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

D2.4: Final Report on Enablers and Mechanisms for Liability-aware Trustable Smart 5G Security Management Framework

Version: v1.0

Deliverable type	R (Document, report)
Dissemination level	PU (Public)
Due date	31/10/2022
Submission date	31/10/2022
Lead editor	Noelia Pérez Palma (UMU)
Authors	Vincent Lefebvre (TAGES), Alejandro Molina, Rodrigo Asensio, Antonio Skarmeta, Noelia Pérez Palma (UMU); Chafika Benzaid, Somayeh Kianpisheh, Amir Javadpour, Tarik Taleb (OULU); Gürkan Gür, Wissem Soussi, Onur Kalinagac (ZHAW); Edgardo Montes de Oca (MI); Pol Alemany, Ricard Vilalta, Raul Muñoz, Charalampos Kalalas, Roshan Sedar (CTTC); Orestis Mavropoulos (CLS), Maria Christopoulou (NCSRD), Chrystel Gaber, Jean-Philippe Wary (Orange); Aleksandra Podlasek (OPL)
Reviewers	Antonio Pastor (TID), Hugo Ramón (TID), Rafal Artych (OPL)
Work package, Task	WP2, T2.4
Keywords	Security Enablement, 5G Security Enablers, ZSM HLA

Abstract

This deliverable reports on an updated description of potential emerging enablers that are relevant to empower fully autonomous smart 5G security management in trustable and liable way. The report specifies the final updated version of the high-level architecture for the security management framework as well as the Security System Model to be delivered by INSPIRE-5Gplus. Additionally, the deliverable further elaborates the automation and closed loop of the infrastructure by introducing an extension of the INSPIRE-5Gplus closed loop model and emphasizing on the Trusted Closed Loop scenarios also deployed by the project demonstrators. Then, through the mentioned demonstrators, the HLA applicability validation performed in previous reports is revisited and evaluated. Finally, the deliverable showcases the impact of the 5G threat landscape monitoring results obtained during the evolution of the corresponding task.

Document revision history

Version	Date	Description of change	List of contributor(s)
v0.1	23/01/22	Table of Content	Noelia Pérez Palma
v0.2	03/03/22	Extended table of content with contributors list	Noelia Pérez Palma
v0.3	06/04/22	Updated ToC	Noelia Pérez Palma
V0.4	28/06/22	First contributions to Section 3	Vincent Lefebvre
v0.5	12/07/22	First contributions to Sections 2 and 5	Edgardo Montes de Oca, Alejandro Molina Zarca, Orestis Mavropoulos, Noelia Pérez Palma
v0.6	31/08/2022	Contribution to chapter 3	Vincent Lefebvre, Jean-Philippe Wary
v0.7	06/09/2022	Polishing of the completed sections	Noelia Pérez Palma
v0.8	13/06/2022	Abstract, Executive summary, Introduction, trusted closed loop	Noelia Pérez Palma
v0.9	19/06/2022	Conclusions	Noelia Pérez Palma
V0.10	22/09/2022	Edition before IR	Noelia Pérez Palma
v0.11	13/10/2022	Add section “Beyond state of the art: closed loop for liability management”	Chrystel Gaber
V0.12	17/10/2022	Final editing	Noelia Pérez Palma
V0.13	20/10/2022	Final editing, version for GA approval	Ellen Tallas
V1.0	31/10/2022	Final editorial check	Uwe Herzog

List of contributing partners, per section

Section number	Short name of partner organisations contributing
Section 1	UMU
Section 2	UMU, CTTC, OULU, MI
Section 3	OULU, MI, OPL
Section 4	OULU, UMU, MI
Section 5	UMU, ORANGE, ZHAW, NCSRD
Section 6	ORANGE, TAGES
Section 7	CLS, UMU, ORANGE, TAGES, OULU, ZHAW
Section 8	UMU

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 provides the final analysis of the security services and enablers already performed in the context of INSPIRE-5Gplus with special focus on the new features and modifications carried out and emphasizing on how these services enhance the foreseen liability and trustworthiness of 5G architecture. In consequence, the evolution of 5G security on the INSPIRE-5Gplus High Level Architecture is further analysed going through each one of the functional blocks and providing a definitive mapping of the proposed services to the corresponding security enablers; the Security Model of the INSPIRE-5Gplus has also been researched in depth; Additionally, a closed loop model extension is illustrated and analysed, paying special attention to the Trust Closed Loop aspects; Automation and Zero touch Management, DLT, Dynamic Liability and Root Cause Analysis are described also as key enablements to operate 5G networks; In a complementary way, AI-empowered Intelligence techniques autonomously operate and defend 5G Systems from potential attacks.

As mentioned, the final set of security services is detailed, their relationship with the identified enablers and more importantly, how this list has evolved in terms of innovative features and updates and how it is currently covered in INSPIRE-5Gplus by the collection of proposed enablers. These services were initially identified by their coverage of security requirements from previous 5G-PPP projects, and the enablers were envisaged within WP3 and WP4, along with their usability and complementarity. Following this methodology and as a closure, this deliverable advises as well on an envisioning picture of more advanced and cutting-edge assets for secure and trustable 5G services.

Considering both the services and the enablers, the evolution of INSPIRE-5Gplus High-Level Architecture is presented alongside its functional blocks and services and the closed-loop model extension. In addition, we elaborate on the validation of such architecture applicability through the proposed project demonstrators. Moreover, a security model of the project framework is described in depth where we discuss the security by design and security by operation processes and at deployment models together with their adoption in INSPIRE-5Gplus.

Additionally, this deliverable presents the description of the aforementioned closed loop model extension, which identifies and specifies the components of the security management framework to be delivered by INSPIRE-5Gplus and defines the interactions between the main components at a macro level. Furthermore, we also dig into a specific Trust Closed Loop Scenario to explore the utilization of novel dynamic and scalable trust management schemes to address the shortcomings of current trust modelling and management approaches.

Finally, an analysis of the impact of the 5G threat landscape is also performed identifying how the principal emerging enablers could be susceptible to attacks due to the increase of the surface to be protected, ensuring their robustness to possible threats and providing mechanisms to improve their trustworthiness. In the same line, emerging 5G/6G threats and security challenges that could be introduced unintentionally by the described enablers and the potential technologies adopted are explored, paying special attention to Artificial Intelligence, Molecular communication, Quantum communication, Blockchain, TeraHertz technology, and Visible Light Communication. We conclude this contribution providing a wrap up analysis about the Impact of this project on the aforementioned emerging threat landscape.

The content of this deliverable includes:

- The analysis and updated descriptions of the resulting services and enablers associated to the enablements defined in previous project phases.
- Outlines an elaborated list of security services and their mapping with the existing enablers.
- Evolves the High-Level Architecture proposed by INSPIRE-5Gplus and describes it in detail.
- Defines a Security Model for the INSPIRE-5Gplus.
- Describes a Closed Loop Model extension and explores the enforcement of liability and trustworthiness among the involved elements of the architecture by showcasing a Trust Closed

Loop scenario.

- Provides an analysis of the impact of the 5G threat landscape monitoring results.

The work that has been carried out in the scope of WP2 during the whole INSPIRE-5Gplus project, covering the identified enabling technologies and the evolution of the High-Level Architecture leveraging on such technologies with a set of Illustrative use cases to validate the potential of the proposal as a collaborative work of the partners involved, serving as the validation to the development of INSPIRE-5Gplus enablers.

Table of Contents

List of Figures

List of Tables

Abbreviations

5GC	5G Core
AMF	Access control and Mobility Management Function
ASP	Attack Success Probability
AUSF	Authentication Server Function
CU	Central Unit
DLT	Distributed Ledger Technology
DU	Distribute Unit
DVB	Digital Video Broadcast
E2E	End-To-End
EC	European Commission
eCPRI	evolved Common Public Radio Interface
eMBB	Enhanced Mobile Broadband
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
E2E SMD	End to End Security Management Domain
FOSS	Free and Open-Source Software
GAN	Generative Adversarial Network
GDPR	General Data Privacy Regulation
gNB	Next Generation Node B
HOA	Higher Order Ambisonics
JSON	JavaScript Object Notation
mMTC	massive Machine Type Communications
KVM	kernel-Virtual Machines
MANO	Management and Network Orchestration
MEC	Multi-Access Edge Cloud
mMTC	massive Machine Type Communications
MSPL-OP	Medium-level Security Policy Language Orchestration Policy
NF	Network Function
NFV	Network Function Virtualisation
NR	New Radio
NRF	Network Function Repository Function
NS	Network Service
NSA	Non-stand Alone
NSSF	Network Slice Selection function

OS	Operating System
PCF	Policy Control Function
PNF	Physical Network Function
REST	Representational State Transfer
RRU	Remote Radio Unit
SA	Stand Alone
SBA	Service-Based Architecture
SDN	Software Defined Networking
SMD	Security Management Domain
SSLA	Security Service Level Agreement
TCB	Trusted Computing Basis
TSLA	Trust Security Service Level Agreement
UDM	Unified Data Management
UPF	User Plane Function
URLLC	Ultra-Reliable and Low Latency Communications
ZSM	Zero-touch network and Service Management

1 Introduction

1.1 Scope

This report aims at providing the updated list of Enablers, Mechanisms and Services for liability-aware trustable smart 5G security. This deliverable revisits the set of architecture level requirements to provide liability-aware trustable and smart 5G security based on a set of emerging enabling technologies. The deliverable also provides a final list of services and their relationship with the emerging enabling technologies and enablers to finally depict the evolution of the proposed INSPIRE-5Gplus High Level Architecture. The present deliverable addresses, as well, the proposed Security Model and brings an extension of the previously introduced Closed Loop Scenarios.

1.2 Terminology

- **Security Asset**

A security asset is any component that supports security related activities (protection, detection and/or mitigation). It can correspond to hardware, software or virtualised functions.

- **Security Enabler**

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

- **Security Enablement**

Security Enablements are defined as new initiatives and technologies/techniques possessing the potential to significantly contribute to 5G security evolution (e.g., AI techniques, Distributed Ledger Technology (DLT), Automation and Zero Touch management, etc.). An enablement is therefore the technology and abstraction on which Security Enablers are based. The enablements, unlike enablers, are not limited by actual technology or the scope of the project. They are thought to be the building blocks on which present and future enablers can be categorized. One security Enabler can rely on multiple Security Enablements.

- **Security Management & Orchestration Functions**

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

1.3 Target audience

The target audience of this deliverable are stakeholders related to security of 5G technologies and infrastructure. The deliverable describes technical terms and technologies that are used to increase the security posture of 5G systems and use cases.

1.4 Structure

The main structure of this deliverable is summarized as follows:

- Section 2 updates the proposed High-Level Architecture (HLA) relying on the architectural level requirements and describes the last developments related to the emerging enabling technologies based on which a liability-aware trustable and smart 5G security solution is based.
- Section 3 addresses the mapping of the emerging enabling technologies to the corresponding security services.
- Section 4 presents the project's Closed Loop Model extension, going through the Trust Closed Loop scenarios deployed at each project demonstrator.
- Section 5 revisits the HLA applicability validation performed previously through the mentioned demonstrators providing a closure for the proposed test cases.
- Section 6 describes the Security System Model of INSPIRE-5Gplus Framework.
- Section 7 elaborates on the impact of the 5G threat landscape monitoring results.
- Section 8 concludes this deliverable.

2 INSPIRE-5Gplus High Level Architecture

In this section we describe the High-Level Architecture (HLA) functional blocks and services that are relevant to empower fully autonomous smart 5G security management in a trustable and liable way. It is important to note that, this section emphasizes on the updates made since the initial HLA version described in D2.2 [27], providing details on newly added services and/or service capabilities. Services that have been removed or renamed are also detailed in this section with its corresponding description of their current status.

With a view to reach the desired architecture described in previous project phases; an exhaustive methodology has been pursued with a special effort for mapping the envisioned services to the corresponding infrastructure enablers provided by the project contributors. In such way, the procedure of mapping started by classifying the enablers that were actually offering the foreseen services, describing at the same time whether any of such services presented new features given the progress of the project. Once this first step was accomplished, we also worked on identifying new potential services derived from the enablers' development stage. Finally, after analysing all services a small group were determined to be removed since their functionality was not imperative or it was already covered by alternative means. In Figure 1, the updated version of the HLA is presented, for both E2E and SMD domains. The specific mapping of the INSPIRE-5Gplus services and enablers explained above is also outlined in Table 16).

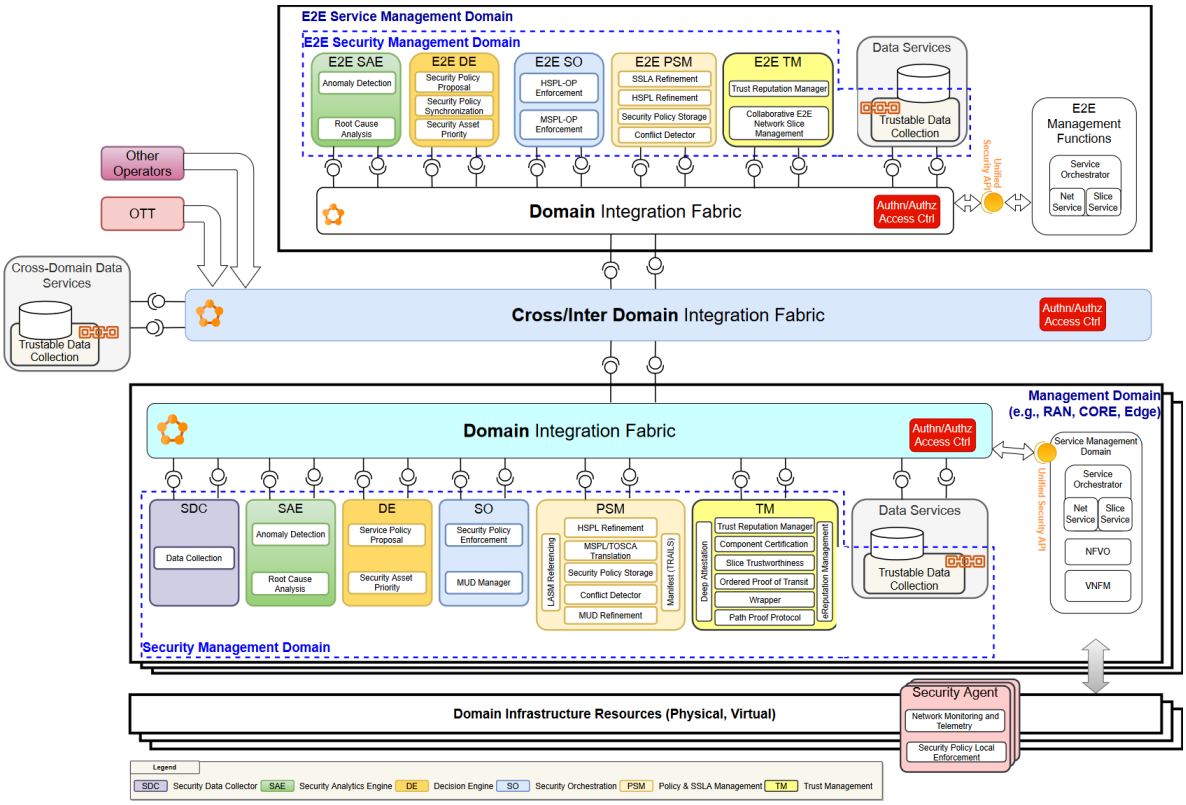

Figure 1 - INSPIRE-5Gplus High-Level Architecture - Final Version.

2.1 HLA's Functional Blocks Description

2.1.1 Security Data Collector

2.1.1.1 Function

The main function of the Security Data Collector (SDC) is to gather all the data coming from the security enablers at the domain level, in particular the security agents. This data will be used by the security management functions (e.g., Security Analytics Engine) for the detection of anomalies and security breaches. It includes datasets and meta-data for different analytics functions such as real-time detection and forensics analysis. The types of data collected by the SDC may include:

- Performance monitoring data (e.g., counters and statics data).
- Security monitoring datasets (e.g., traffic meta-data, packet capture, session data).
- Event/alarm data (e.g., system logs, application traces, system traces).
- Machine learning reference data sets for learning and prediction phases.
- External data (e.g., Cyber Threat Intelligence, external open source or shared data sets).

2.1.1.2 Provided Services

Table 1 - Services provided by Security Data Collection Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Data Collection Service	This service sets up and launches the mechanisms for collecting data from the different security agents, security enablers and network devices.	Data translation	External/Internal	Security Analytics Engine Policy & SSLA Management
		Data fusion/aggregation		
		Data extraction or filtering		
		Data temporal persistence and transaction		
		Data capture		

2.1.2 Security Analytics Engine

2.1.2.1 Function

The main function of the Security Analytics Engine (SAE) is to derive insights and predictions on a domain's security conditions based on data collected in that specific domain or even from other domains. In the context of INSPIRE-5Gplus, the SAE provides Anomaly Detection and Root Cause Analysis (RCA) services. The Anomaly Detection service has the capabilities of detecting and/or predicting anomalous behaviour due to malicious or accidental actions by identifying patterns in data or behaviour that do not conform to the expected normal behaviour. It leverages data aggregated by the SDC from the managed entities of the domain, including performance and security monitoring data, events and alarms, generated by system logs and packet traces. The RCA service identifies the cause of the observed security incidents by analysing and correlating data from other services (e.g. Anomaly Detection service). The Root Cause determines the origin of the anomaly and the location in the network where a corrective action should be applied to prevent the problem from occurring. As a result, the RCA service may provide the information needed by other security functions to determine

the actions that should be triggered to correct or prevent the security incidents in the 5G networking environment.

The techniques for the detection of anomalies and root causes include ML/AI, feature extraction, Complex Event Processing, Deep Packet Inspection, Change Point Analysis and more. They can be applied and have been applied in INSPIRE-5Gplus's technical WP3 and WP4, in many different use cases. These are, for instance, the detection of DDoS, the analysis of encrypted network traffic, the detection of V2X misbehaviour, anti-GPS spoofing, assessment of encrypted channel protection, security SSLA assessment, and RCA in Industrial Campuses. The SAE is an essential component providing the information needed by the Decision Engine, Orchestrator, Moving Target Defence, etc. for the prevention, mitigation and reaction to cyber-attacks.

2.1.2.2 Provided Services

The two main functions provided by the SAE are Anomaly Detection and Root Cause identification.

Table 2 - Services Provided by Security Analytics Engine Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Anomaly Detection Service	This service has the capabilities of detecting and/or predicting anomalous behaviours due to malicious or unintentional actions.	ML-based behaviour analysis Publish results to subscribers Notify consumers of detected anomalies	External/Internal	Domain Decision Engine Domain Data Services Operators
Root Cause Analysis Service	This service identifies the cause of the observed security incidents by analysing and correlating data from other services (e.g., Anomaly Detection Service) and learning from past experience.	ML-based cause analysis Publish results to subscribers Notify consumers of probable causes of security incidents	External/Internal	Domain Decision Engine Domain Data Services Operators

2.1.3 Decision Engine

2.1.3.1 Function

The Decision Engine (DE) manages the security mitigation using the possible security reactions in the scope of a SMD. It fits between the events and notifications emitters, as for example the Security Analytics Engine (SAE), and the security enforcers, such as the Security Orchestrator (SO). These respective communications take place through the integration fabric for decoupling each component with their deployment details. The DE can initiate the security mitigation in proactive or reactive fashion. In the scope of the INSPIRE-5Gplus project, the DE focuses on the reactive part. The possible reactions are orders understandable by the Security Orchestrator and stretch from network reactions, such as filtering a device, to services reactions, like the redeployment of a virtual network security function (VSF). The DE also has a link with the E2E DE to share state or mitigation taken in a SMD or

receive orders from the global oversee.

2.1.3.2 Provided Services

Table 3 - Services provided by Decision Engine Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Service Policy Proposal Service	This service creates and proposes security mitigation for enforcement in a local SMD	Creation, Update, Deletion, Trigger a reaction	Internal/External	Security Analytic Engine
Security Asset Priority Service	This service manages the associated priority of reactions raised during conflict and concurrent mitigations in a local SMD	Update reaction priority	Internal/External	Operator, SMD & E2E Decision Engine

2.1.4 Security Orchestrator

2.1.4.1 Function

The Security Orchestrator (SO) functions provided in deliverable D2.2 [27] have been extended to orchestrate and enforce the new 5G security slice policies. This is, apart from regular security policies orchestration and enforcement, 5G security slice policies can be orchestrated and enforced. To this aim, new features like multiple orchestration and allocation algorithms are provided. In fact, Trust-based 5G security slice orchestration and allocation has been provided as orchestration algorithm for 5G slices. As it also drives the security management by interacting through the integration fabric with different MANOs and Controllers, Slice MANO interactions are also provided as new feature. As part of the evolved functionalities, proactive/reactive policies enforcement contemplates deployment / configuration of 5G slices as well as the dynamic configuration of each 5G service/security asset/enabler that compose the slice. The SO feeds data services with enforcement results, and it is also fed from data services to retrieve infrastructure information used during orchestration and allocation processes.

2.1.4.2 Provided Services

Table 4 - Services Provided by Security Orchestrator Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Security Policy Enforcement Service	This service allows requesting policies enforcement (including 5G security slice policies) in management domain.	Create/Delete security policy	Internal/External	Decision Engine E2E Security Orchestrator
MUD manager service	This service enables the management of the MUD within the system when a new device is connected to	Enforce/Retrieve MUD	Internal/External	Decision Engine

	it, performing the retrieving of the MUD file with control and deploying related policy within the system.			

2.1.5 Policy and SSLA Management

2.1.5.1 Function

Policy and SSLA Management functions defined in D2.2 [27] have been improved with new features. New 5G security slice policy model has been defined, as well as new policy capabilities such as Proof of Transit or Secured Service MANO. New translation functionalities have been also provided to translate new security policies to different enablers/assets configurations.

2.1.5.2 Provided Services

Table 5 - Services Provided by Policy and SSLA Management Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
MSPL/TOSCA Refinement Service	This service refines MSPL policies into precise configurations, API calls, specific low-level configurations needed to interact with the enablers. It could also translate MSPL to TOSCA to be compatible with some orchestrators (e.g., OSM, ONAP) that support TOSCA.	Convert	Internal	Security Orchestrator
Security Policy Storage Service	This service stores policies enforced by other domain entities to keep track of them. It could be implemented using DLT to assure liability.	Store	Internal	Decision Engine Security Orchestrator
Conflict Detector	This service performs the conflict detection at the SMD level	Integrity Check	Internal	Decision Engine Security Orchestrator
MUD refinement service	This service is in charge of performing the translation from the MUD file to MSPL-OP.			Security Orchestrator
LASM Referencing Service	When a new component is added, this service retrieves data from the Manifest, also called TRAILS, and stores them in an ontology	Convert & Verification /	Internal	Security Orchestrator Decision Engine Security Analytics Engine
Manifest	This descriptor contains			NA

(TRAILS)	SSLA.			
HSPL Refinement Service	This service refines HSPL (High-level Security Policy Language) policies into MSPL (Medium-level Security Policy Language) policies.	Convert	Internal	Security Orchestrator

2.1.6 Trust Management

2.1.6.1 Function

The Trust Management (TM) contains various internal services for the trust related functions in the INSPIRE-5Gplus security framework. Some updates have been carried out since the last versions of the services provided by this block. In the following table the mentioned improvements are detailed.

2.1.6.2 Provided Services

Table 6 - Services Provided by Trust Management Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Trust Reputation Manager	Main updates have been implemented for the algorithm that performs the trust score computation to improve the received data processing and the accuracy in terms of output delivered to the corresponding management entities.	Computes trust and reputation values of the monitored 5G entities and delivers this information to the corresponding security management entities and end users when requested.	Internal/ external	Security Orchestrator
Component Certification Service	This service works at the component level and provides a static evaluation of different 5G network components by measuring trust metrics.	Certificate components using trust metrics	Internal/ external	Security Orchestrator
Slice Trustworthiness Service	As defined in D2.2, this service ingests slice-related data (static and dynamic properties) and scores the slice, based on parameters that can be used by the end-users or other system components. Due to its low TRL, this element has not been evolved since D2.2.	Compute slice trust score	Internal/ external	Security Orchestrator
Ordered Proof of Transit Service	This service verifies the correct order of nodes on the network path followed by a flow. It provides trust	Compute network path verification	Internal	Security Orchestrator

	in the guaranteed confinement of flows in a specific slice or slices, or for inter-domain trust.			
eReputation-Management	This service computes some components reputation (assimilable to some Trust level) metrics over a VNF infrastructure	Calculation of Trust	Internal	Security Orchestrator and SAE (for RCA services)
Wrapper Service	Systemic wrapper hardens executable files (programs and library functions) against confidentiality, integrity. In the scope of the project, aside the progress made on security (e.g., automatic leverage of TEE), Systemic offered services expand from the hardening (i.e., security) to deep monitoring. The collective research work has resulted in the significant expansion of the services tailored for inter-connected telecom software permitting a centralized deep run-time monitoring. One can also depict the progress made as deriving a stand-alone and static security offer to a fully dynamic solution, integrated in the orchestration.	Elaboration of novel and disruptive deep monitoring services conferring a deep and continuous monitoring of deployed instances at runtime, with monitored security properties, able to change telecom software security landscape.	Internal/ External	Security Orchestrator
Path Proof Protocol	This service allows to prevent deviating the traffic on a given route (hijacking attacks). The PPP enabler addresses the issue application-layer approach) thank to a two-party cryptographic-based anomaly detection protocol.	It measures the communication time between users and performs statistical analysis upon these measurements and a trusted sample.	internal	"Decision Engine" and the Security Management Domain".
Deep Attestation Service	This service could be deployed as a resident service for each virtualized infrastructure. It allows to collect evidence of security properties (thank to cryptography)	As long as the infrastructure or Domain owner is in capacity to deliver way to evaluate a specific technical property, the DeepAttestation	internal / external	"Decision Engine" and "Security Analytic Engine"

		service will be in capacity to deliver evidence of the right measurement over the right component.		

2.1.7 E2E Security Analytics Engine

2.1.7.1 Function

The E2E Security Analytics Engine (E2E SAE) derives cross-domain insights and predictions based on data collected from different domains. It has a role similar to the SAE but at the cross-domain level. This function is necessary for analysing the data provided by the SDCs from different domains or stored in the Cross-Domain Data Service to detect any anomalies that can only be detected using information from more than one domain (e.g., SIEM-type analysis that correlates events captured in logs) or to make the detections more effective and precise (e.g., reduce the number of false positives and improve the number of detected incidents). It generates notifications that will be used by E2E Decision Engine to trigger the necessary remediation or prevention procedures.

The SAE is a generic service that integrates many different techniques that can be applied for the detection of attacks and the identification of their causes at the domain level, but also at the cross-domain level.

2.1.7.2 Provided Services

As for the domain level SAE, the E2E SAE has two main functions: Anomaly Detection and Root Cause Analysis.

Table 7 - Services Provided by E2E Security Analytics Engine Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Anomaly Detection Service	This service analyses the data provided by the different domain SDCs or stored in the E2E Data Service to detect anomalies that can only be detected using information from more than one domain. Similar to a SIEM (Security Information Management System).	Complex event processing ML-based analysis Policy compliance analysis	External	E2E Decision Engine
Root Cause Analysis	Similar to the RCA service defined in DE but operates at E2E level to identify cascading effects between different domains.	ML-based cause analysis Publish results to subscribers Notify consumers of probable causes of security incidents	External/Internal	E2E Decision Engine E2E Data Services Operators

2.1.8 E2E Decision Engine

The E2E Decision Engine (E2E DE) is first, the augmented SMD Decision Engine and shares the same features. In some deployments, services may be deployed at the E2E level which dictates a local mitigation loop. Second, the E2E DE gathers notifications from the underlying SMD domains and manages the overall mitigations. Those mitigations are enacted by the E2E Security Orchestrator. Using this holistic point of view, the E2E DE can select and propagate escalated reactions from a targeted domains to all other domains.

2.1.8.1 Function

2.1.8.2 Provided Services

Table 8 - Services Provided by E2E Decision Engine Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Security Policy Proposal service	This service creates and proposes security mitigation for enforcement at the E2E level and all SMDs.	Creation, Update, Deletion, Trigger a reaction	Internal/External	E2E Security Analytic Engine
Security Asset Priority Service	This service manages the associated priority of reactions raised during conflict and concurrent mitigations at the E2E level	Update reaction priority	Internal/External	Operator, E2E Decision Engine
Security Policy Synchronization Service	This service allow the SMD DEs to escalate reactions and to receive new reactions manifest from the E2E DE	Reaction's escalation, reaction management from in primary/secondary context.	Internal/External	SMD Decision Engine

2.1.9 E2E Security Orchestrator

2.1.9.1 Function

The E2E Security Orchestrator (E2E SO) has been extended from deliverable D2.2 [27] to support 5G E2E security slices orchestration by defining a new orchestration algorithm that contemplates the requirement of deploying different sub-slices in each involved domain in order to fulfil the functionality specified by the E2E slice which is received as MSPL-OP.

Future directions, taking into account the last development in WP4, consists in integrating an optimal placement algorithm into the E2E SO. The developed algorithm relies on an exact solving of the E2E chains of micro-services placement problem. This problem is formulated as an integer programming formulation that allows to model exactly the isolation and latency requirements as constraints, with the objective to minimize the resources usage. Optimal solutions offer the guarantee that isolation and security level requirements will never be violated, even in case of scarce physical resources.

2.1.9.2 Provided Services

Table 9 - Services provided by E2E Security Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
MSPL-OP Enforcement Service	This service enforces and controls MSPL-OP cross-domain through interaction with SOs at domain level. Capable of enforcing 5G Security Slices	Create, 5G-Security-Slice	Internal/External	E2E Decision Engine SSLA Manager
HSPL-OP Enforcement Service	This service enforces and controls HSPL-OP cross-domain through interaction with SOs at domain level.	Create	Internal/External	Other Operators

2.1.10 E2E Policy and SSLA Management

2.1.10.1 Function

The E2E policy and SSLA management (E2E PSM) block has been extended from deliverable D2.2 [27], the slicing support have been extended at E2E policy operations thus providing conflict & dependency detection of the different sub-slices at E2E level and storing the different policies related to tenant & slice identifiers.

2.1.10.2 Provided Services

Table 10 - Services provided by E2E Policy and SSLA Management Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
HSPL Refinement Service	This service refines HSPL policies into HSPL policies intended for the domains	Convert	External	E2E SO

	underneath or MSPL policies.			
Security Policy Storage Service	This service stores policies enforced by other domain entities and relates them to specific tenant & slice to keep track of them. It could be implemented using DTL to assure liability.	Store	Internal	E2E Decision Engine E2E Security Orchestrator
Conflict Detector	This service performs the conflict detection at the E2E level considering the e2e slice capabilities and its different sub-slices.	Integrity Check	Internal	E2E Security Orchestrator E2E Decision Engine
Security SLA Refinement Service	This service refines SSLAs into HSPL/MSPL-OP policies for orchestration.	Convert	External	User/System operator Other ISPs

2.1.11 E2E Trust Management

2.1.11.1 Function

The E2E Trust Management (E2E TM) facilitates E2E trust services across multiple domains, relying on the domain-resident TMs. It has been improved to compute, based on information aggregation and domain's TRM outputs, final trust scores of the involved domains. Additionally, allowing any security management entity to request the needed cross-domain trust scores. For instance, the trust score of a given domain can be requested by E2E SO to operate in compliance with E2E security requirements, policies and SSLAs.

2.1.11.2 Provided Services

Table 11 - Services provided by E2E Trust Management Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Trust Reputation Manager Service	This service has been envisioned to compute the resulting trust score of a given domain based not only on the output of the TRMs at domain level but also including information about previous versions.	Data aggregator Calculation of trust	Internal	TRM Security Orchestrator
Collaborative E2E Network Slice Management	This service aims to allow a cooperative and collaborative management of Network Slices with the use of Blockchain	Control and management of trust network slicing	External	E2E Management Function (Network Slice Managers)

	technology.	resources.		

2.1.12 Domain-Level and Cross-Domain Data Services

2.1.12.1 Function

Apart from the functionality described in D2.2 [27], Data Services are extended to support the orchestration process, including the 5GSlice orchestration processes. The design of the system model has been extended to consider new assets, enablers as well as domain info capabilities. Data services provides the enablers the required information to perform their procedures properly, such as entry points of the security management domains.

Figure 2 shows the Data Services architecture used to model the information required by the system to perform operations, the main entities are:

- **Slice**: Main entity used to represent slice information, which is distinguished by its unique ID.
- **Orchestration Policy**: Identifiers of the orchestration policies associated to a specific slice.
    - **Policy**: identifier of the policies belonging to an orchestration policy, every orchestration policy is at least composed of one policy, but it can contain several policies belonging to different domains.
- **Connection**: represent the information of the connection of specific slice such as the status, if it is managed or if it is virtual.
- **Tenant**: tenant to which the slice belongs. Each tenant can have multiple slices.
- **Device**: device which will host software and it is located in certain domain. Each slice can be composed of several devices to deploy all the capabilities needed.
    - **Device group**: group of devices gathered by logical use (e.g. group of devices used to perform certain capability or selected by a slice)
    - **Phy device**: represent if device is virtual or physical.
    - **Flavor**: hardware capabilities of the image that the device will host. The same flavour could be load in several devices, but one device can only have one single flavour.
    - **V instance**: virtual instance identifier of the device.
    - **Location**: place where the device is located, it is specified as a unambiguous physical and/or virtual location.
- **Policy Translation**: identifier of the translation procedure that relates a policy with its final configuration translation.
- **Network interface**: Identifier of the NIC used by the device to stablish a connection, it can be specified if it is virtual or physical and the port to which is connected among other attributes.
    - **Flow**: information of the IP connection on specific NIC such as source port, source address, destination port and destination address.
    - **Network Interface Info**: information related to the NIC used for a connection such us address, if it is virtual, mac, etc.
    - **SixLoWPANInterface**: information about if the interface belongs to SixLoWPAN tech.
- **Software Instance**: identifier of the instance deployed in a device of a software type.
    - **Software**: information about the software instance.
    - **Configuration**: configuration carried on specific policy to be deployed on specific software to make an enabler perform certain required capability.
    - **Credentials**: to access and configure specific software.
    - **API**: information of API available on specific software.
- **Enabler**: represent an enabler of the system, where an enabler is a software that can be configured and perform certain capabilities.
    - **Domain**: domain in which a device can be deployed. Each domain has a group of enablers that represent the number of capabilities that can be enforced in that domain.

- **Capability**: identifies the different capabilities that a device can perform.

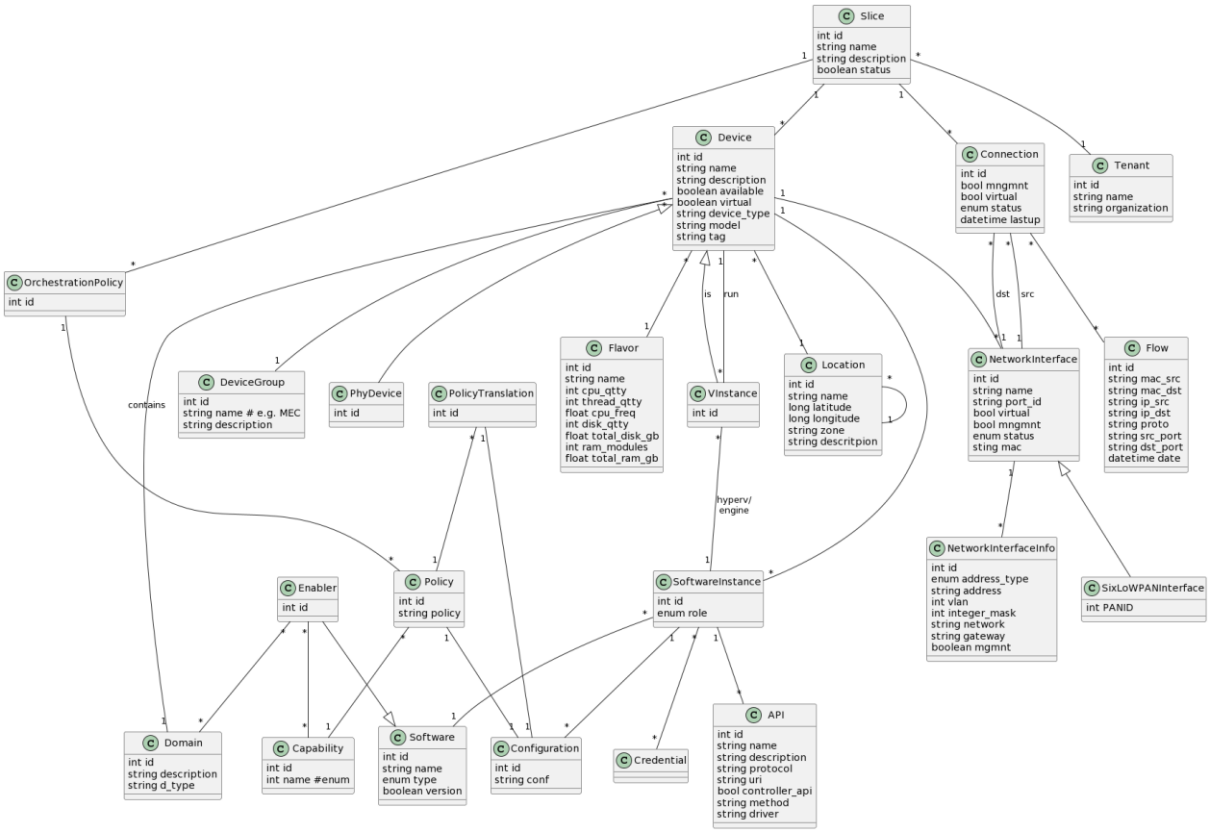

Figure 2 - Data Services architecture

2.1.12.2 Provided Services

Table 12 - Services provided by Domain-Level and Cross- Domain Data Services Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Data Access Service	It allows retrieving, update, remove different kind of information about current status of the infrastructure from data services.	Access control, data persistence, data life cycle, data security policy management	Internal / External	All

2.1.13 Integration Fabric

2.1.13.1 Function

Integration Fabric is designed to enable the intra and inter SMD communication, it also performs registration and discovery services among other intra/inter management functionalities. In addition, Integration Fabric has been designed to perform communication-related security features in a service mesh.

The ZSM approach relies on the use of integration fabrics. These fabrics provide communication and security capabilities between and within the SMDs as well as other service management features such as registration, discovery that needs to be performed inter/intra-domain. For instance, it allows access

to data services, but it is also able to ensure certain security properties in the fabric communications. This is, Integration fabric provides not only communication capabilities in different ways but also other interesting security and management features in a service mesh like authorisation/access control.

2.1.13.2 Provided Services

Table 13 - Services provided by Integration Fabric Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Management services registration service	The implementation allows register services, even if they are outside of the service mesh.	Services Registration	External/ Internal	All
Management services discovery service	As part of the implementation of the integration fabric, Istio provides service discovery capabilities	Service Discovery	External/ Internal	All
Management communication service	The implementation allows communicating services in different ways such as, REST APIs, custom flows or messaging queues. Security properties can be also applied to these communications	Service Communication	External/ Internal	All
Management service invocation routing service	Current implementation allows services invocation through services routing. Besides, security properties can be applied dynamically for the services invocation such as traffic shifting, circuit breaking, mirroring or load balancing among others	Service Invocation	External/ Internal	All

2.1.14 Security Agent

2.1.14.1 Function

The Security Agent (SA) is a security asset for monitoring and managing security at a local or external observation point (e.g., network interfaces of electronic circuit cards or virtual machines, switch port mirroring - SPAN, Test, Terminal, or Traffic Access Point - TAP). It is able to capture data needed by other security functions and/or perform actionable behaviour decided locally but managed by other security functions (e.g., security orchestrators). The SAs communicate with the INSPIRE-5Gplus management plane in their security domain based on configurable security policies. An SA may provide security data to the analysis and management functions from the traffic plane, acting for instance as an active or passive probe.

Preconfigured data for initial configuration is assumed to be injected or loaded at SA instantiation (e.g., by the NFV-MANO). An API for runtime configuration could also be available (e.g., NETCONF, REST). The SA's main function is to provide interoperability between the INSPIRE-5Gplus management plane and the security enablers in the **data and control planes** in an active or passive mode. Security enablers

can vary in typology and nature. In some domains, they can be dedicated security network probes. In others, they can be existing VNFs or PNF with security capacity. In all cases, it is expected that the SA function helps translating security policies (e.g., MSPL) to specific or proprietary enabler configuration formats and collects the data required from the network to perform security analyses. This component will expand the interoperability between different vendors and solutions in the 5G domains.

2.1.14.2 Provided Services

Table 14 - Services provided by Security Agent Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Security Policy Local Enforcement Service	This service receives a security rule, SSLA or security policy (e.g., MSPL) in a standard format and translates it to the security enablers' associated formats to be able to apply it (i.e., act as an active probe).	Translate security policy Enforce security policy	Internal	Decision Engine (DE) Security Orchestrator (SO)
Network Monitoring and Telemetry Service	This service is in charge of generating on-demand data (logs, alerts, network telemetry, network datasets, statistics, trends). Acting as passive or active probe.	Generate data	Internal	Security Analytics Engine (SAE) Security Data Collector (SDC)

2.1.15 Unified Security API

2.1.15.1 Function

The Unified Security API was defined to be the set of commands/rules that allow the exchange of information between the Management Functions elements (e.g., Network Slices, Network Service) and the multiple components within the HLA, especially with the Security Orchestrator.

This API allows interactions in both directions “from and to” the HLA and the Management Functions elements. It should be deployed in both the E2E and the multiple management domains but the multiple commands themselves should differentiate between E2E and lower domains.

Since its first description, the Unified Security API has not had a significant revolution as it is a list of calls to request different actions to the HLA modules based on the REST model.

2.1.15.2 Provided Services

The Unified Security API is focused on offering one single service, which has been called as “Network Service Actions”. More details in the table below:

Table 15 - Services provided by Unified Security API Module

Service	Service Update	Service Capabilities	Service Visibility	Potential Consumers
Network	This API defines the format/structure	Services/Network deployment, re-	Internal	INSPIRE-5Gplus modules (essentially the Security

Service Actions	(i.e., syntax and semantics) of the requests or list of requests from the INSPIRE-5Gplus framework asking a Service Orchestrator to perform certain actions.	configuration and termination actions (e.g., Channel Protection, Monitoring, Network slicing).		Orchestrator) Different services managers (e.g., Network Slice Managers and Service Orchestrators)

3 INSPIRE-5Gplus HLA services and enablers mapping

This section elaborates on the coverage of the HLA functionalities by the security and trust enablers developed in WP3 and WP4, respectively. Table 16 illustrates the mapping between WP3/WP4 enablers and the services provided by the different functional blocks of INSPIRE-5Gplus HLA. In addition to WP3/WP4 enablers, we also listed a set of assets that have been used in INSPIRE-5Gplus but developed in other projects. The integration of those assets was possible thanks to the service-based design principle adopted by INSPIRE-5Gplus HLA. For sake of clarity, WP3/WP4 enablers and used assets are referenced by their enabler ID; the full names of the enablers and assets can be found in Table 17.

It is worth mentioning that the aim here is to provide a comprehensive summary of how the services of the INSPIRE-5Gplus functional architecture are covered and implemented by WP3/WP4. For more details on WP3/WP4 enablers and the mechanisms and enabling technologies they are using to implement INSPIRE-5Gplus HLA functionalities, we invite the reader to refer to WP3/WP4 deliverables, particularly D3.4 [24] and D4.4 [25].

Table 16 demonstrates that WP3/WP4 enablers achieved a full coverage of the INSPIRE-5Gplus HLA, providing the capabilities to implement one or several of the identified HLA's services. It is worth noting that while the enablers covering the anomaly detection and root cause analysis functionalities at the domain level are theoretically able to provide those services at the E2E domain level, we did not map them as no practical tests have been performed so far to corroborate their efficiency in an E2E scenario.

Table 16 - Mapping between WP3/4 Enablers and INSPIRE-5Gplus HLA Functionalities

Functional Block	Service of the Functional Block	INSPIRE-5Gplus Enablers
Security Data Collector (SDC)	Data Collection Service	WP3-01, WP3-02, WP3-03, WP3-04, Asset01
Security Analytics Engine (SAE)	Anomaly Detection Service	WP3-01, WP3-02, WP3-03, WP3-05, WP3-06, WP3-07, WP3-08, WP3-09, WP3-20, WP4-01
	Root Cause Analysis Service	WP4-01, WP4-02, WP4-03
Decision Engine (DE)	Security Policy Proposal Service	WP3-01, WP3-02, WP3-03, WP3-10, WP3-11
	Security Asset Priority Service	WP3-11
Security Orchestrator (SO)	Security Policy Enforcement Service	WP3-12, WP3-13, WP3-14, WP4-04
	MUD manager service	WP4-14
Policy and SSLA Management (PSM)	HSPL Refinement Service	WP4-05
	MSPL/TOSCA Refinement Service	WP3-15
	Security Policy Storage Service	WP3-15
	Policy Conflict Detection Service	WP3-15, WP3-17
	SSLA Storage Service	WP3-16
	MUD refinement service	WP4-14
Trust Management (TM)	Trust Reputation Manager	WP4-06, WP4-07

	Component Certification Service	WP4-08
	Slice Trustworthiness Service	WP4-09
	Ordered Proof of Transit Service	WP4-10
	Wrapper Service	WP4-11
	Path Proof Protocol	WP4-12
	Deep Attestation Service	WP4-13
E2E Security Analytics Engine (E2E SAE)	Anomaly Detection Service	
	Root Cause Analysis Service	
E2E Decision Engine (E2E DE)	Security Policy Synchronization Service	WP3-11
	Security Policy Proposal service	WP3-10
	Security Asset Priority Service	WP3-11
E2E Security Orchestrator (E2E SO)	Security Policy Enforcement Service	WP3-12
	Security MTD Policy Enforcement Service	WP3-14
E2E Policy and SSLA Management (E2E PSM)	Security SLA Refinement Service	WP3-23
	HSPL Refinement Service	WP3-15
	Policy Conflict Detection Service	WP3-15
	Security Policy Storage Service	WP3-15
E2E Trust Management (E2E TM)	Trust Reputation Manager Service	WP4-06
	Collaborative E2E Network Slice Management	WP4-09
Domain-Level & Cross-Domain Data Services	Data Access Service	WP3-18
Integration Fabric (IF)	Registration Service	WP3-19
	Discovery Service	WP3-19
	Invocation Service	WP3-19
	Communication service	WP3-19
Security Agent (SA)	Network Monitoring and Telemetry Service	WP3-20, WP3-21
	Enforcement Point Service	WP3-22, WP3-27, WP3-28 WP4-14, Asset02, Asset03, Asset04
Unified Security API	Network Service Actions List	INSPIRE-5Gplus enablers can interface with different tools, such as Kubernetes, OpenStack, and OSM.
	Network Slicing Management	WP3-23, WP3-24

Service Management Domain (SMD)	Network Digital Twin	WP3-26
E2E Service Management Domain (E2E SMD)	Network Slice Brokering	WP3-25

Table 17 - List of WP3/4 enablers and other assets developed/used in INSPIRE-5Gplus

WP3/WP4 Enablers	Enabler ID
DDoS Detection & Mitigation in Network Slicing (DDoS Mitigator)	WP3-01
DDoS Detection & Mitigation in Network Slicing (DDoS Detector)	WP3-02
Lightweight and Space-efficient Authentication with Misbehavior Detection	WP3-03
Data Collector	WP3-04
Multi-domain, multi-tenant AI-based DoS Detection	WP3-05
SSLA Assessment and Enforcement	WP3-06
MMT - Advanced Traffic Analysis in 5G Planes	WP3-07
Security Analytics Framework	WP3-08
UAV Anti GPS Spoofing	WP3-09
OptSFC	WP3-10
PyrDE - Decision Engine	WP3-11
Security orchestrator	WP3-12
I2NSF IPSEC	WP3-13
MOTDEC - Moving Target Defense Controller	WP3-14
Policy Framework	WP3-15
SSLA Manager	WP3-16
Threat assessment. DiscØvery	WP3-17
Data Services	WP3-18
Integration Fabric	WP3-19
Smart Traffic Analysis	WP3-20
MMT - Probe	WP3-21
Virtual Channel Protection	WP3-22
Secured Network Slice Manager for SSLAs	WP3-23
Katana Slice Manager	WP3-24
SFSBroker	WP3-25
Dataset generation based on Network Range-Digital twin (MOUSEWORLD)	WP3-26
Security Agent - 5G Core & Radio Agent	WP3-27
Security by Orchestration for MEC	WP3-28
GRALAF	WP4-01
RCA: Root Cause Analysis	WP4-02
Root Cause Analysis for VNF	WP4-03
LASM: Liability-aware Security Manager	WP4-04
MANIFEST	WP4-05
TRM - Trust Reputation Manager	WP4-06
eTRM: e-Trust Reputation Management	WP4-07

CCT - Component Certification Tool	WP4-08
Trusted Blockchain-based Network Slices	WP4-09
POT: Proof of Transit	WP4-10
Systemic VNF Wrapper	WP4-11
PPP: Path Proof Protocol	WP4-12
Remote Attestation Protocol	WP4-13
Behavioral Profiles	WP4-14
RAGs: Risk Assessment Graph	WP4-15
Security by Orchestration	WP4-16
Cyber Threat Intelligence Service	Asset01
vAAA	Asset02
Virtual Channel Protection	Asset03
Virtual Privacy (CP-ABE proxy)	Asset04

4 Automation and Closed Loop

4.1 INSPIRE-5Gplus Closed Loop Model extension

In D2.2, we proposed a typical interaction scenario between one Security Management Domain (SMD) closed loop and the End-to-End Security Management Domain (E2E SMD) closed loop. In this section, we extend the proposed interaction scenario to include another SMD, showing both, proactive and reactive part of the closed loop as well as how a security incident mitigation in one domain triggers the deployment of security enablers in another domain.

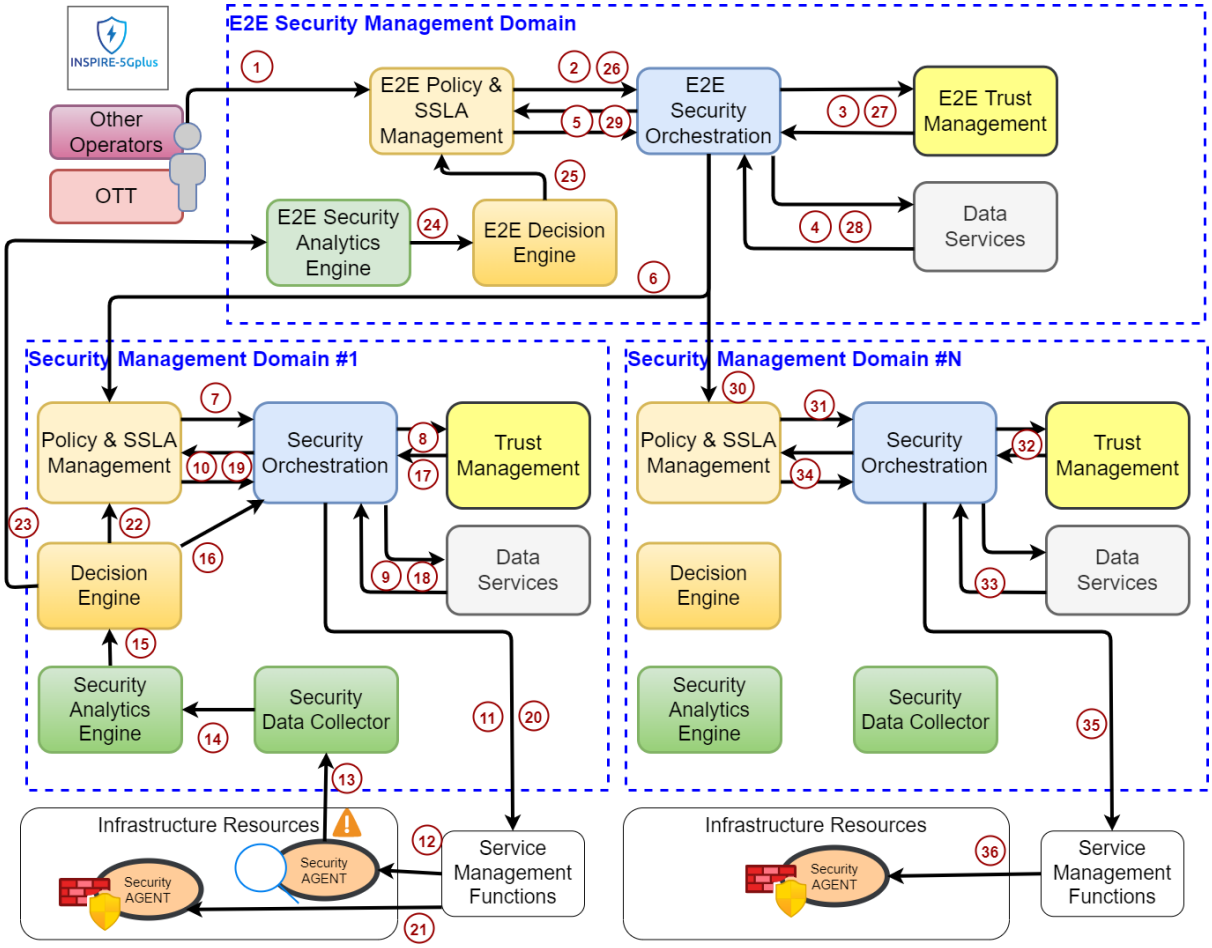

Figure 3 - SMD and E2E SMD closed loop.

Figure 3 shows the INSPIRE-5Gplus closed loop model workflow for both SMD and E2E SMD. Specifically, it shows the following proactive (steps 1-12) and reactive (steps 13-36) interactions for instantiating, configuring, detecting, reacting and mitigating:

(1) – The operator's security administrator or an external entity (e.g., OTT), requesting secure services to the operator, provides the initial requirements to E2E Policy & SSLA Management, which transforms the request into E2E SSLA / Security Policies. If the initiator is the operator's security administrator, this first step of the proactive part of the closed loop could be also initiated directly by providing HSPL/MSPL proactive policies. This is, a SMD security administrator could trigger steps 2 or even 6 manually if desired.

(2) After checking for potential conflicts and/or impossibility of fulfilment, the E2E Policy & SSLA Management module communicates the requested proactive E2E SSLA/Security Policy to E2E Security Orchestrator for enforcement.

(3 - 5) – Trust scores and data (e.g., SMD capabilities, services) are retrieved to prioritize and select between SMDs in case there is more than one suitable candidate. E2E orchestration process uses these parameters to generate, orchestrate and distribute per-domain proactive policies. The E2E Security Orchestrator relies on E2E Policy & SSLA Management services to refine the E2E SSLA /Security Policy, providing medium-level description of the E2E policy. If security policies were already provided as medium-level policies (e.g., experimented admin providing medium-level proactive policies or E2E medium-level reactive policies automatically provided by the E2E DE), the refinement step is not needed. Per-domain policy generation process is also assisted by E2E Policy & SSLA Manager. Data services also contains data needed for the security assessment with capabilities such as vulnerability scans of the VNFs deployed on the running network slices, checking for vulnerabilities defined with the

Common Vulnerability Enumeration (CVE) system maintained by the National Institute of Standards and Technology (NIST) in their NVD database[2].

(6) – Each domain receives its corresponding domain-level proactive policy that will be first checked for potential conflicts and/or impossibility of fulfilment by the Policy & SSLA Management module before being transmitted to the Security Orchestrator for enforcement.

(7 - 10) – Trust scores and data (e.g., SMD capabilities, services) are retrieved to prioritize deployment solutions that are enforced or going to be enforced. An orchestration and enforcement plan is computed according to the retrieved parameters. The Security Orchestrator relies on Policy & SSLA Management services to translate the domain-level policy into low-level actions that can be enforced on the domain infrastructure.

(11) – Depending on the situation, the proactive security policies can be enforced directly on the resources (e.g., configuration of new rules on a deployed vFirewall) or via the Unified Security API offered by the network/service orchestration services (e.g., migration/redeployment/instantiation of new security VNFs/Slices).

(12) – Security Agents/secured services/slices are deployed and configured (e.g., DDoS detector).

(13 - 14) – Data on the network performance and security are collected by the Security Data Collector from the Security Agents and analysed by the Security Analytics Engine to detect any potential violation of the policies; Data is also stored in Trustable Data Services from where the Trust score can be computed. SAE can be also configured in proactive/reactive manners to process the data collected in different ways. For instance, it can be configured so that each vulnerability found is evaluated based on impact, exploitability, and threat values as defined by the Common Vulnerabilities Scoring System (CVSS)[3]. CVSS scores are then processed by the SAE to learn about the dynamic attack surface evolution of the network and finalize the network security assessment. The results of the assessment are fed to the DE.

(15) – If an anomaly is detected, the Security Analytics Engine informs the Domain's Decision Engine.

(16) – The Decision Engine generates a Domain-level mitigation decision, in the form of reactive security policy (e.g., Filtering, Moving Target Defense (MTD) operations, with the objective of mitigating the ongoing attack or reducing the exploitability and impact of CVEs during the time when the vulnerabilities are not yet mitigated/patched), and asks the Security Orchestrator for countermeasure enforcement.

(17 - 19) - Again, trust scores and data (e.g., SMD capabilities, services) are retrieved to prioritize countermeasure solutions that are going to be enforced. The Security Orchestrator relies on Policy & SSLA Management services to translate the reaction policy into low-level actions that can be enforced on the domain infrastructure.

(20 -21) – Depending on the situation, the reactive policies can be enforced directly on the resources (e.g., configuration of new rules on a deployed vFirewall) or via the Unified Security API offered by the network/service orchestration services (e.g., instantiation of new security VNFs/Slices). Thus, security agents/secured services/slices are deployed and configured (e.g., DDoS filter).

(22) – Policy & SSLA Manager is informed about the reaction.

(23 - 25) – The data collected cross-domains are analysed for detecting E2E-level anomaly and producing the E2E-level mitigation decision in the form of security policy that will be enforced by the E2E Security Orchestrator after being checked for potential conflicts by the E2E Policy & SSLA Management module. This process may produce a new enforcement from the E2E Security Orchestrator to the Security Orchestrator. For instance, the same SMD countermeasure can be propagated to other domains.

(26 - 29) Trust scores and data (e.g., SMD capabilities, services) are retrieved to prioritize and select between SMDs in case there is more than one suitable candidate. E2E orchestration process uses these parameters to generate, orchestrate and distribute per-domain countermeasures.

(30 - 34) – Trust scores and data (e.g., SMD capabilities, services) are retrieved to prioritize deployment solutions that are enforced or going to be enforced. An orchestration and enforcement plan is

[2] https://nvd.nist.gov

[3] https://www.first.org/cvss/

computed according to the retrieved parameters. The Security Orchestrator relies on Policy & SSLA Management services to translate the domain-level policy into low-level actions that can be enforced on the domain infrastructure.

(35 - 36) – Depending on the situation, the security policies can be enforced directly on the resources (e.g., configuration of new rules on a deployed vFirewall) or via the Unified Security API offered by the network/service orchestration services (e.g., instantiation of new security VNFs/Slices). Thus, security agents/secured services/slices are deployed and configured (e.g., DDoS filter).

4.2 Trust Closed Loop scenario

In this section we go into the details of the trust closed loop, which was only mentioned previously, aiming to illustrate the trustable mechanisms proposed in INSPIRE-5Gplus being the scope of this final deliverable. The trust closed-loop scenario is present across all the interconnected domains and the E2E SMD, mainly involving the deployment of slices with Security SLA (SSLA) to be addressed in a multi-domain 5G network. Thus, to provide trust to this closed loop scenarios, trust enablers are included as part of the HLA Trust Management Block and allow monitoring the components behaviour by considering a trust attribute assigned to each 5G security enabler. This trust attribute is computed using information provided by different INSPIRE-5Gplus enablers and provided, after computation, to the corresponding HLA security management entities.

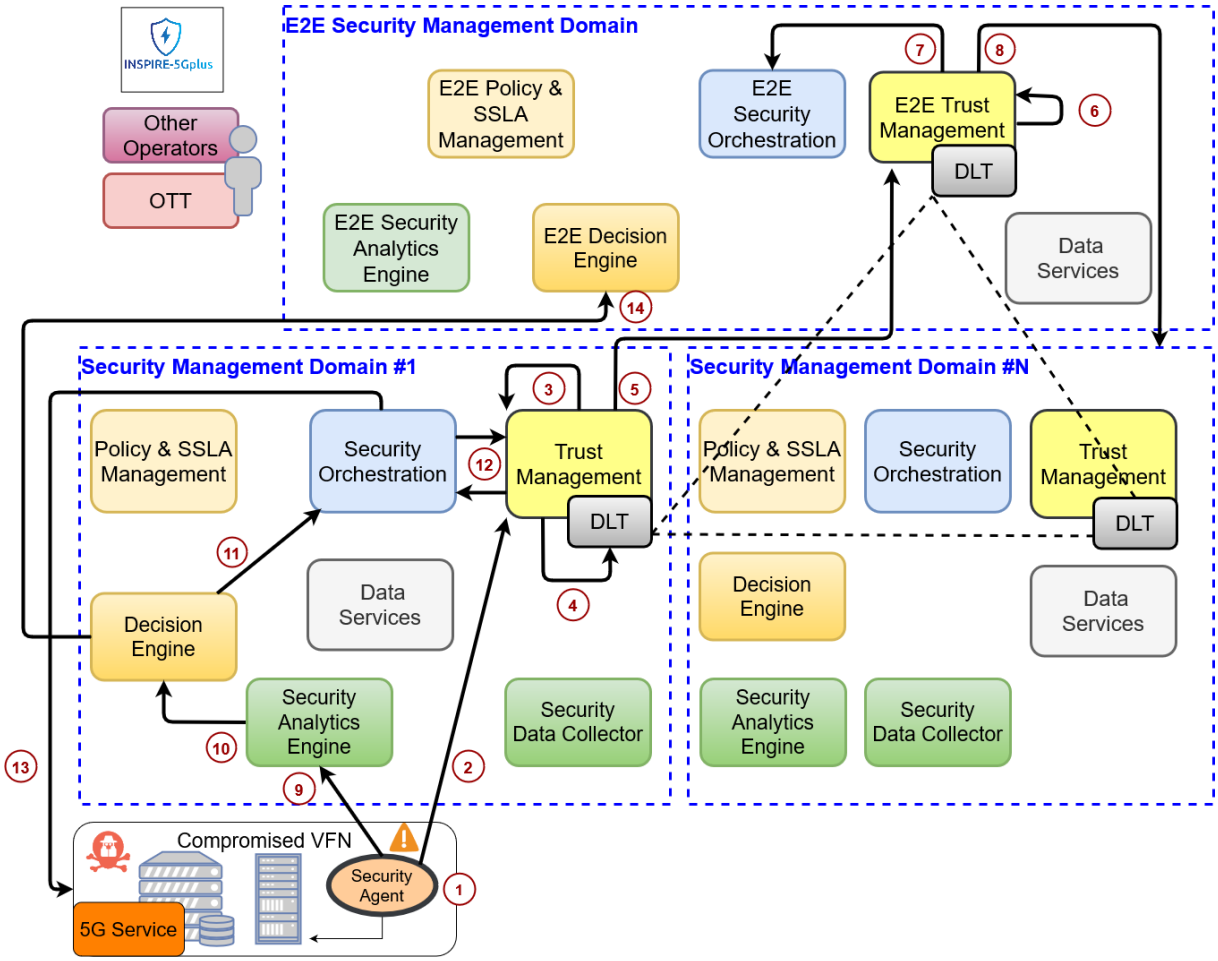

Figure 4 - Trust closed loop steps.

Different kind of system violations could be envisioned to better explain the specific extended closed loop process related to trust.

In this way, monitoring assets previously deployed, such as the Security Agents in Figure 4, detect the issue **(1)** and notify the Trust and Reputation Manager **(2)** in order to update trust metrics of the involved monitored entities (5G service in the figure). It is worth noting that, any enabler (in this case, the Security Agent) should first publish the attack information through the Integration Fabric, using a publication/subscription mechanism that allows the TRM to subscribe to these publications. In such way, the TRM receives the subscribed data through the Fabric. All this gathered information is fed into the trust computation function in order to update trust value of the vulnerable asset and service attacked **(3)**, which in view of this alert, will be decreased until the problem is solved. After that, the enablers' obtained data (information received from the Security Agent), together with the fresh computed trust score are stored in the deployed DLT platform **(4)** for further retrieval or historical post-processing. Finally, any interested enabler may request the value of trust of a given 5G entity through the Integration Fabric. It is also important to point out that, the TRM provides, as well, each enabler's updated trust score to the E2E TRM **(5)** which will compute, partially based on the compromised enabler trust score and security information from each domain, the total domain trust score **(6)**. This domain trust score can be later provided to other security management entities (for instance, the SO in the figure) **(7)** and/or domains that wish to deploy similar entities **(8)** by direct communication through an API.

In parallel to the trust score computation explained above, the security agent (after detecting the mentioned issue) also notifies the Security Analytics Engine **(9**) which, once verified the attack, will notify the Decision Engine **(10)**. At this point, the Decision Engine generates a new security policy to redeploy the 5G service locally in the SMD and provides it to the SO **(11)**. Since the trust has been updated and, in this case decreased, the SO also requests the value of trust of the given 5G entity through the Integration Fabric to the TRM **(12)** to deploy another version of the 5G service as part of the trust-based orchestration process **(13)**, closing the loop at SMD level. Finally, the reaction is propagated to the E2E DE (at the E2E domain) to generate a E2E countermeasure if required, for instance, to apply the same kind of countermeasure in other domains, since they could also contain the compromised component **(14)**, closing the loop at E2E level.

4.3 Beyond state of the art: closed loop for liability management

Before the start of the project, there was little existing work related to liability management for 5G networks. Most existing works either do not cover liability, security or are not adapted to 5G networks. The Cloud Accountability project (A4Cloud) [32] proposed an accountability framework to manage legal requirements related to the management of personal data in the context of Cloud Computing. ETSI [33] defined general principles for accountability management in the context of NVF management systems but this report only considers performance aspects and does not cover security KPIs. Bonhomme et.al. [34] created a decision mechanism for incident reaction in telecommunications network, but it is not adapted for the 5G Slicing context. Hatzivasilis et. al. [35] propose a cyberinsurance tool destined to insurers to perform their risk analysis and decide how they hedge the risks they cover. Therefore, they do not propose any functionality or metric that allows a 5G Service Provider to operate his service. Finally, we found examples of commercial Contract Management Systems, such as ContractWorks [37], Juro [36] and Medius [38] but they are generic tools and cannot be used to operate a 5G Service.

In INSPIRE-5Gplus D4.4 [39], we created several liability-related metrics which can be used as a first brick to pave the way towards the creation of a closed loop for liability-management. The challenge for future works is to investigate how different modules of the HLA can leverage these KPIs. An on-going work initiated by INSPIRE-5Gplus partners ZHAW and Orange started to investigate haw Root Cause Analysis (RCA) and these liability metrics can be used to enhance each other.

5 HLA applicability validation through TCs

HLA Coverage via demos

Within INSPIRE-5Gplus, 3 demos have been carried out in order to test the applicability of the framework for different use cases applicable in real 5G networks. HLA and its closed loops (Section 5.1) are validated through **Demo 1** specified in depth in D5.3. Demo 1 specifically consists of the validation of HLA through reactive and proactive closed-loops, locally and E2E (Section 4.1 . Two SSLAs are used for this purpose, the first one: From the E2E domain, the SSLA requesting the deployment of a 5G network as a service of an E2E slice is received, which must also be secured under certain requirements, such as: protection of the communication channel with encryption, protection of the 5G core against cryptomining and protection of V2X services against DDoS. This SSLA will be translated by the E2E Network Slicer into an MSPL-OP that once received by the E2E Security Orchestrator will be transformed into several MSPL-OPs, one for each domain involved, and each of these policies will represent a sub-slice belonging to the E2E slice. These MSPL-OPs will be sent to the Security Orchestrator of each SMD, which through the trust-based orchestration and the local closed loop will deploy each of the elements specified in the MSPL-OP in an appropriate and orderly manner. The second SSLA focuses on securing the sensors of a private 5G IoT network and the IoT Broker through securization of the communication channels and DDoS protection. Once both SSLAs have been deployed the system is protected against specified attacks, thus if they occur the Data Collector together with the Security Analytics Engine will trigger a reactive closed-loop which starts with the Decision Engine elaborating an MSPL-OP with countermeasures that will be send to the Security Orchestrator and subsequently the countermeasures will be deployed in order to mitigate the attack and maintain the SSLA. If required, countermeasures can be scaled to the E2E Domain in order to perform actions on potential affected domains.

Demo 2 is centred on on-demand (dynamic) Security Level Agreement to adapt to vertical needs, and the way to deliver evidence of SLA effectiveness over the targeted infrastructure. As the Vertical validates the proposed way to evaluate the reality of an SLA deployment before requesting it, Demo 2 is more related to an end-to-end Trust relationship established directly between the infrastructure owner / operator and a potential Client / Vertical. Demo 2 proposal could be seen as an HLA extension at the interface between end-to-end management of services and SLA over multi domains infrastructures, in case of investigating HLA generalization concepts for a multi parties and domains infrastructures (i.e., in term of legal and liability obligations).

Demo 3 focuses on Moving Target Defense (MTD) and implements a closed-loop process instantiating specific HLA parts: data collection -> anomaly detection -> orchestration. The Demo uses AI/ML throughout its workflow. The measurable outcomes of Demo 3 along with its HLA requirements are reported in D5.3.

6 New Security approaches: INSPIRE-5Gplus extensions

6.1 5G imposes technological trust models discontinuity

In document D4.1, we have identified that it is rather difficult to establish a common trust framework for a multi-domain infrastructure between heterogenous parties, that may implement various management systems that use several stakeholders' services. Another complexity degree is introduced by the commitments of each party to focus itself on a specific service to be operated and not the whole service from the end-to-end point of view. The same observation applies to the end-to-end service quality level offered to customers over multi-party / multi-domain infrastructures.

We proposed to address trust and liability concepts over a multiple domains as dual concepts to be applied on each domain or parties' interfaces. Another benefit of our proposal will be its capability to comply with future hybrid schemes chaining some Security Level agreement for some parties with achieved ENISA EUCS[4] certification of other parties (with three level of insurance: Basic Substantial and High as defined inside EU CyberSecurity Act).

For proposed SLA (cf D4.2) or liability commitment (cf D4.3), one important point is the trust level associated with each of collected KPIs or evidence (to measure or qualify an SLA). An interesting proposition of WP4 is to connect each proposed KPI to an attestation framework able to deliver specific properties around the realized measures. Several approaches could reinforce those properties, but one of the more promising approaches will be to operate attestation framework per domain deeply connected with several TEE infrastructure specific to each domain or parties. Those schemes of attestation (reinforced by domain with specific anchoring thanks to TEE technology), allow to commit, deliver and demonstrate the fulfilment of specific requirements that could be used for regulation compliance or product line certification (as requested by new ENISA 5G certification scheme).

An effective way to manage SLA to be operated by a party or over a domain, will be to commit to provide an SLA as well as its evaluation methodology. In this INSPIRE-5Gplus proposed approach, we do not impose an SLA to a party, but each party proposes SLAs associated with a way to collect evidence in its infrastructure thanks to a local attestation framework. This attestation framework could be certified under ENISA EU Cloud Certification Scheme or ENISA EU 5G certification scheme (a first step for a future hybrid scheme to be investigated).

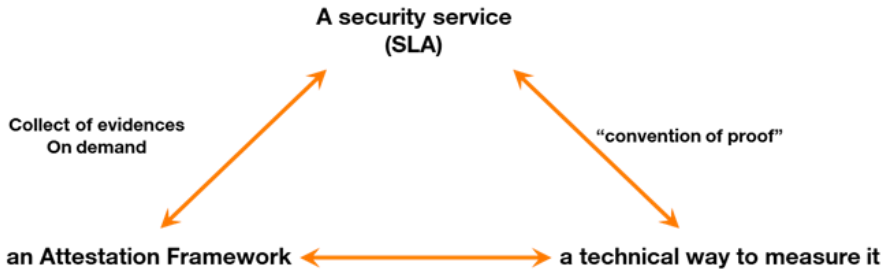

Figure 5 - Diagram.

The E2E service provider is able to qualify if the 'convention of proof' matches its own needs, then elicits a contract with the party that proposed SLA. An interesting point is the ability of the E2E service provider to evaluate at any time the attested SLA (or its effectiveness).

Note: This scheme is demonstrated during the industrial event 'Orange Salon de la Recherche 2022' in Paris and is operated inside Demo 2.

We had established in D4.4 [28] that E2E Service Providers, which have to dynamically compose

[4] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

multiple services from different stakeholders and domains, should find the right balance between liability and supply chain risks, in particular through an on-demand (and proportional) security services framework (rather than implementing the highest level of security throughout the infrastructure).

6.2 5G security extension: an infrastructure virtualisation orchestrated under constraints collected from Clients

MNOs classically operates their security strategy under 2 dimensions: a 'security by design' and a 'security by operation' dimension.

- Security by **Design**: Technical strategy to take into account the risks of ICT products through the processes and technical means structured and designed to cover it before the supply of the whole service (e.g., identification of security and certification/assurance requirements of ICT products based on the risk of their intended use. The technical strategy generally uses state-of-the-art technologies and best practices guidance (e.g., OWASP).
- Security by **Operation**: technical strategy based on Monitoring and Supervising the behaviour of ICT products to detect, in an efficient way, operated services misbehaviour and propose mitigation (already defined and planned for automation, or with experts supports in case of unknown and strange behaviour).

Note: To illustrate those 2 concepts, we could argue that financial smartcard certification (under EMVCo policy or against Common Criteria protection profile) before card issuance is comparable to a security by design concept of smart card (an equipment that should be resistant against known state of the art attacks). Secondly, the Financial Fraud management systems are comparable to security by operation, as financial institutions monitor smartcard and financial services behaviour in order to detect and identify new fraud schemes.

The network softwarization, through virtualization, allows to dynamically adapt 5G network topology. In particular, communication capabilities could be adapted to contextual needs. Concepts of slices allows to operate different network capabilities for different Verticals on the same physical resources. Close Loop approach (see HLA) demonstrate how MNOs can activate on the fly specific security features to mitigate security policy deviation.

Unfortunately, some classes of security needs could not be addressed in a cost-effective way through Security by Design, or Security by Operation approaches or within the Closed Loop concepts. Typically, issues that are difficult to address under the state of the art are isolation commitments:

- Proving isolation between Vertical's components operated in 5G Cloud or MEC infrastructures

  or
- Proving that no non-EU components are used by the MNO to operate a critical Vertical (under NIS2 Directive).

INSPIRE-5Gplus proposes a simple way to address this class of security needs, based on an orchestration of resources under constraints. We proposed to compute (thanks to mathematical optimization approaches) an orchestration placement of resources and components preventing for instance a subset of components to share physical resources with components which have not the same criticality. The problem of isolation (similar to Javacard isolation described in Common Criteria protections profiles PP084 and PP117), which stays a hard problem (complexity and combinatory aspects of origin compromission sources, to be managed and dedicated for each technical hosts in order to warrant a certain level of isolation) under the state of the art, becomes a problem of integrity continuity from the formalization and collection of constraints, the mathematical computed solution until the right deployment and operation of it.

Note: we do not resolve the isolation problem, but we propose 'to escape from it' through specific arrangements in which we may not need to ensure isolation between components. The optimization of components placement allows to resolve several groups of problems, under the same industrial

process. A non-exhaustive list include: end to end latency, energy consumption minimization, multi-cloud hosting cost optimization, CDN and Cache cost optimization in the border of the network. This approach of optimization, if deployed over an infrastructure could be coupled with an attestation framework to demonstrate all constraints are fulfilled.

Note: The *placement optimization results (mathematical results) could be appraised as formal proof and may ease future ENISA 5G certification.*
Note: *The proposed INSPIRE5GPlus enablers (security by orchestration, attestations framework) could be coupled with MTD (ZHAW) enablers to reinforce isolation SLA we could deliver.*

6.3 5G security extension

6.3.1 Towards On-demand security to deliver agility and adapt to Clients real time constraints (for OT and Industry4.0)

Another trend for telecom operators and their clients (i.e., users or service providers) is the concept of on-demand security, which consists of applying security (and its associated penalties in terms of overheads, latency and costs) only to the ones that accept the price without impacting other co-residing tenants' quality of service. The beneficiaries and payers of their demanded security service shall get the means to check that the associated measures are effective and delivered (are in operational state).

6.3.2 Towards proven evidence on Trust SLA to operate critical Verticals

Trust SLAs (TSLAs) can be set and established (from higher to lower layers) between the service vendors to the telecom operators and from the telecom operators to the infrastructure operators. In addition to these explicit written legal agreements, service vendors are supposed to get explicit consent from their users on their respective liabilities.

In all cases, service vendors shall comply with EU common regulations ensuring that the user data are kept confidential, integral and available. User data integrity, confidentiality and privacy is one of the key principles of GDPR EU common law enforceable to any actors interacting with these data. Service vendors will transfer a back-to-back data liability to the telecom operator and the latter will then rely on its SLA towards the infrastructure operators for these data liabilities to be enforced.

The telecom operator shall convert its obligation with data management associated obligations (isolation, storage), deploy the service and associated data management provisions and check them through infrastructure operator-delivered interface. One of the challenges we have found in INSPIRE-5Gplus is to establish technical evidence which attests the confidentiality of a data set. Data confidentiality is always derived from encryption but the statement as "this data is encrypted" never reach certainty whatever analysis method be used (e.g., entropy).

Another challenge is to guarantee that a user data is only made available inside a given area or geographic zone. There is no direct evidence which can be delivered that the data has not been transferred out of the given user-defined restricted zone. In fact, there is a global lack of transparency issue for service vendors towards their associated risks pending on their user data.

One of the directions taken by INSPIRE-5Gplus is to stipulate directly inside the TSLAs the test methods used to check if all liability commitments are met. This transparency in the test methods shall come with the statement of the financial penalties (i.e., maximum coverage of the risks) when these commitments are not met inside the Trust SLA as well.

Defining the method raises the question of the method accuracy, transparency and fairness. Ideally the methods shall be technically unambiguous, beyond auto-declarative statements given by the liable stakeholder. By doing so, one reaches a higher trustworthiness to security property, turning the

commitment of means into a closer commitment of results.

6.3.3 State of the art weaknesses to attest service level user data liabilities

Service level Trust SLAs are essentially related to user data. To comply with EU regulation or with a specific user-defined contractual obligation, data may be located in restricted locations. This requirement can be such that the data in clear can only reside in a given geographic zone or areas either based on political boundaries (e.g., country, community of countries) or locations (e.g., identified cloud farm or utility). The formal evidence cannot be delivered directly as no change, print or marks ever result from a copy or a transfer of this data structure. Detecting a malicious operation or mishandling on the data all along its service life is not possible. There is no formal and proven evidence beyond receiving auto declaration of associated technical means by the different actors interacting with this data, yielding to possible misalignment with property loss scenario. These commitment of means statements are however valuable and meaning and deemed as sufficient between the trusted stakeholders when they are the basis of the TSLA stipulated test method. However, they do not bring a firm and unambiguous evidence that the property is met. A method based on technically proven evidence brings a higher trustworthiness on the property, turning the commitment of means to a plain result delivered by the liable supplier.

Academics such as [29] have developed a method to ensure that data can be only used (possibly badly) inside a set of geo-located cloud utilities. The method relies on encryption and the assurance that the decrypting key needed for the subsequent use of the data (in clear text) is stored into these utilities. Without the key, the encrypted data cannot be used as it is stays encrypted. However, that is a half measure as a malicious use of the deciphered data (on the key-delivered location) may leak the data outside the defined bastion. The same software may be used on that destination location.

The same opacity resides on commitment related to data integrity and confidentiality during their storage, transit and processing. We elaborate below the path to reach technically proven evidence for user data in process.

6.3.4 INSPIRE-5Gplus on-demand Trust SLA

With the objective of establishing evidence on security properties on the different network layers and components, we enumerate below the TSLAs (a non-exhaustive list) which can be established, with their current status as generally generated by the state of the art, the progress made during INSPIRE-5Gplus, the associated challenges and future works. These TSLAs are delivered into four different tables shown in a bottom-up approach and related to respectively the infrastructure, the networks, the software and the data. As it can be appraised, most of the proven evidence are still derived from auto-declarative commitment of means by the liable stakeholder. The paths leading towards technically proven evidence, namely on data-related security (e.g., privacy, geolocation) is drafted here and will lead to further works considered as follow-ups of INSPIRE-5Gplus project.

6.3.5 Elaboration of technically proven evidence related to user data and associated processing software

Table 18 - Towards proven evidence on infrastructure TSLA

TSLA related to infrastructure	**SoTA and progress beyond the SoTA (bSoTA) during INSPIRE-5G**	**Enabler status, challenges and future works, type of measurement-evidence delivered**
Authentication-validation of platform operating system	SoTA: TPM-based remote attestation	Reference: ORANGE deep attestation enabler (DAe)

		to be instantiated as an infrastructure facility by the infrastructure owner.
Authentication-validation of the hypervisor and the VMs	SoTA: Authenticating a VM and the underneath hypervisor is done by single channel (low scalability) and multiple channel (no layer linking) deep attestation alternatives. **bSoTA**: ORANGE deep attestation (DAe) enabler Security enhanced multi-channel approach featuring both scalability and security.	ORANGE's Deep Attestation enabler is composed of several components (local agent, API, remote verifier / Attestation server). Future work: It delivers the service of 'a la carte authentication' directed to customizable attestation from the hypervisor, the VMs and other features extracted from the software through its APIs.
Validation of the hypervisor isolation mechanism	SoTA: infrastructure operator provision auto declarative statement **bSoTA**: easy interfacing made available on Deep Attestation enabler	Future work: A feature-collecting agents shall be developed and installed on the platform and interfaced with Deep Attestation enabler.
Validation of the platform resources (i.e., CPU, memory, TPM presence, TEE presence)	SoTA: platform CPUID and server management resource (e.g., Windows FSRM, Linux cgroups). **bSoTA**: easy interfacing made available on Deep Attestation enabler	Future work: An ad hoc feature extraction agent shall be developed and installed on the platform and interfaced with the Deep Attestation enabler.
Validation of the different process and application on a platform (i.e., white-listing/black-listing).	SoTA: Security by orchestration enabler with a centralized orchestrator-side (orchestrator) whitelist repository and server-side enforcement agents to enforce the control (those white and blacklist to be managed as constrains). **bSoTA**: easy interfacing of the orchestrator with Deep Attestation Enabler	Future work: SNMP (or equivalent protocol) agent shall be installed and interfaced with the DAE (Deep Attestation enabler). DAE will be able to construct the application and process hashes, sign them and exchange with the orchestrator to validate the platform software configuration and the installation of a new process or application. Note: Those interactions could be operated thanks to a future extension of Component certification tool enabler.

Table 19 - Towards proven evidence on service composition TSLA

TSLA related to service composition	**SoTA (at project start)** **Beyond SoTA (bSoTA)**	**Enabler status, challenges and future works, type of measurement-evidence delivered**
Security service composition	SoTA: SSLA management and enforcement. **bSoTA**: • UMU's DLT-based enabler • ORANGE SDLRI (Salon de la Recherche et de l'Innovation, Octobre 2022 – Chatillon – France) on-demand security enforcement demo	UMU's DLT-based SSLA trail and validation tool. ORANGE on-demand security service enforcement. Future work: envisage and implement the connections of potential enablers, apart from the existing ones to the DLT platform to take advantage of the offered features.
Network node validation	SoTA: Proof of Transit (PoT), based on Shamir's Secret Sharing Scheme **bSoTA**: Ordered Proof of Transit (OPoT) based on centralized controller for additional keys distribution and trust metrics collection per network node based on APIs, Path Proof Portocol (PPP) and Deep Attestation (DA) enablers	Future work: increase performance in network nodes by adopting new paradigms such as P4 and add geo-localization information to metrics in nodes.

Table 20 - Towards proven evidence on software TSLA

TSLA related to Software	**SoTA (at project start)** **Beyond SoTA (during INSPIRE-5Gplus)**	**Enabler status, challenges and future works, type of measurement-evidence delivered**
Software development quality	SoTA: Methodology during software development and Component Certification Tool CCT (from TSG)	Future work: An interface between CCT and the orchestrator could be tied to ensure that a component (process or application) under deployment meets a certain level of trustworthiness (from CCT database).
Authentication at start and run time verification	SoTA: Process load time and run-time authentication. Agent-based authentication mechanism. Alternative with Solidshield's self-contained (i.e., agentless) authentication mechanism	Future work: An interface between Solidshield's embedded routine and Deep Attestation enabler will deliver proven evidence that the initial authentication primitive has succeeded for a given process (for

	bSoTA: Expansion of Solidshield's agentless authentication range to the process dependencies (lib functions)	the software and its checked dependencies)
Software confidentiality	SoTA: Against static analysis: code text section (i.e., sequence of instructions) encryption suffices. Against dynamic analysis (i.e., introspection of process memory pages during execution), plain confidentiality is attained with the integral placement of the code inside a TEE (software dependent operation). Ad hoc solutions are based on code or control flow obfuscation. Solidshield's Systemic solution articulates TEE, encryption and obfuscation for setup automation **bSoTA**: Expansion of the confidentiality preservation beyond the process to integrate its dependencies (lib functions)	Future work and challenges: An interface between Solidshield's Wrapping tool (which modifies a binary to confer confidentiality preservation) and Deep Attestation service will deliver proven evidence that the deployed version is confidentiality preserved (within the limits of Solidshield techniques).
Software availability (effective execution)	SoTA: Code execution markers can be coded at design time to trigger unambiguous execution evidence. Apart from this security by design which requires specific engineering, there is no proven evidence that a code runs somewhere.	Future work: Solidshield 's control flow mechanism can be used to bring evidence that the code is alive with an elevated freshness (at each control flow code block change). If interfaced with the DA, these heartbeats could be signed and transmitted to a centralized monitoring location.
Software zoning	SoTA: There are no means to attest that a software only runs in a dedicated location, apart from security by orchestration (installation of a software in an identified machine).	Depending on the technological enablement made available on the platforms (e.g., TPM, SE, TEE, none), several grades of trustworthiness can be brought on the security property and offering different levels of trustworthiness to the property that the code executes at a given place. The plain proven evidence can be delivered with TEE arrangement as described below. The proven evidence derives from a by-design feature. By design, the code has been developed to run into a TEE and to be bound to a specific TEE-provisioned secret. The code is also appended interfaced with a heartbeat

		generation which attests that the code lays on the same TEE and executes there. With the ad hoc interface with the Deep Attestation enabler, the heartbeat; could be signed and transmitted remotely for validation.
Software normal execution	SoTA: There have been several attacks detections research checking the normal control flow or execution trace.	Future research can be made at Solidshield to extract time and space integrated normal execution profile with the intent of emitting deviation alerts or normal execution heartbeats (which can still be signed and transmitted by the Deep Attestation enabler)

Table 21 - Towards proven evidence on data-related TSLAs

TSLA related to data	**SoTA (at project start)** **Beyond SoTA (during INSPIRE-5G)**	**Enabler status, challenges and future works, type of measurement-evidence delivered**
Data quality: Emitting source verification (auth, location, reputation)	SoTA: if a node such as typically a distributed ML model node can be authenticated, geo-localized and reputation verified, there is still an uncertainty gap bridging the node and the data. Metadata shall be appended on the data stream to bind the data and the emitting node, with the associated metadata management at the receipting entity. This mechanism entails by-design changes on the ad hoc data format, impacting the global data structure and management, leading to specific non-scalable solutions.	Future research topics can address some implicit (or explicit if we want to address Zero Trust concepts) cryptographic schemes to deliver proof of origin (authentication, geolocalization, safe device etc...) on each dataflow (for instance: how to manage origin of video control and / or prevent deepfake video). The major locks are the security of the end point (point origin of the dataflow). An interesting point, to be taken into consideration for the future research development is how to deliver SLA establishing compliance of the end point of collect with the new Cyber Resilience Act proposal (EU)[5]
Data security: Emitting software verification (auth, location, reputation)	SoTA: All software by design, by orchestration and above stated TSLA can be enforced on data emitting software.	

[5] Cyber Resilience Act | Shaping Europe's digital future (europa.eu)

Data security: Freshness	SoTA: Data freshness relates to the date of production of the data, which can be added inside the metadata as stated above, with the same limitation of a significant change on the data stream structure and management.	
Data security: integrity and confidentiality during transit	SoTA: Encryption and integrity-prone communication protocols (e.g., TLS, IPSEC) confer confidentiality and integrity. Shamir Secret Sharing has been the basis of various solutions enabling to verify that a traffic transited through a given set of nodes. **bSotA**: The Path Proof protocol enables to detect a traffic hijack.	Facilitate interfacing with the enabler. Integrate the enabler into the attestation framework.
Integrity and confidentiality of the data during storage	SoTA: data encryption ensures confidentiality without integrity (which requires a separate signature appended on the data structure). These mechanisms are by-design enforced.	
Integrity and confidentiality of the data during processing	SoTA: TEE ensures both security attributes	Research shall consider elaborating and develop the mechanism bringing the proven evidence that a data structure resides (in clear text) only in a TEE or deliver evidence that homomorphic cryptography technics are used to keep data confidentiality during the processing phase.
Data availability	SoTA: By-design mechanism for fail-safe (e.g., duplicated) and quiescent (e.g., time-tagged, synchronized) storage.	
Data zoning	SoTA: No proven evidence that a data store is only present (in clear text) into a user-defined zone exists.	As elaborated, research and development could be produced to confer proven evidence that the clear text decrypted data is only present in a set of machines defining a zone. The solution will necessarily implement TEE and the provisioning of the decrypting key inside the zone's machines.

7 Impact of the 5G threat landscape monitoring results

In this section we summarize the results of the threat landscape monitoring that took place throughout the lifecycle of the project, and it was first reported in D2.1. In D2.1 we made an initial assessment of the 5G threat landscape, we classified the 5G assets and the terminology that was used in the project. To elicit the terminology, we made a comparison of the threat taxonomies provides by ENISA, ITU-T X.800, and NIST. After the comparison, the most exhaustive threat taxonomy was the one provided by ENISA, which was adopted in the INSPIRE-5Gplus. Furthermore, we identified several key technologies that were used to improve the security posture of 5G networks, as well as key domains that have specific security requirements.

7.1 Emerging Enablements and their impact on the 5G threat landscape

7.1.1 Automation and Zero Touch management

In deliverable D2.2 [27] we identified potential security threats for Automation and Zero Touch Management approach, and we classified them into 5 categories, namely: Open API's security threats, Intent-based security threats, security threats driven by closed-loop networked automation, AI/ML-based attacks, and attacks due to adoption of programmable network technologies (i.e., NFV and SDN). Besides, we also provided multiple mitigation measure examples for the identified threats.

In addition to our previous findings, in the second INSPIRE-5Gplus white paper [1], we considered that the coordination between multiple management closed loops to ensure system-wide consistency and efficiency may raise serious concerns about privacy and security. Indeed, the closed loop coordination entails hierarchical and/or peer-to-peer interactions between multiple closed loops for either delegation and escalation of goal(s) or issues, or for coordination of actions and sharing of information, respectively. For instance, E2E proactive/reactive security measures usually require enforcing new security requirements according to the current status of the infrastructure in different domains in a coordinated way. To this aim, data sharing and secure inter/intra domain communication are essential. Such interactions and exchange of information between closed loops require mechanisms that allow to establish trust between the communicating closed loops by guaranteeing the accuracy and integrity of the shared information. INSPIRE-5Gplus enablers and features such as E2E SMD/SMD data services, integration fabrics, capability-based and trust-based orchestration along with conflicts and dependencies detection features provide suitable mechanisms to mitigate these kinds of threats.

In addition, managing specific security configurations over the heterogeneous technologies and devices involved on the different domains is also considered part of the ZSM challenge. To provide mitigation mechanisms, INSPIRE-5Gplus relies on a policy-based approach capable of managing security policies/requirements at different levels of abstraction, including refinement/translation processes to generate multi-technology final configurations from security policies.

7.1.2 Trusted Execution Environments

During INSPIRE-5Gplus, Trusted Execution Environment technologies were first studied in D2.1[26] where we had produced our own TEE definition as a common and multi criteria referral used to put light on the main differences between processor vendor technologies. In short, we identified the Trusted Computing Base (TCB) gap between Intel's SGX and AMD's SEV as they are designed to protect two very different type of contents (i.e., security sensitive code for SGX, complete VM for SEV). The document also covers the different operational setup aspects of the technologies. In D2.2, we had considered and identified the risks in using these technologies. SGX security properties were at that time heavily challenged by re-known and responsible academic cyber security research centres. We had produced a deep technical survey of past Side Channel Attacks (SCAs) with our own classification in four successive waves. One important lesson learnt was that all SCAs (targeting SGX) implied a deep knowledge of the TEE-embedded victim code and were all conducted by a malicious sibling process on

the same platform. We had reached the conclusion that these attacks have a very low plausibility in the telecom industry context (e.g., process whitelisting on each infrastructure platform, confidentiality requirement of the proprietary un-known code embedded into the TEE). Moreover, our study of the remediation to these attacks had also shown that TEE are in practice very flexible, not hardware rigid defences one can break for ever. Notably, Intel and AMD have both been pro-active and fast to react with microcode or driver updates to build up hardened bastions against confidentiality and integrity attacks. A collateral victim of the speculative execution type of attacks however can be identified as the hyperthreading (HT) mode, advised by the vendors to be preferably removed to limit risks. However, HT removal recommendation also applies when no TEE is leveraged. We had also reviewed past experiments based on SGX and expanding in various fields of SDN-NFV and AI-ML software. Of course, this perimeter is a small fragment of all possible use cases. Our common thread was on the performance impact and the associated definition of the data and code content of the TEE, influenced by SGX's limited linear space and need of sanitization of the software with system calls exclusion.

On our side, progress was first made to leverage Intel's SGX for virtual function security enhancement. Systemic-SGX software security solution has been designed as a fork to Systemic purely software-based solution and without deviation on its main operational asset, its automated setup. Leveraging SGX on Systemic enables to design a secure regulation of the software hardening, although highly exposed to tampering. Secure and automatic regulation of software security can be elaborated, meeting sustainable and optimized security in highly varying execution context. It also paves the way to change the security profile from a remote supervision utility and during the remote TEE-protected code execution. Secondly, as a result of work on liability, SGX's enablement had fostered Systemics's new generation and transfer of unforgeable monitoring heartbeats, produced inside SGX, to a central supervision position, paving the way to a highly accurate-and-frugal, trustworthy and permanent monitoring of each deployed instances.

Last, it is worth noting that in the recent months, a major strategic turn was taken by Intel with TDX's inception. This event indeed has changed the TEE landscape radically, breaking the TCB gap between the two X-86 domain technologies as both Intel's TDX and AMD's SEV shelter complete VM. We view this as a possible turn to future standardization which would reduce the risk a vendor strategic turns (i.e., solution deprecation). In the same vein, Intel's broke concurrently the 128 Mb linear memory space limit with new processors. These announcements have boosted the interest of all frameworks working on confidential computing and notably those for trusted containerization (TCONs). The perspective of a transparent use of either Intel's TDX, AMD's SEV-SNP and ARM's CCA technologies facilitating the secure migration of containers in the cloud continuum could soon become reality. However, we stress the fact that large TCBs also bring their own security threat as evil TCB (intentionally with a malicious part inside or unintentionally with a vulnerable code inside) can occur more frequently. More, automatic setup will erode the user security acuity and awareness on the security impact. A rogue TCB is in fact more critical as it operates covertly and resists to malware detection tools. Moreover, large TCB expands the risk of our raw hammering attacks overlooked in D2.2 and able to trigger DoS attacks without any prior knowledge of the TCB. If the two TEE essential security properties of confidentiality and integrity are well preserved and reinforced, availability attacks (DoS) could be mounted exploiting the essence of the TEE, their rigid integrity policies. Typically, SGX hard lock strategy of its memory management unit (MMU) rules out instantly any bit flipped DRAM page, causing abrupt process crash. TEE can be viewed as collateral victims of DRAM permissiveness and porosity to bit flipping attacks. Against such availability attacks, it is worth noting that TEE magnifies and simplifies the DoS attack, spawn without any prior knowledge on TCB (i.e., blind attack). The conditions to such attacks are again requiring a rogue sibling process accessing the memory, unlikely to occur in telecom context. However, the "blind" attack mode, its disastrous impact attack and the risk persistence until progress are made on DRAMs, need to be known and reminded. A last risk is the associated cost of TEE as typically, automated TCB generation annihilates all possible memory optimization (i.e., deduplication). A larger use of TEE will impact the global memory requirement.

Our conclusion is that Intel's move closer to AMD and ARM concept, is probably a first step to

standardization and certainly paving the way to a much larger use of TEE in the telecom industry. TEEs have proven to be very flexible and resilient technologies to keep their promises of confidentiality and integrity. Today, the trends are automation and large TCBs. Both trends could bring their security weaknesses with an erosion of user awareness to the associated risks of evil TCB and potential denial of service attacks exploiting TEE strict integrity policy. To reduce the former risk, each VM or container considered for TEE integration shall be vulnerability checked. The latter risk could be theoretically reduced with a more flexible policy against memory page tampering, but this would directly oppose the essence of TEE. A last element to integrate is the performance and memory costs of TEE, notably with no optimization made possible from TEEs on-the-fly encryption. This cost impact calls for principle of on-demand security, leaving the arbitrary decision to the service vendor, according to its acuity of the sensitiveness of its processed data and its related legal obligations.

7.1.3 Artificial intelligence

In the second INSPIRE-5Gplus white paper [1] , we investigated the potential of federated learning (FL) as a key enabling technology for improving privacy awareness, low communication overhead, and low latency, to meet the stringent isolation and performance demands and data sharing regulations of 5G and beyond networks [2], [3]. The conducted investigation allowed us also to extend the AI threat surface defined in D2.2 and [4] to include the adversarial attacks targeting the FL process, namely model poisoning attacks and privacy leakage risks. To mitigate the new identified adversarial attacks, we investigated the promising capabilities of blockchain and TEEs in building robust FL models [1, 5]. In what follows, we extend further the list of defences by advocating emerging technologies and approaches that can play a key role in improving the local models' robustness as well as defeating the poisoning and privacy leakage risks against FL:

- **Interpretable Machine Learning (IML):** IML is the process of establishing the cause-and-effect relationship between the decisions made by an ML model and the input data that caused such decisions. In addition to ensuring accountability, reliability, and transparency [6], IML can be leveraged for detecting and mitigating adversarial attacks against ML models under different attack model settings (i.e., white-, grey- or black-box adversarial attacks) [7]. In fact, IML's model-level interpretation and feature-level interpretation methods can help in better understanding the weaknesses of white-grey box ML models and the relationship between inputs and outputs of black-box models, respectively. Such understanding is vital to develop effective defences to improve the robustness of ML models. While some preliminary work has begun, further efforts are required to investigate how to apply IML for tackling adversarial issues against central and FL models.
- **Generative Models**: There is a consensus in the cybersecurity field that understanding the adversary's tactics is a key for developing effective defences. The potential of generative models (e.g., GANs and Variational Auto-Encoders) in learning the distribution of the original data and generating credible new data can be leveraged to automatically produce realistic and sophisticated adversarial samples. The crafted adversarial samples can then be used to build robust models by adversarially training the models to recognize adversarial examples. While the generative models have recently been examined for crafting adversarial examples in the computer vision domain [8], their application to network traffic has, to the best of our knowledge, not yet been investigated. Initial studies have started but focused on data augmentation or real data replacement for privacy concerns [9]**.**

7.1.4 Distributed Ledger Technologies

In INSPIRE-5Gplus, besides considering the way of providing trust and liability to the system as a whole through the enablers devised up to this point, another key concept is involved in the trustiness assurance process in which, particularly, the implementation of the Trust and Reputation Manager enabler relies on. These are Distributed Ledger Technologies (DLTs) that provide us with a set of benefits such as traceability and security to obtain trust values in a guaranteed way, quantifying in real-time trustworthiness and reputation scores for the management and control entities/services in

5G networks. They also use as baseline historical actions taken, the current context, diverse properties, traffic attestations, and compliance with policies and models.

Some approaches that use them have been previously analysed in [8]. In our case, we employ *Hyperledger Fabric* as a DLT platform that supports Smart Contracts. With such Smart Contracts, that are pieces of code (executable logic), we are able to add the desired results to the ledger as a new transaction. To the best of our knowledge, the project at hand comprises the first design and implementation tackling trustworthiness aspects of the network in such high dynamic scenarios, providing non-repudiation, control-plane and data-plane provenance (e.g., proof of transit) and dealing with liability issues, thereby qualifying which party has not deliver its duties.

7.1.5 Dynamic Liability and Root Cause Analysis

Since zero-risk security cannot be achieved, the capacity to identify responsibilities, investigate incidents and identify responsibilities in the multi-party and multi-layer 5G architecture, is essential to support confidence between parties and compliance with regulation. However, there is very little research in the field of liability management. As shown in INSPIRE-5Gplus D4.4 [28], the existing works are not adapted for 5G due to the fact it is a new architecture mainly based on the network-fits-all approach based on novel virtualisation paradigms such as slicing, NFV and SDN.

INSPIRE-5Gplus D4.4 [26] defines a high-level architecture for liability management and identified three key functions that need to be fulfilled. INSPIRE-5Gplus enablers MUD and TRAILS files are descriptors which can be used to fulfil the first function of a liability management system, namely defining accountability and liability relationships. Enablers which carry out anomaly detection, root cause analysis, attestation and security orchestration are essential to monitor for accountability evidence, which is the second function of a liability management system. Finally, enablers that perform root cause analysis, attestation and orchestration achieve the third function of a liability management system which consists in resolving liabilities and producing reports of compliance or violation. For instance, the enabler GRALAF uses the Istio service mesh to continuously receive communication metrics from the Kubernetes infrastructure [27]. In that way, it can detect changes in the service interactions. When a change is detected, GRALAF re-initiates its learning phase to construct a new Bayesian Network for the root cause analysis of future incidents.

7.1.6 SSLAs and Policy Management

Regarding the policy models, INSPIRE-5Gplus manages security policy models that extends previous research efforts and solutions, specially focused on security, such as the ones provided by I2NSF IETF group as well as some EU project solutions. Specifically, Figure 6 shows the extension/adaptation flow. 5G Security Slice Orchestration Policies defined in INSPIRE-5Gplus, as well as the new security capabilities extend HSPL and MSPL languages used in ANASTACIA H-2020, and previously defined during SECURED EU project, which also extended concepts like multi-level of abstraction policies from Positif EU project, as well as capabilities concept from the IETF working group.

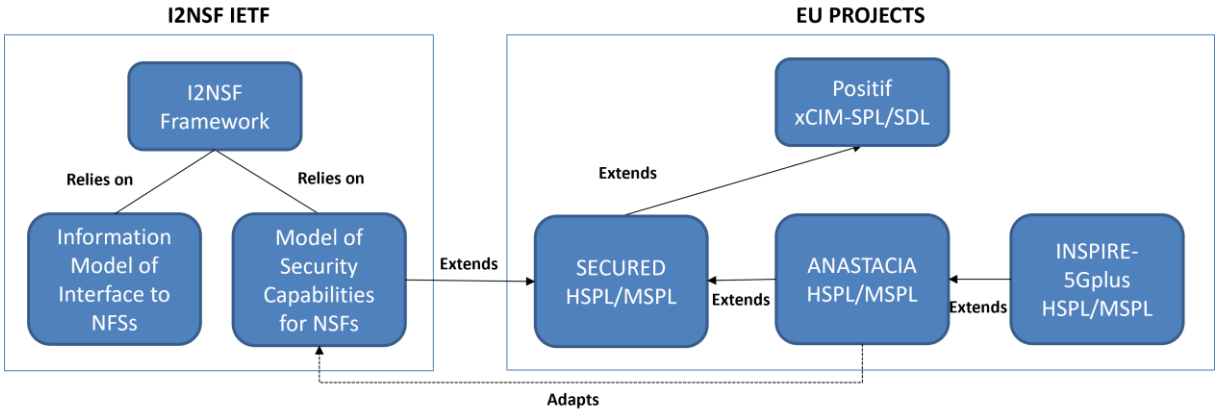

Figure 6 - Policy Models Relationship

Table 22 shows policy models defined/covered by previous projects and solutions. As it can be seen, our solution considers previous works for extending and unifying a wide range of security policies under a single security policy-based solution. Thus, it takes the advantage of using well-defined security policy languages, a capability-based and Event-Action-Condition approaches, to model and implement new 5G security and orchestration features. With this in mind, HSPL and MSPL Orchestration Policy language schemes were extended to enrich current models and fields, also including new capabilities and new models from scratch to provide 5G Security slice features both, at SMD and E2E SMD levels.

Table 22 - Policy models and solutions

Solution	Policy Models
WS-Policy Framework	Specific policy models for web services
Ponder2	Obligation (ECA), Authorization
OASIS (XACML)	Authorization
E-P3P	Privacy
Positif (xCIM)	Authentication, Authorization, Filtering, Channel Protection, Operation
SECURED (HSPL/MSPL)	Authentication, Authorization, Filtering, Channel Protection, Operation, (Other concepts pending to be extended)
ANASTACIA-H2020 (HSPL-OP/MSPL-OP)	Authentication, Authorization, Filtering, Traffic Divert, Channel Protection (also for IoT), Operation, Monitoring, Anonymity, IoT management, IoT Honeynet, QoS, Privacy, Data Aggregation, Orchestration policies.
Proposed extension	Authentication, Authorization, Filtering, Traffic Divert, Channel Protection (also for IoT), Operation, Monitoring, Anonymity, IoT management, IoT Honeynet, QoS, Privacy, Data Aggregation, Orchestration policies, **5G Security Slice, Multi-tenant, Proof of Transit, E2E Channel Protection, 5G Secured Service, Secured Service MANO, Moving Target Defense**.

Whereas it is true that the selected policy models are not currently a standard “per-se”, some concepts were adopted from standardization processes of the I2NSF IETF group. Besides, these security policy models have been previously applied in previous European Projects, they are Open Source, provide a good coverage of security capabilities, can be easily extended, provide multiple levels of abstraction and there are available Open-Source implementations of refinement and translation examples to ease its adoption.

7.2 Emerging B5G/6G threat Landscape

The key areas in 6G as identified in [10], as Artificial Intelligence, Molecular communication, Quantum communication, Blockchain, TeraHertz technology, and Visible Light Communication. Each key technological area is subject to security and privacy issues documented by the academic literature. Artificial Intelligence in 6G and will require robust authentication and fine-grained control processes [11, 12], the ability to detect network anomalies [13], as well as machine learning techniques to prevent information leaks [14], and encryption schemes [15].

Molecular communication and Quantum communication will require novel ways to protect encryption keys [15], and encryption schemes to enhance data security during transmission [16]. Malicious actors

could aim to disrupt the communication process either in the physical or the cyber layer [17].

Blockchain is one of the key technologies of 6G that will require a novel architecture for mobile service authentication [18], as well as access control mechanisms [19] to improve security during transactions [20].

TeraHertz technology will enable 6G to provide high transmission rates in addition to the mm-wave used by the 5G. The TeraHertz technology can make use of electronic signatures as an authentication method [21]. Similarly, how the Visible Light Communication will make use of novel secure protocols for the communication process [22] to minimize the threat of eavesdropping [23].

7.3 Impact of INSPIRE-5Gplus on the emerging threat landscape

INSPIRE-5Gplus so far has made significant contributions to several technological domains relating to the emerging threat landscape of 5G and the upcoming 6G.

In the domain of Automation and Zero-touch management, we identified and classified threat types as well as proposed mitigation mechanisms for each threat type. Additionally, we considered the coordination of multiple closed-loop management systems for data sharing to improve the security posture of networks in a privacy-preserving manner.

In the domain of Artificial Intelligence, we investigated Federating Learning to improve privacy awareness and the communication overhead. We refined the threat surface of AI from previous project outcomes, and we investigated how blockchain and TEEs technologies can be used to mitigate attacks against Federated Learning models. That led us to the techniques of Interpretable Machine Learning (IML), and Generative models to improve the security of our Federated models.

The Distributed Ledger Technologies we used to provide trust values to improve traceability and security in a real-time manner. The Hyperledger Fabric was selected as the DLT platform, and the Smart Contracts feature was used to provide the desired trustworthiness aspects of the network.

In the domain of dynamic liability and root cause analysis, we identified that current works are not adapted to 5G. To fill that gap, we developed the enablers MUD and TRAILS that are used to fulfil the first function of a liability management system (accountability and liability relationships). The second function of a liability management system which monitors for evidence of accountability was addressed by the enablers that provided anomaly detection, root cause analysis, and security orchestration. The third function of the liability management system that resolves liabilities and produces reports of compliance or violation was addressed by the project's enablers such as GRAFAL which provide root cause analysis, attestation, and orchestration.

8 Conclusions

As B5G, and its evolution to 6G, is expected to be a flexible and dynamic network fulfilling multiple use cases with extremely diverse requirements, the potential attack surface will inevitably increase as we have studied during this project. Therefore, such dynamic ecosystems must pay special attention to security while ensuring that the system actions are trustworthy and reliable. To this aim, these deliverable details the integration of a set of security services and their corresponding enablers into the INSPIRE-5Gplus architectural requirements, enforcing security policies while the infrastructure and its security metrics are continuously audited to ensure trust and liability. We have described how each of these enablers contribute to different trust dimensions, devoting special efforts to the integration of these enablers together with the existing ones, in order to provide a higher level of trust information. By monitoring the whole infrastructure, we have been able to ensure trustworthiness on the zero-touch decision making such as the ones orchestrating end-to-end security in a closedloop. We have been also able to validate the described HLA of INSPIRE-5Gplus by means of an enhanced closed loop model extension stressing on the trust closed loop scenario.

For all that, we described the evolution of the High-Level Architecture from INSPIRE-5Gplus, and the framework proposed with a detailed description of the different functional blocks and the proposed services with the final mapping between them. Later on, we presented the automation and closed loop model extension approach adopted by INSPIRE-5Gplus.

Furthermore, in this deliverable we also presented a Security Model to provide liability-aware trustable and smart 5G security. Finally, we provide an overview of the 5G threat landscape monitoring results impact.

The work that has been carried out in the scope of WP2 during the last stage of the INSPIRE-5Gplus project. This deliverable covers the previously identified services, the enhanced enabling technologies and the evolution of the High-Level Architecture leveraging on such technologies with a set of Illustrative demonstrators. Such demonstrators showcase the potential of the proposal as a collaborative work of the partners involved, serving as the validation to the development of INSPIRE-5Gplus enablers.

References

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

[2] O. Hireche, C. Benzaid, and T. Taleb. Deep Data Plane Programming and AI for Zero Trust Self-Driven Networking in Beyond 5G. In Computer Networks, Vol. 203, Feb. 2022.

[3] 3GPP TR 23.700-91 v17.0.0. Study on Enablers for Network Automation for the 5G System (5GS); Phase 2 (Release 17). Dec. 2020.

[4] C. Benzaïd and T. Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?" in IEEE Network, vol. 34, no. 6, pp. 140-147, November/December 2020, doi: 10.1109/MNET.011.2000088.

[5] C. Benzaid, T. Taleb and J. Song, "AI-based Autonomic & Scalable Security Management Architecture for Secure Network Slicing in B5G," in IEEE Network, doi: 10.1109/MNET.104.2100495.

[6] C. Benzaid and T. Taleb. AI-Driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions. In IEEE Network Magazine, Vol. 34, No. 2, pp. 186 – 194, March 2020.

[7] N. Liu, M. Du, R. Guo, H. Liu, X. Hu. Adversarial Attacks and Defenses: An Interpretation Perspective. ACM SIGKDD Explorations Newsletter, 23(1): 86 – 99, June 2021.

[8] C. Xiao, B. Li, J. Yan Zhu, W. He, M. Liu, and D. Song. Generating Adversarial Examples with Adversarial Networks. In Proc. of the 27th International Joint Conference on Artificial Intelligence (IJCAI'18), pp. 3905–3911, 2018.

[9] Mozo, A., González-Prieto, Á., Pastor, A., Gómez-Canaval, S., & Talavera, E. (2021). Synthetic flow-based cryptomining attack generation through Generative Adversarial Networks. arXiv preprint arXiv:2107.14776.

[10] Wang, M., Zhu, T., Zhang, T., Zhang, J., Yu, S., & Zhou, W. (2020). Security and privacy in 6G networks: New areas and new challenges. Digital Communications and Networks, 6(3), 281-291.

[11] L. Loven, T. Leppanen, E. Peltonen, J. Partala, E. Harjula, P. Porambage, M. Ylianttila, J. Riekki, Edge Ai: A vision for distributed, edge-native artificial intelligence in future 6g networks, The 1st 6G Wireless Summit (2019), pp. 1-2

[12] R. Sattiraju, A. Weinand, H. D. Schotten, Ai-assisted Phy Technologies for 6g and beyond Wireless Networks, arXiv Preprint arXiv:1908.09ref93.

[13] S. Dang, O. Amin, B. Shihada, M.-S. Alouini, What should 6g be? Nat. Electron., 3 (1) (2020), pp. 20-29.

[14] T. Hong, C. Liu, M. Kadoch, Machine learning based antenna design for physical layer security in ambient backscatter communications, Wireless Commun. Mobile Comput. (2019)

[15] S.J. Nawaz, S.K. Sharma, S. Wyne, M.N. Patwary, M. Asaduzzaman, Quantum machine learning for 6g communication networks: state-of-the-art and vision for the future, IEEE Access, 7 (2019), pp. 46317-46350.

[16] Y. Lu, M.D. Higgins, M.S. Leeson, Comparison of channel coding schemes for molecular communications systems, IEEE Trans. Commun., 63 (11) (2015), pp. 3991-4001

[17] N. Farsad, H.B. Yilmaz, A. Eckford, C.-B. Chae, W. Guo, A comprehensive survey of recent advancements in molecular communication, IEEE Commun. Surv. Tutorials, 18 (3) (2016), pp. 1887-1919.

[18] S. Kiyomoto, A. Basu, M.S. Rahman, S. Ruj On blockchain-based authorization architecture for beyond-5g mobile services 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE (2017), pp. 136-141

[19] K. Kotobi, S.G. Bilen, Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access, IEEE Veh. Technol. Mag., 13 (1) (2018), pp. 32-39.

[20] P. Ferraro, C. King, R. Shorten, Distributed ledger technology for smart cities, the sharing economy, and social compliance, IEEE Access, 6 (2018), pp. 62728-62746.

[21] I.F. Akyildiz, J.M. Jornet, C. Han, Terahertz band: next frontier for wireless communications, Phys. Commun., 12 (2014), pp. 16-32.
[22] S. Ucar, S. Coleri Ergen, O. Ozkasap, D. Tsonev, H. Burchardt Secvlc: secure visible light communication for military vehicular networks Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access (2016), pp. 123-129
[23] S. Cho, G. Chen, J.P. Coon, Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems, IEEE Trans. Inf. Forensics Secur., 14 (10) (2019), pp. 2633-2648.
[24] D3.4: Smart 5G Security. https://www.inspire-5gplus.eu/wp-content/uploads/2022/07/i5-d3.4_smart-5g-security_v1.0.pdf
[25] D4.4: Liability Management in a 5G Environment. https://www.inspire-5gplus.eu/wp-content/uploads/2022/08/i5-d4.4_liability-management-in-a-5g-environment_v1.0.pdf
[26] INSPIRE5G+ D4.1
[27] INSPIRE5G+ D4.2
[28] INSPIRE5G+ D4.3
[29] N.Paladi, M.Aslam and C.Gehrmann “Trusted Geoloation-Aware Data Placement in the Clouds” in HumanSyst, 2017
[30]
[31] https://istio.io/
[32] http://www.cloudaccountability.eu/
[33] ETSI GR NFV-SEC018 Report on NFV Remote Attestation Architecture, (2019)
[34] G. Hatzivasilis, P. Chatziadam, N. Petroulakis, S. Ioannidis, M. Mangini, C. Kloukinas, A. Yautsiukhin, M. Antoniou, D. Katehakis, M. Panayiotou, IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) Cyber Insurance of Information Systems: Security and Privacy Cyber Insurance Contracts for ICT and Helathcare Organizations (2019), pp. 1-6
[35] C. Bonhomme, C. Feltus, D. Khadraoui, A multi-agent-based decision mechanism for incident reaction in telecommunication network, ACS/IEEE International Conference on Computer Systems and Applications - AICCSA (2010), pp. 1-2
[36] https://juro.com/
[37] https://www.contractworks.com/
[38] https://www.medius.com/solutions/medius-contract-management/
[39] INSPIRE5G+ D4.4

Appendix A References to enabler description

For each enabler the reference to relevant WP3 / WP4 deliverable is indicated in Table 23.

Table 23 - Summary of INPIRE-5Gplus enablers presented in the final set of security uses cases

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

[end of document]