehicular environments. In particular, as illustrated in Figure 17, this use case entails security vulnerabilities that may emerge during the exchange of HD map information between autonomous vehicles. HD maps for autonomous driving are defined as real-time, intelligent maps that provide highly accurate position and traffic information of dynamic and static objects for optimal route and lane selection. In an HD map update scenario, the leading vehicle, in view of an unexpected blockage encountered in its lane, needs to inform the map database about this new road topology information in its surroundings, to ensure traffic safety for neighbouring vehicles. This use case, thus, relies on the cooperative behaviour of vehicles assisted by a communication network infrastructure to avoid hazardous situations that may result in accidents. Other examples of vehicular scenarios where HD mapping can be used include, among others, optimal route selection and route updating in hazardous situations.

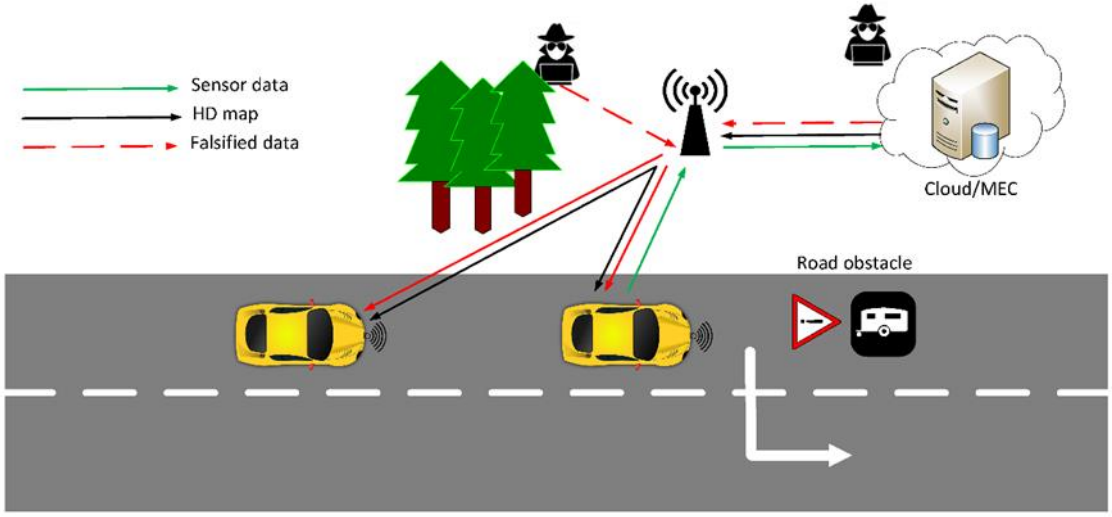

Figure 17: HD map update poisoning use case (can be either real-time or non-real-time)

This use case involves massive information exchange among autonomous vehicles, data servers and map providers. Other aspects that have direct influence on the quality of HD maps are the level of the accuracy of sensor data, the robustness of data fusion algorithms, and the capability of the 5G network for high-rate data exchange at high speeds, especially in the areas with no or poor network coverage.

In this use case, an attacker may manipulate the content of the transmitted information from the leading vehicle and/or falsify the map database contents, e.g., alter/remove road signs, resulting in unavailability of needed information and/or wrong manoeuvres. In both cases, the attacker prevents the vehicles, relying on back-end servers (HD map provider) for their longitudinal and lateral directions,

[3] https://5gcroco.eu/

from accessing the necessary updated map data. In other realizations of this attack, the malicious party may perform information forgery attack by accessing car owner's private data and vehicle trajectory through unsecured third-party means (i.e., map editor, mobile app, etc.). Sensitive user information may thus be inferred to harm user privacy while illegal tracing may compromise the identity and location information of a vehicle.

Threats associated to this use case can be efficiently mitigated by leveraging the security enforcement features of our INSPIRE-5Gplus enabler, coined V2XMisDet, offering two layers of protection. In particular, the enabler prevents unauthorized users (i.e., *outsiders*) from accessing the firmware and vehicle software through (over-the-air) online updates, exploiting the advanced features extending the 5G Authentication and Key Agreement (5G-AKA) procedure. In addition, the misbehaviour detection capabilities of our enabler allow the detection of falsified/inconsistent map data (longitudinal and lateral directions) from authenticated users (i.e., *insiders*), and ensure the accuracy of reported positioning information. This is achieved by processing positioning coordinates at the cloud/MEC, and with accurate detection of erroneous/falsified map update information.

2.6.2 Goals

The employed security enabler for this use case aims at successfully addressing threats and attacks related to the manipulation of HD map information updates reported by autonomous vehicles. Such attacks may either originate from malicious outsiders, which are vehicles/users exogenous to the original system, or from insiders which are already authenticated and possess valid credentials to interact with other legitimate entities in the system. Since HD map distribution often relates to safety-critical driving situations, the timely and highly reliable prediction and detection of such incidents is crucial. Besides detecting falsified map information, the enabler needs to guarantee that the security enhancements will not come at the expense of network performance.

2.6.3 Actors

The actors and roles involved in this UC are:

- Mobile Network Operator
  - RAN, 5GCore (CP + UP), Mobile Edge
- A set of vehicles (legitimate)
- Map supplier
- Malicious party
- Service provider

2.6.4 Preconditions

In case of insider attack model, the malicious party is considered authenticated and possesses valid credentials to communicate with other legitimate members. In case of outsider attack model, the malicious party is able to inject falsified map data either to the reported information by the leading vehicle or by accessing the map database contents at the cloud/MEC. It is further assumed that cloud/MEC is considered a trustworthy entity, e.g., no rogue MEC is present in the scenario.

2.6.5 Basic flow

The basic flow of actions of the actors and the system is as follows:

1. Sensor data are streamed to the cloud/MEC from the leading vehicle (normal operation);

2. Map information is streamed to both vehicles when driving continuously along the road (normal operation);

3. When the map poisoning attack takes place, the attacker injects falsified manoeuvring information during either step 1 or step 2.

4. Map updates communicated to the vehicles contain incorrect and misleading information about the road conditions, being deceived by the poisoning attack in step 3.

5. With the aid of V2XMisDet enabler, map poisoning is correctly detected, traffic originated from the malicious party is isolated, and legitimate map content is sent back to the vehicles by the cloud/MEC.

2.6.5.1 Diagram

Figure 18 illustrates the basic flow of UC F.

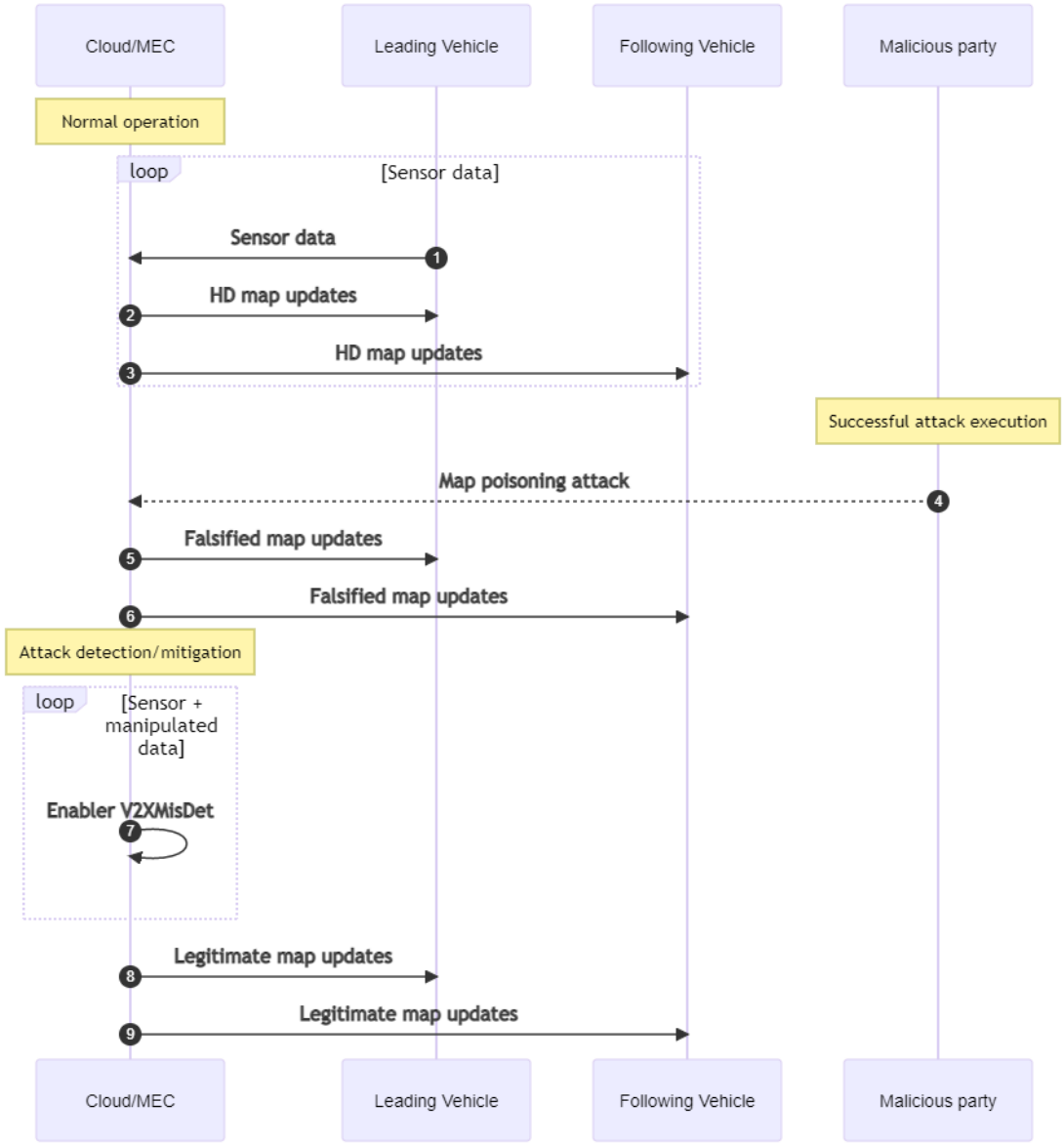

Figure 18: Basic flow of UC F

2.6.6 Post conditions

With the aid of V2XMisDet enabler, map poisoning attacks from outsiders can be efficiently prevented. Otherwise, in the case of map poisoning attacks from insiders, the misbehaviour detection capabilities of the enabler allow the accurate and timely detection of false data injection in the road topology information related to the vehicle surroundings.

2.6.7 Success criteria

Authentication integrity is achieved when the entire HD map information exchanges are protected from any alteration attempted by an outsider. Detection of map poisoning by an insider should be highly accurate, timely and with very low false positive/negative rates due to the mission-critical nature of vehicular communication.

2.6.8 Use case summary

The HD map update poisoning use case entails false data injection attacks that may take place during map generation and distribution in vehicular environments. To this end, an INSPIRE-5Gplus enabler, coined V2XMisDet, offers two layers of protection: i) enhanced authentication against outsider attacks; ii) detection of falsified map content (caused by an insider) in the fused information from vehicles.

2.6.8.1 Mapping on INSPIRE-5Gplus architecture

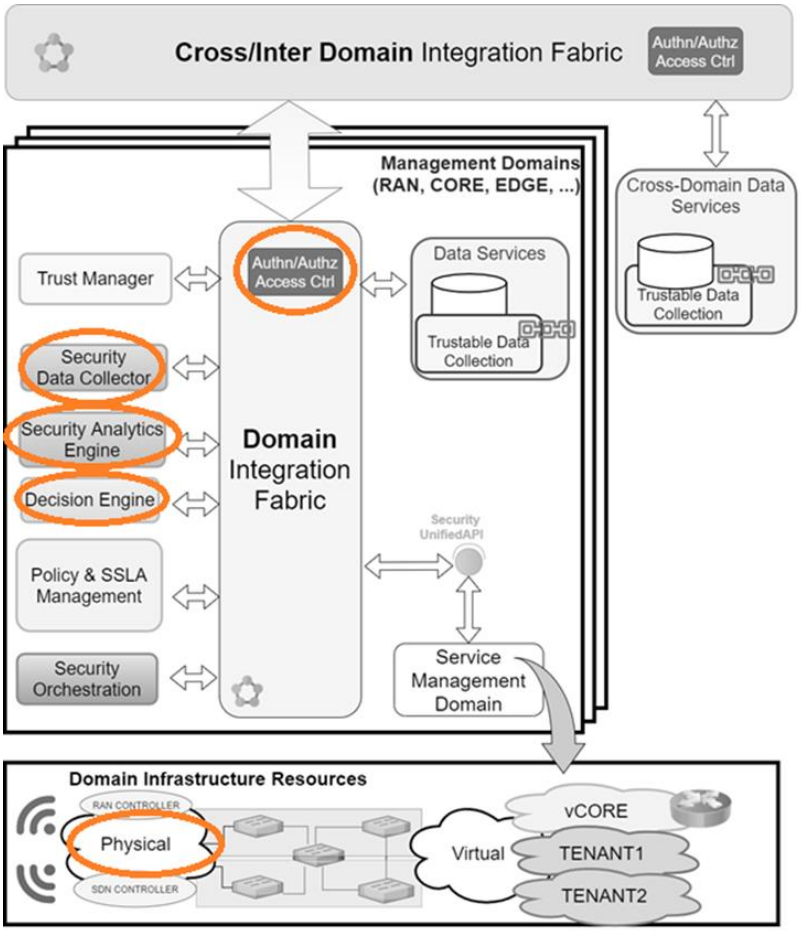

Figure 19: UC F mapping to INSPIRE-5Gplus HLA

2.6.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Lightweight and Space-efficient vehicle authentication enhanced with misbehaviour detection (V2XMisDet)
- Security Data Collector
- Security Analytics Engine

- Decision Engine

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.6.8.3 Comments

This use case is closely associated to the ICT-18 5GCroCo HD map generation and distribution for autonomous driving use case requiring massive information exchange.

2.7 UC G - Definition and assessment of Security and Service Level Agreements

2.7.1 Problem description

SSLAs allow defining the agreed upon security properties of the network and services. However, to be really effective these agreements need to be continuously verified and, if they are violated, the appropriate actions need to be taken. Furthermore, these actions need to be triggered automatically in a ZSM perspective. For this, Real-Time SSLAs have been defined (cf. Section 4.2 of the deliverable D3.2 [2]) in order to be able to specify and continuously assess Security and Service Level Agreements (SSLAs) that establish precisely what must be done regarding the detection and management of security. RT-SSLA serve to specify what is required concerning what type of security breaches should be detected and managed and indicate how the security functions should work. They can be derived from higher level security policies expressed, for instance, in High or Medium-level Security Policy Language (HSPL or MSPL).

Once specified, RT-SSLAs need to be continually monitored to determine that the expected properties are being satisfied and that the security functions are doing their job, or, if it is not the case, generate alarms or trigger the appropriate countermeasures.

2.7.2 Goals

This use case includes the specification of RT-SSLAs; in other words, translating the specified and agreed upon policies to low level rules that can be verified during runtime and in real-time, i.e., in the order of seconds or even milliseconds depending on the requirements and available resources.

RT-SSLAs allow assessing and controlling that the security functions are correctly implemented, the security properties are not violated, and the violations trigger self-healing and self-protection strategies. The MMT security monitoring and analysis framework takes the given RT-SSLAs and uses them to analyse network traffic and information from other sources (e.g., system and application logs) to determine if they are satisfied and if all the required remediation or prevention activity is occurring as defined.

Thus, the main goal is allowing the definition and enforcement of SSLAs, and facilitating the agreements between different constituents concerning the expected cyber-security level and remediation strategies.

SSLAs can be defined for formalising the requirements related to a wide variety of cyber-security issues and concerns. It goes far beyond current intrusion detection and prevention systems, as well as policy control systems, since they are based on real-time metrics that allow fine-grained or more abstract assessment of the security requirements of the different stakeholder involved. They also allow detecting security breaches as well as malfunction of security functions, and integrate remediation strategies that can be triggered automatically with the goal of enforcing the specified SSLAs.

2.7.3 Actors

The actors and roles involved in this UC are:

- Someone (e.g., Mobile Network Operator, Chief Information Security Officer, Service Provider, Vertical Operator, Virtual Network Security Function manager) that specifies the security policies.
- Someone or something (i.e., a malicious cyber attacker or scanner that can be an individual or a machine/bot) that acts as scanner or cyber attacker (e.g., using 5greplay[4]).
- Security function that performs repetitive tasks (e.g., a firewall that provides traces)
- MMT security monitoring framework

2.7.4 Preconditions

The necessary preconditions are:

- The specification of the RT-SSLAs or the manual/automated translation of other specifications (e.g., translation from HSPL or MSPL to RT-SSLA). The RT-SSLAs should include the rules that will detect the security breaches, and the activity performed by a security function targeted by the use case.
- The deployment of the probes that will analyse network traffic and system/application logs or data.
- The execution of a security function that performs reoccurring activity.

The execution by an attacker of a security breach.

2.7.5 Basic flow

The actions of the operator related to this use case are:

- Specification of the RT-SSLA, manually of by translating the defined security policies using the Policy & SSLA Manager.
- Deployment of the Security Agents (SA, i.e., MMT-Probes). This can be done in several ways, e.g., manually, via the orchestrator, or systematically in all the deployed slices.
- Management of the Security Agents (SA) using the MMT monitoring and management framework that acts as Security Analytics Engine (SAE) and interacts with the Security Orchestrator (SO). This includes deploying the RT-SSLAs, and activating or deactivating them.

The following are not shown in the diagram and consist of the attackers and security functions performing their ‘duties”:

- The action of the attacker consists in exploiting a vulnerability to perform the attack.
- The action of the security function consists in performing some periodic activity (e.g., port or malware scanning to detect vulnerabilities in the network or network functions).

2.7.5.1 Diagram

The following flow diagram depicts the main interactions between stakeholders involved in the use case.

[4] Open source tool developed by Montimage for modifying and replaying 5G traffic: https://5greplay.org

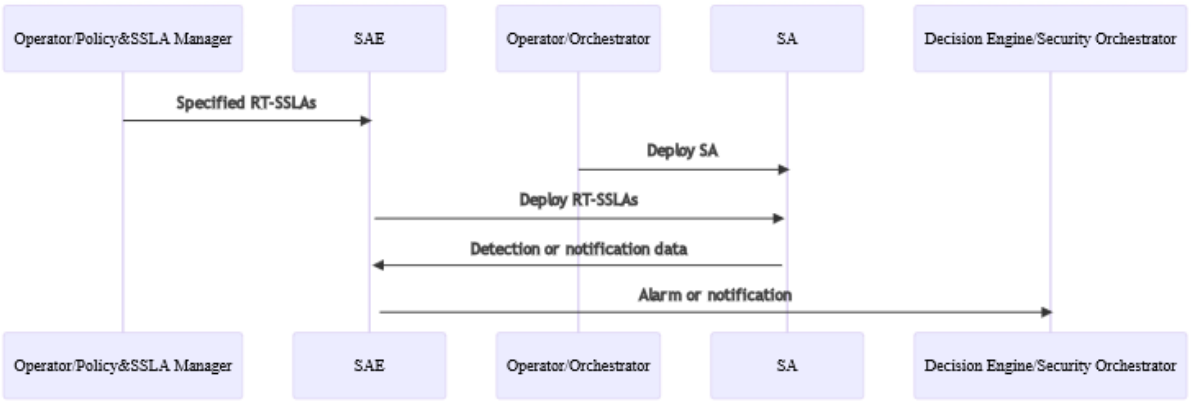

Figure 20: UC G diagram

2.7.6 Post conditions

The use case ends successfully when the specified RT-SSLAs correctly detect what is expected and trigger a response if necessary (e.g., generation of alarms or other actions).

2.7.7 Success criteria

The use case succeeds if the alarm or notification appears in MMT's dashboard informing the user that the specified security property has been respected or the specified security breach has been detected. A further criterion is that no false positive alarms or false notifications are generated.

2.7.8 Use case summary

2.7.8.1 Mapping on INSPIRE-5Gplus architecture

The Figure 21 shows which HLA elements in a domain are involved in the UC and their interactions.

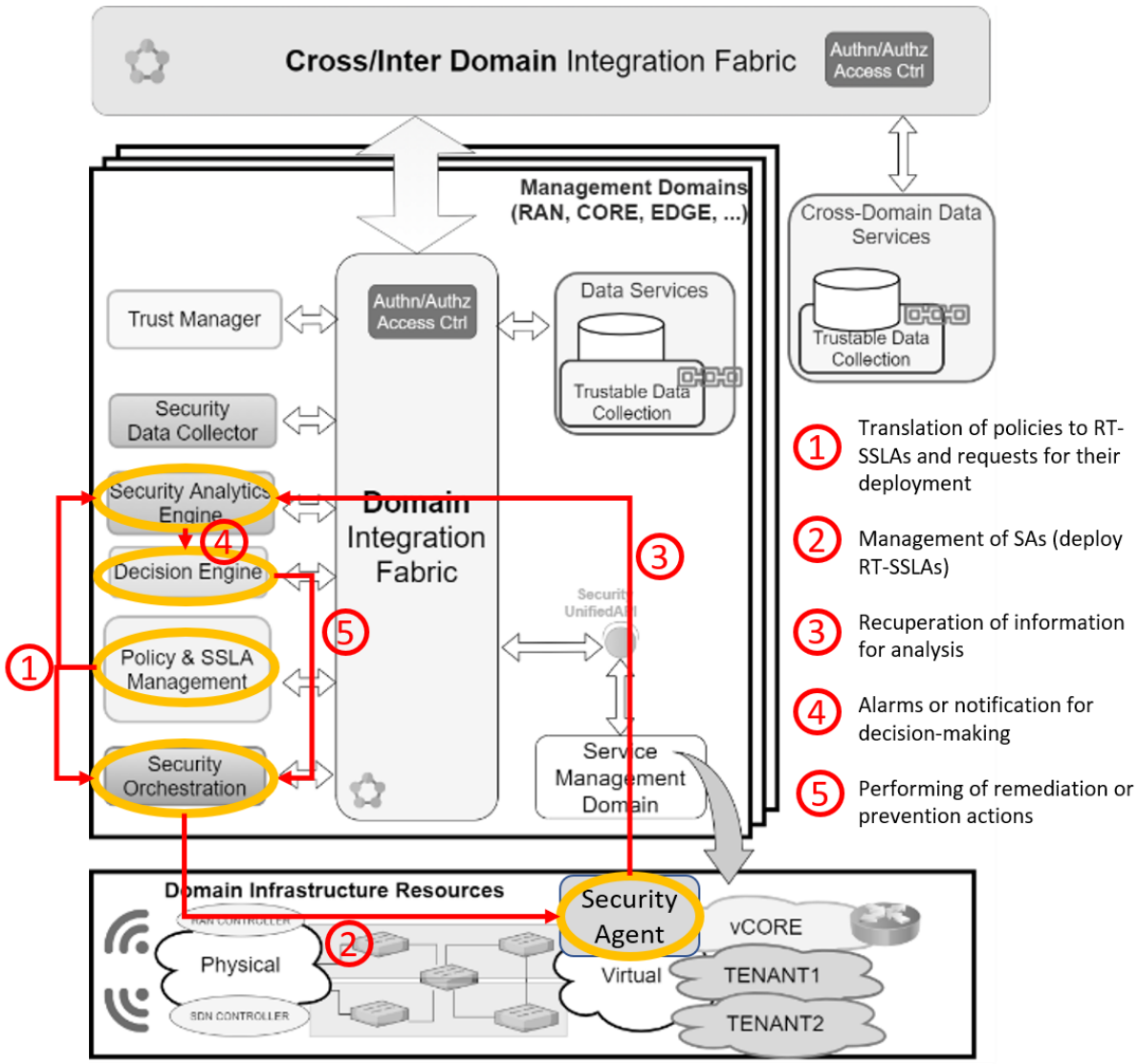

Figure 21: UC G mapping to INSPIRE-5Gplus HLA

2.7.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Policy and SSLA Manager (PSM): that define the security policies from which to derive de RT-SSLAs.
- Security agents (SA): that capture and analyse the data using the RT-SSLAs.
- Security Analytics Engine (SAE): that manages the Security Agents, receives information from them, performs further analysis, and notifies the Security Orchestrator or Decision Engine.
- Security Orchestrator (SO) and Decision Engine (DE): that can process the alarms or notifications and trigger the necessary mitigation or prevention activity.

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.7.8.3 Comments

This use case was introduced in D2.2 [6] as illustrative use case IUC3.

2.8 UC H - Network attacks over encrypted traffic in SBA and security evasion prevention

2.8.1 Problem description

Network operators depends on network traffic monitoring capacity to increase operational efficiency in their platforms. 4G and previous generation use massively a set of management tools, including network probes, to operate and control the communication services. The general trend to encryption of all type of traffic on internet, impacts in the mechanism existing for management and security[5]. In 5G, data plane traffic between the RAN and the Core relies upon the use of GTP-U that is not always encrypted, but the trend is to enable it with IPsec, to increase the security by mobile operators. Ciphering adoption in 5G also applies to control plane. 5G Core includes the concept of Service Based Architecture (SBA). It uses 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 (as represented in Figure 22). The reasoning behind is that cloud environment and microservices, in data centers and hyper-scalers, are the new commodity where deploy network capacity. These environments demand application level E2E encryption over Internet services based on the use of TLS, e.g. DoH (DNS over HTTPS), QUIC (HTTPS over UDP). Consequently, current cybersecurity network tools based on network monitoring, for example deep packet inspection (DPI), will be ineffective in these environments, making it very difficult to detect some common attacks based on botnets, application layer attacks or DDoS. As a result, cybercriminals are adopting TLS encryption as part of their communication and attack channels to make their malicious activities indistinguishable from benign encrypted activities. This evolution introduces new threats over REST APIs channels that are hidden inside TLS. Potential attacks include malware activity, DDoS, application layer attacks on SBA microservices, attacks using exposed roaming encrypted interfaces, etc.

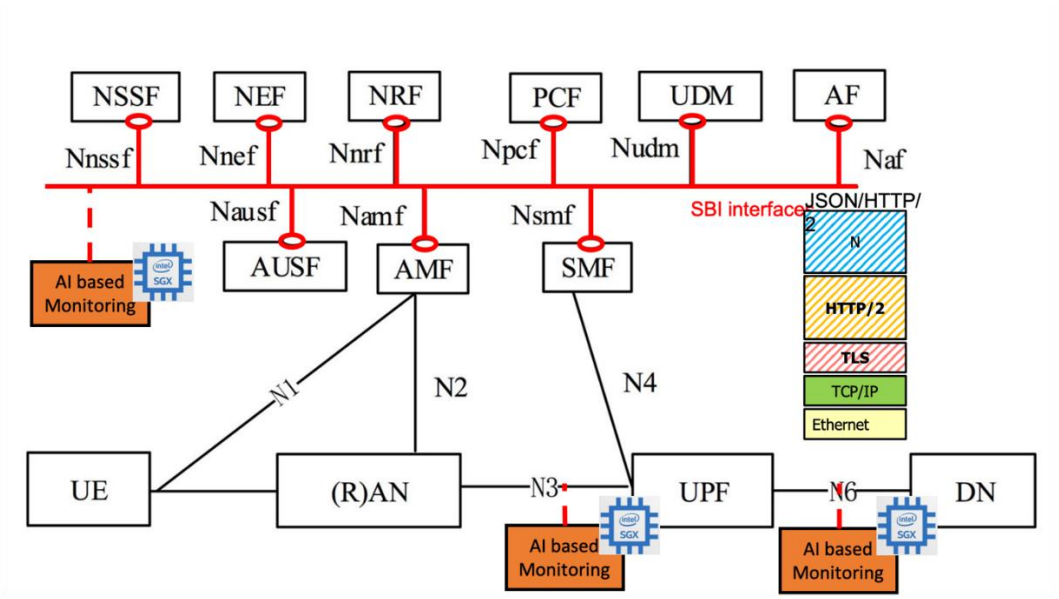

Figure 22: UC H overview

Additionally, the massive adoption of microservices, NFV and Cloud approach in the deployment of 5GCore components and monitoring tools, will open the door for introspection attack (direct access on the software) that can be exploited by a malicious attacker and, in this way, access the software,

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

reverse engineer it and find a way to disable the detection. Evasions will prevent the monitoring function from working correctly. This can be done by making it crash, by reducing its performance resulting in partial traffic analysis, or by introducing unknown attack techniques that remain undetected.

2.8.2 Goals

This use case proposes the evolution of the security network monitoring tools to be capable of analysing encrypted traffic, so it can detect and mitigate attacks based on AI statistical methods. Multiple probes could be allocated in 5G network relevant segments, to receive a copy of the traffic (virtualized or physical taps) a generate security alerts to be addressed by management and orchestrations systems. Additionally, this use case leverages the use of data and software protection techniques empowering TEE techniques (e.g. Intel‘s SGX enclave) to prevent two types of attacks: unauthorised access to data on the one side and detection of software characteristics and behaviour the other side.

2.8.3 Actors

The actors and their roles involved in this UC are:

- 5G network administrator, such as Network/Security Operation Centres (NOC/SOC). The role covers the administrative activities on the network domain, including the security monitoring and remediation. Also, this actor is capable to enforce specific policies in the network, e.g. re-instantiate a component.
- Malicious party. Usually represented by the attacker who wants to materialize the threats identified. For example, degrade the normal behavioural of the 5G components, compromise the system to alter or steal information or other valuable assets. In this case the actor tries to hide his malicious activity in the encrypted traffic or attacking the components (including the monitoring software).
- Security monitoring probes integrated or adapted to the INSPIRE-5Gplus framework to extract relevant information and push it to the analytics engines in charge of detect the attacks.
- INSPIRE-5Gplus Security Management Domain (I5G+ SMD) that provided INSPIRE-5Gplus functionalities: security analytics, decisions, visualization, report of the attacks and enforce corrective actions.

2.8.4 Preconditions

This use case starts with following preconditions:

- 5G network based on SBA 5G Core in normal operation (No attacks or aware of malicious activity).
- A network monitoring capacity over the SBA solution.
- An attacker with capacity to access and compromise some 5G Core components, or the platform where is deployed, such as cloud or NFVI administrator.

2.8.5 Basic flow

1. The attacker initiates actions on the network to compromise some component resources on NFV for its own interest.
2. The administrator detects service performance impact, cause by degradation of some instances of the 5G Network Functions (e.g. a DoS attacks, malware spread, etc., generated by the malicious party), but do not know the cause or the remediation.
3. The administrator deploys monitoring AI agents (Smart Traffic Analyzer or STA) in the network

that can be activated to monitor encrypted control or data plane, i.e. a set of monitoring VNFs in the cloud or on-premises

4. 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
5. To avoid Introspection attacks and reverse engineering, it is necessary to harden the integrity monitoring of the network functions using Trusted Execution Environments (TEE). The runtime integrity verification needs to be backed by a TEE embedded routine.
6. These probes (Security Agents or enablers in INSPIRE-5Gplus architecture) deployed at different points in the network, generate metrics, such as aggregated flows from network traffic in suitable format, to feed its own inference engines trained using AI/ML to identify malicious behaviour patterns in the encrypted traffic.
7. Identified malicious activity by the probes will be reported to the administrator and it will take actions to mitigate the attack, using specific security policies such as, firewalls, or active probes. Alternatively, the affected functions (e.g. an infected container or virtual machine of 5G core), can be cleaned and re-instantiated (with a certificated by vendor version) to remove the problem.

2.8.5.1 Diagram

Figure 23 illustrates the basic flow of UC H.

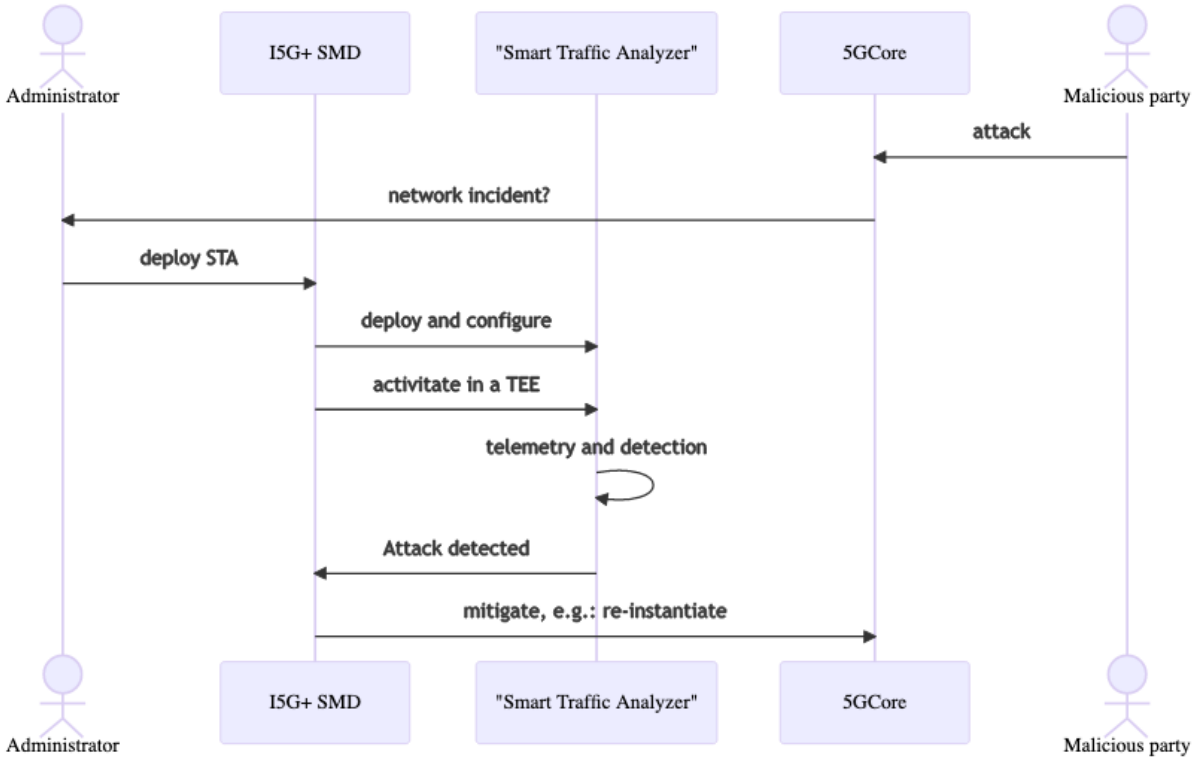

Figure 23: UC H diagram

2.8.5.2 Alternative flow

- The administrator activates some probes in the data plane to monitor and detect attacks as part of a security service for 5G end user.
- The process is similar, but the probes are deployed in data plane instead of Control plane (SBA).

2.8.6 Post conditions

The normal operation of the network is restored, attacks identified and mitigated without deactivating encryption capacity of the network, in terms of privacy and security enhancement.

2.8.7 Success criteria

The success of the use case will be defined by the following factors:

- Network probes will be deployed and configured successfully in specific point of monitoring in the 5GCore network
- Some attack examples will be executed over encrypted traffic. Classical detection with a DPI tool will fail, due to encryption, but the STA probes will be able to identify and differentiate from SBA traffic.
- Any tampering attempt to STA probe for detection is blocked by TEE functionality.
- Network reconfiguration or protection rules will be successfully enforced and will mitigate the specific attack.

2.8.8 Use case summary

This Use Case concerns the detection of network attacks over encrypted traffic in Software-Based Architectures as standardised in 5G[6]. It also includes attacks on monitoring software functions (e.g. reducing their performance, provoking malfunctioning), making attacks undetectable by tampering its integrity. In order to be able to detect malicious activities and patterns from the network despite of the encryption, will need the use of Artificial Intelligence (AI) probes focused in anomaly detection and classification and an automation component to mitigate the attacks such as the defined close loop framework by ZSM. This solution will also require data generation and collection, i.e. network telemetry. Finally, introspection attacks mitigation proposed in this UC will require the applicability of TEE technology.

2.8.8.1 Mapping on INSPIRE-5Gplus architecture

The Figure 24 shows which HLA elements in a domain are involved in the UC and their interactions.

[6] 3GPP TS 23.501 V16.1.0 System Architecture for the 5G System

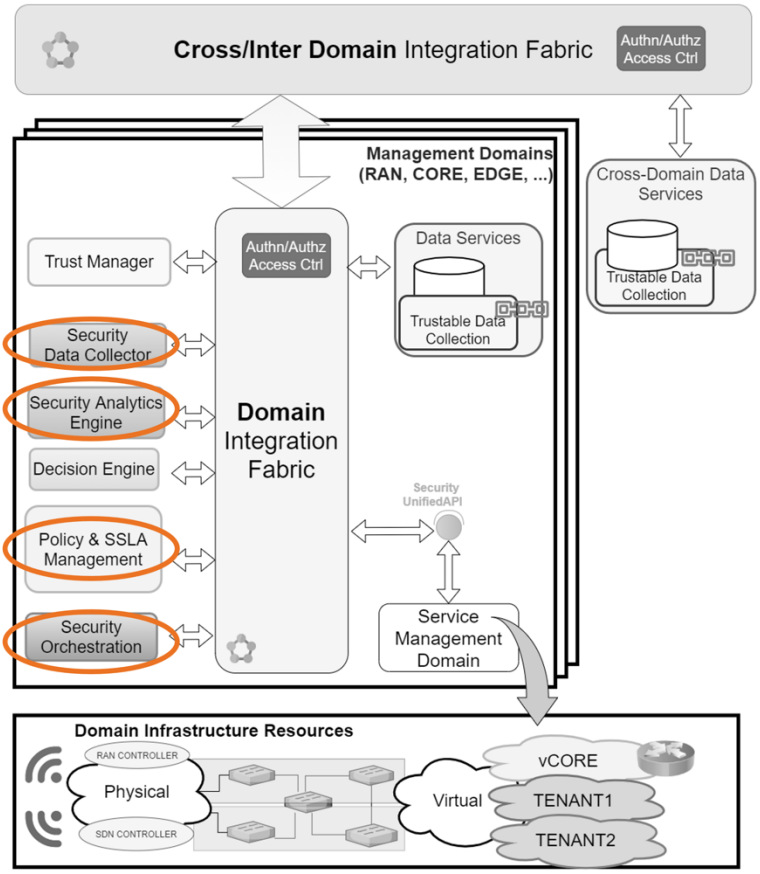

Figure 24: UC H mapping to INSPIRE-5Gplus HLA

Previous Figure 24 shows the mapping for the use case, where Security Data Collector and Security Analytics Engine acts as distributed HLA components to capture and process network traffic related to the 5G core control plane and detect the attacks. Also, the AI classification results identifying the attack done by the analytics engine is used to identify the compromised component. Once identified and based on Human operator decision (e.g. re-instantiate a 5G core component), the Policy Management enforces a specific security policy to mitigate and remediate the attack on the network. The mitigation happens through the Security Orchestration. The communication between HLA components in the domain is supported by the Integration fabric.

2.8.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Systemic
- Smart Traffic Analyzer (STA)
- Security Orchestrator
- Policy Manager

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.8.8.3 Comments

This use case was introduced in D2.2 [6] as illustrative use case IUC4.

2.9 UC I - Evidence of delivering technical KPIs or achieving security objectives

2.9.1 Problem description

In this use case, we have a vertical using an infrastructure provided by an Infrastructure Operator. In order to perfectly and securely ensure his service, the vertical may require and impose some specific properties from the used infrastructure. In this use case, we mainly focus on security properties. For instance, the vertical may require that an antivirus get installed on a specific node / network function / service or that a specific node have a given boot configuration. The vertical can then trust it and build a service upon it. Given that these properties are mandatory for the well running of the vertical service, it is important to verify and monitor it. A straightforward way to verify that a required property is really and correctly ensured is to directly challenge the infrastructure. This option implies that the vertical installs some software on the infrastructure to monitor it, collect some data and check that the required properties are ensured. However, this will arise security issues (e.g., leak of private information, exposure of sensitive software/ function, increase of attack vector, etc.).

2.9.2 Goals

In order to mitigate the security issues previously mentioned, the vertical can securely delegate the management of this kind of software to the infrastructure operator. For instance, the vertical and the infrastructure operator sign an agreement that specifies, inter alia, the properties that must be ensured by the provided infrastructure, the way to collect the data (e.g., the infrastructure operator can make available the source code of the software that will do the collect). The remaining step for the infrastructure operator is to prove that the right software has been used to collect data and provide the expected evidence. To do so, we can use the Remote Attestation (RA) enabler.

In this use case, we aim to provide evidence that a set of security properties (previously specified and agreed between a vertical and an infrastructure operator) have been guaranteed by a given infrastructure while ensuring the privacy and sovereignty of this infrastructure and her owner.

2.9.3 Actors

The actors involved in this use case are:

- Vertical: is the entity that will use the provided infrastructure to offer a service.
- Infrastructure Operator
    - RA server: manages the attestation service. It is the only entry point to get data or evidence about the infrastructure. It can (a) check if a target (i.e., a node in the infrastructure) is RA compliant and so can perform an attestation, (b) push required software on the RA target and make the necessary setup, (c) clean up a target from RA software, (d) return back the active RA targets and (e) run an attestation on a target and verify the result. To ensure all these operations, RA server controls a set of RA Agents.
    - RA agents: collect data from infrastructure and ensure the secure computation and delivery of an attestation result. They are available on the Infrastructure Domain located either on the virtualized layer or on the virtualization management layer and can be in contact with the hardware, namely, a root of trust.

2.9.4 Preconditions

The required preconditions are:

- The agreement: the agreement will specify the code that should be used to collect data, the way to send the attestation result and evidence, frequency (e.g., on demand or periodically)
- In some cases (e.g., hardware-based attestation), a root of trust can be required

2.9.5 Basic flow

Figure 25 gives an overview of the API that can be used by a vertical to verify a given property.

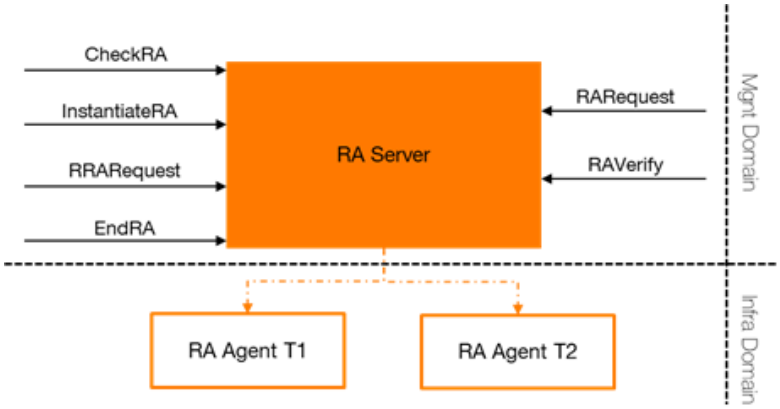

Figure 25: The RA API that can be called by a vertical

Management APIs

- CheckRA (targetID, param): This command enables to check if the node « targetID » is able to run a RA.
- InstantiateRA (targetID, type, param): This command triggers an instanciation of the required code in the node « targetID ». If the instanciation succeeded, the « targetID » is added to the internal register « RunningRA »
- RRARequest: This command returns the list « RunningRA ».
- EndRA (targetID, param): This command triggers the deletion of the RA related code running in the node « targetID ». If the deletion succeeded, « targetID » is deleted from the internal register « RunningRA »

Service APIs

- RARequest (targetID, type, param): This command run the RA code on the node « tragetID » if the node « targetID » existes in the internal register « RunningRA ».
- RAVerify (SIG, targetID, param): This command enables the verification of the result of a « RARequest » if the node « targetID » existes in the internal register « RunningRA ».

“param” is an empty field that can contain additional information.

2.9.5.1 Diagram

In Figure 26 we show the exchanges between the Vertical and the Infrastructure Operator (RA Server, Agents) to have an attestation from a target. The attestation will help the Vertical to check whether the target ensures a given property. For the sake of simplicity, we schematize only two agents, but we can have more agents associated to an RA server. The agents can be on the same target or in different targets. We also omit the parameter of the commands.

Step 1: Check if the target is RA compliant

Sequence (1-3)

The vertical provides a target ID to the RA server to check if this target can perform an RA. The target ID can be for instance an IP address.

Step 2: Instantiation of the RA service

Sequence (4-12)

If the target is RA compliant, the vertical can ask to instantiate the RA service on it. Upon receiving this request, the RA server checks first whether the target is already instantiated and ready to perform attestations (6). If it is the case, the vertical can ask for an attestation (Next sequence). Otherwise, the RA server will upload and instantiate the target.

Step 3: Attestation request

Sequence (13-20)

In this sequence, the vertical should precise the type of the requested attestation (e.g., deep attestation [9]). He can also provide some parameters needed to compute and verify the attestation like a nonce. Upon receiving the request, the RA server triggers the corresponding agents running on the target.

Step 4: End of the service

Sequence (21-24)

When the vertical receives the requested attestation, he can decide to clean up the target from all the RA materials.

2.9.6 Post conditions

The use case ends successfully if:

- The target is RA compliant, i.e., can install the RA software and can run the RA protocol.
- The RA Agent correctly installs the RA software
- The quote (computed by the RA agent) is valid:
  - The signature is valid
  - The key certificate is valid
  - The signed message (i.e., measures) is valid.

2.9.7 Success criteria

Our goal in this use case is to find the right balance between the security of the service provided by the vertical, the security and privacy of the used infrastructure, and the sovereignty of her Infrastructure Operator. In this context, RA enabler can be of interest. Indeed, RA protocol can enable the vertical to check that a given property is ensured by a specific node. However, this can breach the privacy and security of the infrastructure (threatening the sovereignty of the Infrastructure Operator). Indeed, the vertical must upload some software in the designated node and hence can collect private data and interfere with the basic operations of the infrastructure. In order to prevent this kind of security breaches and reduce the attack vector on the used infrastructure, the main idea is that only the Infrastructure Operator can directly communicate with his infrastructure. To verify a property on the infrastructure, the vertical has access to an API provided by the RA Server. Obviously, this implies that the vertical and the Infrastructure Operator (i.e., RA server) previously agreed on the means (e.g., the software to be used, the data to be collected) to check a given property. Consequently, the RA enabler will prove to the vertical that the right means have been used to check a specific property enabling the vertical to trust the results of the RA enabler.

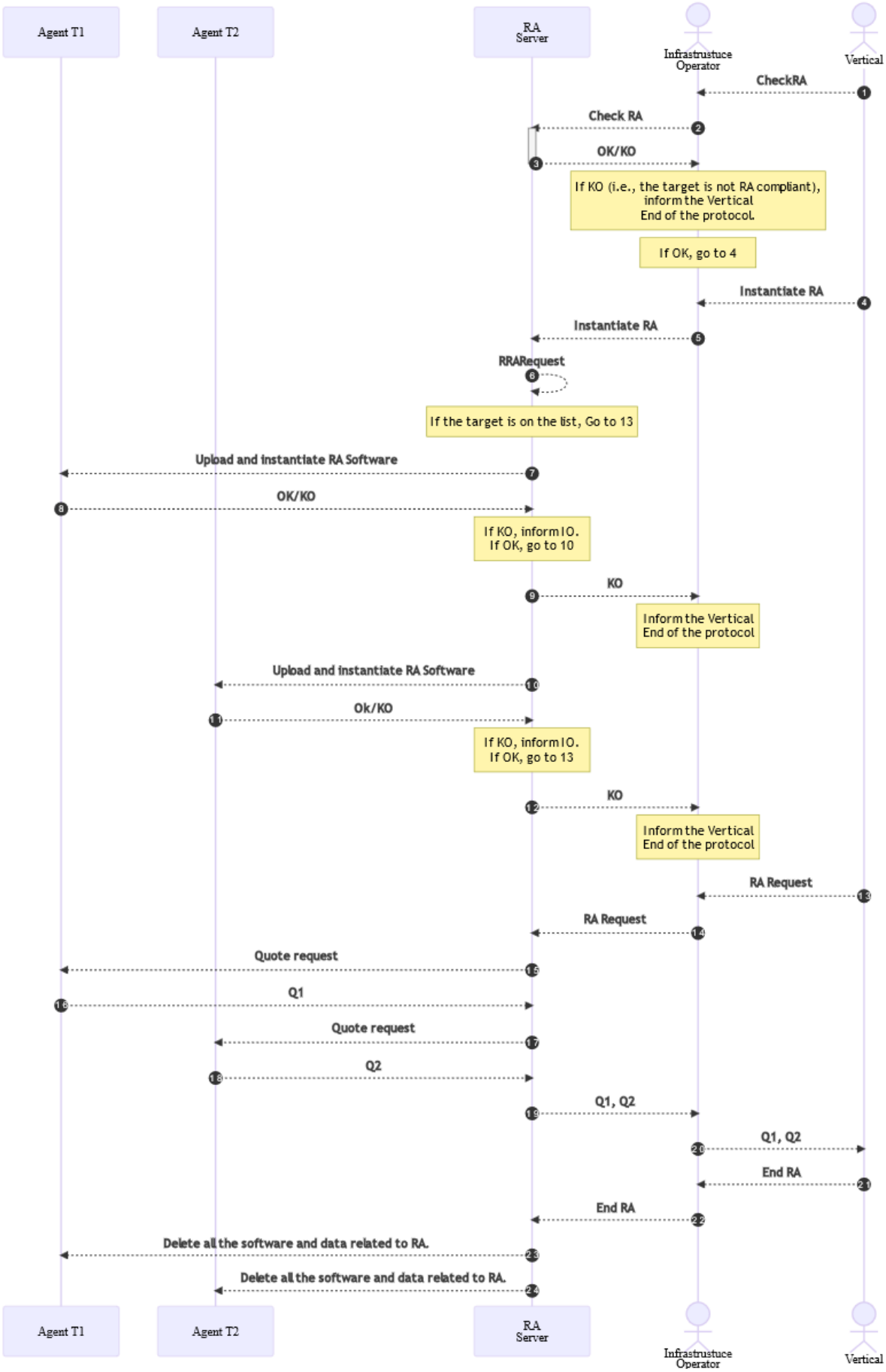

Figure 26: Basic flow for the UC I

2.9.8 Use case summary

The main idea of the use case is to enable a vertical using an infrastructure to verify some security properties about this infrastructure without impacting the privacy and security of the infrastructure neither the sovereignty of the infrastructure Operator. First, the vertical and the Infrastructure Operator agree on the means (e.g., the used software, the type of the collected data, frequency of the checks…) used to check properties. Then, the infrastructure provides an API on the RA server. The RA server will then prove to the vertical that a security property is guaranteed by proving that the right means have used to do so.

2.9.8.1 Mapping on INSPIRE-5Gplus architecture

The RA enabler (designated by the orange circle in Figure 27) can be part of the trust management domain namely the RA server. Regarding the RA agents, they are part of domain infrastructure / resources.

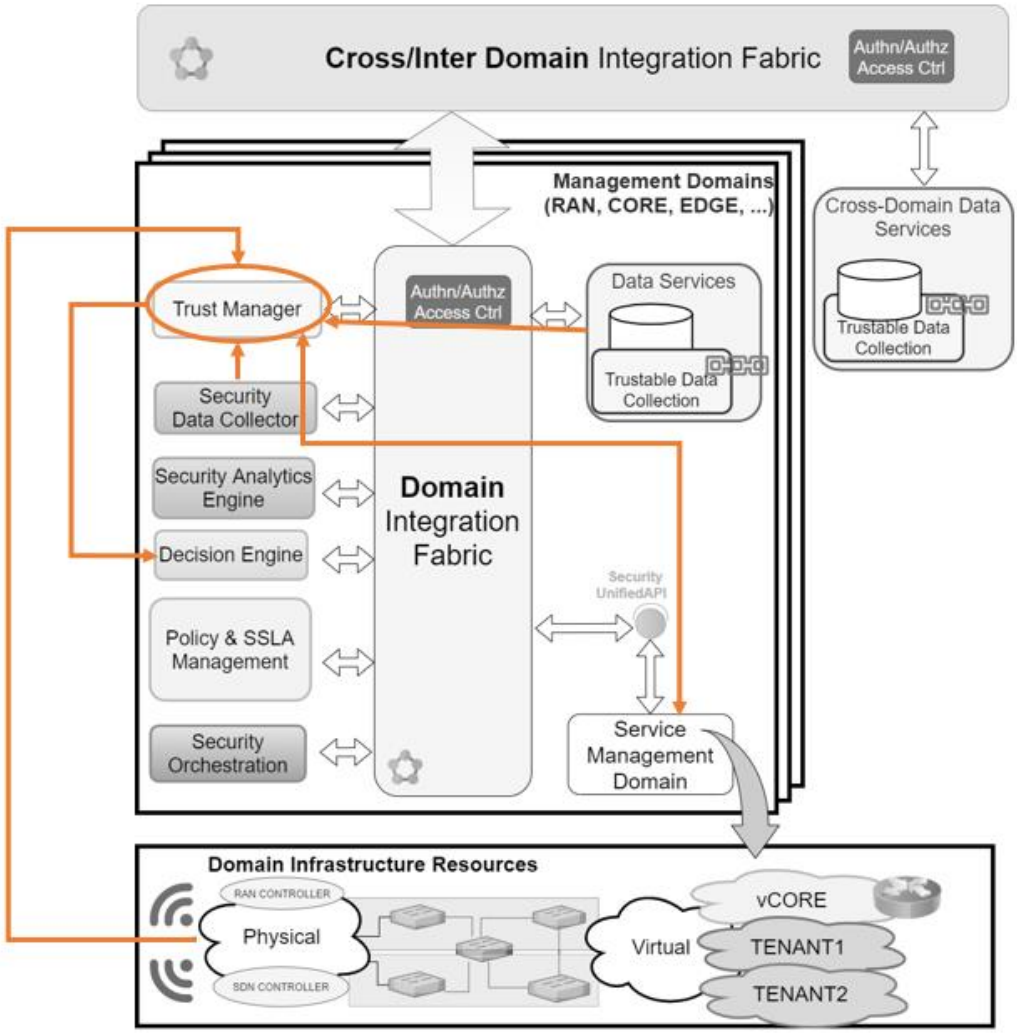

Figure 27: UC I mapping to INSPIRE-5Gplus HLA

2.9.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- RA (Remote Attestation)

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.10 UC J - Isolation of critical components over virtualized infrastructure

2.10.1 Problem description

The aim of this use case is to show a first Trust and Liability management concepts on a virtualised infrastructure for a 5G type ecosystem.

The existing or planned legal and standard frameworks and vertical needs show that 5G and B5G infrastructures will have to meet heterogeneous requirements (e.g. Cybersecurity Act[7], NIS directive[8] and regulations or standards related to 5G verticals like eHealth, Transport, Energy, Vehicular, industry under Seveso[9] directive, etc.), and be able to dynamically (almost in a near real time) adapt. The simple (state-of-the-art) strategy to implement the highest level of security (CyberSecurity Act has defined 3 levels: Basic, Substantial and High for system and product assurance levels) is unrealistic. Some requirements may be incompatible. Most use cases do not need the strongest possible security level. 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 is a massive task that could increase the costs of some configurations in an unbearable manner.

2.10.2 Goals

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

- First, in a virtualized environment, under the state of the art, the request of isolation of critical services from basic services is not resolved and generally leads to the request to put in production dedicated physical infrastructure to operate those critical services (for instance a dedicated physical infrastructure to operate virtualized Lawful Interception services in communication networks). By formalizing those security requirements in terms of co-localization constraints or level of criticality we could support them thanks to a placement optimization algorithm - the new orchestration of physical resources to serve the needs of those services (critical and basic). This placement algorithm takes into account several constraints and could manage in the near future latency (end to end slices) or energy consumption to compute the optimal orchestration over multi-site infrastructures.
- Second, as we commit to isolate critical services from basic services, we need to be able to demonstrate without given direct physical access to the infrastructure that commitment is fulfilled. The Deep Attestation framework proposes an elegant way to resolve this issue as long as we can agree with the Client the way to measure this isolation. In our specific use case, we claim services are isolated between each other regarding their affinity or criticality constraints and deliver the tool to collect on each physical server the cartography of active services and their criticality level. As the Deep Attestation framework operates this security properties on each requested servers and protects (by digital signature) each property thanks to the attestation scheme, we could in consequence deliver evidences directly to Client that we have resolved in the right way affinity and anti-affinity conflicts on each targeted server.

[7] https://eur-lex.europa.eu/eli/reg/2019/881/oj

[8] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[9] https://eur-lex.europa.eu/eli/dir/2012/18/oj

2.10.3 Actors

The actors and their roles involved in this UC are:

- Virtualized Infrastructure Operator
- Client / Vertical which requests isolation of its critical services
- Deep Attestation framework: which operates measure to deliver evidence
- The Placement Optimization System coupled with infrastructure Orchestration System

2.10.4 Preconditions

- Client has predefined its slice or chain of components to be operated over the infrastructure;
- Client and Infrastructure Owner commit to the subset of Client critical components, which need to be isolated from other components (third party) operated by the infrastructure owner;
- Client and Infrastructure Owner commit on the way to measure effectiveness of components isolation, based on tools proposed by Infrastructure Owner.

2.10.5 Basic flow

The basic flow of actions of the actors and the system:

1. Infrastructure Operator deploys components according to isolation requests - it performs components placement optimization with security constraints;
2. The isolation is measured according to the agreed measurement method and the evidence of isolation is delivered to Client;
3. In the component operation phase Client may request delivery of evidence of isolation in an on-demand manner.
4. On each request the isolation is measured according to the agreed measurement method and the evidence of isolation is delivered to Client;

2.10.5.1 Diagram

Figure 28 illustrates the basic flow of UC J.

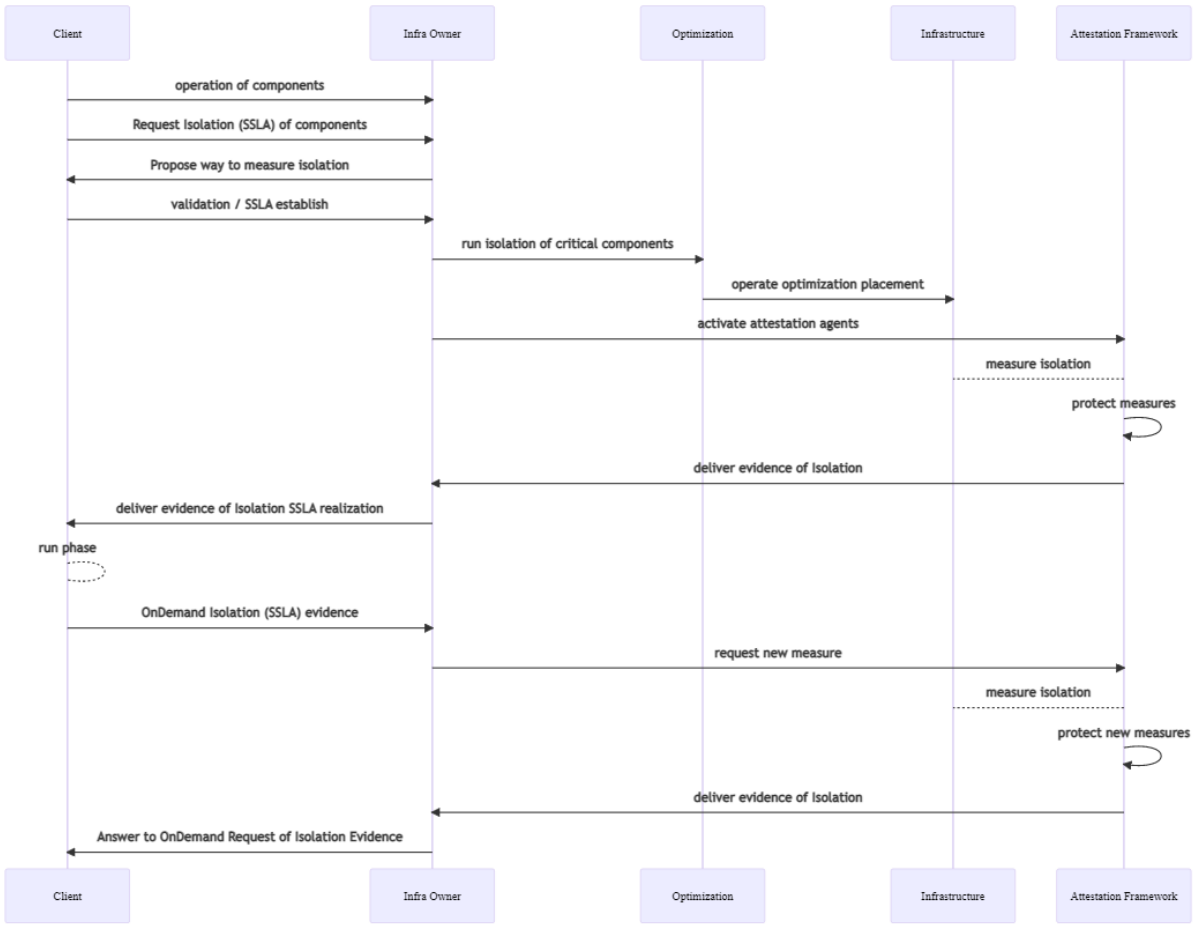

Figure 28: UC J diagram

2.10.6 Success criteria

Client and Infrastructure Owner agree on the real isolation of Client's components thank to the proposed way to measure isolation effectiveness (connected to Deep Attestation framework).

2.10.7 Use case summary

Client requests a specific security service to protect its production chain and the infrastructure provides evidence of this security service effectiveness.

2.10.7.1 Mapping on INSPIRE-5Gplus architecture

The proposed use case can be part of the trust management domain thank to the RA server, and part of domain infrastructure / resources thank to:

- RA agents
- Security by orchestration enabler that controls the orchestration delivered at infrastructure domain.

The Client request for its components isolation is naturally part of Policy and SSLA management component.

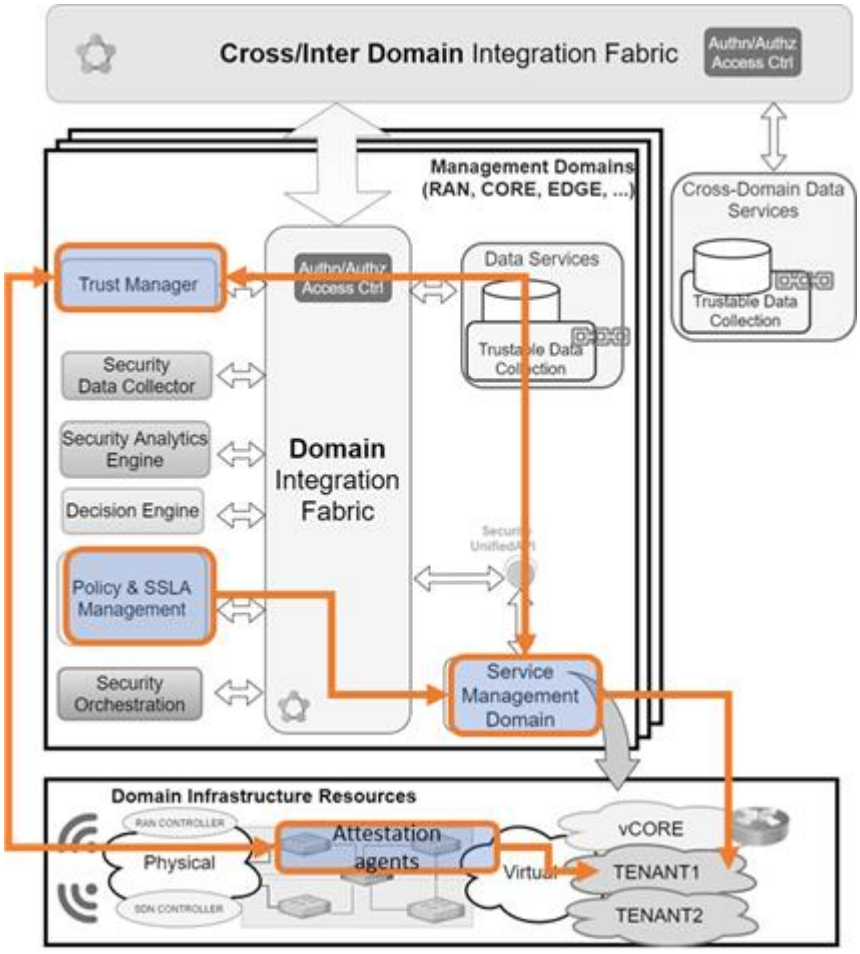

Figure 29: UC I mapping to INSPIRE-5Gplus HLA

2.10.7.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case (in a first implementation level) are:

- Security by Orchestration enabler
- Remote Attestation enabler

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.11 UC K - Placement of MEC Applications with Security Constraint

2.11.1 Problem description

Multi-access Edge Computing (MEC) is one of the key enablers in 5G, offering to external parties computing capabilities very close to end users. The main advantage of MEC is the location of computing resources, that minimizes both the latency of communication between devices and relevant applications and consumed core network bandwidth.

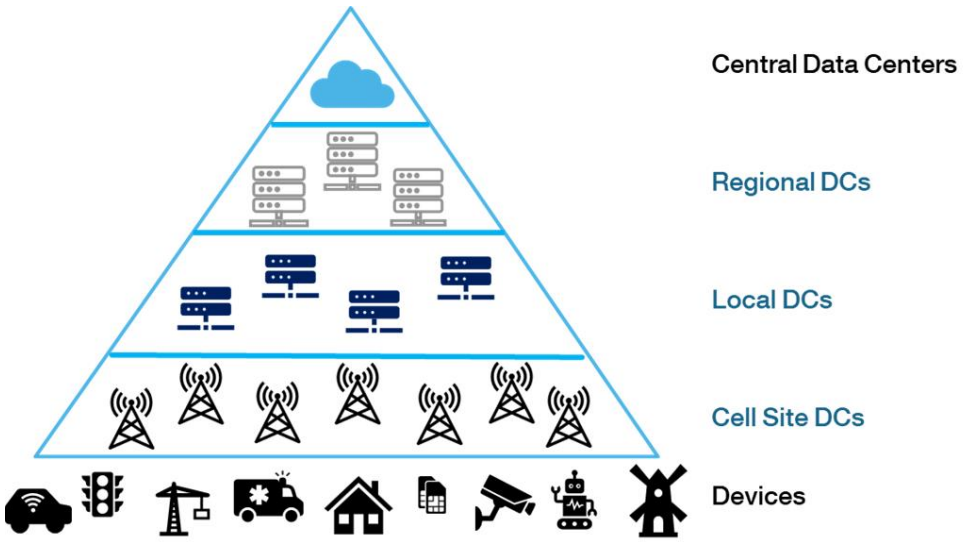

Figure 30: Multi-layer edge hosting infrastructure model

The resources available in multiple geographically distributed locations (Figure 30) are limited and more expensive than in the central cloud, thus the placement optimization of MEC applications becomes competitive advantage for service provider. However, the diversity of the Verticals Industries (e.g. Healthcare, Logistics, Media and Entertainment, etc.) and theirs applications, results in additional heterogeneous requirements related to application hosting services. Security related requirements are often imposed by specific domain security regulations. Requirement of isolating sensitive workloads from non-sensitive ones is derived from fact that the malicious application can be deployed among benign applications in MEC hosting environment that serves multiple tenants and enables execution of user-provided code.

This requirement can be the part of Security SLA related to MEC application hosting and needs to be supported in the application orchestration process.

2.11.2 Goals

The placement of MEC applications in Edge data centres is performed by MEC Orchestrator taking into account required performance and latency. The optimization of applications placement needs to be extended with security constraints (defined in SSLA).

For fulfilling isolation constraints, the following hypothesis is used: *MEC application instances can be placed on the same physical node if and only if each of them has security level equal or higher than the maximum of requested isolation levels by each of them*.

It assumes that security level *sec_lvl* is assessed for each MEC application and application owner may request isolation_level *iso_lvl* not higher than *sec_lvl*:

$$iso\_lvl \leq sec\ \_lvl$$

2.11.3 Actors

The actors and roles involved in this use case are:

- MEC Service Provider (MSP) – entity operating MEC hosting service.
- MEC Infrastructure Provider (MIP) – entity operating MEC infrastructure.
- Edge Application Providers / Verticals (AP1, AP2, ..., APn) - multiple entities delivering MEC applications to be deployed on MEC infrastructure, together with all data needed for application placement (including security constraints).

MSP and MIP can be embodied by the same legal entity.

2.11.4 Preconditions

The preconditions include:

- The detailed description of infrastructure topology is available for MSP and includes parameters of data centres, servers and connections (all infrastructure parameters used for placement optimization)
- Application Providers prepare applications to be deployed in MEC and specify requirements related to latency, isolation level and required resources for each estimated location of application instance.
- The security level for each application is determined in the assessment process.
- MSP's MEC orchestration process is able to perform optimal allocation of resources for applications meeting all requirements (including isolation).

2.11.5 Basic flow

UC K includes the following sequence of actions:

1. Application Providers (Verticals) express their security requirements related to 5G services they use including MEC application hosting (isolation level) - these requirements are included in Security SLA.
2. Application provider requests to deploy the set of MEC application instances according to presented requirements related to latency and isolation level and required resources and location for each application instance.
3. MEC Orchestrator in MSP ingests the description of infrastructure.
4. MEC Orchestrator in MSP aggregates MEC applications data and requests calculation of the optimal placement for all applications instances in the given infrastructure.
5. Based on placement optimization results, MEC Orchestrator sends appropriate MEC application instance deployment requests to respective MEC Infrastructure Manager in MIP which instantiates requested MEC application instances on specific servers of MEC infrastructure.

The modification of placement (changing number of instances, adding or removing MEC applications) requires new placement optimization and deployment cycle. The optimization algorithm should take into account already running instances and minimize their relocation.

2.11.5.1 Diagram

Figure 31 illustrates the basic flow of UC K.

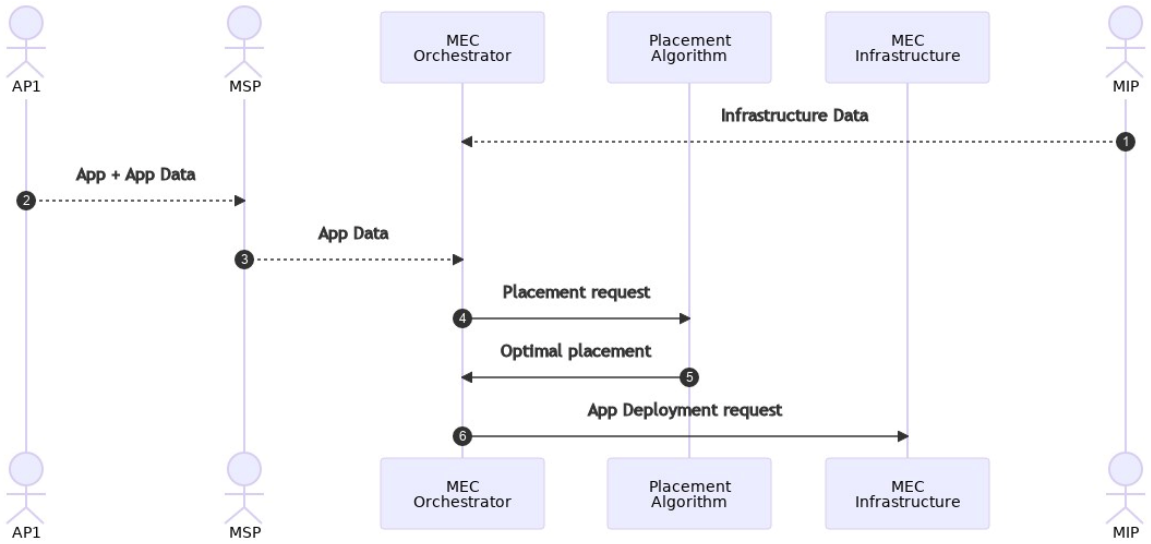

Figure 31: UC K diagram

2.11.5.2 Alternative Flows

The execution of MEC application on indicated server can be protected by anchoring a VM of MEC application instance to a specific location. Various anchoring schemes offering different security levels can be established, all based on a functional dependency from the software to a platform-provisioned secret. The protection of the secret, namely in TEE (e.g., Intel's SGX) enhances the solidity of the link.

2.11.6 Post conditions

After deployment of MEC applications instances on MEC infrastructure, the support of isolation requirement according to the assumed hypothesis should be verifiable. The verification results should be made available to Application Providers.

2.11.7 Success criteria

The placement of MEC application instances should be optimal while keeping the security requirement, the following optimization criteria can be considered:

- Latency – the overall latency of all instances should be minimized: such a placement will offer the best quality (the lowest latency) for application users, but it will enforce use of servers located close to devices (which are typically the most expensive), however, for some applications, improvements of latency beyond the required level can go unnoticed;
- Cost – the cost of running all application instances (the cost of used vCPUs) should be minimized: it will give competitive advantage for application/service providers hosting their application in MEC;
- Energy consumption – the cost of energy for running all application instances should be minimized: it will prefer more energy efficient edge servers to support greener operations.

The final success criterion is optimal placement of MEC applications over available infrastructure while keeping the security constraints defined in SLA.

2.11.8 Use case summary

This use case illustrates how the security requirements related to isolation can be used within MEC

application orchestration process.

The proposed physical separation based on the security level of other applications sharing the same resources is the initial approach to define security constraints. Other solutions can use improved virtualization mechanisms, isolation monitoring during runtime, etc.; but in every case, the isolation constraints impact the placement of applications over available resources.

2.11.8.1 Mapping on INSPIRE-5Gplus architecture

The Figure 21 shows which HLA elements in a domain are involved in the UC and their interactions.

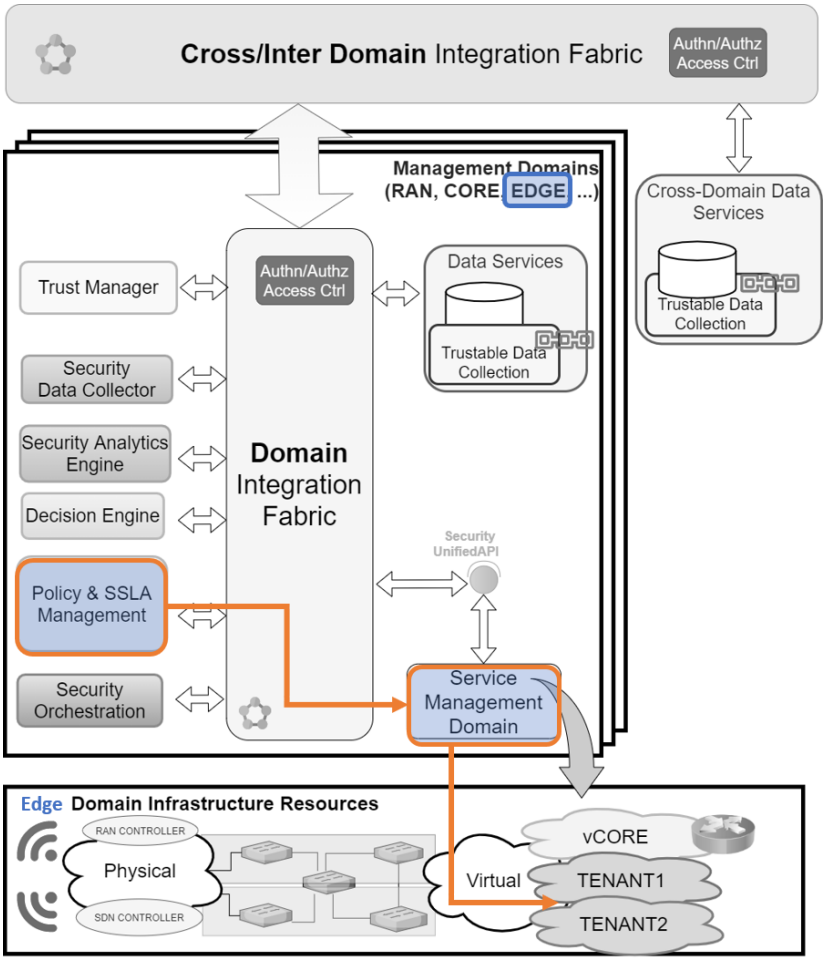

Figure 32: UC K mapping with the HLA functional component

2.11.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Security By Orchestration for MEC enabler - implements the placement optimization algorithm.

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.12 UC L - Secured and Sliced ACCA (Anticipated Cooperative Collision Avoidance)

2.12.1 Problem description

Vehicular communications are expected to generate a considerable traffic volume in the near future, because of the different communications that may occur within and around a vehicle (i.e., vehicle to vehicle, vehicle to pedestrian, etc.). Security becomes important not only for the data but also for the safety of the people. This UC is based on the experience obtained during the development of the Anticipated Cooperative Collision Avoidance test case belonging to the EC 5GCroco project.

This UC is illustrated in Figure 33 and it is focused on the automotive vertical. This UC proposes a road scenario with two Road-Side Units (RSUs) and a Central Node (CN) using an application to exchange messages. The RSUs gather the information sent by a set of vehicles moving across a road and forward it to the CN. By sharing information, vehicles may communicate with each other and inform about the road status (i.e., accidents, traffic jams, etc.) and so, each vehicle may adapt its travel. This UC shows the cooperative vision side of the near-future automotive services and scenarios, for this reason it is necessary to ensure that all the information shared among vehicles and the infrastructure contains what it really happens in the road and near surroundings. For this reason, this UC studies how to protect all the benign nodes from a malicious one aiming to distribute a fake accident (i.e., disinformation attack).

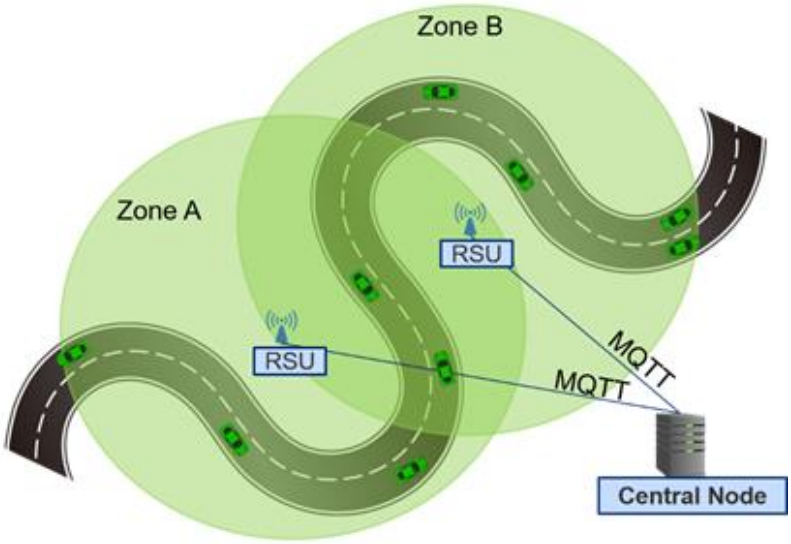

Figure 33: UC L scenario.

2.12.2 Goals

The goals of this UC are the use of Network Slicing and the re-configuration of its elements. More specifically, this UC aims to deploy a Network Slice for a communications vehicle application between the two RSUs and the CN with a set of Security Functions (SFs) containing a Firewall for each RSU and an Intrusion Detection System (IDS) in the CN. The traffic coming from the RSUs will be analysed and the IDS will determine whether a vehicle can be trusted or not. Depending on it, its traffic will be blocked by the firewalls. The main goal is to re-configure an End-to-End (E2E) Network Slice using Security Service level Agreement (SSLA) to block the fake traffic generated by a malicious vehicle.

2.12.3 Actors

The actors and roles involved in this UC are:

- Service Provider (SP)
- A set of vehicles (Ann, Bob, etc.)
- A malicious vehicle (Mallory)
- Mobile Network Operator (MNO) -> Owner of the RSUs and Central Node.

2.12.4 Preconditions

In order to demonstrate the complete use case, a Network Slice using Security Service Level Agreement (SSLA) must be deployed. This Network Slice is illustrated in Figure 34 and it is composed by a V2X Communications Application with a central MQTT Broker and two child MQTT clients. Moreover, attached to them, there are Security Functions (SFs) to control possible intrusions and block them.

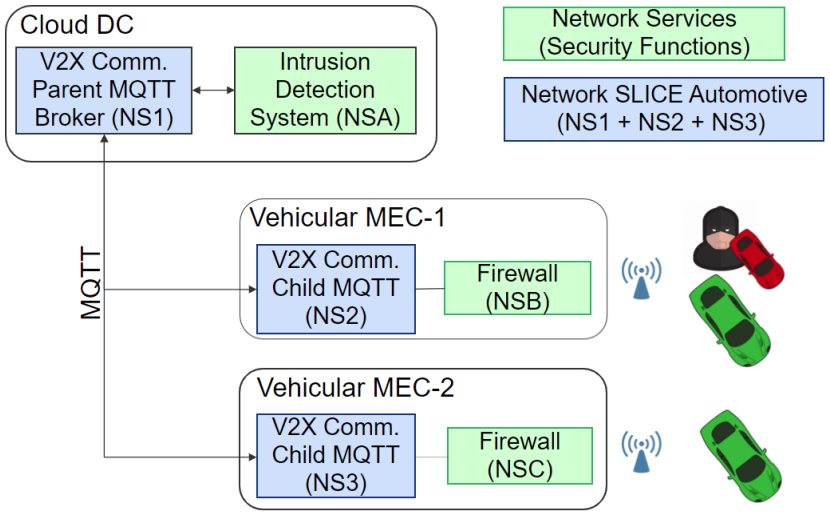

Figure 34: Network Slice Design for the UC L

The first precondition is the correct deployment of the Secured Network Slice. Then the second precondition is the creation of a set of vehicles (Ann, Bob, etc.) with one of them being the malicious attacker (called Mallory).

2.12.5 Basic flow

The basic flow consists of the following steps:

1. Normal Operation: Once the Network Slice and the SFs are deployed, the service is ready to be used by all the vehicles which travel across the road using that service.
2. Attack Begins: Mallory starts to generate fake information describing a car accident to disrupt the normal flow of the traffic on the road.
3. Malicious Data Detection: The V2X IDS detects there is a wrong data flow and based on the SSLA, the appropriate action is applied to solve the situation. The firewalls placed in the Road Side Units (RSUs) are re-configured in order to block the malicious data.
4. Attack Blocked: The malicious data from Rob is blocked and not distributed, and so, all the non-malicious vehicles can get the real data to move normally.

2.12.5.1 Diagram

Figure 35 illustrates the basic flow of UC L.

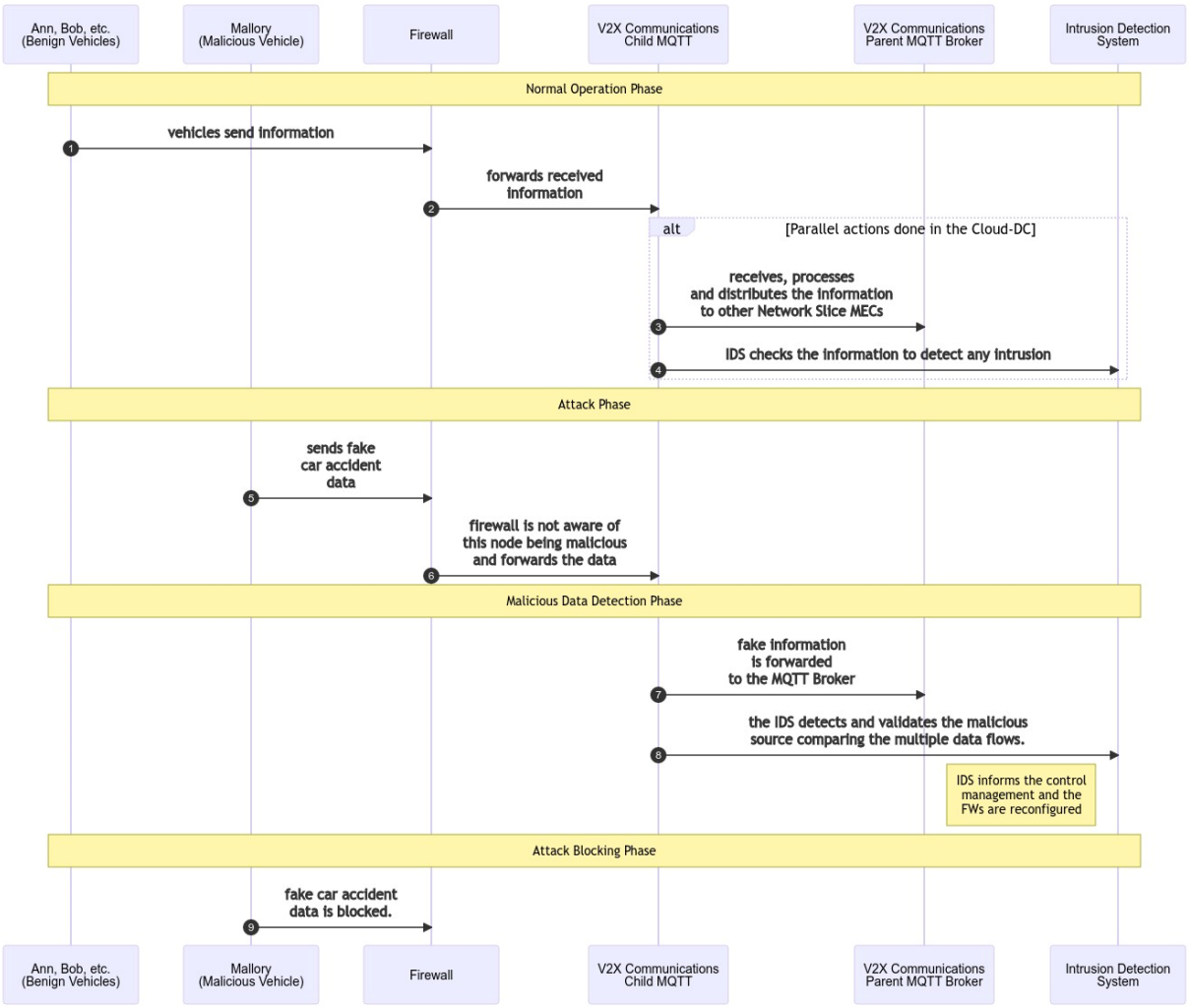

Figure 35: UC L attack and remediation diagram

2.12.6 Post conditions

The final result will lead to the following post conditions:

- the E2E Network Slice and the Security Function containing a Firewall are re-configured and updated. By doing this, the latest information is added in order to block the traffic coming from the evil vehicle.
- the evil vehicle does not obtain any benefit or generate any trouble, so its existence is not a danger anymore.

2.12.7 Success criteria

The goal will be achieved if after the intrusion is detected, the Network Slice is re-configured and the malicious traffic generated by the intruder's IP address is blocked and not shared among the other nodes.

2.12.8 Use case summary

2.12.8.1 Mapping on INSPIRE-5Gplus architecture

This UC focuses on the deployment of a Network Slice and its reconfiguration based on a condition. For this reason, the HLA elements involved in this UC are illustrated in Figure 36.

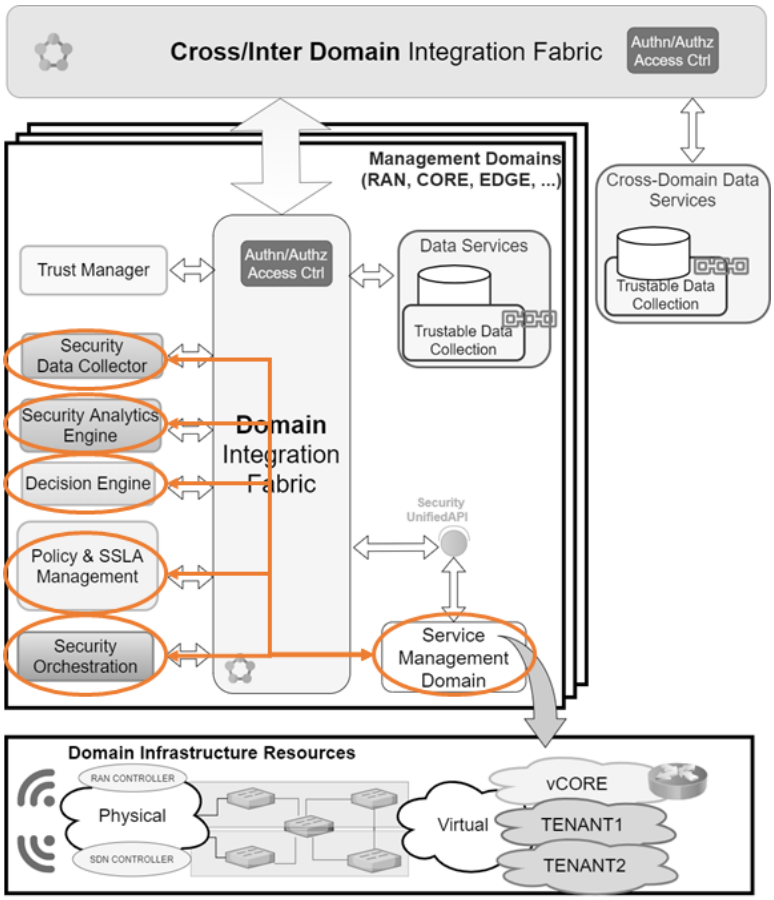

Figure 36: UC L mapping with the HLA functional components

This UC aims to solve security situations generated on a vehicular scenario by using SSLAs to react against an attack that tries to generate fake information. Showcasing SSLAs and Policy Management (Section 2.7 in D2.2 [6]) is the main objective. In this UC, the use of SSLAs at a Network Slicing level will allow to deploy security elements around the Network Slice for an automotive vertical. By using SSLAs, this UC presents how a set of security resources will be configured and then monitored, in order for the whole system to react when a malicious action appears and finally solve it.

2.12.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Secured Network Slice Manager for SSLA: to manage the Network Slicing resources and their association with an SSLA.
- Security Orchestrator: to manage the security policies around the Network Slice.
- SSLA Manager: to manage the SSLA objects available to define the security requirements around the deployed Network Slice.
- Policy Framework: to manage the policies available to be implemented based on certain conditions (an attack, missing resources, etc.)

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.12.8.3 Comments

This use case is closely associated to the ICT-18 5GCroCo Anticipated Cooperative Collision Avoidance use case requiring real-time operation (i.e., high reliability and low latency). Within the context of INSPIRE-5Gplus, it was introduced in D2.2 [6] as illustrative use case IUC1 and it was planned to be part of the test case number 1 described in D5.1 [8], but based on the project requirements, this UC has evolved to become part of one of the final demonstrators (Demo 1).

2.13 UC M - Trusted and Collaborative Cross-border ACCA (Anticipated Cooperative Collision Avoidance)

2.13.1 Problem description

This UC keeps the vehicular environment like the previous UC, but this time its focus is on the deployment of E2E Network Slices in a cross-border scenario. With the co-existence of different operators, a possible distrust among them by lack of a common trust mechanism or public data available may be generated which will need to be managed and solved. While the common solution on this kind of scenarios is the use of contracts and agreements, this UC proposes the use of Blockchain to generate trust among the different operators and other actors and allow the collaboration among them to deploy E2E Network Sliced composed by certified elements. Like the previous UC, this is also based on the experience obtained during the development of the Anticipated Cooperative Collision Avoidance (ACCA) Test Case belonging to the EC 5GCroco project.

2.13.2 Goals

The scenario of this UC is presented in Figure 37: UC M scenario and it aims to use a vehicular scenario in which different cross-border operators work together to deploy an E2E Network Slice for an automotive service by collaborating with each other using Blockchain to control the multiple steps. The deployed E2E Network Slice will be composed only with certified resources.

This UC aims to add trustworthiness to any deployed network slice by ensuring that all the components composing a network slice have been previously certified and its related actions are shared and publicly known among all the players through a Blockchain network. This UC focuses on the fact that in the future, operators will not be an isolated entity, and so, they will need to cooperate and collaborate among them. Blockchain is the key element in this UC as it allows to define and implement a trust-based solution where the service providers may request the deployment of E2E Network Slices across a multi-operator domain scenario. The fact of using Blockchain will allow the definition of a common set of rules (using Smart Contract objects) to ensure a trustworthy and transparent use of the different domain resources.

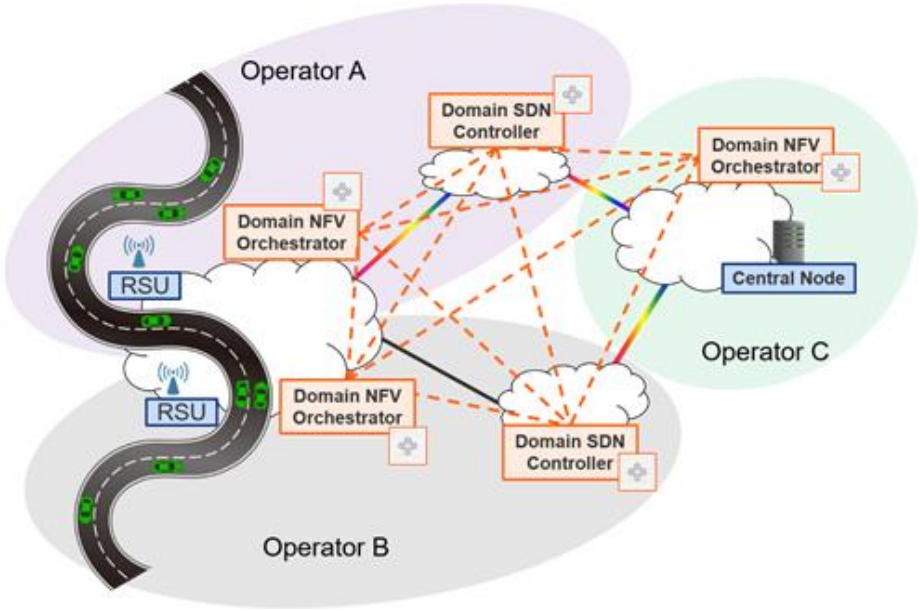

Figure 37: UC M scenario

Blockchain keeps track and makes public the E2E Network Slices and their elements -i.e., network services and functions-. The Blockchain network will be composed by Network Slice Managers (NSMs) and Software-Defined Network (SDN) Controllers belonging to the different operators.

2.13.3 Actors

The actors and roles involved in this UC are:

- Service Provider: The owner of the deployed service.
- Service Developer: The designer of the deployed service.
- (Cross-border) Operators: Owners of the RSUs and Central Node.

2.13.4 Preconditions

A Blockchain must be configured and ready to work having a set of SDN and NFV Controllers/Managers from different domains as its peers.

2.13.5 Basic flow

The basic flow consists of the following steps:

1. Network Slice Resources Design and Certification: A Service Developer designs a set of descriptors to deploy Network Slice resources and checks them with the Component Certification Tool.
2. Network Slice Resources Distribution: If they are certified, they are shared in the Blockchain so the other peers may trust them and requests a deployment of those resources.
3. Network Slice Deployment: A Service Provider may deploy Network Slices using resources from the different cross-border operators in order to offer the automotive communication service.

2.13.5.1 Diagram

Figure 38 illustrates the basic flow of UC M.

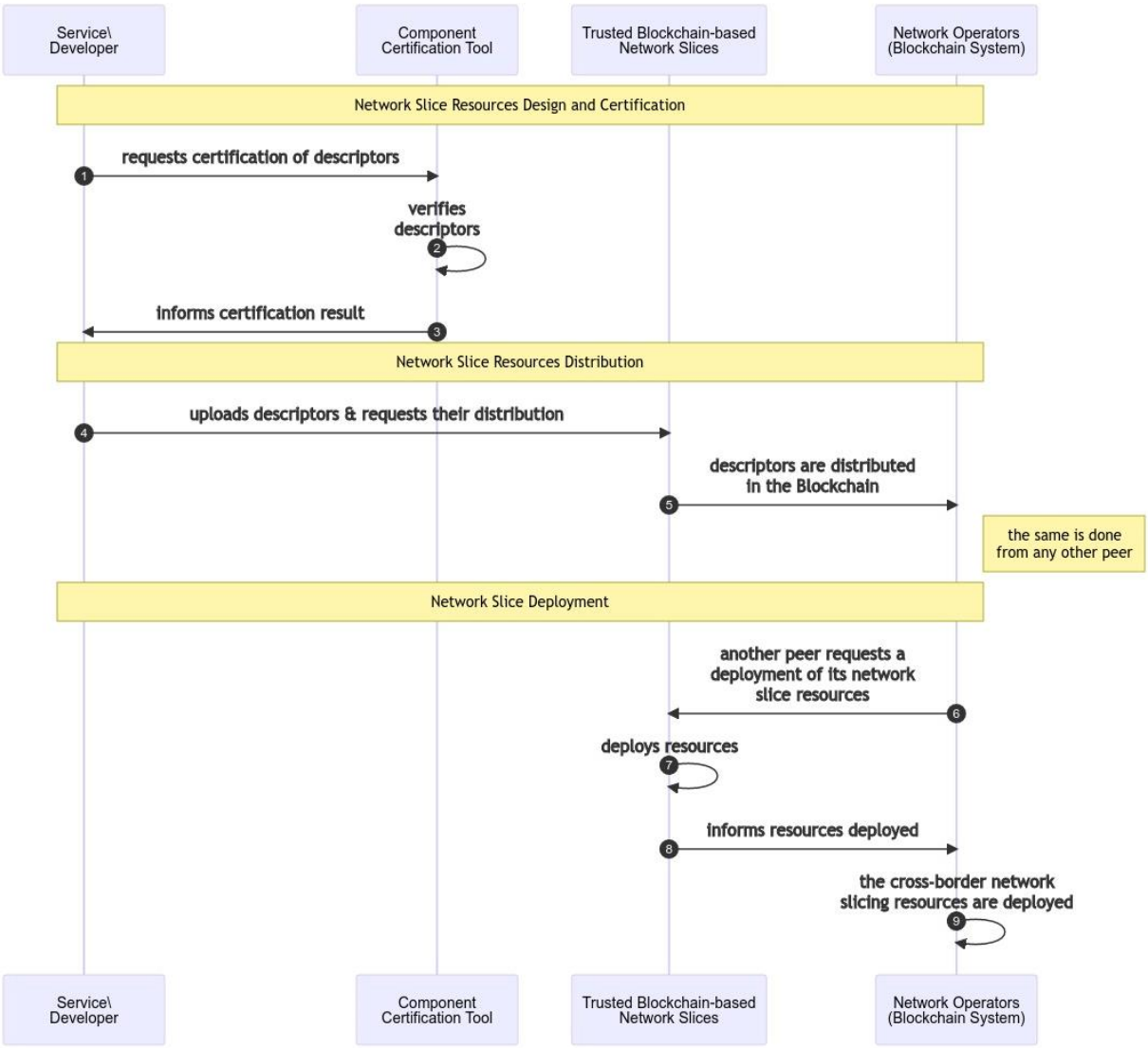

Figure 38: UC M certified blockchain network slice resources selection and deployment diagram

2.13.6 Post conditions

The results should be the acceptance and deployment of the Network Slice Templates (NSTs) and its components that were previously validated and tagged as trustworthy.

2.13.7 Success criteria

The goal will be achieved only if the trustworthy NST and components are accepted and deployed and any Service Provider is able to deploy a non-trustworthy NST using a Network Slice Manager participating in the Blockchain system.

2.13.8 Use case summary

2.13.8.1 Mapping on INSPIRE-5Gplus architecture

As this this UC is based on the use of the DLT technology, within the INSPIRE-5Gplus HLA (Figure 39), it is closely related to the Trustable Data Collection distributed in both: the E2E and the domains below.

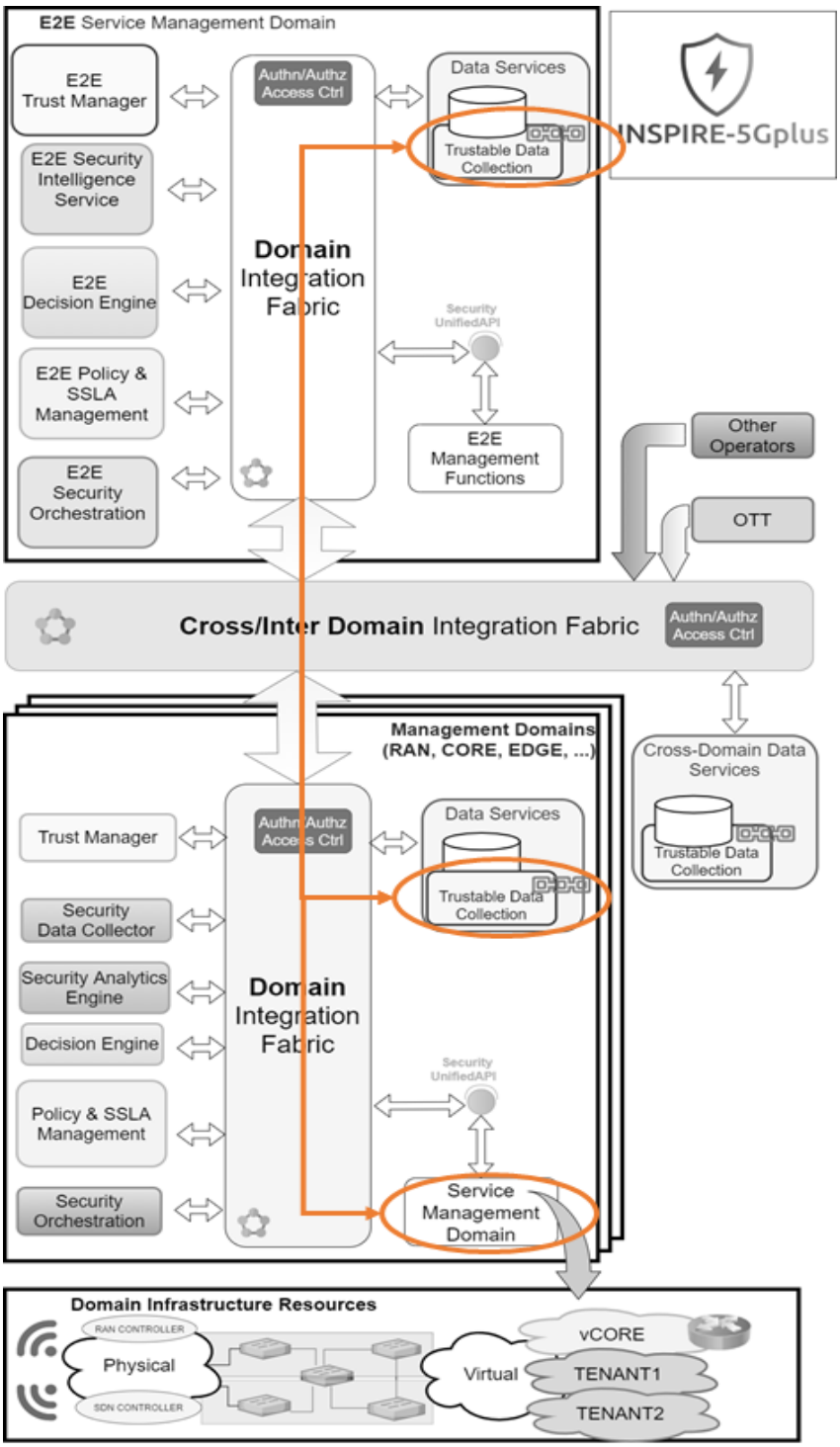

Figure 39: UC M mapping with the HLA functional components

This UC shows a scenario in which trust among different actors is the key aspect. To generate this trust among them, this UC makes use of Distributed Ledger Technologies (Section 3.2 in D2.2 *[6]*). In this UC, the DLT is implemented to manage in a collaborative way the deployment of Network Slices resources in a cross-border scenario. The key element to implement this collaborative procedure is the use of Smart Contracts. Smart Contracts will allow the exchange of information and to trigger different procedures in a public and transparent way, so all the peers involved in the Blockchain network will be aware of any action in the deployment procedure. Within the HLA, the functionalities implemented in the enablers used are the “Service Management Domain” and the “Trustable Data Collection” at both domain and E2E level.

2.13.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Trusted Blockchain-based Network Slices: this enabler allows to a Network Slice Manager and/or an SDN Controller node to become part of the Blockchain network
- Component Certification Tool: this enabler would manage the data objects to certify that the elements describing a Network Slice could be trusted by all the peers in the Blockchain network.

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.13.8.3 Comments

This use case is closely associated to the ICT-18 5GCroCo Anticipated Cooperative Collision Avoidance use case requiring real-time operation (i.e. high reliability and low latency). Finally, this use case was introduced in D2.2 [6] as illustrative use case IUC2 and it was planned to be part of the test case number 1 described in D5.1 [8] but based on the project requirements, this UC has remained as a UC with some enabler initial results delivered in D4.1 [4].

2.14 UC N - End-to-End Slice Protection based on Moving Target Defense and Anomaly Detection

2.14.1 Problem description

Novel telecommunication networks in 5G/B5G present growing complexity as Mobile Network Operators (MNO) get more decentralized, using Multi-access Edge Computing (MEC), and more virtualized, using container-based and VM-based network functions. With MEC, services become distributed over multiple nodes physically closer to end-devices and with direct access to the RAN. With the virtualization, the heterogeneity of the environment increases with the diverse nature of the hosted services, ranging from Ultra Reliable Communication Latency (URLLC) to massive Machine Type Communications (mMTC), and enabling the development of network slices.

Network slices are challenging systems to protect. The main problem relies in their significant attack surface, coming from the above-mentioned properties. They can be attacked at the physical layer, starting from the infrastructure hosting and running them. For instance, MEC edge nodes are usually in public areas and are physically more accessible than the Core Network.

The virtualization layer can also be another root cause for security incidents. For instance, a network slice is composed of several network services (NS), some of which may be shared among other network slices, reducing their isolation. In large-scale systems such as telecommunication networks, the impact of an attack propagating through shared NSs could be catastrophic. Shared VNFs could be tampered, i.e., maliciously modified to use it as a vector for other attacks, such as Command and Control (C&C).

The management of network slices is under the responsibility of the MNO, who generally does not have full access to them as they can be provided to third parties as private networks. Along with the fact that traffic is mostly encrypted, the MNO has to heavily rely on traffic analysis, inferring on what is an expected traffic behavior and what is an anomaly.

To conclude, 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.

2.14.2 Goals

To solve each of the above-mentioned problems, UC N 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 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 Moving Target Defense (MTD), which mechanism 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 (C&C), DDoS, VNF tampering, and network slice compromises.

2.14.3 Actors

The actors and roles involved in this UC are:

- The MNO managing the 5G infrastructure
- The Service Provider (SP) deploying its services over the MNO infrastructure
- The Network Domains of the 5G network (i.e. RAN, Core, Transport, and Edge domains)
- An attacker

2.14.4 Preconditions

For the deployment of UC N, the preconditions required are the same as previously listed in D2.2, namely:

- An operational 5G SA implementation, including the actor Network Domains, a MEC edge node, and end-users connected with UEs.
- At least two network slices running concurrently; one operating as the MNO public network, and one as a private SP network slice. Network slices have different service requirements, e.g., eMBB, URLLC, and/or mMTC.
- An attacker who can get access to an edge node and publicly interfaced VNF or NS.

2.14.5 Basic flow

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 Figure 39) collect monitoring data and send them to the Monitoring Framework.
2. The *Monitoring Framework* parses and processes the raw data, feeding them to the Security Analytics Engine.
3. Different anomaly and attack detection services in the *Security Analytics* Engine (i.e., SAF and System enablers) generate higher-level data and security alerts, feeding them to the *Decision Engine*.
4. *In the* Decision Engine, the OptSFC enabler decides a mitigation or a prevention MTD action, forwarded to the MTD controller for enforcement.
5. The MTD controller, which is a part of the Security Orchestration, coordinates with the network slice manager to enforce the MTD action in the relevant slice(s) component.

2.14.5.1 Diagram

Figure 40 illustrates the basic flow of UC N.

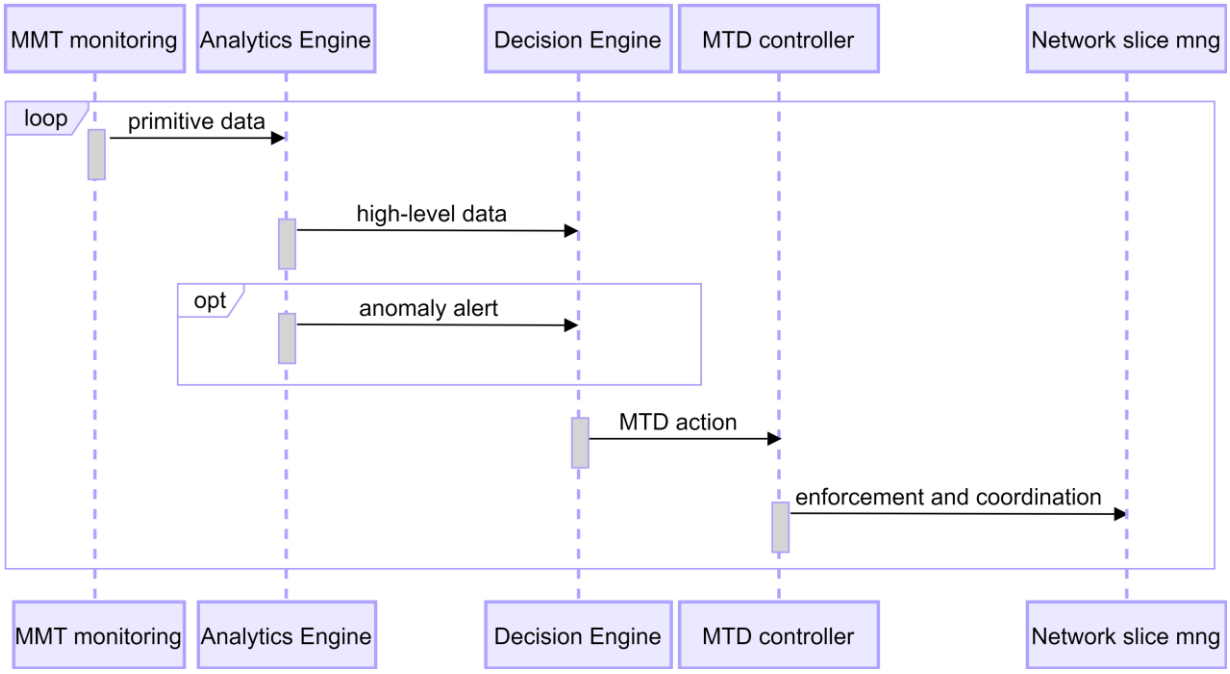

Figure 40: Sequence diagram of UC N basic flow

2.14.6 Post conditions

UC N presents a continuous process following the modus operandi of a closed-loop and self-driven operational flow. The post-condition is a working cognitive cycle of {monitor, analyze, decide, and act} phases as previously described and depicted in Figure 40.

2.14.7 Success criteria

The provided security use case is successful when:

- the probes effectively collect the needed metadata on network traffic and resource consumption
- the Security Analytics Engine positively detects security incidents and tampering attempts and alert the network protection chain for further mitigation actions
- the Decision Engine performs the right decision on an MTD operation that mitigates (in case of alert from the Security Analytics Engine) or prevent (in case of proactive action) security incidents
- the MTD controller and the network slice manager enforces the MTD action over the specific network slice component (VNF or NS)

2.14.8 Use case summary

2.14.8.1 Mapping on INSPIRE-5Gplus architecture

As depicted in Figure 41the HLA components (described in D2.1) involved in UC N are:

- The Security Data Collector, specifically providing monitoring probes
- The Security Analytics Engine, providing an anomaly detection system and a VNF tampering detector
- The Decision Engine, providing a security decision-making system
- The Security Orchestrator, providing an MTD controller
- The Service Orchestrator, providing a Network Slice Manager

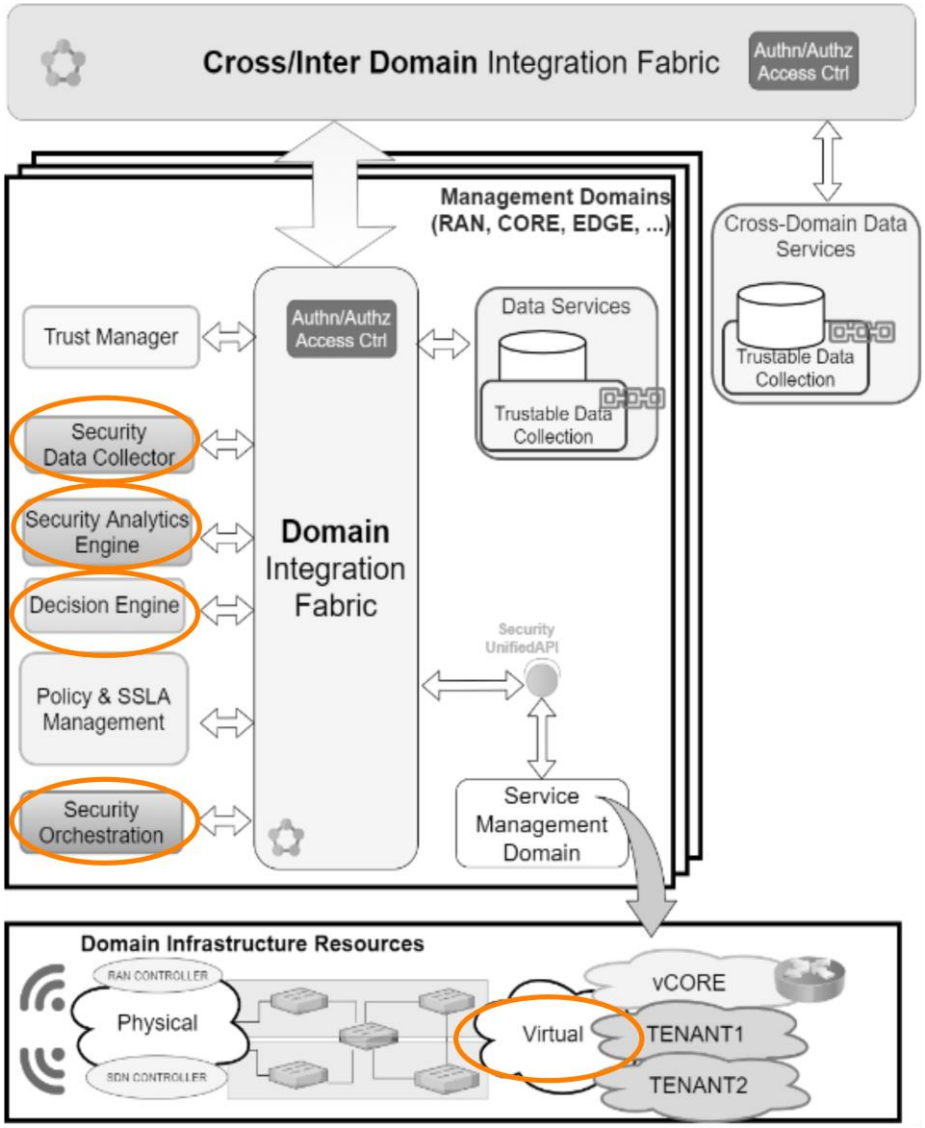

Figure 41: UC N mapping with the HLA functional components

2.14.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- MMT probes
- Security Analytics Framework (SAF)
- Optimizer for security functions (OptSFC)
- Systemic VNF tampering detector
- MTD controller (MOTDEC)
- Network slice manager (Katana)

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.14.8.3 Comments

This use case was introduced in D2.2 [6] as illustrative use case IUC6.

2.15 UC O - Secure and privacy enabled local 5G infrastructure

2.15.1 Problem description

With the advent of the networking and computational services, the users may tend to lease networking and computational resources and data processing services from multiple service providers/operators. These may include larger scale mobile network operators, local 5G network operators, cloud service providers, etc. Local network operators may deploy their network infrastructure including both Base Station (BS) and backhaul networks. A certain customer may request for a network slice that composed of resources offered by multiple operators. Edge computing services are deployed closer to the IoT nodes for local data processing. IoT tenants offer various smart services or contents based on the data collected by IoT devices. IoT tenants may lease the networking and computational resources, and data processing services from multiple service providers/operators. In such a scenario, a brokering mechanism that allows different service providers/operators to come to a common platform and formulate a network slice in a secure and automated way. The challenge is to evaluate the slice resource requirements against the resource availability over different network domains such as RAN, transport and core. Brokering mechanism should not be performed/hosted by a single entity. Which will be again become a centralized architecture. Therefore, using DLT for brokering mechanism will provide a good platform for distributed network architectures.

Further another key challenge is ensuring security requirements of tenants such as user privacy and resource request parameters submitted by each individual.

2.15.2 Goals

Our goal is to use a hierarchical Blockchain network to develop a secure and privacy enabled federated slice brokering mechanism for IoT tenants under the umbrella of a multi operator platform. In our solution federation refers to the orchestration of services (i.e., network functions, computational resources, etc.) offered by multiple local operators. When an IoT tenant initiates a request for a particular service demanding a set of resources, it's the duty of the federated slice broker to orchestrate the life-cycle of the network slice in a secure, automated and scalable manner. In this case the slice broker performs as a mediator between IoT tenants and the local 5G operators. Based on the tenant request, received from IoT tenant, the broker will create a network slice that fulfils the requirements of the requested 5G services. This can be a multi-operator end-to-end slice where network and computation resources can be provided by different operators.

The key objective is to utilize the infrastructure offered by local operators in a secure way while protecting the user privacy to provide them required networking services and resources without revealing their identities.

IoT tenant cluster represents a collection of IoT nodes and edge computing nodes that are restricted to a limited geographical area. Brokering mechanism maintains a common queue to store the past and anticipated service/resource requests emerging from the clients, the possible E2E slice formation that fulfils their requests, availability of networking and computing resources at the providers, traffic status, etc.Operator/Service provider cluster (Infrastructure cluster) denotes the virtual/physical resource/infrastructure providers which are also considered as local operators (Figure 42).

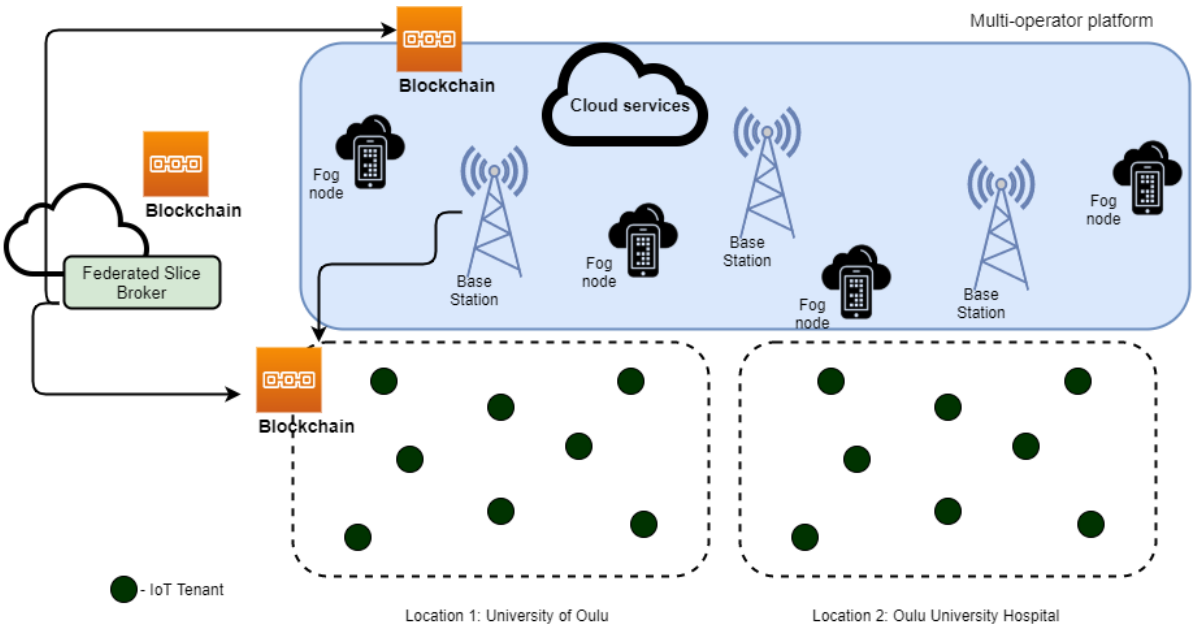

Figure 42: UC O diagram

2.15.3 Actors

The actors and roles involved in this UC are:

- Mobile Network Operator (MNO) / Local 5G operator
- IoT tenant
- Fog nodes

2.15.4 Preconditions

MNOs/Local operators should provide the available network/computation resources and their current status via the respective network slice managers. In addition to that, a reputation metric is assigned to each MNO and this value is taken based on the inputs given by the SSLA manager. These records are stored in a database maintained by the network slice broker. The storage of these records in the blockchain network is intended to perform in a privacy preserved manner.

2.15.5 Basic flow

IoT tenants create the individual service/resource requests to fog nodes. An additional security service is provided by the slice broker to eliminate the possible DoS/DDoS attacks at this point.

Based on the demand asked by the IoT tenants, Fog nodes initiate the resource requests, create the network slice template using secure and federated slice brokering (SFSB) mechanism and broadcast the slice request to MNOs/ local operators.

SFSB mechanism maps the best match for a particular resource request with the network slice offer given by the respective resource providers.

Fog nodes grant access IoT tenants to consume the slice upon selection by the brokering framework.

2.15.5.1 Diagram

Figure 43 illustrates the basic flow of UC O.

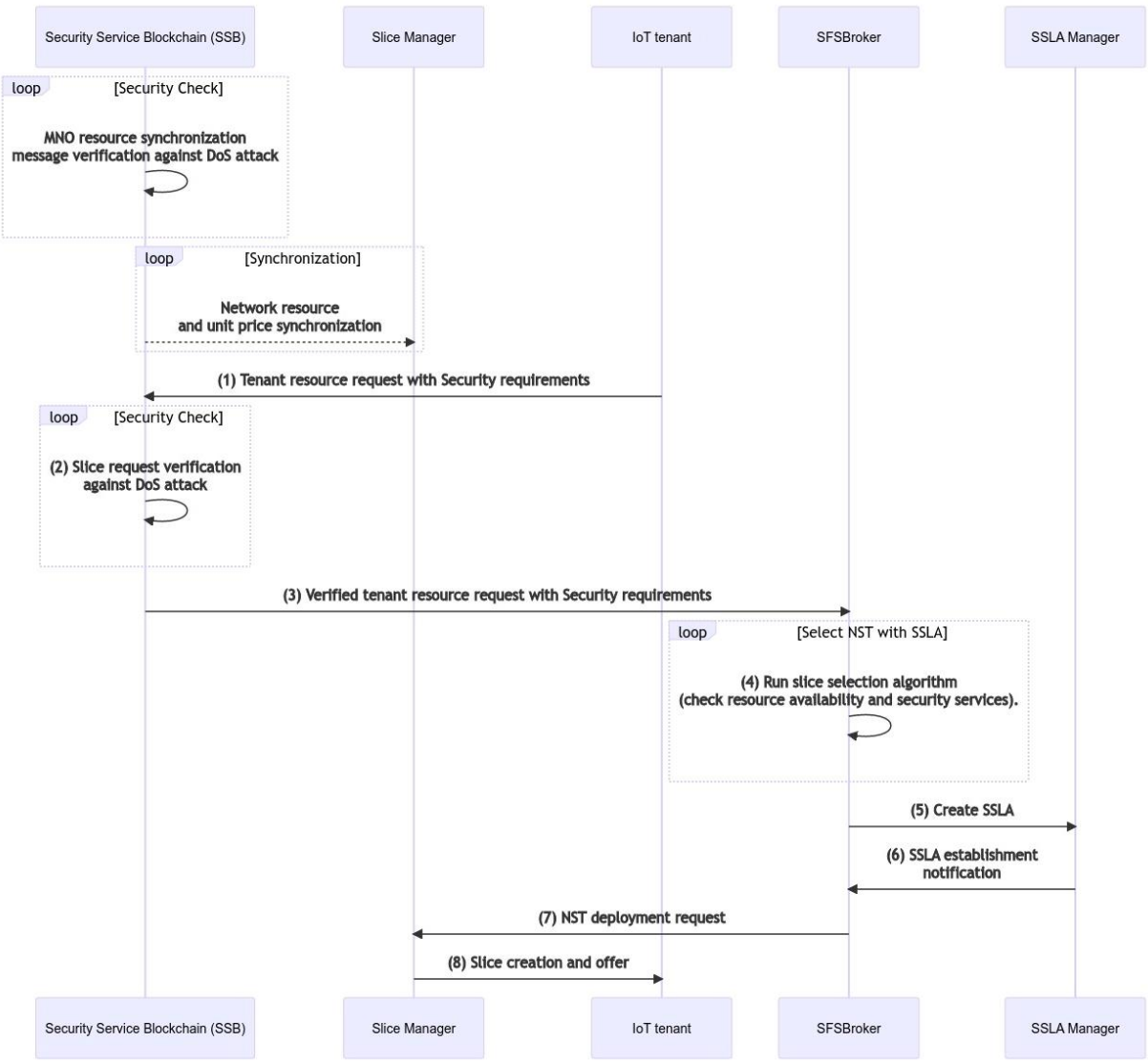

Figure 43: UC O diagram

2.15.6 Post conditions

The use case ends successfully, when the broker is able to formulate the Network Slice Template (NST) dynamically which maps the security requirements and the resource requirements of IoT tenants.

2.15.7 Success criteria

Separate private permissioned Blockchains are maintained to keep the records among IoT tenant clusters, at brokering mechanism and among local operators.

2.15.8 Use case summary

The use case aims to use network slice brokering service to provide end-to-end network slices in a secure, automated and scalable manner under a multi-operator platform. It proposes secure and privacy enabled local 5G infrastructure that support multi-tenant multi-operator scenario in line with the close loop framework by ZSM. Secure network and resource allocation is performed by the network slice broker developed by DLT where the smart contracts are used to activated different functionalities of the slice broker. Secure Slice selection algorithm is designed using game theory and Reinforcement learning and the data bases are maintained in a privacy enabling manner. The slice broker communicates with the slice manager of the local 5G operator to receive the resource availability,

pricing values, and slice creation. The process is also supported by a Blockchain-based SSLA manager service which is running as an additional service on top of the main brokering service.

2.15.8.1 Mapping on INSPIRE-5Gplus architecture

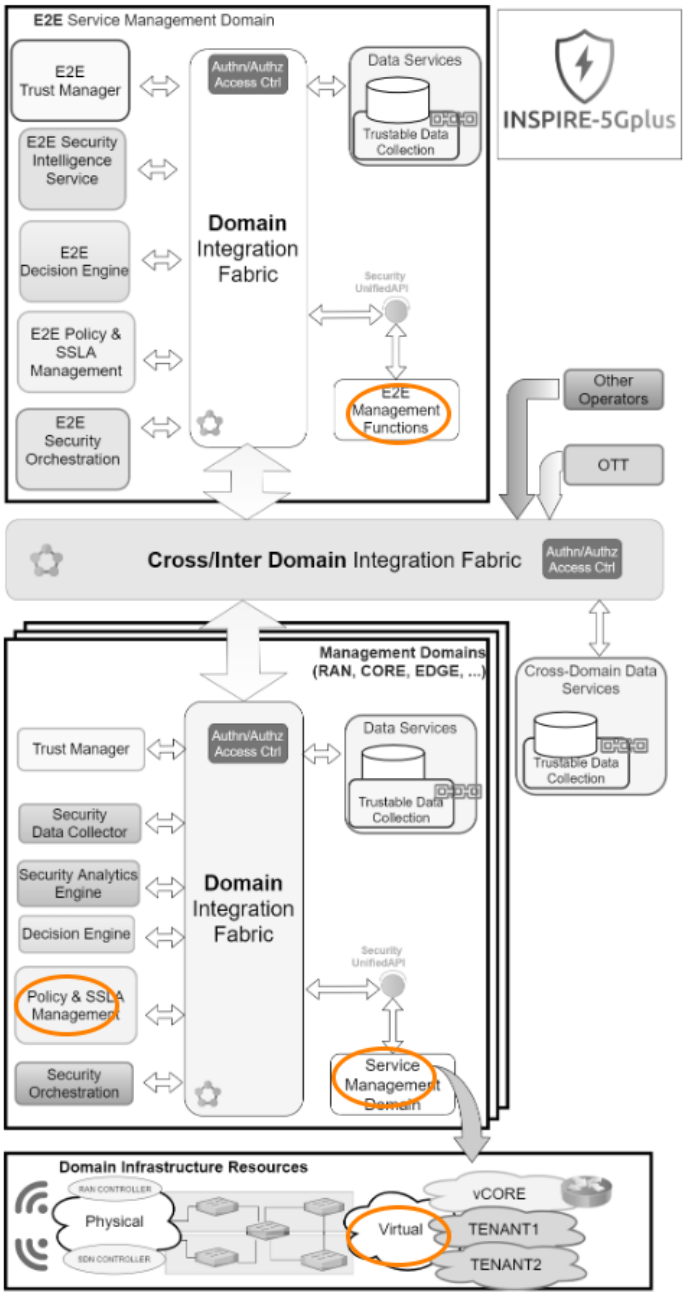

Figure 44: UC O mapping with the HLA functional components

2.15.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- SFSBroker
- Network slice manager (Katana)

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.15.8.3 Comments

This use case was introduced in D2.2 [6] as illustrative use case IUC10.

2.16 UC P - Intelligent and Secure Management of Shared Resources to Prevent (D)DoS

2.16.1 Problem description

Dealing with security threats is a never-ending task where attackers continuously renew their strategies. The security provider needs to always find and adapt to new threats. This cat-and-mouse game leads to moments where attackers have the upper hand with offensive strategies that thwart deployed defences. For instance, the contemporary (Distributed) Denial of Service ((D)DoS) attacks are getting stealthier, having the ability to mimic genuine behaviour with low-bandwidth usage, which allows them to evade the detection mechanisms.

This use case demonstrates the ability to do damage control when a situation in a slice escapes direct threat detection and mitigation. In fact, the interdependence between slices due to virtual network functions and infrastructure resources sharing rises the risk of indirect (D)DoS; that is, the direct (D)DoS exhausts the resources of one slice, which may influence the resources shared with other slices, affecting the availability and performance of provided services. In this fuzzy context, the INSPIRE-5Gplus platform needs fallback / fail-safes mechanisms that protect shared resources from starvation. As illustrated in Figure 45, an uncontrolled scaling up/scaling out of Slice B's resources may lead to exhausting the shared resources, causing potential performance degradation for Slice A or preventing the creation of new slice C.

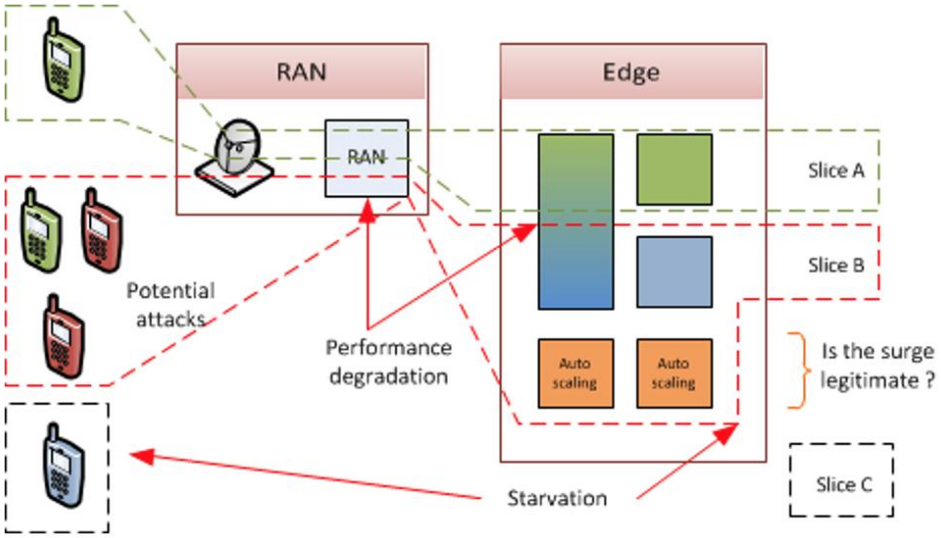

Figure 45: UC P scenario.

2.16.2 Goals

This Use Case solves situations where undetected slice attacks trigger resource starvation in shared infrastructure that affect other critical slices. While the UC P does not directly mitigate the threat, it provides damage control to protect shared resources and minimizes the impact on uncorrupted slices. or services.

2.16.3 Actors

The actors and roles involved in this UC are:

- Malicious party (Mallory)
- Mobile Network Operator (MNO):
    - RAN, 5GCore (CP + UP), Mobile Edge
- Legitimate mobile device users (Alpha, Bravo)
- Malicious mobile users (Yankee, Zulu)

2.16.4 Preconditions

- The main precondition for the UC P is that attacks are undetected and un-mitigated by the security enablers.
- The attackers need to use un-disclosed security threats or manage to game the deployed security protection.
- The direct victim and the indirect targeted slices are sharing the same physical or virtual resources.

2.16.5 Basic flow

The basic flow consists of the following steps:

1. Two services (A and B) are running inside a 5G core on the users' data path. The resources allocated to these two services are (logically) isolated in two respective slices that span from the devices, the RAN domain, to the Core Domain of the MNO infrastructure. These services are associated to specified SLAs.
2. The malicious party (Mallory) triggers an attack from compromised devices bound to the slice B. The compromised devices are used to launch a stealthy DDoS attack against service B.
3. The currently deployed security assets (e.g., firewall, IDS) are unable to (timely) distinguish the malicious traffic from legitimate traffic.
4. The attack affects the service's SLAs of slice B, which leads the system to trigger repeated auto-scaling operations, such as a scale-up (i.e., increasing resources for the VNF) or a scale out (i.e., increasing the number of VMs serving the VNF) to deal with performance degradation.
5. The repeated auto-scaling operations may result in exhaustion of resources shared with slice A: CPU, memory, network queues, application caches, disk I/O, file descriptors, etc. For example, the resource blocks managed by the RAN can be depleted in favour of the malicious slice.
6. A damage control component should then minimize the impact on the slice B by validating and potentially blocking the new resource allocations.

2.16.5.1 Diagram

Figure 46 illustrates the basic flow of UC P.

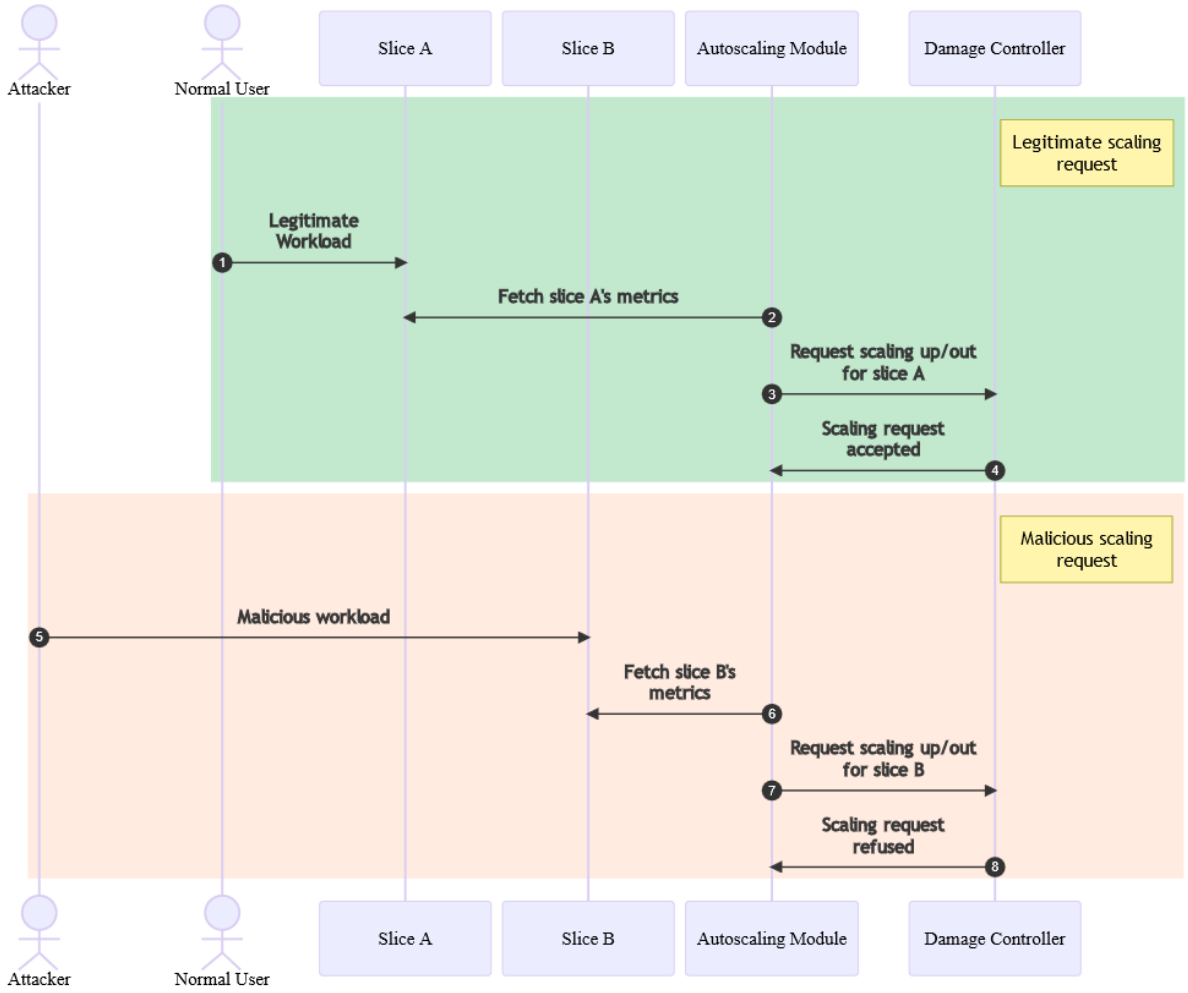

Figure 46: Basic Flow of UC P.

2.16.6 Post conditions

The malicious requests for scaling up/out the resources are blocked.

2.16.7 Success criteria

The main success criteria are:

- The legitimate service's SLA are maintained.
- The resource starvation for critical or new-coming service is minimized.
- Over protection when a legitimate surge in resources consumption happens is avoided.
- The operator is notified and/or the security attack model is kept for future preventions.

2.16.8 Use case summary

The main goal is to protect shared resources within slices under un-mitigated DDoS attack. It demonstrates the protection of resources in the event of over provisioning under an unmitigated (D)DoS attack. This over provisioning is created by the self-scaling ability of the infrastructure that horizontally scales the used resources attached to a slice to cope with the demand. To prevent malicious auto-scaling operations, the damage control component leverages Machine Learning (ML)

to detect whether the scaling up/out is due to legitimate workload or rather malicious workload caused by an application-layer DDoS attack. If the workload is malicious, the scaling operation is refused.

2.16.8.1 Mapping on INSPIRE-5Gplus architecture

As depicted in Figure 47, the UC involves the "Security Data Collector" to collect data on resource usage and performance metrics from the slices via deployed monitoring probes. The collected data are analysed by the "Security Analytics Engine" to forecast the values of slice's resource usage and performance metrics. Comparing the forecasted values to the actual ones, the "Decision Engine" is notified if the forecasting error is above a predefined threshold, in which case, the scaling operation is prevented, and further measures may be taken to mitigate the attack. This could include analysing network traffic to identify the origin of the attack and block the attackers, and/or retraining the intrusion detection system on the new malicious network traffic to improve its capabilities in detecting the attack in the future.

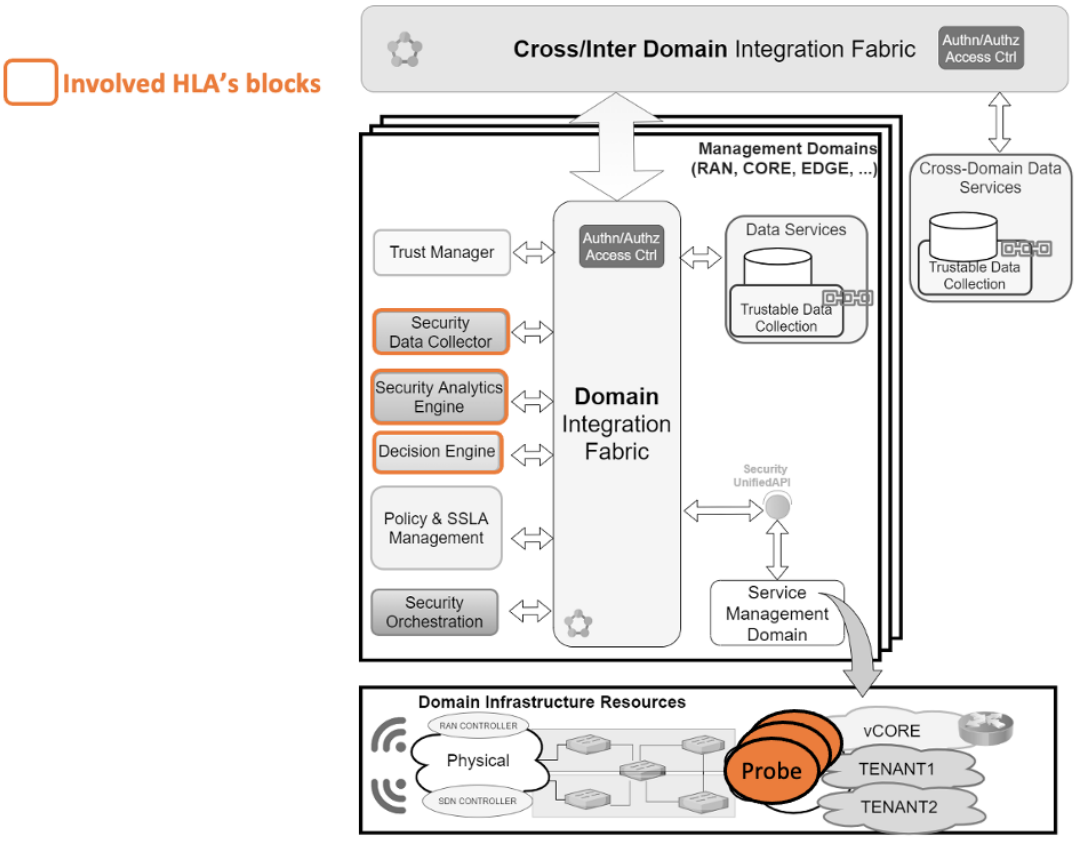

Figure 47: UC P mapping to INSPIRE-5Gplus HLA.

2.16.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Security Monitoring Framework (MMT Probe)
- Admission Controller Delegator (Auto-scaling Module)
- DDoS Mitigator (Damage Controller)
- Decision Engine

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.16.8.3 Comments

This use case was introduced in D2.2 [6] as illustrative use case IUC8.

2.17 UC Q - GPDR aware counterparts for cross-border movement

2.17.1 Problem description

Each country in the EU has its own laws in terms of data privacy and the EU itself defined the GDPR as a mean to control data leakage and data transfer on third parties, making special distinction for cloud providers. There is a need to ensure that the data uploaded by roaming users complies with local laws and, where it does not, to be able to clear liabilities.

In this context, every communication established using GDPR protected devices must be GDPR compliant, when a lack of compliance is detected, actions must be registered for further clarification of liability.

vOBUs (virtual On-Board Units) which are designed to address GDPR enforcement, must be flexible enough to migrate from one law context to other guaranteeing the channel protection between the UE/car and the cloud in heterogeneous and dynamic environment, where its actions must be trustfully and non-refutable stored in the operator infrastructure (see Figure 48).

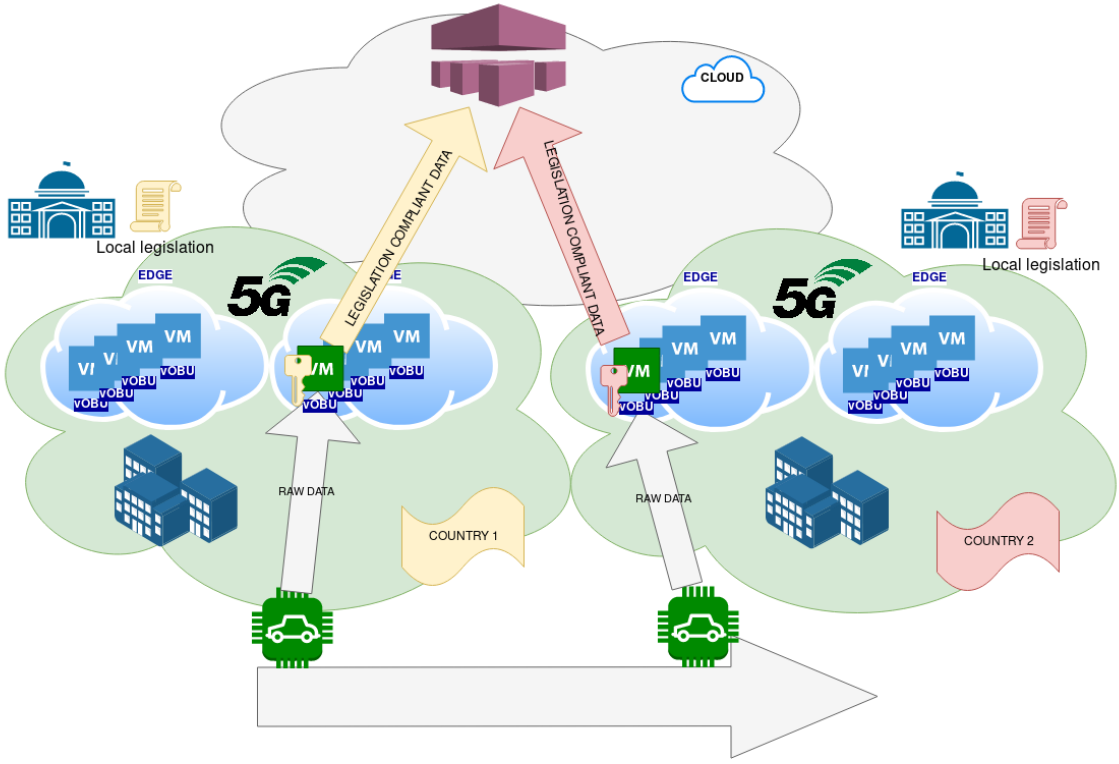

Figure 48: Cross-border virtual counterpart migration concept

2.17.2 Goals

This use case focus on the following goals:

- Perform 5G secured mobility through cross-border domains.
- Migrate the instantiated vOBU maintaining its security association with the OBU guaranteeing the confidentiality.
- Perform transparent action to maintain continuous connectivity while migration procedure.
- Achieve continuous GPDR compliance on vOBU traffic
- Maintain updated the trust score of different solutions involved in the procedures (eg. vOBU, compute nodes).

2.17.3 Actors

The actors and roles involved in this UC are:

- Vehicle1
- Mobile Network Operator - MNO1
- Mobile Network Operator - MNO2 (or Radio Access Network (RAN) in another country from MNO1)

2.17.4 Preconditions

The UC requires the following pre-conditions:

- Two operational 5G SA/NSA implementations, including OBU UE, RAN, Core, Transport and Edge infrastructure TEE capable.
- A multi-domain integration fabric
- DLT with stewards nodes capable to participate in the validation process and maintain the DLT.
- Trust reputation assessment based on historical behaviour of virtual and physical entities.

2.17.5 Basic flow

The UC includes the following subsequent actions:

The car starts and gets connected to the 5G network. Car's onboard unit (OBU) is associated with a virtual counterpart or virtual OBU (vOBU) on the operator's EDGE capable of proxying any communication and analyze the content. The connection between OBU and vOBU is protected. The vOBU is trusted by the operator thanks to it being certified by the Trust Reputation Manager. That vOBU fulfils local laws.

The initial set of security policies to be applied to the connectivity of the UE can be determined by means of employing behavioral profiles, established by vendors and retrieved by the network in order to help in the customization of security policies per device type.

When the car moves to another country, a new virtual counterpart needs to be created, this new vOBU is entrusted with the fulfilment of the visiting country law. The Trust Reputation Manager employs historical tampered data stored in the Trustable Data Services to produce a score to the vOBU image which needs to be instantiated on operator's edge, but also about the compute nodes themselves, therefore fostering the migration of the resources triggered by car movement.

Depending on the specific context of vOBU migration, it can be done as a full copy of the VM, so that the behaviour needs to be changed programmatically, by creating a new VM with shared data that may contain or not the cryptographic material. In any case, the network needs to take care of the migration of the connection between the OBU and the corresponding vOBU.

2.17.5.1 Diagram

Figure 49 illustrates the basic flow of UC Q.

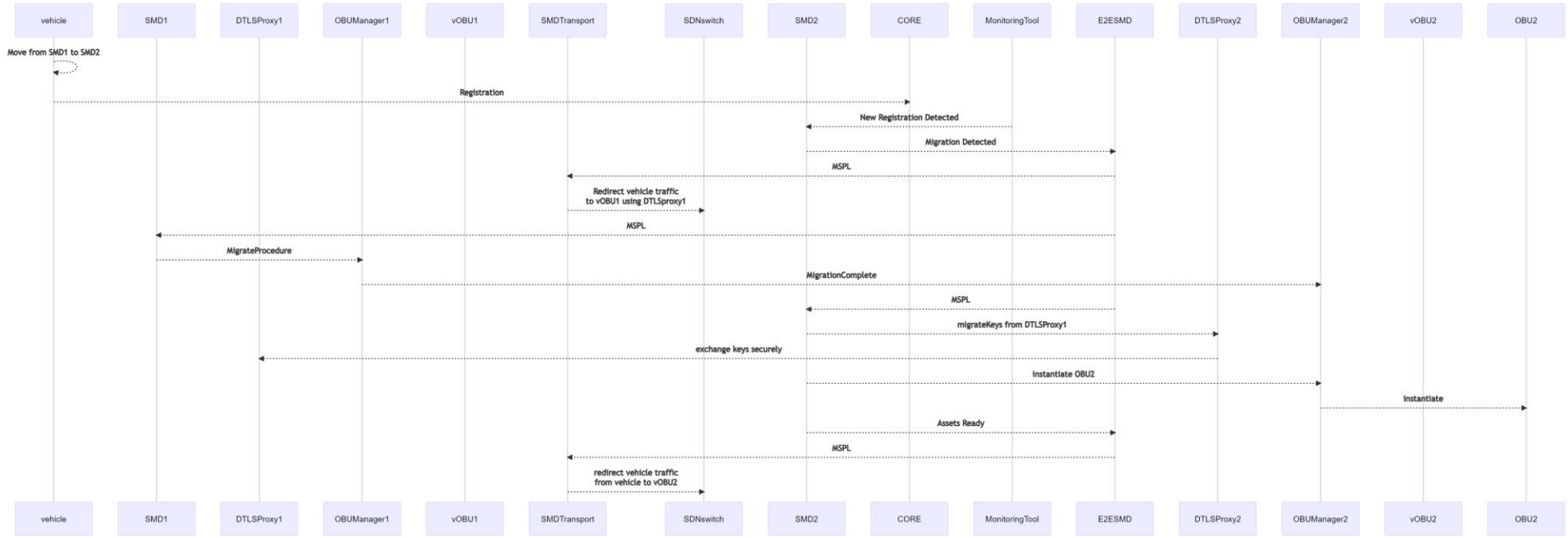

Figure 49: UML Diagram migration process of DTLSProxy and vOBU

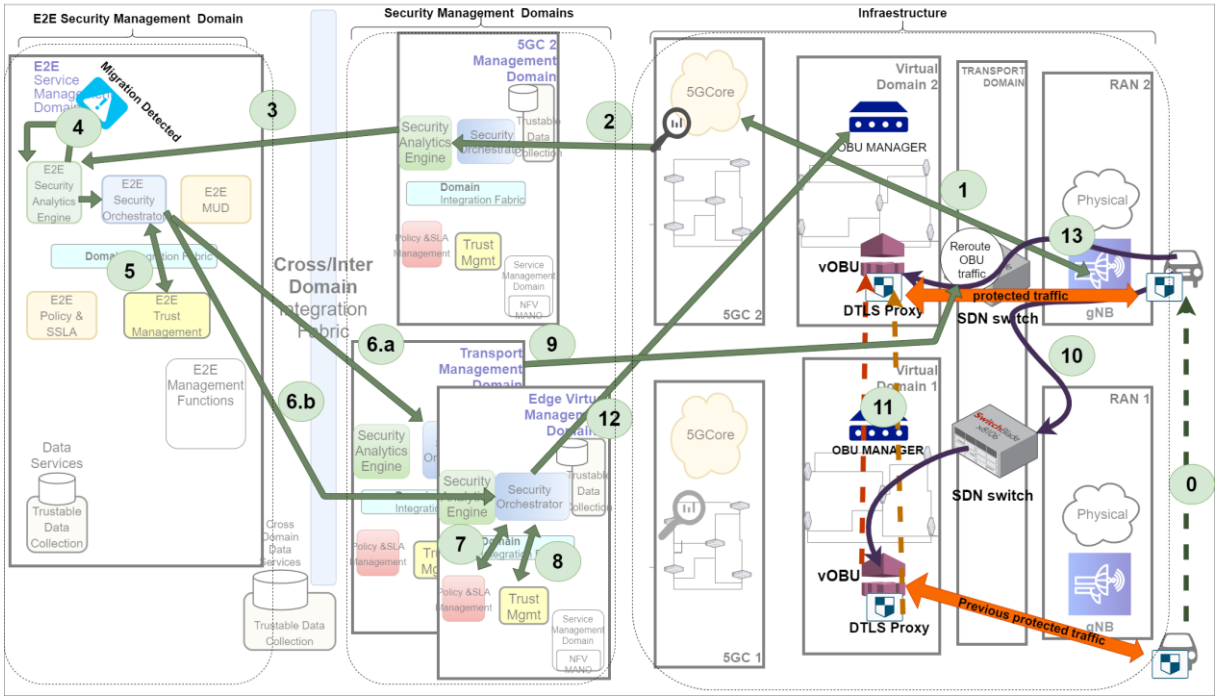

Figure 50: Illustrative Diagram of Use Case Workflow

2.17.6 Post conditions

The successful result of the UC relies on the following outcomes:

- The car has moved to a new location in terms of 5G connectivity.
- The vOBU has been migrated to the new location and a security association with the OBU remains valid with confidentiality warranted thanks to DTLS Proxy.
- The network transparently redirects the packets to the new vOBU from the OBU.
- The vOBU traffic is analysed and is compliant with the GDPR and score of the source image is maintained.
- Score for compute nodes is updated based on the success of the operation.

2.17.7 Success criteria

The network has established customized security policies based on OBU vendor behavioural profile.

The OBU has established a security association with the vOBU which is maintained upon vOBU migration originated by OBU network movement.

Cryptographic material does not leave the enclave and the data non-compliant with GDPR or other business policies does not leave the vOBU.

The time for VM migration and security assets calculations such as Trustiness level or communications encryption are unnoticeable and transparent to the end-user.

2.17.8 Use case summary

This use case demonstrates a multi-domain policy enforcement ecosystem that evaluates trustworthiness of the enforcement therefore driving the decision and election of possible actions. It proposes a multi-domain scenario that relies on the definition of high-level security policies (D2.2

[6]Section 2.7) that are enforced on a multi-domain scenario with the consequent responsibility delegation that with the ZSM closed loop (D2.2 Section 2.1) provided by the Inspire-5Gplus High-Level architecture (Section 4). The mobile devices will establish encrypted tunnels to their virtualized counterparts that will change with the location migration of the device, the cryptographic material protection is envisioned by means of Trusted Execution Environment (D2.2 section 2.2) techniques. The information generated during the operations is stored inside a DLT (D2.2 Section 2.5), thus being registered in a non-reputable way. Smart Contracts are also used to provide some trust to the deployment, therefore providing a trustiness level related to the virtual counterpart, allowing the automated deployment system to decide whether it should be used or not.

2.17.8.1 Mapping on INSPIRE-5Gplus architecture

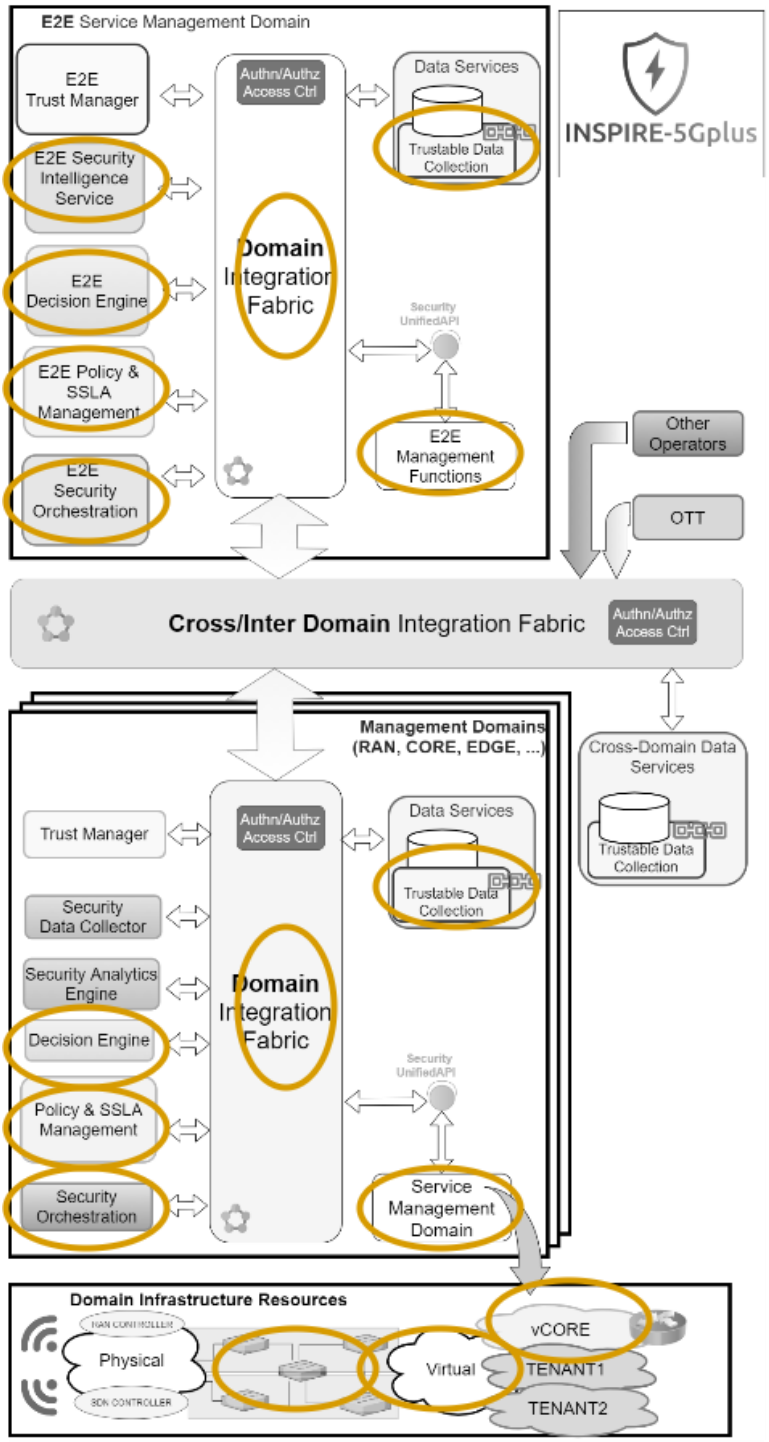

Figure 51: UC Q mapping to INSPIRE-5Gplus HLA

2.17.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Virtual Channel Protection with DTLS Proxy
- Policy and SSLA Management
- Data Collector enabler and connectivity maintainer SDN Controller

Monitoring asset

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.17.8.3 Comments

This use case was introduced in D2.2 [6] as illustrative use case IUC7.

2.18 UC R - VNF security properties management

2.18.1 Problem description

In 5G infrastructure, the complexity of multi-tenant, multi-operator, multi-domain context where all network and business functions are softwarized and virtualized, presents a broader attack surface for cyber threats. Therefore, there is a need to guarantee the integrity of the VNF deployed as they support all the functions.

2.18.2 Goals

Since multi-operators may be involved in the deployment of a slice, the integrity check of the VNF should be accessible from Service Providers so that they can monitor security and trust of the slice at design-time, but also at run-time. More technically speaking, trustable properties shall be added to the VNF description. These attributes shall be accessible to the VNF Management functions so that the VNF could be chosen at design-time for its trustable properties. At run-time, the HLA components shall check if it conforms to the SSLA and TSLA or if it violates it, triggering a remediation.

2.18.3 Actors

The actors and roles involved in this UC are:

- Service consumer (SC)
- Service provider (SP)
- Operator
- Security Operator
- Attacker

2.18.4 Preconditions

A minima, the use case can be demonstrated with a VNF implementing a service. Then both Systemic and CCT enablers are needed to perform the security and certification functions.

The full chain of security Management is demonstrated with the deployment of a Slice associated with the High-Level Architecture (HLA).

2.18.5 Basic flow

Four main phases are presented in the basic flow.

Initial protection

The first phase related to the initial protection. Systemic enabler transforms a simple VNF into a protected VNF. Several protections are deployed:

1. The binary of the VNF wraps an auto-attestation boot verifying the integrity and the trustable origin at start;
2. During execution, the control flow and the integrity checks are obfuscated to prevent attacks at that level;
3. Security Meta-data are added to describe the VNF, to advertise about its security protection.

Before wrapping the VNF into a protected VNF, Systemic sends the meta-data (including an identifier fingerprint) to the Component Certification Tool (CCT).

CCT certifies the VNF including the meta-data and produces a Digital Trustworthy Certificate (DTwC). The DTwC also wrapped with the meta-data when producing the protected VNF.

Provisioning

When an end user or Service Consumer (SC) wants to use a service, they send a request to their Service Provider with a description of the requirements for the service. These requirements can be expressed by a Service Security Level Agreement and a Trust Service Level Agreement. The Service Management Functions receiving the SC request passes it to the HLA components in charge of SSLA and TSLA, that is to say the Policy and SSLA Management and the Trust Management. Together with the Security Orchestrator, they can poll the meta-data of all existing VNFs to find which ones fit best the requirements of the SC. Finally, the choice of the right chain of micro-services is done and the Security Orchestrator orchestrates it to fit the right Level of Service. The Management functions takes in charge the provisioning of the service to the Service Consumer.

Normal operating mode

In normal mode, the components of the HLA can regularly check about the security metadata of the VNF, and about its integrity checks performed by the Systemic routine. When an attacker tries to modify the VNF, the Systemic routine embedded into the protected VNF detects it and sends a report to the SAE. This leads to a critical operating mode.

Critical operating mode

When receiving a report of integrity violation, the components of the HLA compute a remediation. According to the severity, the remediation can be a simple request for the transfer of the full violation report, or an order for slow termination of the process, or for immediate stop.

2.18.5.1 Diagram

Figure 52 illustrates the basic flow of UC R.

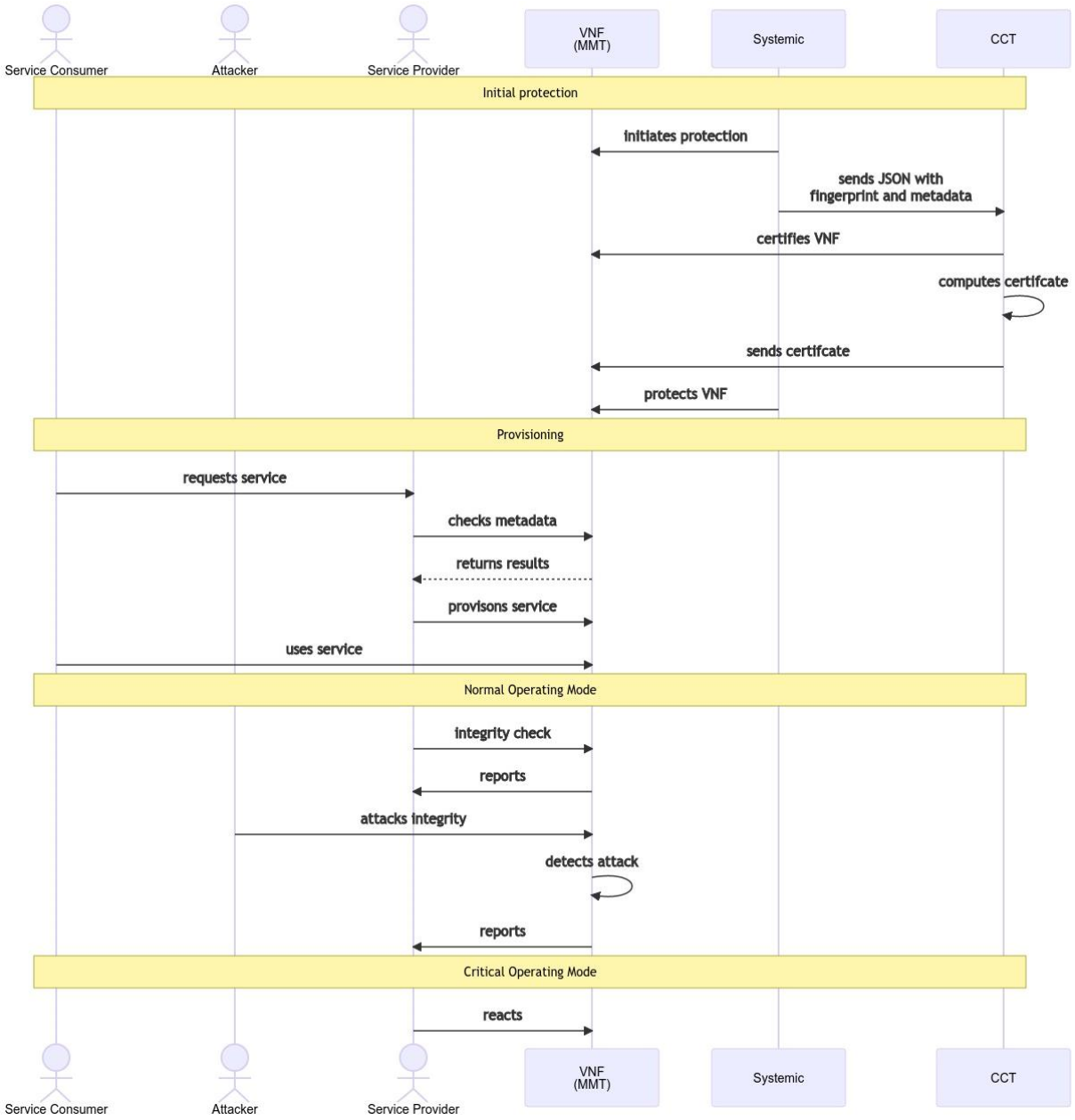

Figure 52: UC R diagram

2.18.6 Post conditions

Several steps are described in the process, each of it having its own post-condition.

Initial protection

The protected VNF is produced, embedding the DTwC.

Provisioning

Meta-data of the VNF are used at provisioning of the service.

The DTwC certificate signature is verified.

Normal operating mode

SAE exploits VNF reports.

Critical operating mode

VNF applies HLA components critical remediation orders.

2.18.7 Success criteria

The production of the protected VNF embedding the DTwC is the first success criterium.

The verification of the certificate is a second success criterium.

2.18.8 Use case summary

A Service consumer (SC) or tenant uses a slice for their business. They may have signed a contract with a Service Provider (SP) including Security, Trust and Liability clauses expressed under Security Service Level Agreement (SSLA) or Trust Service Level Agreement (TSLA). The underlying infrastructure put in place by the SP relies on several Domains operated by different Operators. The SP itself may improve the Quality of Service by bringing in some functional or non-functional services. Most of the services are softwarized and virtualized. For a given operator, the chance to be selected in the whole package hangs on its capacity to report about its security, trust and liability. Therefore, it will put in place accountable means for the Service Provider to be able to find the characteristics of the operator services at design-time, as well as to monitor it at run-time. Also, if an Attacker tries to change the VNF, a routine report for this modification. The central security functions of the SP have means to request about the protections of the VNF, its metadata and its report about the attack.

2.18.8.1 Mapping on INSPIRE-5Gplus architecture

The following schema presents how the use case fits into HLA.

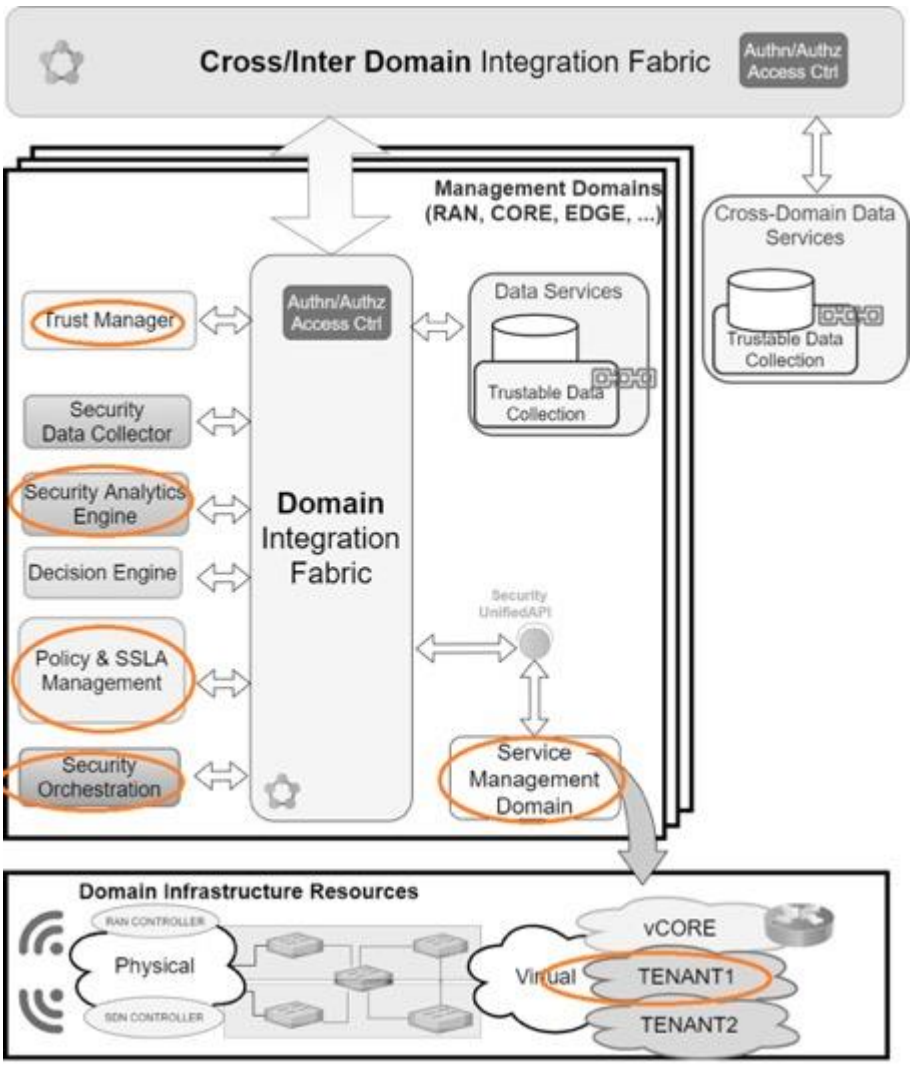

Figure 53: UC R mapping on INSPIRE-5Gplus HLA

2.18.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Systemic
- Component Certification Tool (CCT)
- Security Analytics Engine
- Security Orchestrator
- Policy and SSLA Management
- Trust Management.

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.19 UC S - Trusted Smart Infrastructure

2.19.1 Problem description

Making smart cities a real use case scenario has become a challenge due to many urban technology concerns such as transportation, waste management, and environmental protection. Moreover, issues on security and malicious behaviour prevention are, in many cases, still neglected. Additionally, the actual implementation of new smart security technologies is not often discussed in research works,

neither the questions that might arise on how smart city security affects traditional policing and urban planning processes [11].

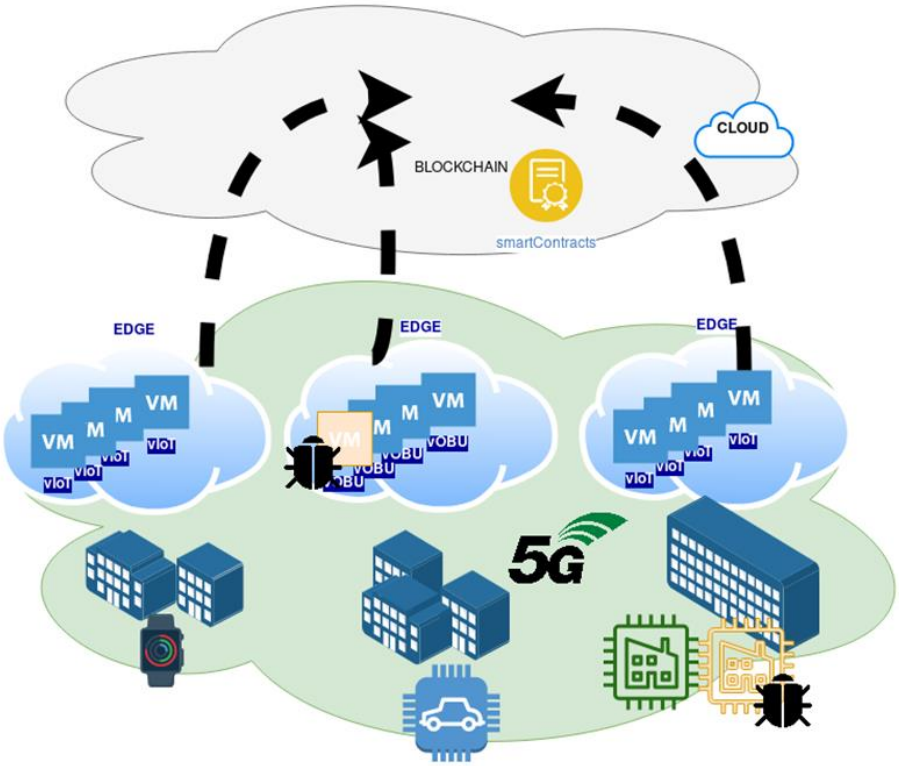

Figure 54: Smart City illustrative picture

2.19.2 Goals

As shown in Figure 54, given a smart-infrastructure which might be a city (smart city), an ITSS environment or the Industry 4.0 where virtual counterparts are envisioned as ways of sharing/securing resources, detection of fraudulent information and/or behaviour must be considered. By detecting abnormal behaviours occurring in the traffic flows of the infrastructure, corresponding mitigation measures are applied to reach a security compromise of the device or its counterpart.

The idea is to employ historical information signed in a DLT and external information such as the MUD [10] file to detect the improper behaviour.

One of the challenges is to distinguish and react differently when the attacker is the device itself or its counterpart. In the second case, the device is a victim that can be affected by the countermeasure.

2.19.3 Actors

The actors and roles involved in this UC are:

- The device
- The virtual counterpart, which is the element assigned by the network to the hardware device to offer security services/functions. One of the most important key advances of 5G communications is the virtualization of computing and network functions. These advances have enabled the possibility to easily implement the Multi-access Edge Computing (MEC) capabilities that aim to offload tasks performed by mobile devices and ensure low latencies responses due to the proximity of the computing facilities to the point of attachment. In the specific case of a vehicle, the virtual counterpart of the OBU is the vOBU. The vOBU can replace the OBU from the network point of view and offer edge services to the OBU, in order to integrate all the required virtual resources for each OBU. The idea of instantiating virtual

substitutes for these OBUs (vOBUs) has been proved to be beneficial in terms of device access delay, reliability against wireless disconnections or data cache. Thus, the existence of this virtual counterpart is explained by the fact that, being closer, functionalities not supported by the OBU can be applied, for example DTLS. And from a top-down point of view, bandwidth can be saved by serving as a cache instead of saturating the 5G spectrum.

- Service Provider

2.19.4 Preconditions

- SSLA limiting access to device via virtual counterpart and minimum delay virtual/real needed.
- E2E Security Orchestrator and Policy Framework deploy virtual counterpart on the nearest to device's SMD. Then, the trust scores of that specific SMD, of virtualization elements, of virtual image, etc., are checked.
- SMD Security Orchestrator and Policy Framework deploy a proxy to register the behaviour on Trusted Data Services (DLT based). Behavioural profile (MUD/Threat MUD) is downloaded and Data Collector and Security Analytics Engine configured with behaviour is deployed.

2.19.5 Basic Flow

1. Traffic flows from/to device via virtual counterpart.
2. The Security Analytics Engine detects unwanted behaviour based on a discrepancy between the MUD file and the way the device is used and then, notifies the Decision Engine.
3. The Decision Engine applies proper mitigation through the Security Orchestrator:
    a. Filter device – if it is decided to be the attacker.
    b. Redeploy virtual counterpart – if the device is decided to be victim.
    c. Redeploy trusted virtual counterpart on a second round if the attack is not mitigated (image in VIM is corrupted).
4. Security Orchestrator requests Trust Manager (TRM) about the trust score of the entity over which the countermeasure is going to be applied.
    a. SO requests trust score to TRM.
    b. TRM computes the corresponding trust score.
    c. TRM updates the new trust score to the DLT to protect keying material.
    d. Trust scores need also to be multi-domain aware to avoid repeating previous errors on neighbouring domains, so TRM sends the new domain trust score to the E2E trust manager.
    e. TRM returns the trust score requested to the SO.
5. Security Orchestrator orchestrates according to the mitigation specified by the Decision Engine and the entity trust scored obtained.
6. Finally, the Decision Engine notifies the Threat MUD manager the information of the potential mitigation to be shared with other domains.

Eventually, the device will move to another domain and the E2E coordination will be needed to redeploy/migrate the virtual counterpart.

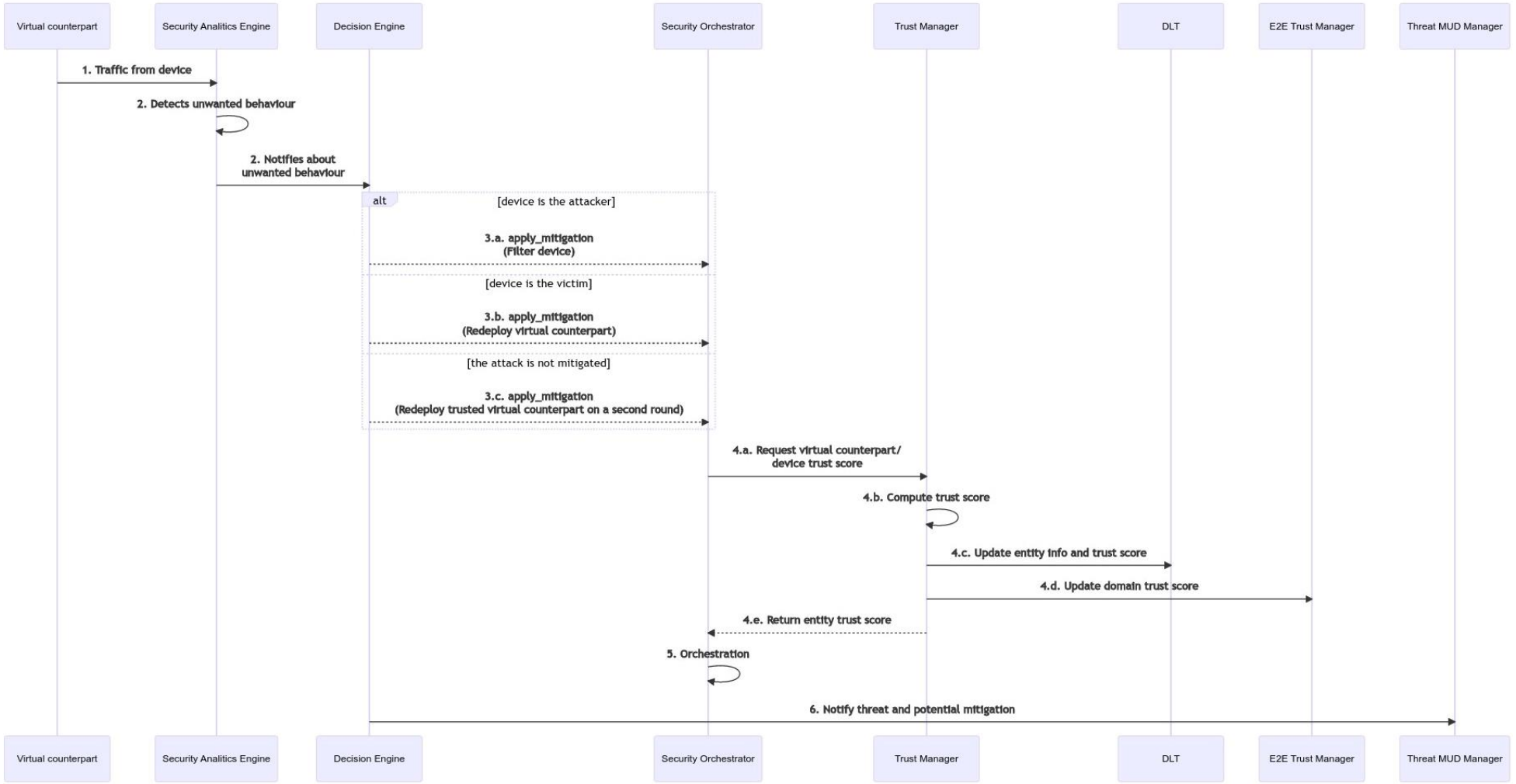

Figure 55: Sequence diagram of the UC S basic flow

2.19.6 Post conditions

The use case will end up successfully if the Security Analytics Engine has been able to detect malicious behaviours and react accordingly to the situation, whether the attacker is the device itself or its counterpart.

2.19.7 Success criteria

The goals presented are achieved by detecting unwanted behaviour at the Security Analytics Engine and notifying the Decision Engine. After that, the Decision Engine applies mitigation through Security Orchestrator.

2.19.8 Use case summary

Eventually, the Security Analytics Engine will detect unwanted behaviour on the traffic flows, with the consequent notification to the Decision Engine.

In sight of the previous notification, the Decision Engine applies proper mitigation through the Security Orchestrator to filter or redeploy the device/virtual counterpart according to the obtained analysis of the attack.

Finally, the SO notifies the Threat MUD to avoid repeating previous errors on neighbouring domains.

2.19.8.1 Mapping on INSPIRE-5Gplus architecture

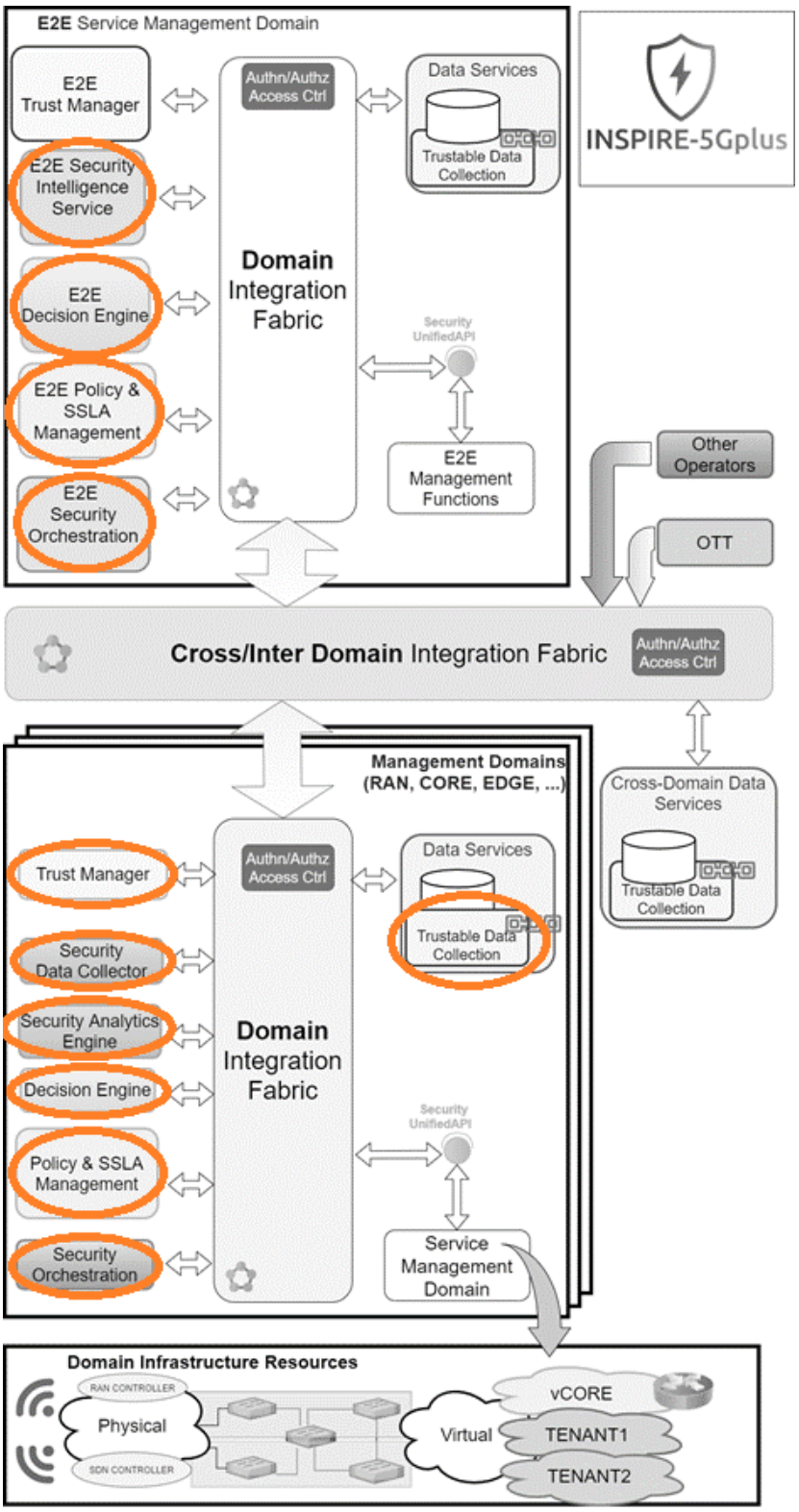

Figure 56: UC S mapping to INSPIRE-5Gplus HLA

2.19.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- SSLA Manager
- [E2E] Security Orchestrator

- [E2E] Policy Manager
- [E2E] TRM
- [E2E] Decision Engine
- MUD/Behavioural profiles
- Trusted Data Services
- Data Collector
- Security Analytics Engine

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.20 UC T - Attack on anti-Malware Software Defined Function

2.20.1 Problem description

Virtual Security Functions (VSFs) such as anti-malware software defined functions are targets of choice and more exposed to reverse engineering and tampering attempts simply because the network security is their mission and because they are deployed and execute on distributed and remote nodes over the network (i.e., off-premises). For a sustained efficiency, VSFs must dynamically mitigate new and mutating threats. We describe a use case which integrate a VSF enabler and a binary hardening tool which injects security on that code. We illustrate the risk of introspection and tampering and demonstrate how this risk is mitigated efficiently. The use case highlights a peculiar characteristic of VSF as their dynamic and permanent updating necessary to maintain their malware detection efficiency over time. As software versatility opposes to security and configuration stability, the use case demonstrates the associated peculiar requirement for the security solution.

Off-premise operation of computing resources imply the loss of control on maintenance operators and operations performed on the machine, its system and on the virtual machines and their contents. This introduces new risks, such as Introspection. Introspection involves the use of hypervisor and virtual machine monitor APIs for exposing low-level virtual machine system information. Service Level Agreements signed between the telecom operator and the cloud service provider define the obligation of means to contain this type of risk but without obligation of results. As a matter of fact, this risk may be coming from outside the cloud vendor itself. Introspection risk is the term used to characterize all possible ways that a malicious operator, or a distant player, can use to break the confidentiality and integrity on processed data or executed software. Network data confidentiality and isolation are then possibly broken as well as abnormal network behaviour or denial of service can more easily be performed.

The use case positioning is at platform-level as an introspection attacked is worked out at platform level. The backlashes of the attack on a VSF span over the platform to reach any verticals which employ the VSF on the platform.

2.20.2 Goals

The goal is to demonstrate what can be simply done to abate the risks associated to VSF introspection-tampering attacks.

2.20.3 Actors

The actors and roles involved in this UC are:

- The network operator, with its own network security constraints and consideration of benefiting from the normal execution of the VSF security service, from its supplier (the VSF vendor)

- The VSF vendor, with its intent to satisfying its client, thus deploy the efficient security service from its VSF.
- The Security Service vendor, offering its solution to armor the VSF against reverse engineering and tampering attacks.

2.20.4 Preconditions

Figure 57 details the virtual security function (i.e., MMT-Probe) internal structure. It contains two main attack paths possibly taken and which are directly related to the structure of the VSF and namely its split into two interacting components: the main MMT-Probe "static" software and the dynamically generated rule called by MMT-Probe. The first path consists in tampering the MMT-Probe. The second one consists in tampering or alternatively creating from scratch a rule called by MMT-Probe.

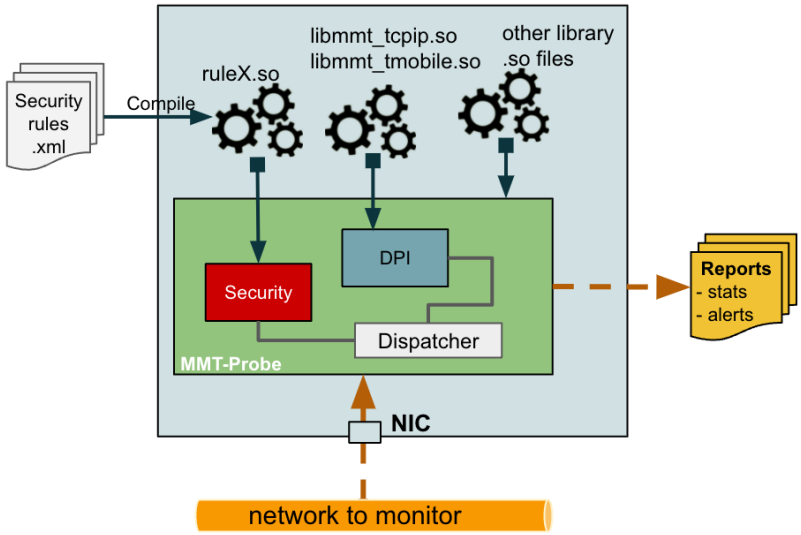

Figure 57: MMT-Probe high level architecture

To mount different types of attack, the attacker can alternatively:

1. Intercept and tamper the shared object (i.e, rule.so file) in transit to the main VSF executable (i.e, MMT-Probe).
2. Alternatively, create from scratch new rule (with a prior understanding by reverse engineering of the rule caller: MMT-Probe code)
3. Get access to MMT-Probe storage file (in the VNFI repository or elsewhere in the architecture).
4. Get access to the operating platform of MMT-Probe for code introspection by dynamic analysis (when MMT-Probe is running) and by tampering its memory pages. A prerequisite is the ability to get MMT-Probe executing as well as the right to debug-trace it.

2.20.5 Basic flow

2.20.5.1 Standard basic flow

The most logical process flow is driven by the actors.

The network operator may not influence this decision as of today in the current perimeter of offered security properties. If case additional security properties are brought such as digital right management, execution control aimed at enforcing the execution in trustworthy locations, the network operator would likely join the decision-taking.

The decision to protect MMT-Probe is discretionary to its owner only. For materializing this decision, the VSF vendor mounts her code to Systemic SECaaS server and access with her credentials to the UI for selecting the adapted protection pattern (i.e., list of security functions to apply). Once the SECaaS has applied the protection by binary rewriting, appending the needed systemic routine inside the code, the protected version of the VSF can be downloaded and deployed.

Once an introspection attack is detected, an alert is transferred from the Systemic appended routine to Montimage Security Analytics Engine, which then defines the corresponding action plan (interrupt the MMT-probe at that location, keep alive until maintenance replacement, proceed to further investigation before removal).

The sequence diagram of the use case is shown in Figure 58 below.

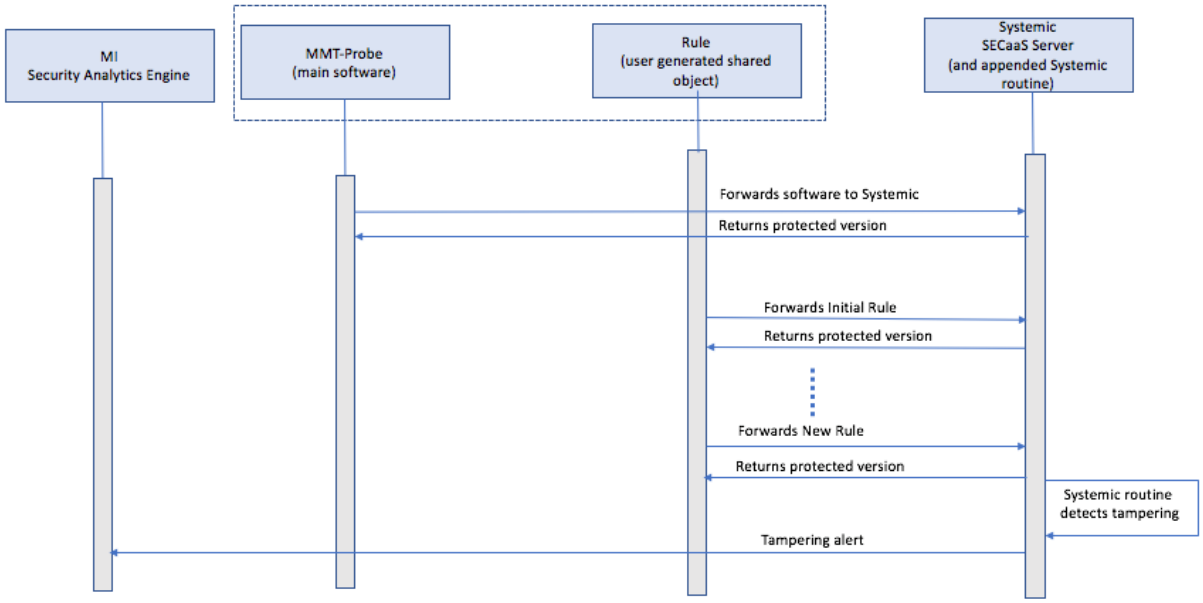

Figure 58: Sequence diagram of UC T

The workflow diagram shows the interfaces of Systemic SECaaS server which consumes unprotected binaries and instructions-templates from either a security orchestrator or a user. It also shows the resulting packaged protected binary which is appended with the protection routine which itself is executed in trusted execution environment for its own security, being either software based or hardware based (e.g., Intel SGX). As one can directly notice, leveraging the hardware TEE is worked out automatically whatever and independently to the incoming original binary. The logic behind this fact resides on the perimeter of code which is translated to the TEE, our common to all systemic routine. Once inside the TEE, Systemic protection routine protects the rest of the code located outside. This scheme is a pain saver in many respects, as it first precludes to the need of application specific Intel SGX licence, as well as it precludes to any uneasy source level changes for the integration of the application code inside SGX.

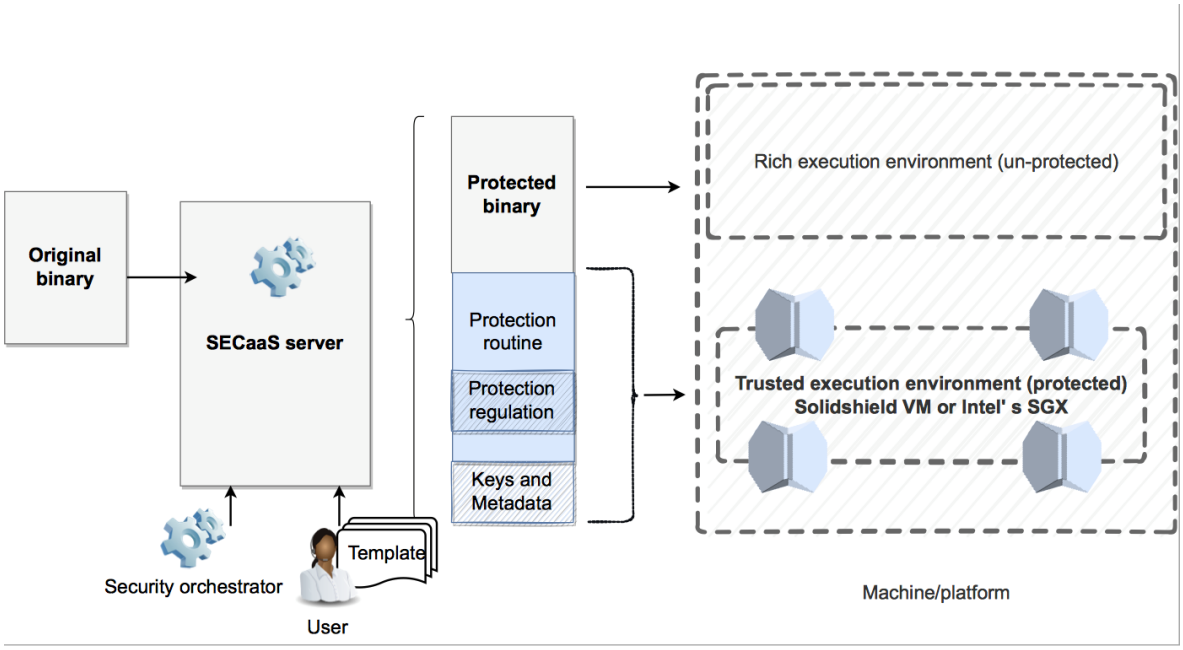

Figure 59: SECaaS general workflow

2.20.5.2 Special processing flow of rules

The structural design of MMT probe as described in Preconditions chapter above, induces a modified basic flow superposed to the standard basic flow. Hence, in addition to the standard basic flow operations as stated above and which relates to the protection of the main MMT-Probe software, additional operations must be fulfilled to protect the rule shared objects once compiled in order that MMT-Probe main software, when loading a rule makes a prior verification of the authenticity of the rule which means that the rule has been produced at a licit platform and is unchanged from its generation. A detailed description of the flow is detailed in the Figure 60. The figure upper part shows the line of actions for the generation of the authenticated protected rules while the lower part illustrates the due processing of the authenticated rule by main software (MMT-Probe).

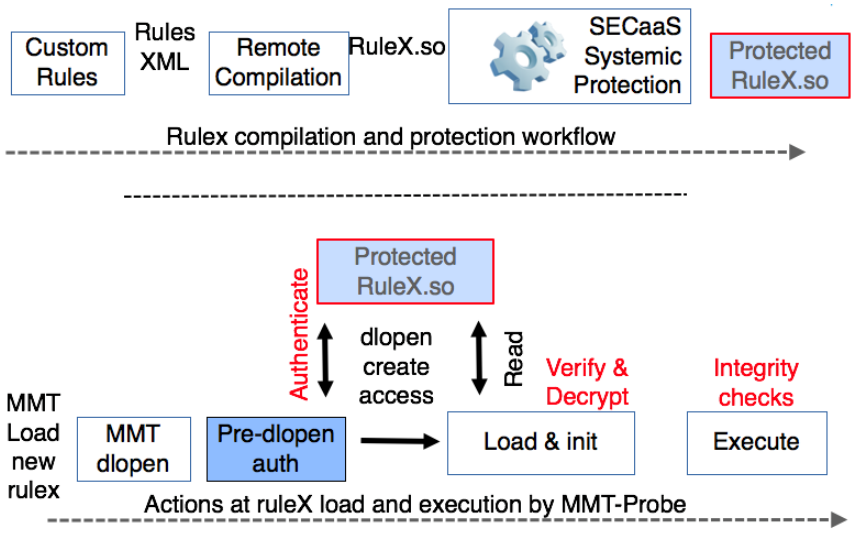

Figure 60: Generation of authenticated rule and their ingestion by MMT-Probe

2.20.5.3 Alternative Flows

As an alternative, the SECaaS service can be activated by a security orchestrator without human interaction and by use of the SECaaS application programming interfaces.

2.20.6 Post conditions

The post conditions can be viewed as the taken actions from the tampering alerts. The final decision to take falls to the operator of the service being either the VSF vendor or its client (the network operator), by integrating the operational considerations implied by the order to keep alive or to interrupt the VSF. Ideally, the solution should go further than alert transmission. The user should opt-in in the user interface several alternatives for terminating the process (graceful termination, alert transmission, keep alive).

2.20.7 Success criteria

- The protected VSF is truly protected against introspection. Tampering attacks are detected and alerts transmitted to Montimage Security Analytics Engine.
- The protected VSF is truly protected against reverse engineering by means of static file analysis (by encryption)
- The protected VSF when loaded is first authenticated to prevent rogue instance mounting.
- The performance degradation (latency at start and overhead in operation) caused by the security functions as defined above is acceptable.
- The protection set-up work-flow is considered easy, fast and intuitive.

2.20.8 Use case summary

The use case highlights the risks (reverse engineering and tampering) pending to any (highly exposed) VSFs when deployed on the network as well as the direct benefits of employing Systemic SECaaS to mitigate these risks.

2.20.8.1 Mapping on INSPIRE-5Gplus architecture

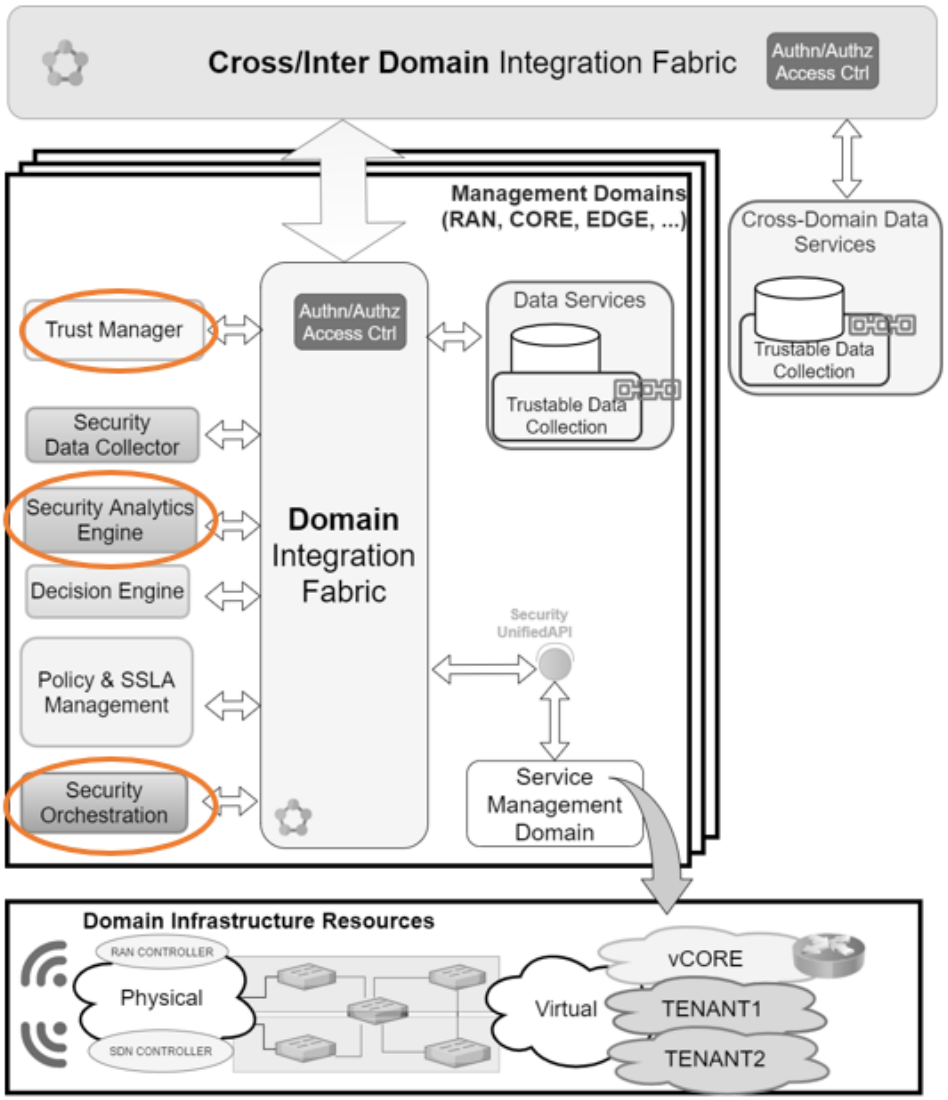

Figure 61: UC T mapping on HLA

Figure 61 shows the main block of the HLA interacting in the use case.

The use case refers to the Trust manager as Systemic delivers a trustworthiness property (i.e., the protected code is integrated), the Security Analytics Engine receiving tampering alerts and the Security orchestration derived from a VSF (i.e., MMT-Probe).

2.20.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- Montimage Security Analytics Engine
- Montimage MMT-Probe
- Tages Systemic software protection SECaaS

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.21 UC U - Security posture assessment and threat visualization of 5G networks

2.21.1 Problem description

The aim of this use case is to reduce the complexity of assessing the security posture of 5G networks. Since 5G networks make heavy use of virtualized assets and resources in a dynamic manner, security analysts need tools and frameworks to properly visualise them and assess them. The use case analyses the cyber threats that impact connected vehicles during a cross-border scenario[10] with the use of 5G networks. We will make use of the DiscØvery enabler to express the assets of 5G networks to assess their security. The modelling language of DiscØvery provides a framework for security analysis of 5G networks, based on hardware, software components, users, policies, and other aspects of the network that affect its security.

2.21.2 Goals

The goals of the use case are to (1) facilitate the security assessment of 5G networks in cross-border applications, through a modelling methodology and processes; (2) provide security related insights to improve the security posture of cross-border applications either with high-level policy recommendations or with low-level security mechanisms.

2.21.3 Actors

The actors and roles involved in this UC are:

- Vehicle A
- Vehicle B
- Vehicle C
- Emergency vehicle
- Mobile Network Operator
- MEC

2.21.4 Preconditions

Initial Condition: Connected vehicles A, B, C and the Emergency Vehicle are moving on a highway.

  - Vehicles B, C are on the right lane at moderate speed (90-100km/h) with some distance between them (e.g., 100m)
  - Vehicle A approaches on the left lane (10 -20 seconds away) moving a bit faster (110 - 130 km/h, eventually overtake)
  - Emergency Vehicle is about 20 - 30 seconds away from Vehicle A at 130 km/h

- Event: Emergency Vehicle turns its emergency state on (electronically); DENM notification are sent periodically
  - This triggers an emergency vehicle warning with the Estimated Time of Arrival (ETA)
- Reaction: The overtaking lane needs to be cleared by the cooperative vehicles, therefore

[10] https://5gcarmen.eu

- Vehicle A needs to shift lane and the slowdown to a moderate speed
- Depending on the ETA and speed differences:
  - ETA much bigger than overtaking time: Vehicle A ends the overtake
  - ETA much smaller than overtaking time: Vehicle A shifts lane and queues behind Vehicles B, C

ETA in between: Vehicles B, C keep on the right lane, and do a cooperative lane merge with Vehicle A. The security analyst will use the DiscØvery enabler to model the components of the use case and then perform a security assessment based on the inputs and suggestions provided by the enabler.

2.21.5 Basic flow

Figure 62 describes the basic analysis flow of the Use Case U.

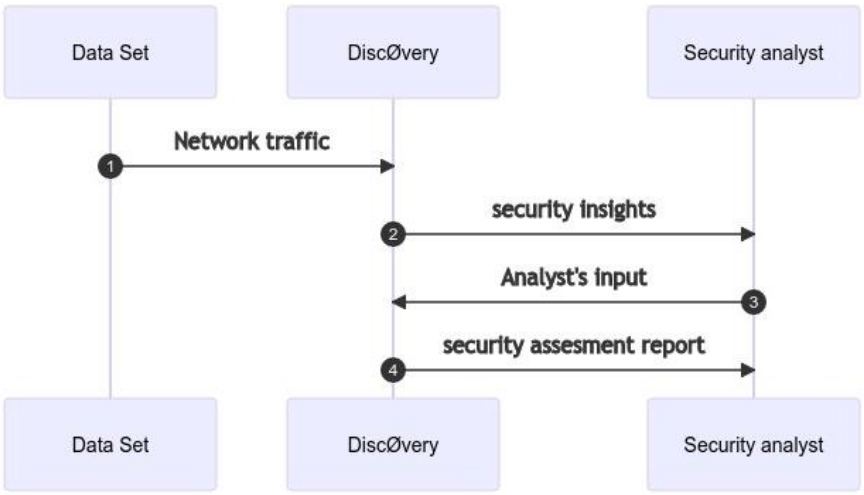

Figure 62: UC U analysis flow

2.21.5.1 Diagram

The following Figure 63 shows the diagrams of the UC U.

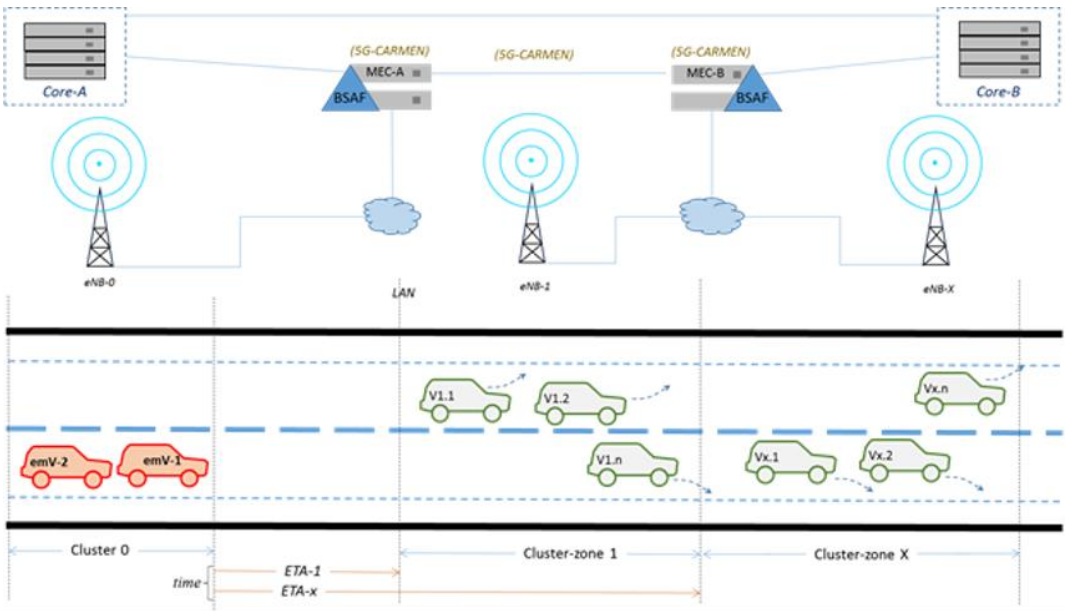

Figure 63: UC U state diagram

2.21.6 Post conditions

The Emergency Vehicle passes undisturbed on the cleared overtaking lane, without any 5G asset being compromised or impacted by a malicious actor.

2.21.7 Success criteria

The aim of the use case is the demonstration of the DiscØvery enabler as a software-based solution to facility the security assessment of 5G networks. The use case is focussed on analysing the security issues of connected vehicles in cross-border scenarios. DiscØvery will provide a list of suggestions and insights on the improve the security posture of the network based on its properties and characteristics.

2.21.8 Use case summary

The use case aims to highlight the security issues and challenges 5G networks have in complex environments, specifically during cross-border scenarios. Such scenarios involve several actors, and security enablers, which makes assessing the overall security posture of the network challenging. The use case illustrates the use of software aided security analysis for cross-border scenarios of 5G networks.

2.21.8.1 Mapping on INSPIRE-5Gplus architecture

In Figure 64 we show the relation of the UC U to the HLA. The main block that interacts with the HLA is the E2E Policy and SSLA management in the E2E Service Management Domain.

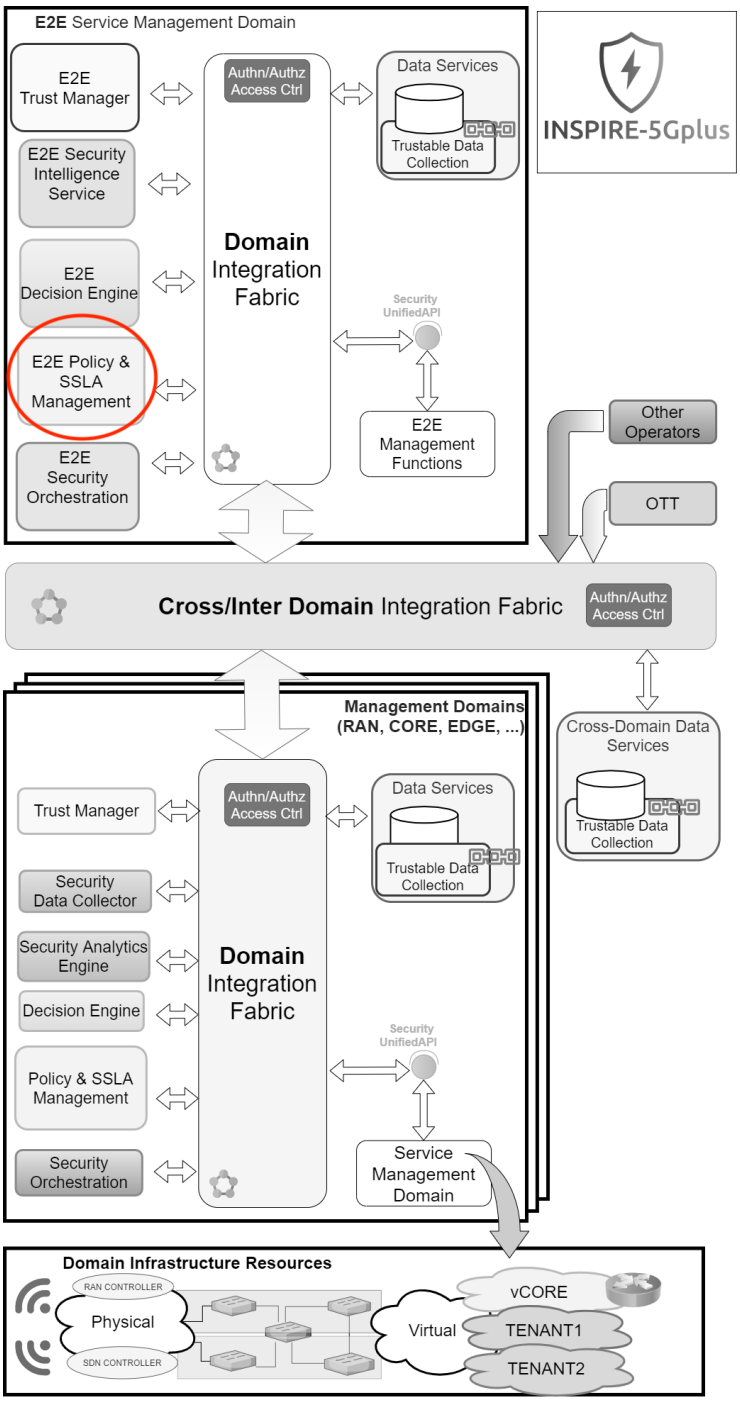

Figure 64: UC U Relation to the HLA

2.21.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case is the DiscØvery enabler.

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.21.8.3 Comments

This use case was introduced in D2.2 [6] as illustrative use case IUC9.

2.22 UC V - Liability integrated RCA for 5G cloudified service environment

2.22.1 Problem description

Since 5G networks are multi-party and multi-layer, management and orchestration choices must be distributed across various entities. Responsibility for management decisions involving end-to-end services becomes ambiguous if no effective liability and accountability system is implemented. Liable parties can be held responsible for bodily harm, economic losses to third parties, and data security breaches. Considering that zero-risk security cannot be achieved, novel solutions for defining liabilities and detecting the causes of security breaches need to be developed for ensuring liable end-to-end delivery of 5G services.

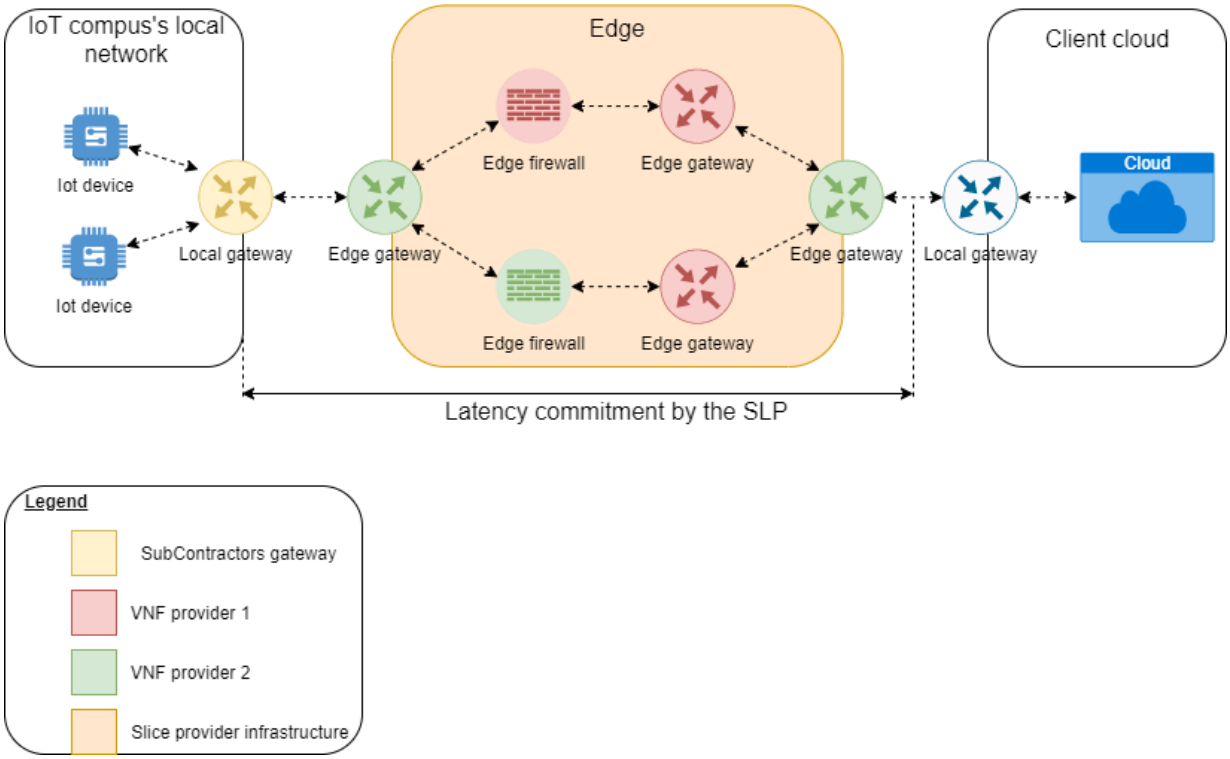

Figure 65: UC V scenario

2.22.2 Goals

The goal of this UC is to provide in case of an incident that impact the Slice Providers (SLP)s commitments an incident report. Based on the evidence collected from an RCA, this report provides a list of the liable parties responsible of the incident and the possible penalties and/or refunds. In this UC, a Service Provider (SP) deploys a service on a SLP's infrastructure spanning from the Cloud to an IoT campus. SLP routes the packets collected from SP's devices in the IoT campus to SP's cloud application through its edge infrastructure. This infrastructure is composed of VNFs provided by two different providers. SLP subcontracts the routing of the packets from the IoT compus's local network to the edge to a SubContractor (SC). For an efficient service, SLP commit to ensure a low latency. For that SLP is responsible toward SP of any incident that impact latency and occurs between the local gateway of the IoT compus's network and the end of the edge infrastructure.

2.22.3 Actors

The actors and roles involved in this UC are:

- Service Provider (SP) which provides a service spanning from the Cloud to IoT devices based on an offer by the Slice Provider SLP
- VNF Software Provider 1 (VNFSP1)
- VNF Software Provider 2 (VNFSP2) SubContractor (SC) which provides a data collection and monitoring service of the IoT Campus. There is a contract between SC and SLP. SC is responsible for managing its service as per the commitments detailed in its contract with SLP.
- Slice Provider (SLP)SLP has a contract its customer SP. SLP is responsible for operating its infrastructure, deploying/updating VNFs software provided by VNFSP1 and VNFSP2 in a way that ensures that fulfils the commitments made in the contract with its customer SP.
- GRALAF which dynamically analyses and identifies the root cause of security and service incidents
- Liability-Aware Service Manager (LASM)

2.22.4 Preconditions

Liability must be expressed in TRAILS (sTakeholder Responsibility, Accountability and Liability deScriptor) by Service Level Agreement (SLA)s given their penalties and triggers. The signature of commitments, as well as the usage conditions, are necessary to achieve the liability criteria. Also, TRAILS assures responsibility by integrating SLA in the properties committed by each actor. For the root cause analysis (RCA), there should be a certain time frame before the anomaly was detected and all microservices in the cloud microservice should run reliably during this time frame.

2.22.5 Basic flow

The basic flow of actions of the actors and the system is devised in three parts:

1. LASM initialization, consist on putting in catalogue the available network components and their TRAILS's profile:
    a. The VNF providers and SubContractors transmit a TRAILS archive to SLP
    b. The administrator adds the TRAILS archive in his catalog by sending the archive to the LASM Referecing Service (LRS).
    c. LRS validates the compliance of the TRAILS archive by verifying the directory pattern, signatures, topology and syntax. Then, it stores the TRAILS archive in a database with the status "Not evaluated".
    d. LRS requests LASM Ontology Service (LOS) by sending TRAILS data to evaluate the associated TRAILS archive with regards to a referencing policy.
    e. LOS is populated with the instances that correspond to the information provided in TRAILS archive.
    f. The TRAILS archive is evaluated with regards to a referencing policy. A status will be assigned to the TRAILS archive such as "Accepted", "Rejected" or Accepted plus operation limitation to be executed before the instantiation of the component.
    g. LRS receive the status from the LOS and modify it.
2. GRALAF initialization:
    a. GRALAF receives configuration data from the LASM that include the extended MUD file and information about the normal behaviour of the components.
3. Latency anomaly, GRALAF detects the latency anomaly with GRALAF module

a. GRALAF sends to the LASM the evidence collected during the Root Cause Analysis which include the root cause list and the traces related to the incidents that triggered the root cause.

2.22.5.1 Diagram

Figure 66 illustrates the basic flow of UC V.

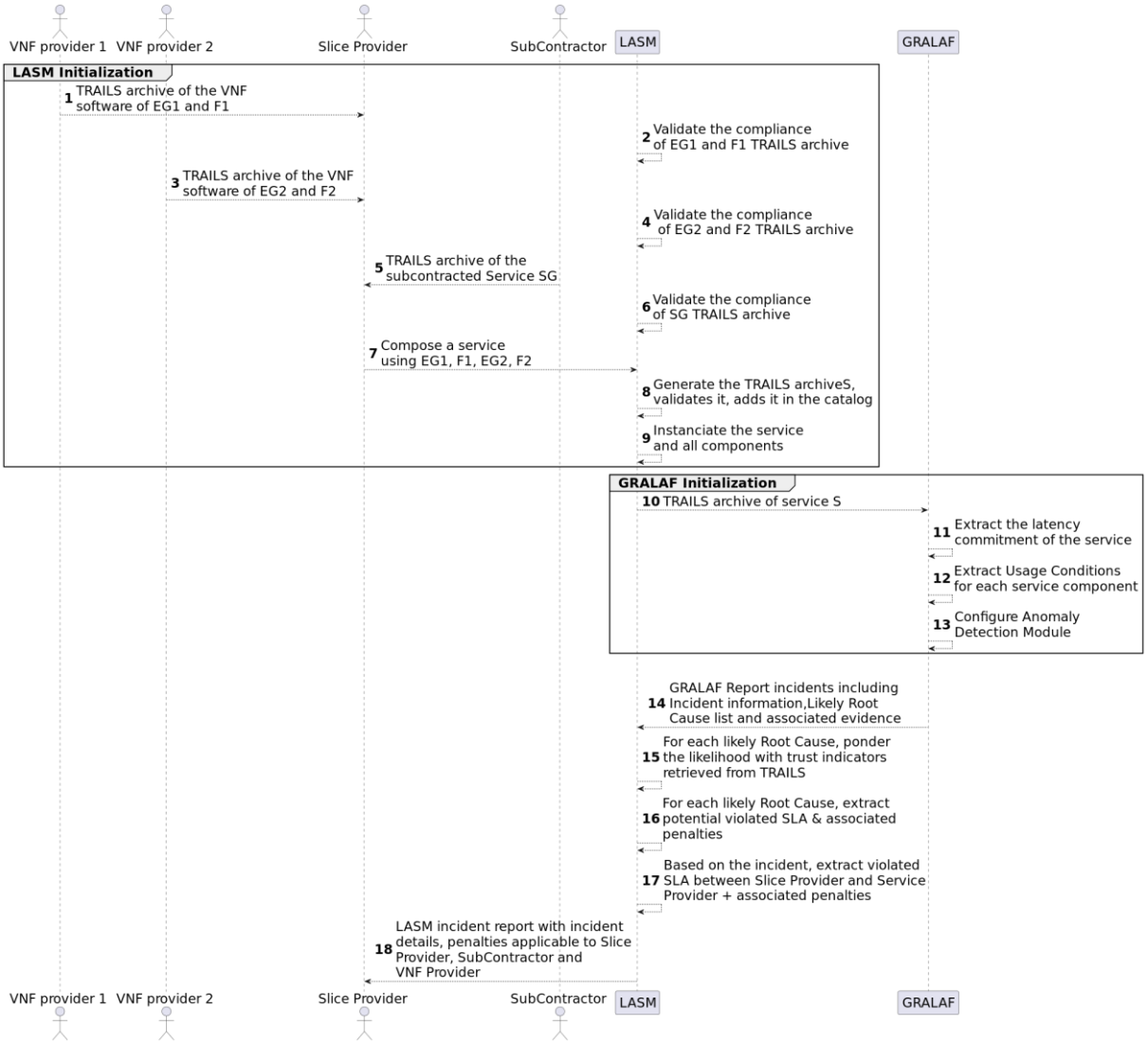

Figure 66: UC V diagram

The data flow for the liability analysis is given Figure 67.

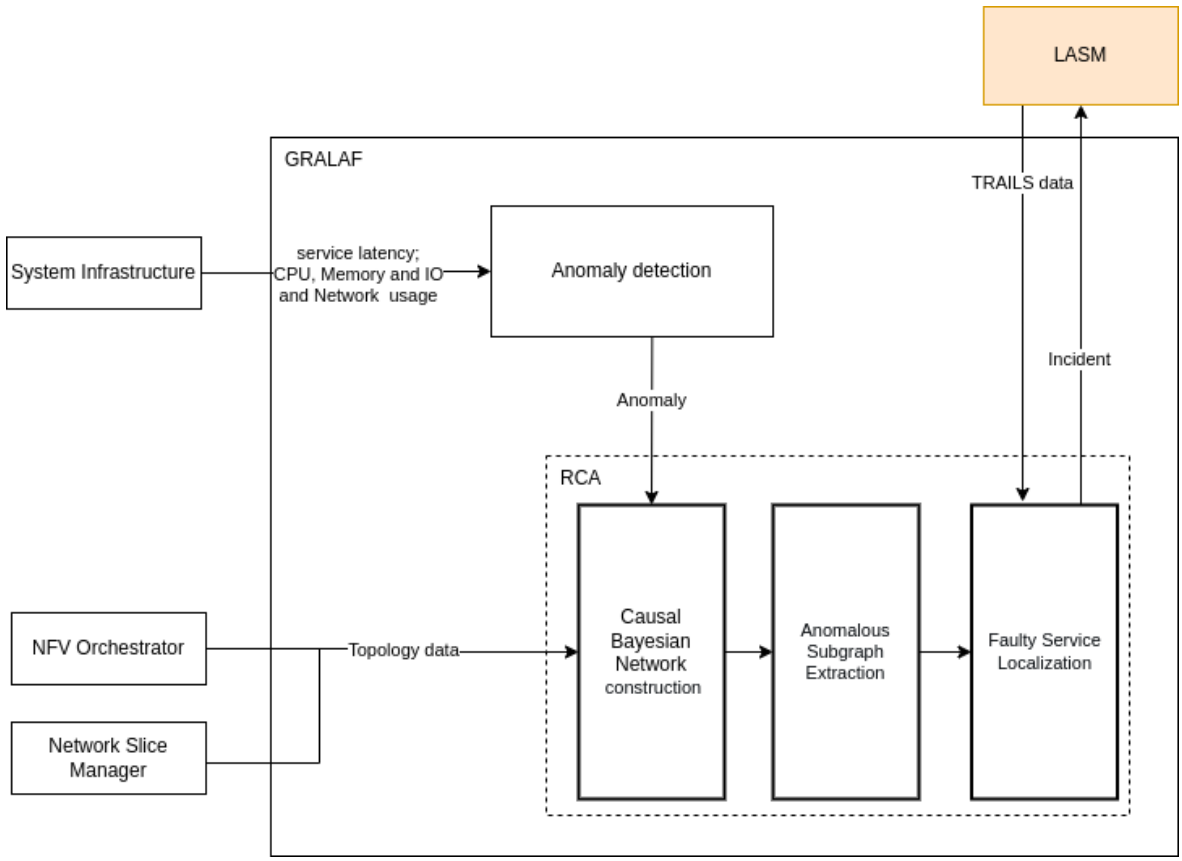

Figure 67: Liability analysis data flow

2.22.6 Post conditions

The final result will lead to the following post conditions:

- The system administrator sends the LASM report to the responsible parties, along with the evidence.
- Incident liability negotiation can be held among the responsible parties.
- If the negotiations fail, parties may go to court.

2.22.7 Success criteria

The goal will be met if, after the intrusion has been detected, the most likely responsible parties with the appropriate accountability are identified and reported.

2.22.8 Use case summary

This UC aims to distribute legal and financial responsibility proportionately among any liable parties involved in cloud service in 5G contexts. Showcasing GRALAF, TRAILS and LASM is the main objective. Firstly, the description of the responsibilities and accountabilities of supply chain actors will be provided through TRAILS. Secondly, GRALAF will detect the probable root cause of failures and report incidents by using graph-based approaches and TRAILS data received from LASM. Finally, LASM shall distribute the responsibilities proportionately among the parties and generate a report.

2.22.8.1 Mapping on INSPIRE-5Gplus architecture

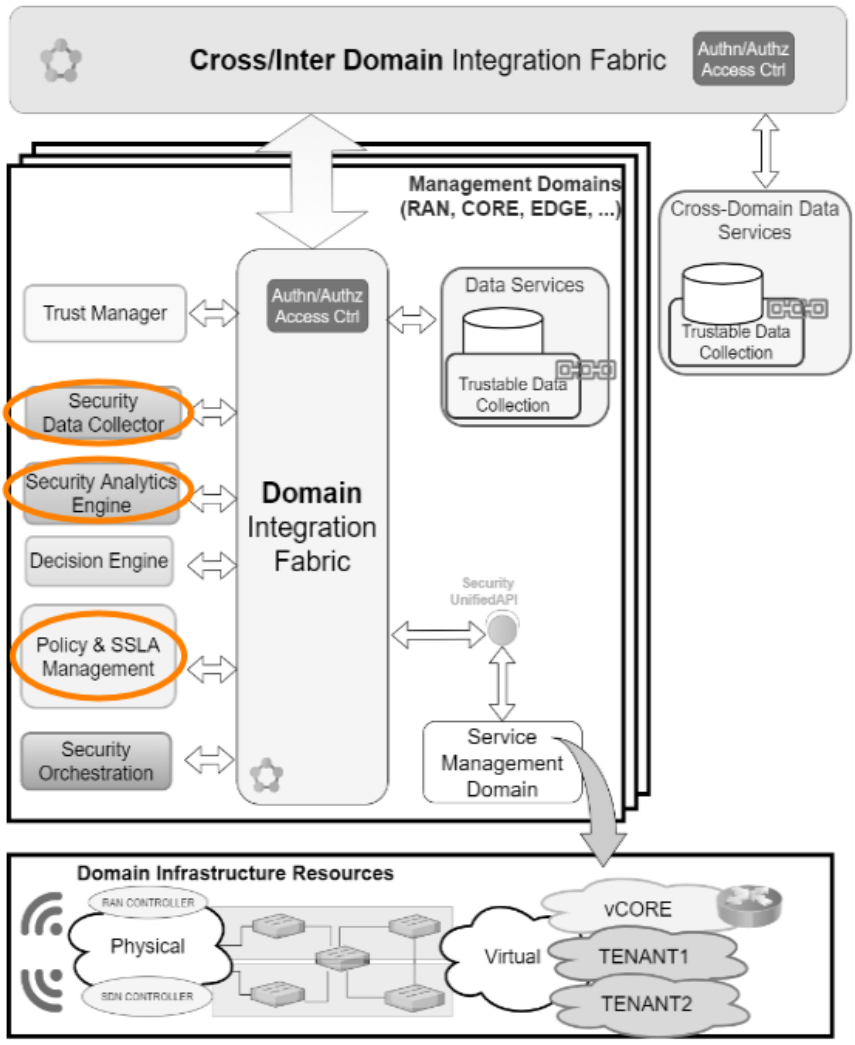

Figure 68: UC V mapping to HLA

2.22.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- GRALAF
- TRAILS (sTakeholder Responsibility, Accountability and Liability deScriptor)
- Liability-Aware Service Manager (LASM)

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

2.23 UC W - E2E Encryption TEE secured SECaaS

2.23.1 Problem description

5G verticals use slices across multiple domains to exchange sensitive data. E2E slices provide, to some degree, the privacy needed through traffic isolation between slices; but E2E cryptographic protection is also needed to provide data confidentiality, integrity and extra privacy as well. Besides, the data protection in the different 5G network domains (Access, Transport, Core) is not always well homogeneous managed. Static permanent keys, or very long key and certificates refreshment, open more opportunities for attackers to access the content. While end-to-end communication may be encrypted, it is also true that latest computer processor vulnerabilities open the door to memory introspection to extract keys (such as AES).

2.23.2 Goals

The use case proposes solve above problems with two requirements to be fulfilled: endpoint mutual authentication, and data encryption using a centralized management solution based on specified policies. Therefore, Zero Touch VNF-based E2E encryption over 5G MECs is proposed following the centralized SDN control paradigm for key distribution and renew and, at the same time, hardware-based enclaves on the MEC, take profit of SGX to protect cryptographic material usage, by performing encryption-decryption operations in the TEE.

As an extra secure communications layer, VNFs acting as proxies can be deployed dynamically to protect communications end-to-end. It is the case for IPSec, for layer 3 communications between infrastructure sites (e.g. gNB to Edge or Edge to 5GCore data center) and also for DTLS in case of UDP communications as is usually seen at application level for IoT environments. The basis of both encryption systems is based on key derivation which in turn can be done centralized or on the hosts.

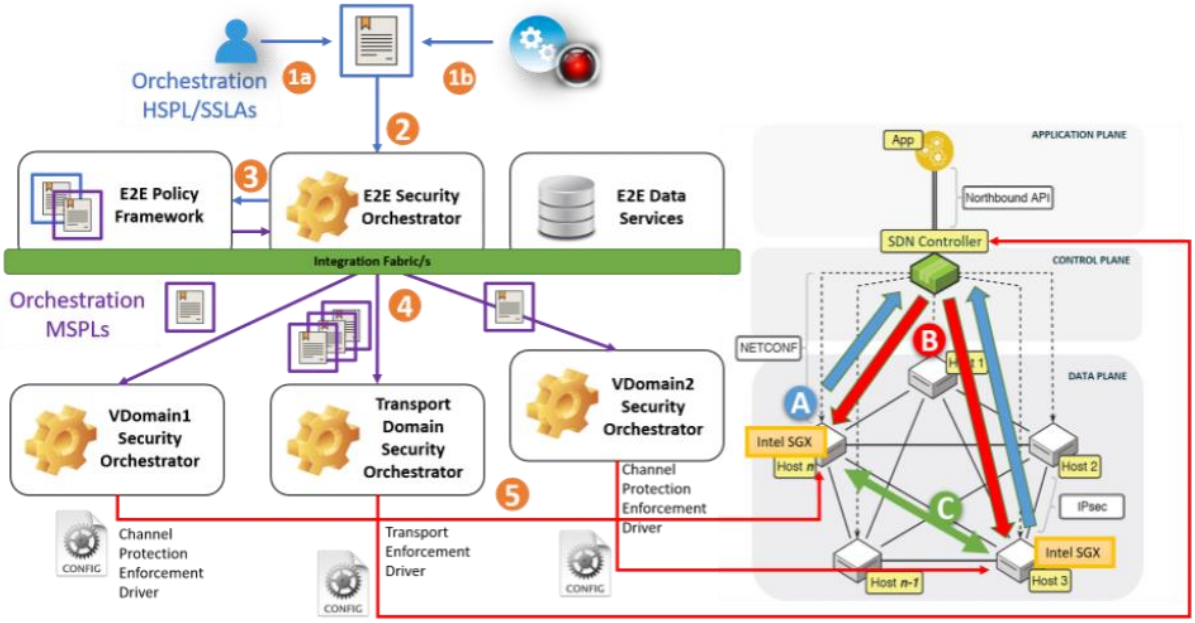

Figure 69: Use case W diagram

2.23.3 Actors

The actors and roles involved in this UC are:

- End-users (including verticals applications and IoT devices) with sensitive data.
- System Administrator/NOC. In charge of the E2E encryption security policies

- Network domains involved (Access, Core, transport, datacentres, MEC)

2.23.4 Preconditions

The UC requires the following pre-conditions:

- End- users are authenticated and given access to the 5G network
- Administrators manage all Domains, access, edge, transport and cloud.
- There is a need for data path traffic protection (IPSec, DTLS) by administrator/NOC decision or as an incident response
- Edge nodes are located nearby the RAN to which end-users are connected. Need for traffic redirection capability in the Edge.
- Intel SGX is available in the Edge nodes or cloud nodes.

2.23.5 Basic flow

Figure 70 shows the UC subsequent actions:

1. Either the administrator/NOC (a), Security Intelligence Service or Cognitive Decision Engine (b) decides that there is a need for protecting traffic between two devices or between a device and the cloud. Also, include the algorithms and keys to use, and the re-keying policy aligned with end-user demands.
2. A security policy (HSPL) and probably a SSLA is generated that defines the E2E encryption need.
3. There is a translation and conflict detection process, to decide the best configuration and where to apply it.
4. Subsequent definitions are generated for each 5G connectivity management domain. At the very least two virtual domains, the transport network and the RAN, to divert traffic to the vdomain.
5. vIPSec enabler is deployed in an infrastructure that supports Intel SGX enclaves,
6. E2E connectivity and configuration of the vIPSec enabler from the centralized management based on I2NSF protocol entity (SDN Controller) is performed.
    a. Network Interfaces discovery
    b. SAD/SPD models enforcement
    c. Traffic E2E is protected.

In the main flow the administrator defines the policies in the E2E domain for encryption. As a results parallel flows are triggered to deploy the TEE-protected vIPsec enabler in each vDomain and the configuration from the Transport Domain. The latter can periodically update the keys and algorithms from a central point without involvement of end-users.

2.23.5.1 Diagram

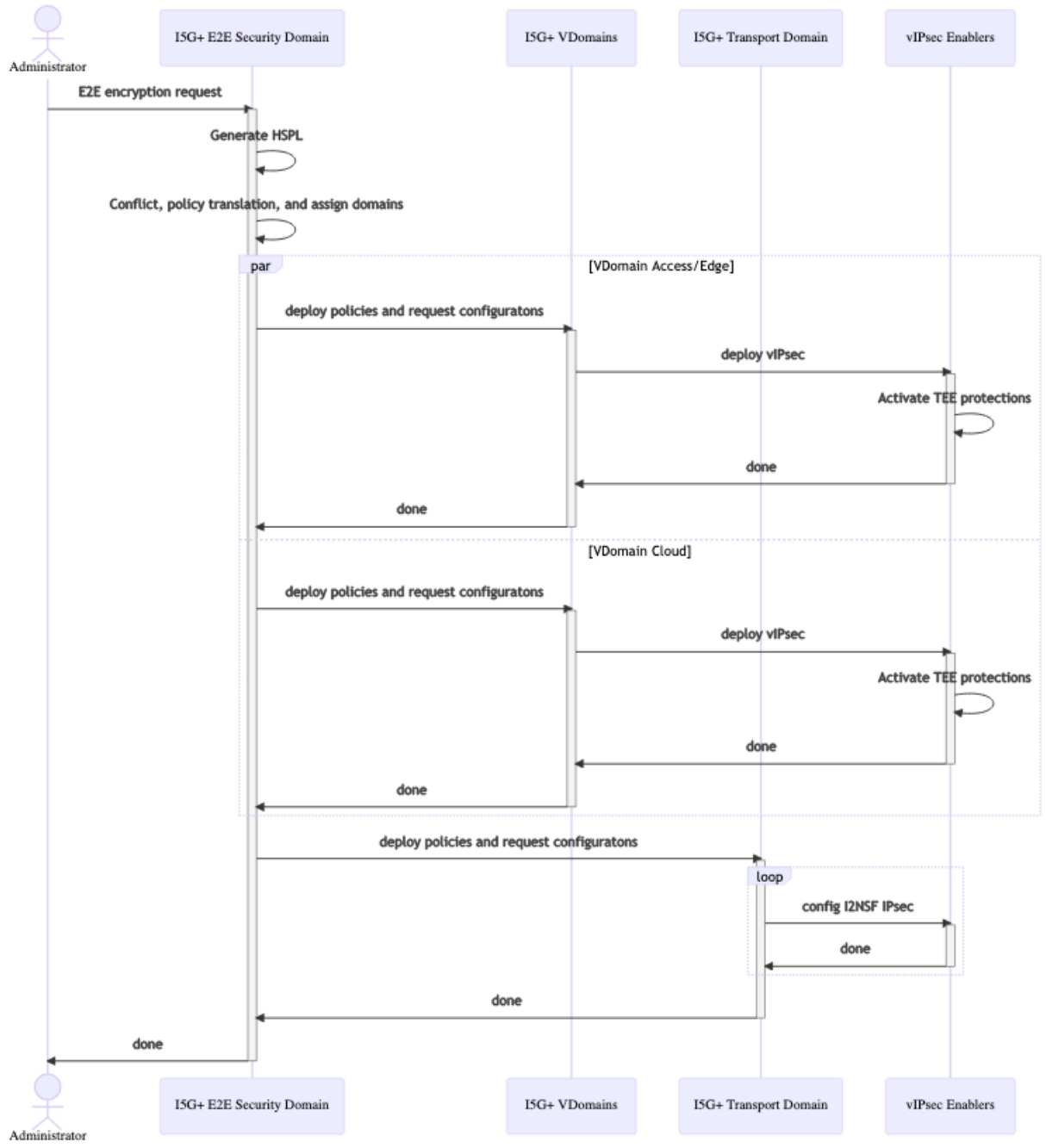

Figure 70: Flow for UC W

2.23.5.2 Alternative Flows

Instead of the use of vIPsec VNFs for Edge to cloud layer 3 protection, specific application flows can use a DTLS proxy VNFs if the solution wants to address some specific IoT applications and not all traffic in the slice. The Administrator will trigger a different policy (HSPL) that will deliver different VNFs and the orchestrator interfaces to control VNFs.

2.23.6 Post conditions

The traffic requested by the Administrator for End-users is E2E protected with an encryption solution based on IPsec (alternatively DTLS) and the use of TEE.

2.23.7 Success criteria

The connectivity is achieved over the transport networks. Monitoring the traffic will confirm that the traffic is encrypted with technological solutions designed (IPsec or DTLS). Additionally, key material is renewed and traffic re-encrypted from the centralized INSPIRE-5Gplus Control plane.

2.23.8 Use case summary

Traffic is protected/encrypted over the transport network in an independent slice transparently to the user equipment (UE). Operations are performed within the TEE Enclave. It illustrates a Zero-Touch encryption policy management and enforcement. Besides, the cryptographic material and routines (using such material) are going to be implemented in virtualised network functions (VNF) and protected by Trusted Execution Environment techniques. All of these are operated in a ZSM closed loop based on the definition of high-level security policies and possibly SSLAs that are enforced on a multi-domain scenario.

2.23.8.1 Mapping on INSPIRE-5Gplus architecture

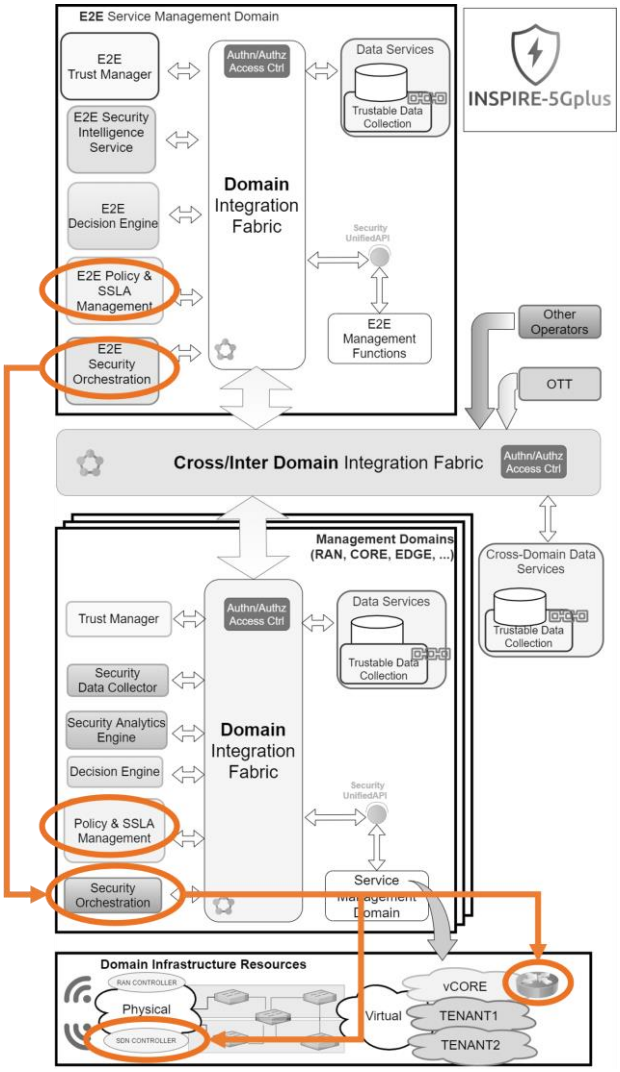

Figure 71: UC W mapping to INSPIRE-5Gplus HLA

2.23.8.2 INSPIRE-5Gplus cybersecurity enablers

The INSPIRE-5Gplus cybersecurity enablers or assets involved in this use case are:

- E2E Security Orchestrator and Domain Security orchestrator, for management and orchestration configurations.
- Policy Orchestrator for translation and reconciliations actions
- Virtual Channel protection with DTLS proxy for centralized orchestration
- I2NSF IPsec enabler (based on IETF standard) as the SDN controller and IPsec gateway for encryption and dynamically configurable by policies.

The references to detailed INSPIRE-5Gplus enabler descriptions are placed in Appendix A.

3 Analysis of Use Cases

3.1 Mapping use cases to security challenges/trends

The following table shows correlation between the security gaps that were identified in D2.1 [7], and the use cases in INSPIRE-5Gplus that tackle them. In D2.1 we identified several security gaps and the relevant technologies that aim to address them. We grouped the developed use cases into the technology domains to provide a high-level view of the security gaps that we aim to address.

Technology	Security Gap. Progress axis	Use Case
Artificial Intelligence and Machine Learning	• Devise efficient and effective AI-driven mechanisms for intelligently detecting and mitigating 5G security threats. • Investigate one unexplored space: AI-based threat detection over encrypted data flows (as 50% of today traffic is encrypted). • Tackle with the concept of Network Digital Twins. • Tackle with the concept of (data) streaming telemetry (based on Yang-based model) to ease and experiment the selection and processing of most relevant and restricted data flow (best qualifiers).	UC A UC E UC F UC H UC P
Authentication	• Lack of coordinated authentication processes for services and consumers for multi-domain applications	UC E UC F
Automation and Zero-touch Service Management	• Define a minimal viable ZSM, avoiding the "calamity of over-arching solutions," which spans over a complete E2E slice over several domains. Practical implementations delivering measured improved security are to be drawn and implemented. • Comprehend the research and standardization works by ETSI and ITU-T: GANA architecture, ZSM concept and its derivations at ONAP and OSM frameworks, ENI working group, ITU FG-ML5G and its unified high-level architecture (ML pipeline, ML sandbox and ML function orchestrator).	UC M UC W
Cyber threat intelligence and data sharing	• Define the ad hoc usable sources for cyber threats to operators. • Devise how to move from a static threat landscape to evolving or new threats. • Consider the benefits of new risk assessment frameworks of complex ICT systems with notably the progress on risk assessment graph.	UC U
DLT	• Devise pragmatic paths to DLT usage over the networks over three possible implementations: DDoS attacks, AAA, and SLA management.	UC L UC S
Dynamic Liability and Root Cause Analysis (based on ML)	• Deliver fast and timely faulty source information. • Ability of the RCA to grasp the network structure (model representation) ever evolving. • Devise the most relevant learning and diagnostic methods-approaches with a special focus on Deep learning • Reduce the domain space to highly signing datasets only.	UC J UC V

Technology	Security Gap. Progress axis	Use Case
	• Define the most relevant network status indicators, with the help of Principal Component Analysis.	
MEC security	• More exposed to introspection, MEC security is a main concern. Devise a resource-efficient security solutions resident in the MEC	UC U UC K UC S
MTD and Cyber Mimic Defence Techniques	• Devise the real benefits of these techniques (which by-default generate network structure automatic variations and instabilities) when applied in a complex multi-domain, multi-operator, multi-tenant, and cross slice scenario (with their set of security constraints). • AI for MTD	UC N
NFVI, VNF, MANO and interface security (API	• Investigate the security and the performance of latest controller North Bound and South Bound APIs including NETCONF, TAPI, JOX	UC R UC Q UC W
SDN security, SD-SEC and SECaaS	• Investigate how software security service (dealing with Identify, Protect, Detect, Respond and Recover) can be expanded in a multi domain/multi-tenant environment.	UC T UC M UC Q UC W
Secure 5G radio access	• Devise and define a smart (more secure for delivering both confidentiality and integrity, performance acceptable, easy workflow) E2E data flow encryption.	UC E UC F UC Q
Securing Artificial Intelligence - SAI	• Embrace, comprehend and advance the works made at ETSI Industry Specification Group on securing artificial intelligence 3ISG SAI)	UC H
Security service level agreement	• Define an open (i.e., adaptive to any liable parties of the agreement), dynamic (i.e., QoS or security rules can evolve) and secure SLA template management framework enabling SLA in the context of the varying 5G services and of the complexity and size of a service value chain (made up of several suppliers).	UC R UC M UC V
Security solutions oriented towards verticals	• Devise solutions for securing network slicing and hardware root of trust (when highly security-sensitive OT in vital infrastructure is concerned)	UC T UC I UC Q UC J UC K UC W
Service isolation	• Lack of secure hardware infrastructure to deploy isolated services.	UC R UC W
Trust models and liability analysis in 5G	• Devise a trust management solution and its associated processed metrics, inputs, aggregation methods delivering accurate and pertaining trust level assessment in the context of 5G complex service value chain. • Grasp the concept of forwarding accountability and strong accountability concepts to elaborate trustworthiness. • Grasp the work related to liability expressiveness (and associated domain specific language) as well as delegation of obligation	UC R UC I UC J UC M UC V

Technology	Security Gap. Progress axis	Use Case
	• Grasp the practical aspects on defective algorithm accountability, packet proof of transit (how effective, benefits and trustworthiness of brought information.	
Trusted Execution Environments	• Define a smart way to bring to network functions provable integrity and confidentiality guaranties, through a by-default, zero-touch workflow, generating low overhead.	UC T UC H UC I UC W
Vertical CCAM	• Lack of integration and leveraging CCAM customized AI/ML for greater Quality of Experience and Service Availability	UC E UC F

Table 1: Security gaps addressed by use cases

3.2 Mapping to 5G generic architecture

Use cases described in Section 2 refer to various 5G usage scenarios and security problems located in various domains of 5G System. Figure 72 presents the relation of each use case to 5G asset groups of the simplified 5G System view. Use cases address security problems occurring within entire system starting from mobile devices (UE) through network components and underlying technologies ending in E2E service and additional security assets.

However, since INPIRE-5GPlus framework covers both multiple domains and E2E level and many security enablers and mechanisms can be applied to various domains, use case are often relevant to more than one 5G asset group.

As depicted in figure the proposed set of use cases demonstrates the potential of envisaged INSPIRE-5GPlus enablers to efficiently solve security problems spanning the whole 5G System.

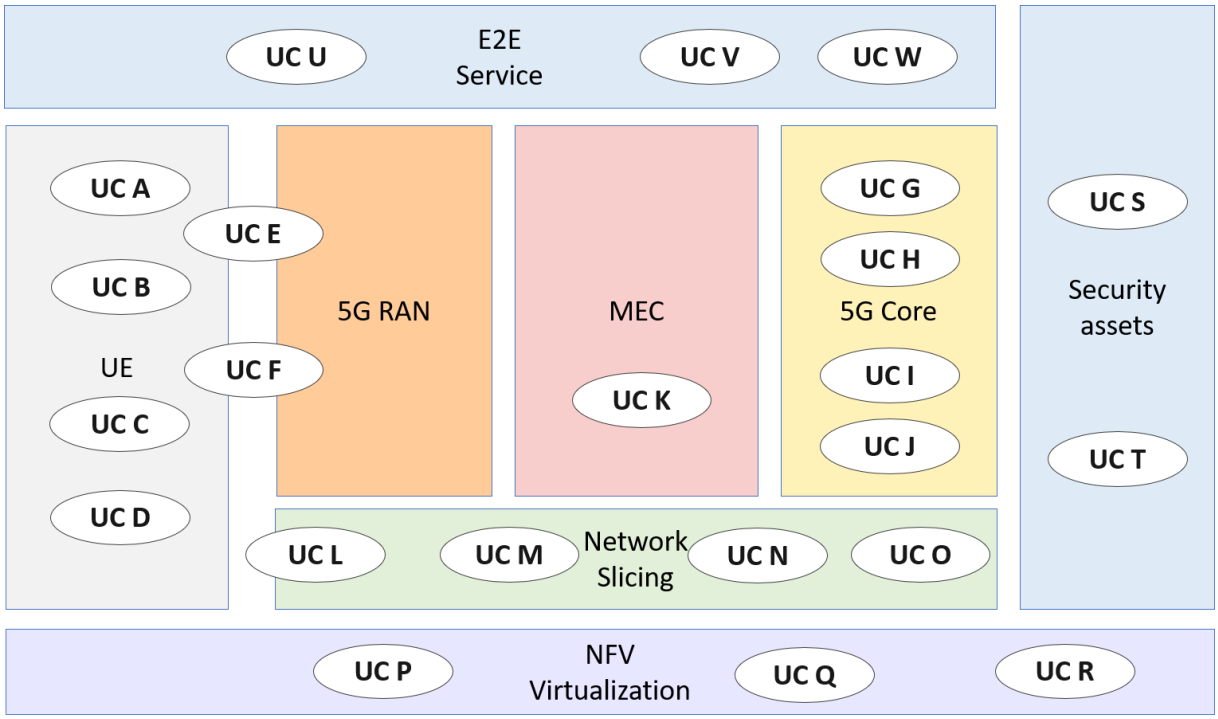

Figure 72: Relation of use case to specific assets of 5G system

3.3 Mapping use cases to security enablements

D2.2[6] included summary of enabling technologies used in illustrative use cases. Table 2 includes extension of that mapping with the described above final set of use cases. In INSPIRE-5Gplus the following enabling technologies are distinguished:

- **ZSM** - Automation & Zero touch management
- **TEE** - Trusted Execution Environments
- **AI** - Artificial Intelligence
- **ACST** - Advanced CyberSecurity Techniques
- **DLT** - Distributed Ledger Technologies
- **DL & RCA** - Dynamic Liability and Root Cause Analysis
- **SSLAs & PoI** - SSLAs and Policy Management

	ZSM	TEE	AI	ACST	DLT	DL & RCA	SSLAs & PoI
UC A	X		X				
UC B	X		X				
UC C			X			X	
UC D			X				X
UC E			X	X			
UC F			X	X			
UC G				X	X		X
UC H	X	X	X	X			
UC I		X		X		X	
UC J		X		X		X	X
UC K		X					X
UC L							X
UC M					X		
UC N	X		X	X			
UC O	X		X		X		X
UC P	X		X				X
UC Q	X						X
UC R	X	X				X	X
UC S					X		
UC T		X		X			
UC U			X	X			X
UC V						X	X
UC W	X	X					X

Table 2: Use cases and enablements mapping

3.4 Reference to demonstration scenarios

INPIRE-5Gplus consortium works together to develop demonstration scenarios that help to validate the general approach of the Project in the real environment. Proposed scenarios are based on presented use cases and show possible integrations of considered enablers into comprehensive solutions.

3.4.1 Demo 1

To show the INSPIRE-5GPlus potential as a full framework in which test cases help validate the general approach, demo1 implements different security aspects from a variety of use cases across multiple Security Management Domains as part of a unified storyline. Thus, *demo 1 displays the request of two Security Service Level Agreements (SSLAs)*, one for the protection of the communication between the UE access domain and a 5G service domain located in separated Security Management Domains and the second one for securing sensor data exchange between IoT sensors in remote sites and a global IoT supervision.

- UC H: Network attacks over encrypted traffic in SBA and security evasion prevention. Abnormal 5G behaviour is detected and mitigated by analysing encrypted traffic benefiting from the evolution of the security network monitoring tools based on AI statistical methods. Additionally, unauthorised access to data and detection of software characteristics and behaviour are prevented.
- UC N: End-to-End Slice Protection based on Moving Target Defense and Anomaly Detection. After collecting network metrics to detect anomalies, the use case performs Moving target defense as a reaction to protect a 5G slice deployed for IoT communications, reducing the time window attackers have to perform the attack and mitigating ongoing detected attacks.
- UC E: Remotely controlled manoeuvring manipulation. V2X monitoring solution is used to detect abnormal behaviour (DoS) in one of the SMD, thus addressing threats and attacks related to manoeuvring information manipulation by either malicious outsiders or insiders of the system and still guaranteeing network performance.
- UC Q: GPDR aware counterparts for cross-border movement. Trust security enablers have been included on demo1 to demonstrate a multi-domain policy enforcement ecosystem and evaluate its trustworthiness to derive possible actions. Besides, achieving GPDR compliance on the network traffic and maintaining trust values updated for the solutions involved.
- UC T and UC W: E2E Encryption TEE secured SECaaS. E2E encryption is provided as part of a 5G security slice. SECaaS protects a monitoring module and its rules in one of the SMDs. It showcases the risks related to the deployment of VSFs on the network and the gains of Systemic SECaaS used for risk mitigation.
- UC S: Trusted Smart Infrastructure. Trust security enablers have been included in demo1 to detect abnormal behaviours occurring in the traffic flows of the infrastructure. Thus, applying the corresponding mitigation measures to reach a security compromise of the device or its counterpart.
- UC P: Intelligent and Secure Management of Shared Resources to Prevent (D) DoS. DDos detector has been included in one of the SMDs to solve situations where undetected slice attacks trigger resource starvation in shared infrastructure that affect other critical slices. It provides damage control to protect shared resources and minimizes the impact on uncorrupted slices or services.
- UC G: Definition and assessment of Security and Service Level Agreements. The proactive part of the demo uses SSLAs definitions to generate proactive security policies.
- UC L: Deployment and management of Multi-domain Network Slices with associated SSLA to enforce a Quality of Security Level. The Network Slice Manager planned in this UC has evolved into the E2E Network Slce Manager in Demo 1.

3.4.2 Demo 2

To show the INSPIRE-5GPlus potential as a full framework in which test cases help to validate the general approach, demo2 implements different security aspects from different use cases as part of a unified storyline.

- UC I: remote attestation framework allows to collect evidence on pre-agreed KPI or way to evaluate security properties on some components.
- UC J: an orchestration under constraints, in particular constraints linked to Client SLA (request of isolation for instance) may allow to manage efficiently some energy, latency or security requirements.
- UC K: an orchestration under constraints at MEC level linked to Client SLAs (request of isolation for instance) may allow to manage efficiently some energy, latency or security requirements in central (UC J) and specific technical domain like MEC.
- UC T: SECaaS protects monitoring module when required by the Client and UC I allow to control that the SECaaS is effectively deployed and active.

3.4.3 Demo 3

Demo 3 will present a MTD focused protection strategy using security assets mapping to different security enablers developed in the project. It brings together AI/ML driven decision making, network monitoring, security incident detection and security orchestration to lay out a n integrated scenario for end-to-end slice protection. The main purpose of Demo 3 is to highlight and quantify the utility of MTD in a relevant security scenario in 5G networks. Therefore, it will elaborate on a single use case especially designed towards this goal:

- UC N: Smart MTD for improving the proactive and reactive protection of network slices by collecting resource usage and network metrics through multiple points of the 5G network and assessing the network state in real-time and detecting anomalies or security incidents such as intrusion and network attacks

4 Conclusions

In this deliverable we presented the set of security use cases answering the need for developing and deploying secure and reliable 5G services for various usage scenarios. Proposed 5G security use cases serve to demonstrate the potential of security enablers developed within INSPIRE-5Gplus project. Use cases were developed with emphasis on presenting the cooperation of enablers delivered by different Project partners within proposed High-Level Architecture and were selected to cover the vast majority of targeted enablers. Each use case was described in uniform way: starting from indication of particular security problem, through presentation of flow of actions performed by each use case actor and ending with summary of results and involved security enablers.

In addition, use cases were analysed with respect to identified previously 5G security needs, emerging security enabling technologies considered in the project and the relation to 5G assets being the subject of security problems.

Finally, the references of use cases to envisioned demonstrations validating selected security assets in the real environment were pointed out showing the coherence of project activities.

References

[1] INSPIRE-5Gplus D3.1. 5G security assets baseline and advancements - https://www.inspire-5gplus.eu/wp-content/uploads/2021/05/i5-d3.1_5g-security-assets-baseline-and-advancements_v0.7.pdf

[2] INSPIRE-5Gplus D3.2. 5G Security drivers and associated software-defined models - https://www.inspire-5gplus.eu/wp-content/uploads/2021/11/i5-d3.2_5g-security-drivers-and-associated-software-defined-models_v1.3.pdf

[3] INSPIRE-5Gplus D3.3. 5G security new breed of enablers - https://www.inspire-5gplus.eu/wp-content/uploads/2022/03/i5-d3.3_5g_security_new_breed_of_enablers_v1.0.pdf

[4] INSPIRE-5Gplus D4.1. Trust mechanisms for 5G environments - https://www.inspire-5gplus.eu/wp-content/uploads/2021/09/i5-d4.1_trust-mechanisms-for-5g-environments_v1.0.pdf

[5] INSPIRE-5Gplus D4.3. Liability mechanisms for 5G environments - https://www.inspire-5gplus.eu/wp-content/uploads/2021/11/i5-d4.3_liability-mechanisms-for-5g-environments_v0.91.pdf

[6] INSPIRE-5Gplus D2.2. Initial Report on Security Use Cases, Enablers and Mechanisms for Liability-aware Trustable Smart 5G Security https://www.inspire-5gplus.eu/wp-content/uploads/2021/05/i5-d2.2_initial-report-on-security-use-cases-enablers-and-mechanisms-for_v0.14.pdf

[7] INSPIRE-5Gplus D2.1. 5G Security: Current Status and Future Trends - https://doi.org/10.5281/zenodo.4569519

[8] INSPIRE-5Gplus D5.1. 5G security test cases - https://doi.org/10.5281/zenodo.4569524

[9] Ghada Arfaoui, Pierre-Alain Fouque, Thibaut Jacques, Pascal Lafourcade, Adina Nedelcu, Cristina Onete, Léo Robert: A Cryptographic View of Deep-Attestation, or how to do Provably-Secure Layer-Linking. ACNS 2022.

[10] Matheu, Sara Nieves, et al. "Extending MUD profiles through an automated IoT security testing methodology." IEEE Access 7 (2019): 149444-149463.

[11] Laufs, Julian, Hervé Borrion, and Ben Bradford. "Security and the smart city: A systematic review." Sustainable cities and society 55 (2020): 102023.

Appendix A References to enabler description

For each enabler the reference to relevant WP3 / WP4 deliverable is indicated in Table 3.

Enabler name	WP	Enabler description
Admission Controller Delegator (Auto-scaling Module)	WP3	D3.3[3]
Anti-GPS Spoofing	WP3	D3.3[3]
Component Certification Tool (CCT)	WP4	D4.1[4]
Data Collector	WP3	D3.1[1]
DDoS Mitigator (Damage Controller)	WP3	D3.3[3]
Decision Engine	WP3	D3.1[1]
DiscØvery	WP3	D3.2[2]
GRALAF	WP4	D4.3[5]
I2NSF IPsec	WP3	D3.2[2]
Liability-Aware Service Manager (LASM)	WP4	D4.3[5]
Lightweight and space-efficient vehicle authentication enhanced with misbehaviour detection	WP3	D3.3[3]
MMT probes	WP3	D3.3[3]
MTD controller (MOTDEC)	WP3	D3.2[2]
MUD/Behavioural profiles	WP3	D4.3[5]
Network slice manager (Katana)	WP3	D3.2[2]
Optimizer for security functions (OptSFC)	WP3	D3.3[3]
Policy and SSLA Management	WP3	D3.2[2]
Policy and SSLA Manager	WP3	D3.2[2]
Policy Framework	WP3	D3.2[2]
Policy Manager	WP3	D3.1[1]
Policy Orchestrator	WP3	D3.1[1]
Remote Attestation	WP4	D4.3[5]
Root Cause Analysis	WP4	D4.3[5]
Secured Network Slice Manager for SSLA	WP3	D3.2[2]
Security agents	WP3	D3.3[3]
Security Analytics Engine	WP3	D3.3[3]
Security Analytics Framework (SAF)	WP3	D3.3[3]
Security by Orchestration (K8s)	WP4	D4.3[5]
Security by Orchestration for MEC	WP3	D3.2[2]
Security Data Collector	WP3	D3.1[1]
Security Monitoring Framework	WP3	D3.2[2]
Security Orchestrator	WP3	D3.2[2]
SFSBroker	WP3	D3.2[2]
Smart Traffic Analyzer	WP3	D3.3[3]
SSLA Manager	WP3	D3.2[2]
Systemic/SECaaS	WP4	D4.1[4]
TRAILS (sTakeholder Responsibility, Accountability and Liability deScriptor)	WP4	D4.3[5]
Trusted Blockchain-based Network Slices	WP4	D4.1[4]
Virtual Channel Protection with DTLS Proxy	WP3	D3.2[2]

Table 3: Summary of INPIRE-5Gplus enablers presented in the final set of security uses cases

[end of document]