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

D4.2: Trust management in multi-tenant/multi-party/multi-domain 5G environment

Version: v1.0

Deliverable type	R (Document, report)
Dissemination level	PU (Public)
Due date	30/04/2022
Submission date	12/05/2022
Lead editor	Edith Félix (TSG)
Authors	Jean-Philippe Wary, Chrystel Gaber, Marc Lacoste, Jose Sanchez Vilchez, Morgan Chopin, (Orange), Edgardo Montes de Oca, Vinh-Hoa La (MI), Noelia Pérez Palma (UMU), Pol Alemany, Ricard Vilalta, Raul Muñoz, Javier Vílchez (CTTC), Antonio Pastor, Juan Carlos Caja Diaz (TID), Orestis Mavropoulos (CLS), (NCSRD), Gürkan Gür (ZHAW), Vincent Lefebvre (TAGES), Laurent Morel (TSG)
Reviewers	Chafika Benzaid (UOULU), Antonio Gomez Skarmeta (UMU)
Work package, Task	WP4, T4.2
Keywords	Trust, Trust Service Level Agreement, TSLA, Trustworthiness

Abstract

Based on the outcomes of T4.1 and T4.3, this document presents the results of T4.2 Trust management in multi-tenant/multi-party/multi-domain 5G environment. The task focuses on the feasibility of Trust Service Level Agreement to be monitored and delivered to the end user. The deliverable reports on advanced tools and techniques and framework investigated and/or developed to manage a trustable 5G environment and the way to demonstrate them.

Document revision history

Version	Date	Description of change	List of contributor(s)
v0.1	18/11/21	Initial draft with table of content	Edith Félix (TSG)
v0.2	11/02/22	First list of TSLA, Initial metric for key TSLAs, Generic definition of TSLA, Trust enablers status and mapping to HLA	Edgardo Montes de Oca (MI), Vincent Lefebvre (TAGES), Chrystel Gaber (ORA), Edith Félix (TSG), Pol Alemany (CTTC), Raul Muñoz (CTTC),
v0.3	31/02/22	Trust state of the art, Content of Trust enablers status and mapping to HLA	Jose Sanchez Vilchez (ORA), Morgan Chopin (ORA), Antonio Pastor (TID), Noelia Pérez Palma (UMU), Orestis Mavropoulos (CLS)
v0.4	08/03/22	Improvement and consistency of sections 1 to 4 Section 5, demonstrations	Antonio Pastor (TID), Noelia Pérez Palma (UMU), Gürkan Gür (ZHAW), Jean-Philippe Wary (ORA), Marc Lacoste (ORA), All
v0.5	31/03/22	Introduction, conclusion, Executive summary, Data act, Trust management discussion	Edith Félix (TSG), Jean-Philippe Wary (ORA)
v0.6	29/04/22	Implementation of reviewer comments completed	Edith Félix (TSG)
v0.91	02/05/22	Final editing	Uwe Herzog, Anja Köhler (EURES)
v1.0	10/05/22	Executive Summary revised; GA approval obtained.	Jean-Philippe Wary (ORA)

List of contributing partners, per section

Section number	Short name of partner organisations contributing
Section 1	TSG
Section 2	TSG, MI, ORA, TAGES, CTTC, TID
Section 3	TSG, MI, ORA, TAGES, CTTC
Section 4	TSG, MI, ORA, TAGES, CTTC, UMU, TID, CLS
Section 5	TAGES, ORA, UMU, TID, ZHAW, TSG
Section 6	TSG
Section 7	TSG, ORA

Disclaimer

This report contains material which is the copyright of certain INSPIRE-5Gplus Consortium Parties and may not be reproduced or copied without permission.

All INSPIRE-5Gplus Consortium Parties have agreed to publication of this report, the content of which is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License[1].

Neither the INSPIRE-5Gplus Consortium Parties nor the European Commission warrant that the information contained in the Deliverable is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using the information.

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

The deliverable D4.2 compiles work performed in the context of the Task 4.2 “Trust management in multi-tenant / multi-party / multi-domain 5G environment” of the INSPIRE-5Gplus project. This contribution has been delivered while considering already achieved results of project, in particular the High-Level Architecture (WP2).

The Document D4.2 introduces the new concept of “Trust Service Level Agreement” (TSLA) and identifies its differences with the Trustworthiness concept (as already defined in the State of the Art). After an investigation of attributes and metrics commonly used, we introduce our Trust Service Level Agreement concept and focus our investigation on three major TSLAs, that we consider the most significant in the 5G context addressed by the project: Data Protection, Isolation and Geolocation.

We review the status of WP4 Trust enablers (D4.1) towards the High-Level Architecture and investigate their coverage of Trust / Trustworthiness attributes to propose a general mapping over the investigated TSLA.

We analyse the usage of these three TSLAs in the project’s global demonstrations (WP5) as in [31], [32].

Finally, we investigate potential future directions of Trust Management architecture and potential inclusion of non-technical attributes to take into consideration new ethics, ecology and sobriety concerns.

Table of Contents

List of Figures

List of Tables

Abbreviations

5G-PPP	5G Infrastructure Public Private Partnership
AAA	Authentication, Authorization, Accounting
AI	Artificial Intelligence
AMF	Access and Mobility Management Functions
AUSF	Authentication Server Functions
CBOR	Concise Binary Object Representation
CML	Confidential Machine Learning
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
CPU	Central Processing Unit
EAP	Extensible Authentication Protocol
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
ICT	Information and Communications Technologies
Intel SGX	Intel Software Guard Extensions
IT	Information Technology
IV	Initialization Vector (cryptography)
KPI	Key Performance Indicator
ML	Machine Learning
NFV	Network Function Virtualization
NST	Network Slice Templates
OS	Operating System
PKI	Public Key Infrastructure
RCA	Root Cause Analysis
(R)REPEATS	Reproducibility, Robustness, Fairness, Privacy, Explainability, Accountability, Transparency, Security
SCA	Side-Channel Attack
SDN	Software Defined Network
SLA	Service Level Agreement
SMD	Security Management Domain
SSLA	Security Service Level Agreement
TCB	Trusted Computing Base
TEE	Trusted Execution Environment
TSLA	Trust Service Level Agreement
UPF	User Plane Functions
VNF	Virtual Network Function

1 Introduction

This deliverable D4.2 reports about the work performed in the context of Task 4.2 of INSPIRE-5GPlus WP4. This work leverages the High-Level Architecture described in WP2. As WP3 develops how Security is managed in 5G environments, WP4 focuses on the Trust and Liability concepts. Since Security is a more mature field, some lessons can be applied to the Trust field. Both of these technical work-packages present enablers going to enforce the different concepts on the 5G slice. Finally, WP5 translates the WP2 use cases into demonstrations of the technical concepts of the technical work-packages. This deliverable fits in this project organisation, linking the different aspects developed in the different work-packages. It follows a progressive development organised around the following parts:

- Section 2 proposes a generic definition of TSLA. It starts from a state of the art on the Trust concept, and on its difference to the Trustworthiness concept. It includes an explanation about attributes and metrics. It introduces also the concept of Service Level Agreement, which leads to the definition of Trust Service Level Agreement.

  A first typology of TSLA is proposed. Then the section focuses on some Key TSLAs with an attempt to define them.

- Section 3 details how three key TSLAs are mapped to technical Trustworthiness metrics. A methodological introduction explains the rationale behind this mapping, and how it is defined. Then the three key TSLAs are described: Data Protection, Isolation and Geolocation. A synthetic table is proposed, at the end, to ease the technical reading.
- Section 4 situates the WP4 Trust enablers towards the High-Level Architecture. A first subsection sets the scene with a recapitulation of the Trust Management block in the HLA. Then, for each Trust enabler, a mapping to the HLA and a sequence diagram with the main concerned HLA components are provided. Finally, synthetic tables are provided to show the coverage of the Trust attributes by the Trust enablers, as well as an analysis of the Trustworthiness Attributes coming from the Trust enablers in this bottom-up approach.
- Section 5 presents how the three key TSLAs are addressed through the project's demonstrations.
- Section 6 discusses about the future works as they seem to fill the gaps not addressed yet by the deliverable. This concerns the Trust Management architecture, the speciality language useful to express the needs, and probably the inclusion of less technical attributes such as ethics and ecology/sobriety, which also count on one's decision to adopt a service.
- Section 7 concludes the deliverable by a synthesis.

2 Trust Service Level Agreement

2.1 Generic definition of TSLA

2.1.1 Introduction

This section explores first the Trust concept in its own. It then distinguishes the Trust from the Trustworthiness; the first one being subjective, while the second one being an objective technical concept. Both Trust and Trustworthiness have several dimensions, captured under different Attributes. Each Attribute is itself qualified by means of metrics. Finally, all these concepts prepare to the management of Trust Service Level Agreement which are contracts between an end user or service consumer with requirements, and a service provider providing an adapted level of service.

2.1.2 Trust concept

INSPIRE-5Gplus D4.1 [1] investigates trust concepts and mechanisms and defines trust as follows: "The concept of trust is complementary to liability, accountability, transparency, and responsibility. Each covers a different aspect related to the accomplishment of a task and the management of the underlying risks".

At the crossroads of these concepts, trust reflects the belief of whether **the trustee is able to perform the task, meet the objectives and report relevant meaningful information**. Ultimately, **trust measures to what extent the trustor is confident to accept the risks of delegating the task to the trustee**."

[1] also highlights that the major challenge for 5G trust management consists in monitoring the trust of 5G networks and 5G services due to the complexity of these infrastructures which are heterogeneous, service-based and multi-party. As described in [2], such a complex environment results in competition between providers who offer different (albeit similar) levels of guarantees and trust. Ensuring an overall level of trustworthiness thus requires a dynamic and intelligent system which is able to adapt to the diversity of its subsystems and their trust relationships.

To dive into a deeper state of the art, [3] analyses the corpus of the research from diverse disciplines going from philosophy, psychology, sociology, organisational management, international relation to automation and computer and networking. The source of the assessment process relates to the threats and the risks for the trustor to trust the trustee, but also to a wide range of situations or motivation which affect trust relationship. Figure 1 presents an analysis of the trust assessment process according to the authors.

[4] distinguishes Trust in people and Trust in technologies, based on the nature of Trustor's expectations. Therefore, it proposes some attributes to qualify Trust in technologies, which shows slight differences from attributes qualifying Trust in people:

- Functionality versus Competence related to Trust in people
- Helpfulness versus Benevolence for Trust in people
- Reliability versus Predictability/Integrity for people

Telecommunication standardisation organisations use Trust Models to describe the evolution of the patterns related to the successive telecommunication generations (2G to 5G). It is interesting to note that 3GPP [5] bases its Trust model on the four viewpoints of Quality of Service (QoS) from ITU-T [6]. In 5G Ensure European project, [7] extends the state of the art on Trust to threats and risks modelling. It also develops Trust model over IT use cases. ETSI NVF Security and Trust Guidance [8] also uses Trust models to describe different patterns of trust relation between Virtual Network Functions or entities. In Appendix, [9] describes a typology of Trust models as patterns of development of a Trust relationship, according to the context, history, culture, and intermediation between the organisations. [10] defines Trust anchors in the different domains of a 5G network and describe the relationship between them.

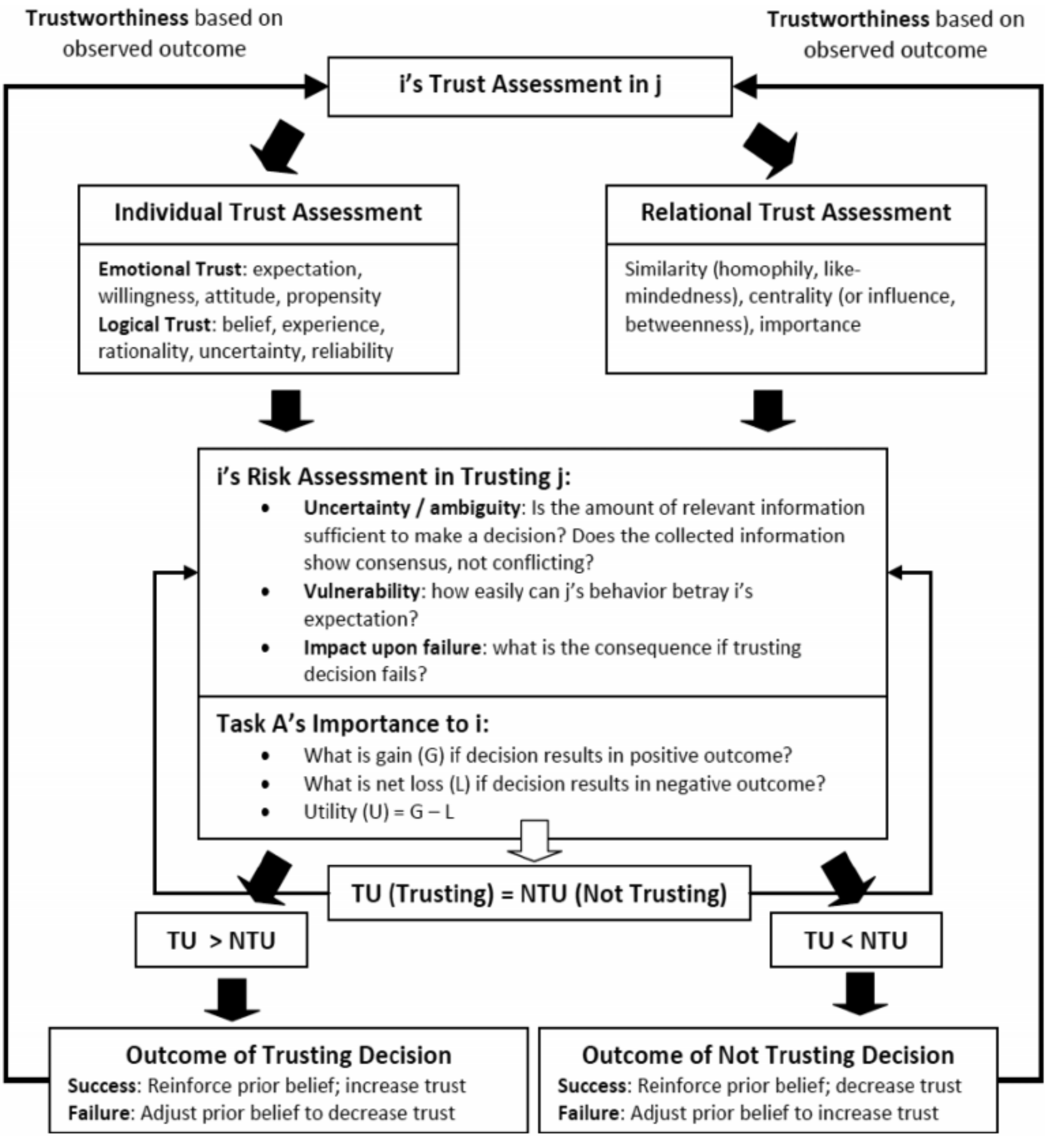

Trustworthiness based on observed outcome
Trustworthiness based on observed outcome
i's Trust Assessment in j
Individual Trust Assessment
Emotional Trust: expectation, willingness, attitude, propensity
Logical Trust: belief, experience, rationality, uncertainty, reliability
Relational Trust Assessment
Similarity (homophily, like-mindedness), centrality (or influence, betweenness), importance
i's Risk Assessment in Trusting j:
Uncertainty / ambiguity: Is the amount of relevant information sufficient to make a decision? Does the collected information show consensus, not conflicting?
Vulnerability: how easily can j's behavior betray i's expectation?
Impact upon failure: what is the consequence if trusting decision fails?
Task A's Importance to i:
What is gain (G) if decision results in positive outcome?
What is net loss (L) if decision results in negative outcome?
Utility (U) = G – L
TU (Trusting) = NTU (Not Trusting)
TU > NTU
TU < NTU
Outcome of Trusting Decision
Success: Reinforce prior belief; increase trust
Failure: Adjust prior belief to decrease trust
Outcome of Not Trusting Decision
Success: Reinforce prior belief; decrease trust
Failure: Adjust prior belief to increase trust

Figure 1: Analysis of the trust assessment process as in [3].

2.1.3 Trust versus Trustworthiness

In [9], NIST defines the concepts of Trust and Trustworthiness. Trust is an important concept related to Risk Management. The way an organization evaluates the level of trust which it has in another organisation will influence the way it will handle the risks to interact with it. Trustworthiness of an IT system expresses the capacity of the system to preserve the security of the information during its whole life-cycle, and while exposed to any threats. The Trustworthiness attributes can be applied to a system, but also people, a process, or a technology. It can be measured, at least in relative terms if not quantitatively.

[11] states that although trust and trustworthiness appear interchangeably in common vernacular, they are distinct concepts. Trustworthiness is a characteristic or property of an individual; trust is an attitude or belief we have about those who are trustworthy.

[12] provides a comprehensive Trust model involving the trustor and their motivation placing or not Trust in the trustee and their capabilities demonstrating Trustworthiness. Other depicted entities are claims, commitments and evidence for direct trust, and third parties for indirect trust, as shown in Figure 2: A comprehensive Trust model as in [12]..

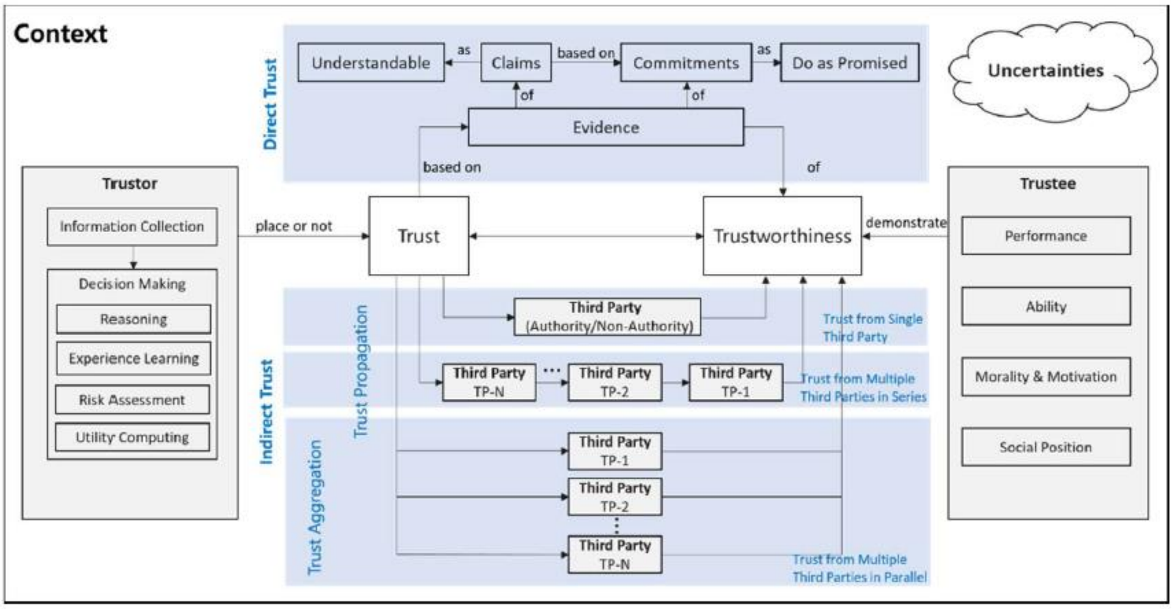


Figure 2: A comprehensive Trust model as in [12].

Finally, Trust is a subjective concept related to the belief a user has on an organisation or system, when Trustworthiness is a technical objective attribute or property, which is measurable on a technical system.

2.1.4 Attributes and Metrics

According to NIST in [9], "the Trust relationships are key factors in risk decisions made by senior leaders/executives". Trust and Trustworthiness are associated with different attributes describing one aspect of the Trust respectively Trustworthiness performance, and each of which being associated with metrics.

Metrics are commonly used in a wide range of disciplines. In IT technology, a security metric is a description of a process that measures a particular characteristic of an information system. They provide Key Performance Indicators (KPIs) of the information security management system.

ETSI Security and Trust Guidance for NFV [8] works on the Trust relationship within and between VNFs. It exposes that trust hangs on contextual parameters which will serve as Attributes for Trust evaluation. The most decisive is the Time (elapsed since last relation). Others are Geographical location, Jurisdiction/regulatory location (public/private), Logical (network) location, hardware capabilities, Hardware provenance and history, Software capabilities, Execution instance history, Chain of trust, Time elapsed since last trust audit/check, Date, Time of day, Ownership of hardware, Security of network, Appropriate use of encryption techniques, Extent to which the software is initially hardened, Measures in place to maintain the integrity of the software, and Physical security of the various locations over which the NFV components are deployed.

The Cloud Audit Metrics Catalog of the Cloud Security Alliance [13] proposes a catalog of security metrics for an information system. There are 34 of them. To present some of them, let's give some examples: percentage of running production code that can be directly traced back to automated security and quality tests that verify the compliance of each build, or the percentage of critical vulnerabilities that are not fixed or marked within the time specified by the policy. Each metric is associated with a description, an expression (often mathematical), rules and a target objective for the Information system to be performing. Trust in an IT system could be defined as the ability of the system to fulfil equal or higher scores than the objectives recommended for the security attributes in the catalog. Here, the security attributes play the role of Trustworthiness attributes.

[12] proposes six high level Trustworthiness attributes: Resilience, Security, Privacy, Safety, Reliability, and Availability.

2.1.5 Service Level Agreement

A Service Level Agreement corresponds to an agreement or contract signed between customers and service providers or different stakeholders or tenants which specifies services, quality and security expectations [2]. ETSI defines in [14] a generic model of SLAs which is composed by all involved parties, high level description of constraints, a description of the services, their guarantees along with their detailed objectives (called SLO), indicators (called SLIs), and SLA violations and associated penalties. It also allows the definition of the management actions to be performed by the provider to meet the SLOs defined as well as the cost of the services and associated guarantees.

Based on the SLOs and SLIs, the providers are expected to build the technical metrics reported by the technical infrastructure (that we also call technical KPIs). Based on these metrics, the providers are expected to monitor and optimize their infrastructure and ensure that the objectives set by the SLA are met.

A standard for SLA expression is proposed by ETSI [14] including the parties, the description of the service, the service level objectives, the guaranties, the cost, the SLA violations and penalties and other constraints. Figure 3 presents [14] SLA generic model.

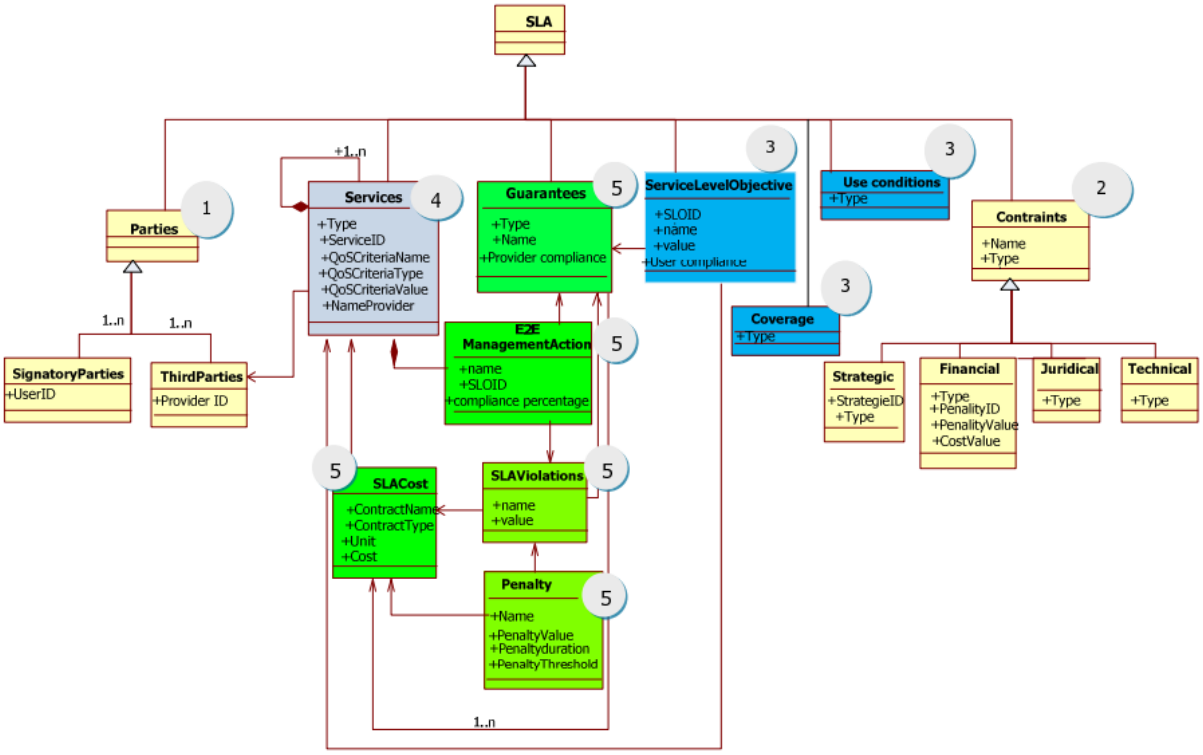


Figure 3: ETSI 202 009-3 [14] SLA Generic model.

In the field of security, specific Security SLA can be set up to focus on the security aspects of an ICT system. INSPIRE-5Gplus D2.1 [15] mentions in section 5.4.3 that Security SLAs is a subset of the global SLA that tackle the security and compliance engagements for both parties including, in the case of 5G networks, aspects related to both the infrastructure and the provisioned services (e.g., infrastructure security, resiliency controls, data protection). These SLAs are typically written in natural language (often in a strict legal notation). Currently no widely adopted format has arisen. The SPECS XML SLA Framework[2] proposes a machine-readable format of Security SLAs. INSPIRE-5Gplus D2.2 [16] section

[2] https://bitbucket.org/specs-team/specs-utility-xml-sla-framework

2.7 explains the relation between SSLAs and Security Policy Management. Both are intended to introduce the business and security requirements as established by humans into a fully automated environment, therefore driving the behaviour of the system. As, SSLAs establish a contract between operators to ensure a certain level of security that subjugates the system, Security Policies provide the abstraction and the formalism to enforce such SSLAs or other security restrictions.

2.1.6 Trust Service Level Agreement (TSLA)

A parallel between the Security SLAs dedicated to all security objectives, and the Trust SLAs providing the viewpoint of Trust can be established. This section proposes a first core definition for Trust SLA and extends the discussion to the main usages of it.

Core TSLA Definition

TSLAs are trust-related agreements established between a customer and its service provider, or between different stakeholders and tenants. They are formal contracts documenting the trust features of delivered services and related quality expectations called Service Level Objectives (SLOs). TSLAs are a subset of the global SLAs that tackle the trust and compliance engagements for both parties including, in the case of 5G networks, aspects related to both the infrastructure and the provisioned services. TSLAs are typically written in natural language and define the list of properties for achieving the desired Level of Trust (LoT). These properties or attributes can be related to several Trust dimensions: security (service and infrastructure); liability; reputation; controls for resiliency and availability; data protection (e.g., certificates used); data privacy; multi-* aspects (i.e., indicators applicable to particular domains/tenants); etc. They include the remedies and the penalties that would be applied if the agreement is violated.

Beyond the above definition, the usage of TLSAs serves the disciplines of Quality-of-Service Monitoring, and Risk Management and Assurance. As SLAs include the quality requirements expressed by the end user or trustor, it makes it possible to hand on a Monitoring framework to follow if a runtime system complies or violates the expected requirements. Both violation descriptions and penalties are included in the description of the TSLAs, facilitating its usage in the context of Zero Touch Service Management.

To qualify the risks associated to the system according to the expectations of the end user, experts analyse the assurances given by the service provider, the history of the events monitored at runtime on the system, and also their experience and knowledge of similar contexts and systems. Among assurances, one can notably refer to the assurances coming from the Development Life Cycle:

- Development quality (for SW and HW);
- Regulation taken into account;
- Security threats taken into account and existing security controls implemented to balance risks;
- Compliance for the usage and regulations application;
- Existing certifications, etc.

Among the history track, one can notably follow data in the form of metrics for runtime monitoring of Trust:

- Metrics measuring Trust properties;
- Security breaches (attacks, remediations);
- Availability;
- Reputation or feedback coming from users;

2.2 List of main TSLAs with their definition

The goal of this section is to give an insight of the directions to define TSLAs. It is not yet an exhaustive and mature proposal ready for standards. Nevertheless, the on-going research shows first orientations inspiring the development of TSLAs focusing on different aspects of the ICT systems.

Although a Service Level Agreement refers to a complete contract specifying all aspects of the Trust relation from the requirements to the penalties, only a single and main Trust attribute is used below to qualify a type of contract. On the field, a TSLA might be composed with a list of requirements related to several different Trust attributes. Please note that in all the project deliverables, the terms TSLA and Trust attribute may be used interchangeably.

The following Table 1 proposes a typology of TSLAs.

A first important category of TSLA relates to data, its protection and its privacy. Generally speaking, in ICT systems, data represents the most valuable assets to be protected. With European General Data Protection Regulations (GDPR), privacy has not only become a regulatory concern for all ICT operators, but also a commercial incentive to gain the Trust of the consumers. Data protection hangs on classical security dimensions such as Confidentiality, Integrity and Access Control.

A second straightforward category of TSLA consists in evaluating a general Level of Trust, or Trust Score, to publish a mean value of the Trust guaranties of a service, or a list of Key Trust Indicators (KTIs). Several different lists of controls can be used to check the capabilities of a service and its underlying infrastructures with regards to the implementation of good practices or controls that are viewed as Trustworthiness attributes. The Cloud Alliance published an example of such control Catalog in [13].

A third set of TSLA mirrors technical Trust aspects theoretically proposed by researchers, or practically implemented by Trust enablers. Cybersecurity, geolocation, isolation, and trustworthiness for AI are such of technical aspects to be taken into account in the design of a solution, and which requires to be advertised to the end user to evaluate the suitability of the service to their usage, in case specific security issues apply. On the other hand, INSPIRE-5Gplus Trust enablers propose a rich palette of technical Trustworthiness attributes, such as Proof of Transit, or Interface to Network Security Functions (I2NSF). In these later cases, a Trust attribute is created to translate and communicate the technical Trustworthiness attribute as an end user concerning value.

The fourth category definitely takes place in the Trust relation to have in the chain of providers of a service in multi-provider context. Indeed, trust can also be built upon past observations of the propensity of providers to fulfil their commitments towards their partners or customers. Reputation or monitoring of violations of commitments, as expressed in Manufacture Usage Description (MUD) or MANIFEST, are some examples of this category of SLAs that enable to evaluate the provider and the confidence one can have in the way they handle the service. This category of SLA is not in the scope of D4.2.

Finally, it is necessary to open a fifth category for other ways and concepts to express Trust.

Reference	TSLA category	Example of derived TSLA	Comment
1	Data protection and privacy	-Data protection -Data privacy -Confidentiality, Integrity & Access Control (CIAC)	Relating to data and how it is accessed and by whom
2	Security Key Trust Indicators (KTIs)	-Level of Trust (LoT) or Trust Score (TS) -Security Level	Derived from Security controls See [13] from the Cloud Alliance for a complete set of security controls
3	Technical Trust aspects	-Proof of Transit (PoT) -Trustworthiness for AI	Mapping all kinds of technical aspects or

Refer ence	TSLA category	Example of derived TSLA	Comment
		-Interface to Network Security Functions (I2NSF) -Cybersecurity -Geolocation -Isolation -Trust metrics related to: TEE, slice, VNFs…-Targets of Monitoring (ToM) or Targets of Trust (ToT)	Trustworthiness Attributes
4	Provider Commitments	-Reputation -Manufacturer Usage Standard (MUD) or MANIFEST -Liability	Relating to the provider of services
5	Other capabilities	Extensibility	Based on capabilities required for the future developments of the service

Table 1: Typology of TSLAs.

2.3 Focus on some Key TSLAs

The following describes in more detail a selection of some main TSLAs that will be considered in INSPIRE-5Gplus demonstrations, mainly: Data protection and privacy, Isolation, and Geolocation. These have been selected due to their importance in assuring the security and trust in virtualised environments adopted in 5G (i.e., network slicing, NFV, SDN). Following these descriptions, other TSLAs are briefly described.

2.3.1 Data protection and privacy

The EU General Data Protection Regulation (GDPR) harmonizes personal data protection laws in the EU. At the same time, 5G standards address privacy issues right from the start. GDPR regulations most relevant to 5G stakeholders and standards involve the following issues.

The complexity and dynamicity of 5G virtualised network environments (e.g., slices) require ensuring data protection and privacy in an automated fashion. This includes real-time monitoring, E2E management, forensics data collection, management of consent, as well as of certain rights (e.g., defining certain restrictions, the right to be forgotten, the right to data portability).

More recently in February 2022, European Commission launched the Data Act, targeting to make the EU a leader in a data-driven society. It proposes a new European way of data governance to enable a single market for data and to facilitate data sharing across sectors and Member states. “The Data Act clarifies who can access and share data and on what terms. It provides legal certainty, and it aims at removing barriers to data sharing,” said Commission digital chief Margrethe Vestager. The tendency is to facilitate cloud switching for a better interoperability between cloud providers.

There is also the need for proactive data protection by design and by default. 3GPP standards and working groups (e.g., SA WG3) have defined identifiers, protocols, and test cases for assuring data protection and privacy in 5G. So, all network service and solution providers should conform to these specifications and provide privacy impact assessment built into their products or services' lifecycle, as well as inform users and operators of any limitations and impacts.

Operators are responsible for protecting personal data, but the users can define the extent to which this protection is needed. Since data and privacy protection has a cost (e.g., in resources, performance), users need to define in more detail when data protection is required, and the protection needs to be considered with respect to the risk involved. Thus, TSLAs can specify what data needs to be protected and what data does not. They can also define the frequency of the controls, their level of consent to the use of their personal data to perform analytics, the level of encryption, the level of integrity protection of stored data, the anonymization and pseudonymisation of data, the separation of data according to the level of required protection, the authorized access mechanisms used, the lifespan of personal data, etc.

Of course, end-users should not be required to specify very technical details. For this, more abstract TSLAs are needed that can be those defining the Level of Trust (LoT) or the Level of Security (LoS). But in turn, these levels need to be defined by the more detailed TSLAs described above.

Example:

As a customer, I want <my data/sensitive data/critical data/application data/topology data> to remain <confidential/integral> during its <complete lifecycle, transmission, storage, processing>

2.3.2 Isolation

As explained in [19], 5G characteristics (virtualisation, slicing, multi-domain, multi-tenant, etc.) make isolation an important enabler for security and, thus, is required for improving trust and delimiting liability. But in 5G many isolation requirements and techniques coexist that need to be specified and managed. Furthermore, as indicated in the article, "elasticity and agility are strongly connected with isolation" and the isolation level should be considered an important parameter for defining a service or a network slice. [19] identifies several isolation properties. These include, for instance:

- Isolating slice resources (storage, processing, memory);
- Isolating or limiting the communications or accesses between slices;
- Assuring intrusion detection or prevention between different slices;
- Isolating different functions (e.g., signalling and management functions, virtualised and non-virtualised functions).

Several isolation techniques exist that can be used, as for instance those identified in [19]: language-based isolation, Sandbox-based isolation, Virtual Machine (VM)-based isolation, security protocol-based isolation, Operating System (OS) kernel-based isolation, Hardware-based isolation, and physical isolation. Some are more adapted for the isolation of services, network slices, network media interfaces, and infrastructure/virtual infrastructure.

With respect to security protocols, there is a wide choice of techniques: Multi-Protocol Label Switching, VLANs, VPNs, IPSec, SSL/TLS (Secure Socket Layer/Transport Layer Security), DTLS (Datagram Transport Layer Security), MPPE (Microsoft Point-to-Point Encryption), SSTP (Secure Socket Tunneling Protocol), SSH (Secure Shell), etc.

Isolation targets and techniques can be grouped to define isolation levels that present a more abstract view and can be specified using TSLAs. Furthermore, the TSLAs can specify the scope, such as E2E, inter-slice, inter-domain, inter-tenant, and even the allowed type of interactions between slices and with shared functions/resources (e.g., based on specified finite state machines or behaviour patterns).

Example:

As a customer, I want my slice's <processing/data/network> to be isolated <E2E/on a given domain>

2.3.3 Geolocation

Geolocation relates to the capacity to define the geographic area (e.g., European Community, country, data centre, platform) where data are located and processed, and where software is located and executed. One key difficulty is that both software and data are by their very nature transportable (and copyable). The associated trustworthiness to an operator statement as "your data, software, service are there" does not extend to "and only there". This technical limitation does not erode the legitimate need to know where a service is technically implemented and data are stored.

The geolocation as discussed below relates to the need to know where my data and my service are located. Geolocation is considered to be personal data by the GDPR, as detailed in Article 4(1), and its collection and processing is governed by the GDPR. Article 3(2) states that, "This Regulation applies to the processing of personal data of data subjects who are in the Union."

From the technical point of view, when no GPS-backed system is in place (e.g., drone, car), all geolocation verifications rely on the IP-MAC mapping protocol. IP address is delivered by DNS server and can be used to estimate the country, city, or ZIP code, determining its geographical location.

As it can be rapidly determined from the trustworthiness attribute description, today geolocation is exclusively delivered in the form of auto declarative statements from the operators.

No technical proof or evidence can be produced to confirm that a data is present in a specific place, it is however possible to trace and know if a data has been located into a safe place (of various kinds) from which it cannot be extracted. This enables binding a software to a pre-provisioned and non-extractable secret which confers a geolocation evidence of the software, which can only operate at this secret-provisioned platform. Indirectly, it is possible to assess, with several levels of certainty, that a software operates at a given place and to collect cryptographically-proven evidences that it truly executes there.

2.3.4 Other aspects covered by TSLAs

2.3.4.1 Cyber security

NIST defines Cybersecurity as the process of protecting information by preventing, detecting, and responding to attacks. The NIST Cybersecurity Framework (CSF) [20] helps organizations to understand their cybersecurity risks (threats, vulnerabilities and impacts) and how to reduce those risks with customized measures. As NIST organises its framework around Identify, Protect, Detect, Respond, and Recover functions, ISO 27000 standard [21] series fully defines the organisation of an Information Security Management System (ISMS).

A variety of publications develop different aspects of the field. European Union Agency for Cybersecurity has published the Computer Security Incident Response Teams' Maturity framework [22] that is intended to contribute to the enhancement of the capacity to manage cyber incidents. Closer to INSPIRE-5GPlus challenges, it published a guide for NFV Security in 5G [23]. After an analysis of attack scenarios, it defines a set of categorized best practices.

Including [13] mentioned above, these types of publications can provide a framework of controls to be checked to guarantee a certain level of security and give evidence of a trustable computing or service environment. All kinds of technical security aspects are included in these frameworks.

Example:

As a customer, I want to be notified of a <anomaly/security breach/...> with a delay of <X> minutes after it occurred

As a customer, I want an IDS to analyse the network traffic flow of my <service/network/end point/...>

Or if we want to be more specific:

As a customer, I want all the network traffic sessions using the protocol(s) <...> to be controlled by

<the default/the custom/all/a predefined set of> <rules/algorithms> available

As a customer, I want all the network traffic sessions using the protocol(s) <...> to be controlled in such a way as not to introduce an overhead in the <latency/performance/...> of <X> %

2.3.4.2 Trustworthiness for AI

Advances in AI and machine learning (ML) brought European commission to publish the AI act[3]. Clarifying the trust and trustworthiness assumptions for AI-based systems is key for the adoption of such technologies. Several high-level TSLAs should thus be identified for **trusted AI systems.** The Linux Foundation for Artificial Intelligence identified for instance the (R)REPEATS (reproducibility, robustness, fairness, privacy, explainability, accountability, transparency, and security) principles to build trusted AI systems [24]. Among some key categories, one may find [25]:

- **Security and privacy:** the AI system must be immune against attacks (confidentiality, integrity, availability) and guarantee data protection, including for privacy-sensitive data (e.g., unlinkability).
- **Transparency and explainability:** the AI system should include information regarding the purpose of and manner of use.
- **Ethics and fairness:** there should be no bias during steps of the AI workflow. The AI system should also be beneficial to humans (e.g., for healthcare, to improve security).
- **Robustness:** the AI system must be immune to failures of one or several nodes, notably for safety and reliability of autonomous systems (e.g., vehicles).

Protection of ML assets such as data, ML model, and ML programs has been particularly explored at the system-level due to potential security breaches or leak of privacy-sensitive information during training and inference. This sparked the new field of **confidential ML** with many approaches and solutions [26].

Confidential ML computations notably build on **confidential computing** to protect data in use. Threats include privileged attacks when running applications on untrusted settings such as public clouds and the edge. Trusted Execution Environments (TEE) is a core security primitive to guarantee isolation. Hardware-assisted primitives may be combined with other system mechanisms such as containers, distributed sandboxes [27], library OSes, or other privacy-preserving schemes, either cryptographic (e.g., fully homomorphic encryption, secure multiparty computation) or perturbation-based (e.g., differential privacy).

The landscape of solutions includes multiple assets to protect, e.g., data (training, inference), the ML model (architecture, parameters), and the ML program (hyperparameters); multiple players, e.g., the data owner that provides the data, the cloud provider to run the ML service, and the program owner that owns the ML model; and multiple security goals, sometime hard to reconcile. Two broad situations should be distinguished: confidential ML over untrusted environments, and in multi-party settings.

Confidential ML in untrusted environments

By design, TEEs such as Intel SGX enclaves provide protection against unauthorized software access (or direct memory access) through hardware isolation based on memory encryption. Remote attestation allows to extend assumptions on the trustworthiness of the initial state of applications to remote parties. The TEE can provide a foundation for confidential ML (CML).

Two broad types of threats should be considered:

[3] https://artificialintelligenceact.eu/

- **Side-channel attacks (SCA):** several generic attacks may threaten isolation using controlled channels (e.g., syscalls, interrupts), micro-architectural side-channels, or memory bus side-channels and allow extracting memory access patterns or execution times from outside the TEE. For ML, this may enable to infer information from protected queries or on the ML model. Countermeasures include oblivious approaches such as [29] or careful ML algorithm redesign to reduce dependence of primitives on input data, but with significant performance penalties.

- **GPU vulnerabilities:** hardware accelerators are considered untrusted components and are thus not part of the Trusted Computing Base (TCB). Threats include insecure GPU-CPU communications or GPU side channels, for instance due to multi-tenancy which may allow to gather information about the ML model. Countermeasures include obfuscation with probabilistic verification of the computation results, or deploying a TEE on the GPU, with so far, no industrial implementation. Secure hypervisor approaches are also possible, but less secure.

Multi-party confidential ML

In the distributed case, parties are generally mutually distrusting, the attack surface is larger, and the desire for privacy even more acute. The TEE is no longer enough but should be combined with other privacy-preserving mechanisms, in the cloud and/or at the edge.

Two broad classes of scenarios may be distinguished.

- **Cloud-centred scenarios** include collaborative ML, where multiple data contributors collectively train a common ML model which may be protected using a trusted enclave and a privacy-preserving scheme. In multi-party ML-as-a-Service, different data contributors and model owners perform a joint computation. Distributed and controlled sandboxing of data processing services using a TEE allows to guarantee both ML model confidentiality and data protection [27].

- **Edge-centred scenarios** cover ML computing on edge devices, where the TEE may guarantee ML confidentiality. In federated ML settings, the TEE may allow to guarantee training integrity on the edge side, and confidentiality of gradient aggregation on the cloud side [30].

Yet, multiple engineering challenges remain to be addressed to reach trustworthy confidential ML. First, enclave memory limitations for ML workloads, which may be addressed by careful selection of the ML layers to protect, workload partitioning, or optimizing memory usage. Second, performance overheads, which may be reduced by limiting state transitions between in-enclave and out-of-enclave code. And third, the porting cost of using TEE with ML frameworks, which may somewhat be alleviated using containers [28].

2.3.4.3 Level of Trust or Trust Score

Despite trust is a human subjective concept, it is being used in IT scenarios since many years ago using certain type of organizations usually called authorities. For these authorities to work, the other players (i.e., users, providers, operators, etc.) need to accept them. This relationship model has been working and it worked until nowadays due to the fact that up until now, there were few players and they knew each other. With the future networks models in which the number of players will increase with new and many more players (i.e., operators, providers, certification authorities, etc.), it becomes necessary to have a common way to understand whether a player can be trustworthy or not, based only on statistics and objective data.

Several approaches can be mapped to define a generic Trust Score (TS) or Level of Trust (LoT), according to the scope of the requirements. There are several technical reports and standard entities defining how trust should be managed and generated among entities such as the ETSI Security and Trust guide for NFV [8], the CSA catalogue [13], the ISO 27000 standards [21], etc.

Specifically, ETSI in [8] describes the fact the trust depends on multiple aspects and pieces of information such as geographical location, date, software capabilities, etc. but the most important aspect is time. When relations (between people, entities, players, etc.) are not checked continuously over time, trust will gradually decrease.

For this reason, it is commonly accepted that trust needs to be re-evaluated and this re-evaluation should depend on multiple requirements such as confidentiality, intrusion resistance, integrity, security/vulnerability/risk assessments, resiliency, availability and others. To do so, the use of security functions (i.e., access control, certificates, encryption protocols, security/monitoring functions, resiliency mechanisms, etc.) will be of the most absolute importance and in order to monitor them, a set of associated metrics with a Service level Objective (SLO) are necessary. These metrics may be defined on a very high-level point of view such as the scale inspired by ETSI (i.e., Shall, Could, Must have, et.) or in a more detailed vision as presented in [13]. In any of the two cases, the usage of the full set of metrics probably involves the deployment of several enablers, each of them measuring a sub-set of the metrics. For this reason, a Trust Manager might be the key element to join all the measured metrics.

Based on the use of multiple metrics, trust might be computed. In fact, within the INSPIRE5G-plus project, one idea has been discussed in order to define a TS or LoT. This idea consisted on the fact that trust is generated based on the reputation of doing different actions. For example, the reputation to accomplish the expected SLA metrics (i.e., the provider's monitoring system works) or the reputation to deploy a requested service (i.e., the provider has no lack of resources).

Reputation allows to define/describe how good is a player/service/entity on doing a specific action. Due to the massive number of actions and aspects to be considered within the network resources management and services provisioning, a reputation value should be implemented to define how good is each resource/service provider at each action (i.e., deploying services, solving SLAs violations, using encryption techniques, etc.). So, a service/resource requester may evaluate the reputation on different aspects and decide which provider is better for its interests.

With the use of the reputation values (i.e., performance with respect to one or more metrics), a TS based on all the previously described reputation values could be the solution for any player to understand and see if another player can be trusted or not.

A first approach being studied within the INPSIRE5G-plus project is the use of a set of reputation values that are combined in a mathematical model to generate a single TS value. While the initial works do consider few actions (i.e., requests acceptance, deployment rate, SLA violation resolution rate), a further evolution of the TS should consider as many reputation values as possible based on both activated functions (i.e., access control, encryption protocols, etc.) and activated controls (i.e., confidentiality, integrity, etc.). By doing so, all the players could be sure that multiple aspects are considered.

The fact of having a single value allows to compare and classify the different entities and so, to define different LoT to identify which entities are more trustworthy with respect to the others on one or more actions or scenarios.

3 Key TSLA attributes mapped to Trustworthiness metrics

3.1 Methodological introduction

D4.2 investigates how the key TSLA detailed in section 2.2 can be refined into technical Trustworthiness attributes and further into technical KPIs that can be used for trust management. Again, Trust is first a subjective value given by the consumer of a service to the service provider. With the convergence of Telecommunication and Information Technologies, Trust evaluation is even more complex since we evolve in a multi-tenant, where the infrastructures are shared between different consumers, multi-party, where the underlying infrastructure is operated by different operators, and multi-domains where computing, storage and telecommunication are converging and dispatch across the infrastructure.

Therefore, the concept of Trustworthiness is complementary of this of Trust. Trustworthiness attributes correspond to technical attributes. These technical Trustworthiness Attributes are qualified by means of metrics. WP4 Trust enablers are worth implementing such metrics to measure and monitor Trustworthiness of the technical infrastructure at design-time and at run-time.

The following Figure 4 proposes an overview of the principles of the relationship between Trust Attributes, Trustworthiness Attributes and metrics. For a given service, Trust requirements are expressed by means of a Trust Service Level Agreement (TSLA), composed by several Trust Attributes. The management of these Attributes at Design-time and their monitoring at run-time is performed by means of Trustworthiness attributes, implemented by Trust enablers. These Trustworthiness attributes are associated with metrics which enable to give a value to the Trustworthiness Attribute. This value may be binary (yes or no), could fit in a scale with discretionary degrees, or get a continuous value (percentage, etc.).

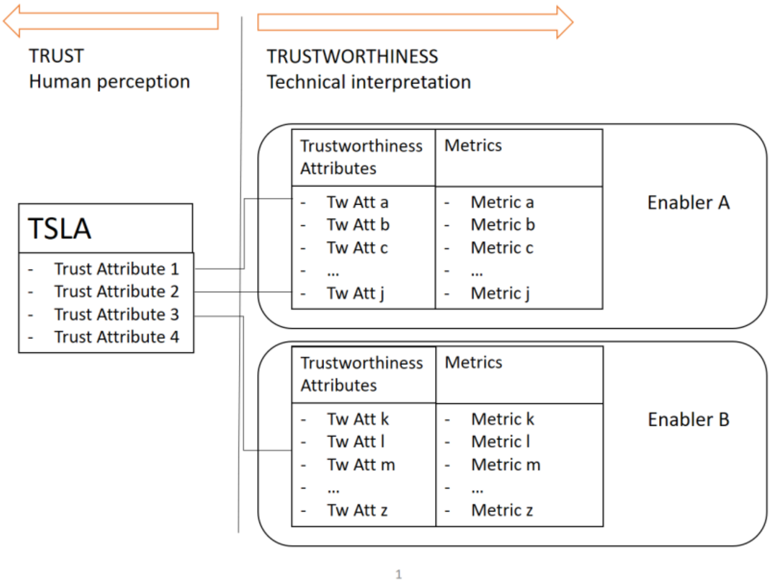


Figure 4: Principle of the relationship between Trust attributes, Trustworthiness attributes and metrics.

Section 3 proposes a top-down approach. Three key TSLA or Trust Attributes are extracted from the main TSLA typology since they seem emblematic of most of the cloud services concerns. To justify the choice of these three key TSLA, a brief review of the use cases has been conducted. Here is a synthetic report of this review. First, data protection is the first aspect of the data protection and privacy category. As soon as Data is produced or consumed, its integrity and confidentiality are at risk. Authentication of the source and access rights are involved. Further, some technical trust aspects are studied covering the data lifecycle when at storage, in process, and in transit. As second Trust Attribute to be investigated, Isolation has been picked up since it is a very typical technical aspect on which hangs the 5G slices. Slices concept has typically been developed to ensure the separation of communication services and software means dedicated to different multiple tenants, even if these services run over the top of a common infrastructure. Third and finally, Geolocation looks a key Trust Attribute to guaranty the legal aspects of data management practices of a world-wide, multi-providers infrastructure.

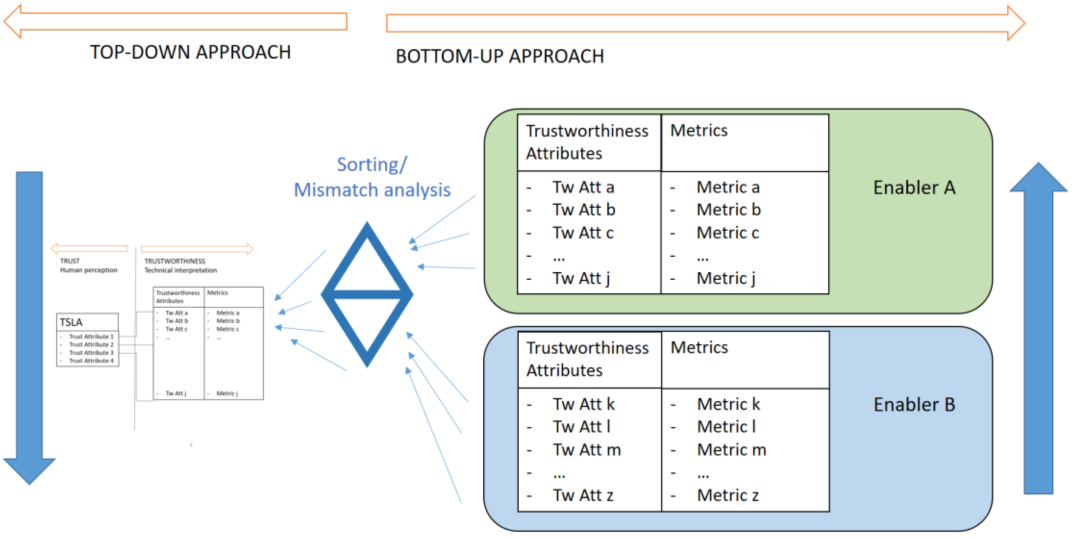
The following sub-sections investigate the mapping of the three key TSLA towards Trustworthiness Attributes. This is a theoretical top-down approach based on our knowledge of the state of art and related generic techniques to implement it. As a result, it provides, for each of the TSLA, a list of Trustworthiness Attributes. Each Trustworthiness Attribute is described by the following fields:

- a name;
- a description or definition;
- a metric, which tends to give a method of expressing a value; the metric may be composed by several KPIs;
- evidence for the metric, that is to say the technical means to read the value of the metric;
- a Trust enabler, or by default the component of the High-Level Architecture which would theoretically take in charge the Trustworthiness Attribute.

A synthetic table is given in the last sub-section of section 3 showing the three key TSLAs and their full description.

Section 4 analyses the Trust enablers to provide a bottom-up approach. Each Trust enabler is studied showing a focus on its insertion into the High-Level Architecture. Furthermore, a sequence diagram of the interaction of the Trust enabler towards the other architecture components is detailed, as well as a first list of Trustworthiness Attributes it supports.

Figure 5 below presents a picture of the methodological approach with the top-down approach on the left side, the bottom-up approach on the right side, bringing the need for a gap analysis represented by the sorting triangle.



Trustworthiness Attributes	Metrics
- Tw Att a - Tw Att b - Tw Att c - ... - Tw Att j	- Metric a - Metric b - Metric c - ... - Metric j

Trustworthiness Attributes	Metrics
- Tw Att k - Tw Att l - Tw Att m - ... - Tw Att z	- Metric k - Metric l - Metric m - ... - Metric z

Figure 5: Method: consolidation between the top-down and the bottom-up approaches.

Finally, Table 14 of the last sub-section of section 4 analyses the gaps between the top-down approach and the bottom-up approach.

3.2 Data protection

Data protection is the first Trust Attribute related to the Data protection and privacy main category. Several technical dimensions enable to better qualify different aspects of data protection. In order to trust a data, it seems important to check that its issuer is known; its issuer is tamper-resistant for the integrity of the source to be trustable; its issuer has a high reputation on the way they produce the data; the location of the source is known, so that no surprise can arise on the legal aspects applied to the data; information is given related to the freshness of the data; infrastructure preserves confidentiality and integrity at cold storage; it prevents dump; integrity and confidentiality of data are guaranteed in process; data copy is prevented; data integrity and confidentiality are guaranteed in transit.

These aspects are mapped to Trustworthiness Attributes associated to metric and evidences.

Known issuer: Received data was issued from known source and is integrated from its issuance. As a metric, a boolean states if a X509 certificate authenticating the issuer has been verified. Received data is verified at receipt before being used. Verification checks that the received data was issued by a known source and integrated from its issuance by use of authentication mechanism. The evidence is the verified certificate test boolean.

Tamper-resistant issuer: Received data has been produced by a tamper-resistant software. As a metric, a test states if an integrity check X509 certificate time-stamped and signed by an authenticated and trusted entity has been verified. As a KPI for this metric, the freshness of the integrity verification messages brings better information than a simple boolean. A run time integrity verification of the software which has generated the received data is produced. As evidence, the time tagged run time verification of the code is used.

High reputation source: Received data has been produced by high reputation node or software. The metric is defined by a centralized high reputation management third party implementing a reputation ranking method. The evidence is the score published by the centralized eReputation management service.

Located source: Received data comes from a validated node (location). Several metrics can be proposed as developed in the geolocation section. If the data source location is known, a X509 certificate can include the GPS location (metric) of the source and be produced as evidence

Freshness: Received data freshness. As evidence, a Trustable time-stamp can be produced. As metrics, the difference between the current date and time and the one from the time-stamp. An additional KPI relates to the verification of the certificate authority delivering the time-stamp.

Data confidentiality at cold storage: This can be achieved through data encryption. Metrics of the encryption are the following:
- encryption strength (algorithm, key size, post quantum...),
- management of encryption keys by (either the operator, the data issuer, a third party...)
- other operational considerations (ease use, easy management of keys, decryption latency, ...)
As evidence, a certificate with all the parameters can be produced.

Data integrity at cold storage: Several technical means can be deployed to guarantee data integrity at cold storage: 1/ storage access policy enforcement. 2/ Authentication mechanism on cold storage data. 3/ Non writeable disc partition 4/ Integrity certificate; etc. Metrics can be provided by the O.S. or Kernel. As evidence, a certificate with all the means deployed can be produced.

Data dump prevention: This relates to memory dump. Means can be enforced for memory pages not to be accessible, and thus dumped. Technical means can be deployed such as TEE placement or DRAM page dump prevention leveraged by embedded system OS.

Integrity and confidentiality of data in process: As of today, TEE are the most popular technical mechanisms to implement it. In the future, homomorphic processing will develop. The metric relies on system level to get the evidence of a TEE placement for data processing.

Data copy prevention: Data copy prevention on disc relies on system administration best practices such as disc partitioning, namespace, etc. Again, a certificate could be produced to list the means deployed at system level.

Data integrity and confidentiality in transit: Typical means to implement data integrity and confidentiality in transit is to implement encrypted channels such as IPSec or DTLS. Metrics are defined according to the following KPIs:

- robustness level of the cipher suites used,
- centralized cipher suite configuration,
- Key and initialisation vector (IV) length,
- Key refreshment policy.

Data criticality: This attribute has to be standardized in order and widely spread among the large public of data producers to indicate to which extent the data is critical. The same KPIs as in Disaster Recovery Plans should be used:

- Importance or value of the data: A full classification could be proposed such as state critical, organisational critical, personal important, personal casual, etc.
- Bearable interruption of the service: A value in time: 1 millisecond, 1 hour, 24 hours, 1 week, etc.
- Bearable loss of data: 1 second, 1 minute, 1 day, 1 week, etc.

3.3 Isolation

Isolation is a fundamental Trust Attribute in the context of 5G and slices. It expresses mainly the technical capability of the slice providers to ensure true sealing between the different services using the same infrastructure. The Trustworthiness Attributes associated to Isolation are the following:

Service level isolation: this is achieved at the level of service orchestration by coupling it with SLA policy management (affinity/anti-affinity, resources requirements, ...). A security orchestration can help support additional functions to provide sharper security definition in the SSLA requirements.

- Metric: Orchestrator based boards of running process per platform

Payload level isolation: this is achieved at the level of the VM Hypervisor to implement memory segregation or container-based isolation mechanisms. Metrics and evidences shall be provided by kernel (hypervisor of container layer).

- Metric: Isolation evidence-metrics by kernel (hypervisor of container layer)

Process level isolation: this is achieved at the level of the process by use of such mechanisms as TEE or OS memory segregation (RTOS).

- No direct evidence of the memory protection leverage

Isolation during Transit: finally, other mechanisms can rely on managing the path of the slice in order to enforce isolation. This is achieved at the level of the Software Defined Network (SDN) controller.

- Metric: Controller logs

3.4 Geolocation

The geolocation Trustworthiness attributes can be defined as follows:

Data stored in geographical area (e.g., European Community, country, data centre, platform).

- Metric: Auto-declarative and de-facto statement delivered by the service or infrastructure operator. No mathematically-proven evidence reflecting the location of the real data.

- The TSLA management shall receive and manage these elements.

Data transits in a geographical area (e.g., European Community, country, data centre, platform, and network device).

- Metric: Packets level processing telemetry in a network node in a specific geographical area. Telemetry data is used to validate with cryptographic algorithms that the packet cross the specific node. Info can be auto-declarative and de-facto statement delivered by the service or infrastructure operator or share the metrics for external validation if required.
- The TSLA management shall receive and manage these elements.

Data processed in geographical area (e.g., European Community, country, data centre, platform).

- Metric: Auto-declarative and de-facto statement delivered by the service or infrastructure operator. No mathematically-proven evidence reflecting where the data is actually processed.
- The TSLA management shall receive and manage these elements.

Remark: Encryption and the associated key distribution (in due location only included into a TEE) is the only mean to guarantee that the data is executed (in a decrypted form) at a given location. Refer to data protection section.

Code stored in geographical area (e.g., European Community, country, data centre, platform).

- Metric: Auto-declarative and de-facto statement delivered by the service or infrastructure operator. No mathematically-proven evidence reflecting where the data is actually processed. The code file shall be viewed as a data file.
- The TSLA management shall receive and manage these elements.

Code executed in geographical area (e.g., European Community, country, data centre, platform).

- Metric: Auto-declarative and de-facto statement delivered by the service or infrastructure operator. No mathematically-proven evidence reflecting where the data is actually processed.
- The TSLA management shall receive and manage these elements.

Two progresses related to the actual state of the art can be notified:

Shamir shared secret Proof of Transit establishes with cryptographically proven evidence that all pre-defined nodes (where known network functions are residing) have been traversed. The nodes geolocation is defined with the IP-MAC node address identification used for spawning the partial secrets in each of the nodes). Node impersonation attacks are still possible and consist in placing a node software in an arbitrary platform where introspection attack can be mounted.

A further progress delivering higher trustworthiness in the software location in a given platform can be attained by frustrating the above-mentioned migration of the software to an arbitrary node. For that, a solution consists in creating a semantic dependency on the software to a secret and the location of that secret into a pre-provisioned platform. DRM solutions (e.g., PC video game licence enforcement) employ such mechanism known as machine binding. The solidity of the link depends on the solidity of the link which associates the key and the machine as well as on the density of the semantic associations between the key and the software. Typically, one-off key use at software start is fragile as the code will be totally dumpable and migrable elsewhere from this initial stage. The ultimate scheme is to generate variants which are all semantically attached to a different secret which is pre-provisioned into one single machine’s TEE. This solution delivers certain levels of certainty that one software executes in one identified platform only. This solution can also provide cryptographically proven evidence that the code truly executes in this known platform.

3.5 Synthetic table

The following Table 2 provides a synthetic view of the Data Protection, Isolation and Geolocation Trust Attributes presented above. For each Trust Attribute, a list of Trustworthiness Attributes is associated, described by its name and description, as well as a metric and the type of evidence to collect them. Furthermore, the reference of a Trust enabler or a block in the High-Level Architecture is given.

Trust Attribute	Trust-worthiness attribute	Trustworthiness metric or KPI	Evidence	HLA component
Data Protection	**Known issuer:** Received data was issued from known source and is integrated from its issuance	X509 certificate of the issuer is verified. Received data is verified at receipt before being used. Verification checks that the received data was issued by a known source and integrated from its issuance by use of authentication mechanism).	Verified certificate test boolean	Security enablers Any PKI
	Tamper-resistant issuer: Received data has been produced by a tamper-resistant software	Integrity check X509 certificate time-stamped and signed by an authenticated and trusted entity. KPI: freshness of the integrity verification messages. A run time integrity verification of the software which has generated the received data is produced.	Time tagged run time verification of the code	Trust management CCT enabler
	High reputation source: Received data has been produced by high reputation node or software	Centralized third party High reputation score. Reputation ranking method	Score from the Centralized eReputation management	Trust management TRM and eTRM enablers
	Located source: Received data comes from a validated node (location)	X509 certificate including a GPS geolocation. The data source location is known. The location is associated and related to the public key delivered with the certificate. Other technique can be considered (e.g., IP address of the data emitting node)	Verified certificate including a GPS geolocation. Other means: IP address, other location and associated metrics	Trust management No existing INSPIRE-5Gplus enabler
	Freshness: Received data freshness	Trustable time-stamp – KPI : freshness of the data Age of the data (from its generation)		Security enablers No existing INSPIRE-5Gplus enabler
	Data confidentiality at cold storage	Data encryption – KPIs : - encryption strength (algorithm, key size, post quantum...), - management of encryption keys by (either the operator, the data issuer, a third party,...) - other operational considerations (ease use, easy management of keys, decryption latency, ...)	Certificate with all parameters How can we prove a data is trully encrypted? (by decrypted the encrypted data before authentication verification?, other means...?)	Security enablers No existing INSPIRE-5Gplus enabler

Trust Attribute	Trust-worthiness attribute	Trustworthiness metric or KPI	Evidence	HLA component
	Data integrity at cold storage (reminder: encryption does not strictly prevent the encrypted data to be tampered)	Deployment of data integrity means: 1/ storage access policy enforcement. 2/ Authentication mechanism on cold storage data. 3/ Non writeable disc partition? 4/ Integrity certificate	Certificate with all the means deployed O.S or kernel delivered metrics.	Security enablers No existing INSPIRE-5Gplus enabler
	Data dump prevention (memory)	TEE placement: Data pages cannot be accessed (then dumped). DRAM page dump prevention (leveraged in embedded system OS)		VNFI
	Integrity and confidentiality of data in process	Today ready Trusted Execution Environment. Future (+15 years) Homomorphic processing.	TEE placement.	Security enablers Trust management
	Data copy prevention (on disc)	System administration (disc partitioning, namespace, ...)		VNFI
	Data integrity and confidentiality in transit	Crypto algorithms Cipher suites profiles robustness level, centralized configuration, Key refreshment policy, Key and Initialisation vectors (IV) minimum length	Applying IPSec or DTLS.	Security enablers + Trust management
	Data Criticality	Importance or value of the data: a classification to be set-up Bearable interruption of the service: (in time) Bearable loss of data: (in time)	Availability Statistics Back-up frequencies	Policy and SSLA Management (Availability Management) Trust Management and TSLA Management
Isolation	**Service level isolation**	Orchestrator based SLA policy management (affinity/anti-affinity, resources requirements, ...)	Orchestrator based boards of running process per platform	MANO Security orchestrator
	Payload level isolation	Hypervisor (for VM) memory segregation or container-based isolation mechanisms	Isolation evidence-metrics by kernel (hypervisor of container layer)	MANO

Trust Attribute	Trust-worthiness attribute	Trustworthiness metric or KPI	Evidence	HLA component
	Process level isolation	TEE; OS memory segregation (RTOS)	No direct evidence of the memory protection leverage	VNFI
	Isolation during Transit	Controller-based slice-path isolation management	Controller logs	MANO
Geolocation	**Geolocation of data in storage**	Auto-declarative and de-facto statement delivered by the service or infrastructure operator.	No mathematically-proven evidence reflecting the location of the real data.	Trust Management TSLA Management
	Geolocation of data in transit	Packets level processing telemetry in a network node in a specific geographical area. Proof of transit: List of specific IPs or nodes where traffic is crossing over: The traffic goes over specific links and nodes (warning: PoT cannot block the traffic to pass over non-PoT nodes)	POT crypto evidence at recipient: Nodes involved and validation status Network telemetry (e.g. traceroute, int-band network telemetry, etc.)	Security enablers + Trust management TSLA Management Proof of transit
	Geolocation of data in process	Location of the processing (= node) Auto-declarative and de-facto statement delivered by the service or infrastructure operator.	Does TPM bring geo location? Process to machine binding delivering relative evidence. Alternative leveraging TEE-anchoring	Trust management TSLA Management
	Code stored in geographical area	Auto-declarative and de-facto statement delivered by the service or infrastructure operator.	The code file shall be viewed as a data file. No mathematically-proven evidence reflecting where the data is actually processed.	Trust management TSLA Management
	Code executed in geographical area	Auto-declarative and de-facto statement delivered by the service or infrastructure operator.	No mathematically-proven evidence reflecting where the data is actually processed.	Trust management TSLA Management

Table 2: Key Trust attributes

4 Trust Enablers status and mapping to the HLA

D2.2 [16] proposes a High-Level Architecture (HLA) to map all INSPIRE-5Gplus contributions in a common landscape.

D4.1 [17] provides an overview of the position of the Trust enablers in INSPIRE-5Gplus HLA.

This section provides a focus on the Trust Management block described in this HLA and the way it interacts with the other entities of the HLA.

Further, this section provides more details about the integration of the different Trust enablers in the way they interact with other entities of the HLA, and the way they can support Trustworthiness attributes to contribute to Trust Management.

4.1 High level description of the Trust Management block in the HLA

As 5G networks usually involve multiple operators and multiple tenants, the INSPIRE-5Gplus framework is composed by several service management domains. This enables the management of the assets at the level of each domain by means of a set of functional modules. Figure 6 below shows INSPIRE-5Gplus HAL schema. When it comes to security, each service management domain includes a *security management domain* (*SMD*), involving a set of modules, e.g. a Security Data Collector, a Security Analytics Engine, a Decision Engine, a Security orchestration, Policy and SSLA Management as well as Trust Management.

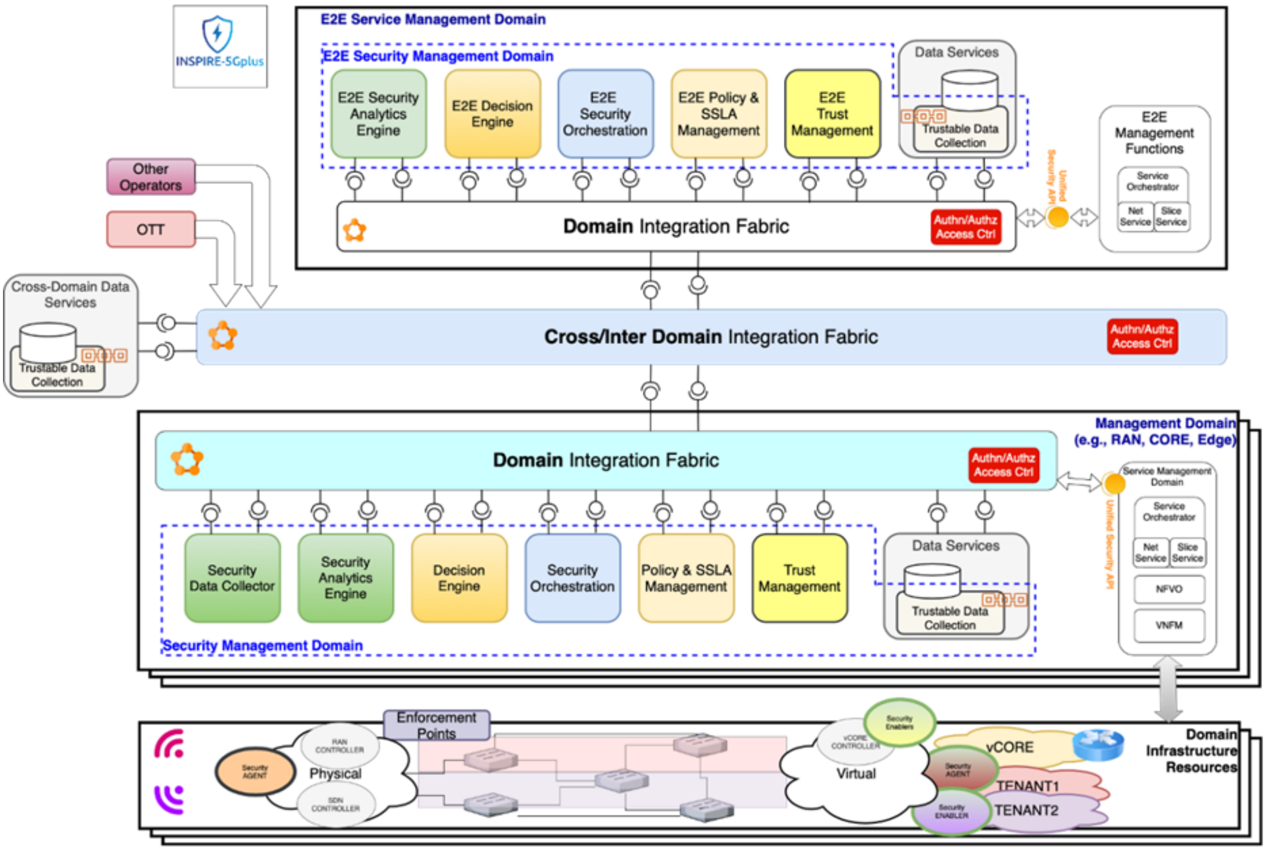


Figure 6: INSPIRE-5Gplus High-Level Architecture[4]

[4] D2.2 Figure 14

The various security management services provided by these modules are exposed within the same domain but also cross-domain through an *integration fabric*. The integration fabric provides a bridge between a given SMD with its Domain Integration Fabric, and a transverse SMD managing end-to-end policies between multiple SMDs by means of its Cross/Inter Domain Integration Fabric.

On both End-to-End SMD and the SMD of a given domain N, a yellow box represents Trust Management.

In this functional block, it is expected to fit the majority of all T4.2 Trust enablers which implement Trustworthiness Attributes to serve the management of Trust attributes.

D4.1 provides this mapping in Section 5, Figure 17 as reproduced below in Figure 7.

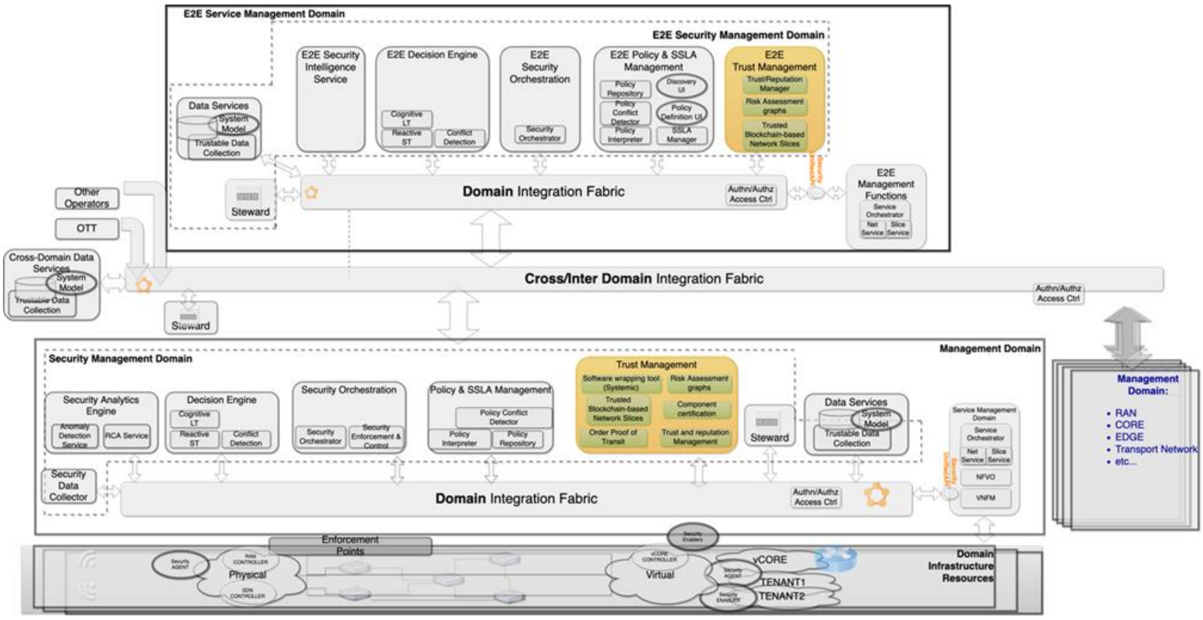


Figure 7: Trust in INSPIRE-5Gplus High Level Architecture (HLA)[5]

Probably the same pattern as for WP3 Security Management should be applied to Trust Management, even if the field is less mature for Trust. Mainly, security policies are deployed across the computing continuum of a 5G infrastructure by means of a chain of micro-services or enablers. These micro-services need to be configured and orchestrated to implement a given security policy. This requires mainly two components:

- A Security (and Trust) orchestrator to orchestrate the enablers. An end-to-end Security orchestrator orchestrates multi-domain, multi-operator policies, with a local relay in each domain.
- A Policy and SSLA (and Trust SLA) Management block enables to express policies as well as requirements by means of Security (and Trust) Service Level Agreement, and manages the compliance of the infrastructure towards the SLA.

Furthermore, one main challenge of the HLA is to meet the requirement of Zero Touch service Management (ZSM), bringing in the landscape other functional blocks such as a Security Data Collector, Security Analytics and Decision engine.

In this deliverable, all Trust enablers will be mapped to the HLA. This mapping will focus on the two entities presented above, answering the following questions:

[5] D4.1 Figure 17

- Is the enabler part of a simple SMD, or is it part of the End-to-End SMD? Does it fit to the Trust Management yellow box versus E2E Trust Management yellow box?
- Can the enabler be managed at the level of its domain? Does it have an interface to the Domain Integration Fabric?
- Can the enabler be involved in a multi-domain architecture? Can it be exposed to the Cross/Inter Domain Integration Fabric?
- Does the enabler support a Trust policy language which could be used to configure Trust policies? is it possible to trigger an update of the configuration of the enabler by means of the Security/Trust Orchestrator? is it possible to write a new Trust policy by means of the Policy and SSLA Management?
- Does the enabler support TSLA? Is it possible to evaluate the TSLA by means of the Policy and SSLA Management or by the Trust Management?
- Does the enabler implement the close loop, interacting with Security Data Collector, Security Analysis and Decision engine?
- What are the interactions of the enabler with other entities of the architecture?

4.2 Trust enablers status and mapping

This section gives an overview of the contribution of the Trust enablers in INSPIRE-5Gplus landscape. First the deliverable where to find the complete description of the enabler is referenced. Then, the interaction of the enabler is presented on the HLA big picture figure as in Table 6 or a focus on a part of it. To be more precise, an UML sequence diagram details the interaction with the main HLA components for Trust Management. Finally, for each enabler, an overview of the Trustworthiness attributes is presented.

Table 3 below gives the list of the Trust enablers.

Enabler Name	Owner	Latest published description
Systemic VNF Wrapper (SYSTEMIC)	TAGES	D4.1
Proof Of Transit (POT)	TID	D4.1
Component certification tool (CCT)	THALES	D4.1
eTRM: e-reputation management	ORA	D4.1
Network Slice Manager for Trusted Blockchain-based Network Slices (TBNS)	CTTC	D4.1
RAGs: Risk Assessment Graphs	ORA	D4.1
Trust Reputation Manager (TRM)	UMU	D4.1
Behavioural profile	UMU	MS8 (final description is presented in this deliverable)
DiscØvery	CLS	MS8

Table 3: List of T4.2 enablers.

4.2.1 Systemic VNF Wrapper (SYSTEMIC)

Systemic Wrapper detailed description is given in D4.1. Its design, objectives, limitations as well as the potential interactions and interfaces are provided.

Systemic is given to be a WP4 enabler, as it provides trust properties to a binary software. The trust properties can be viewed as security functions too, however.

The Figure 8 below shows the integration of Systemic wrapper into the Trust Management functional block. Security orchestration can order a binary wrapping order and interact directly with the Service management domain to collect the original binary image to create and load a protected variant.

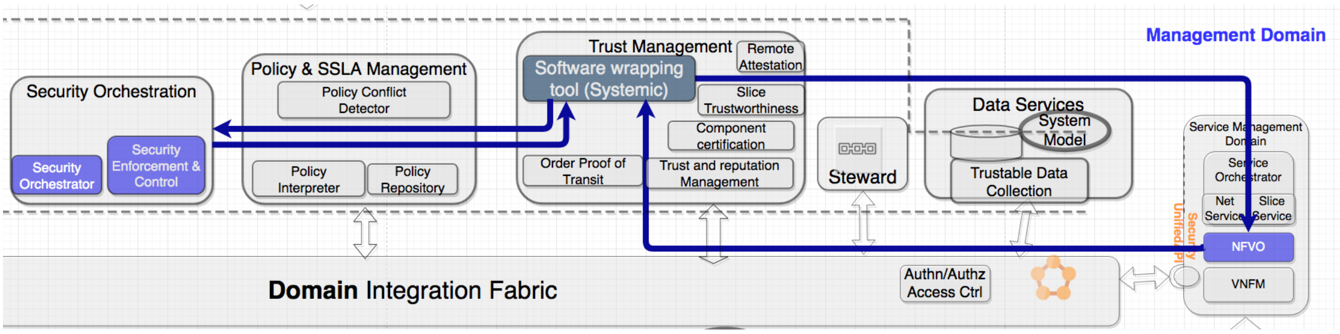


Figure 8: Systemic Software wrapping tool (Systemic) inside the HLA (and Trust Management functional bloc).

The Figure 9 below shows Systemic Sequence diagram.

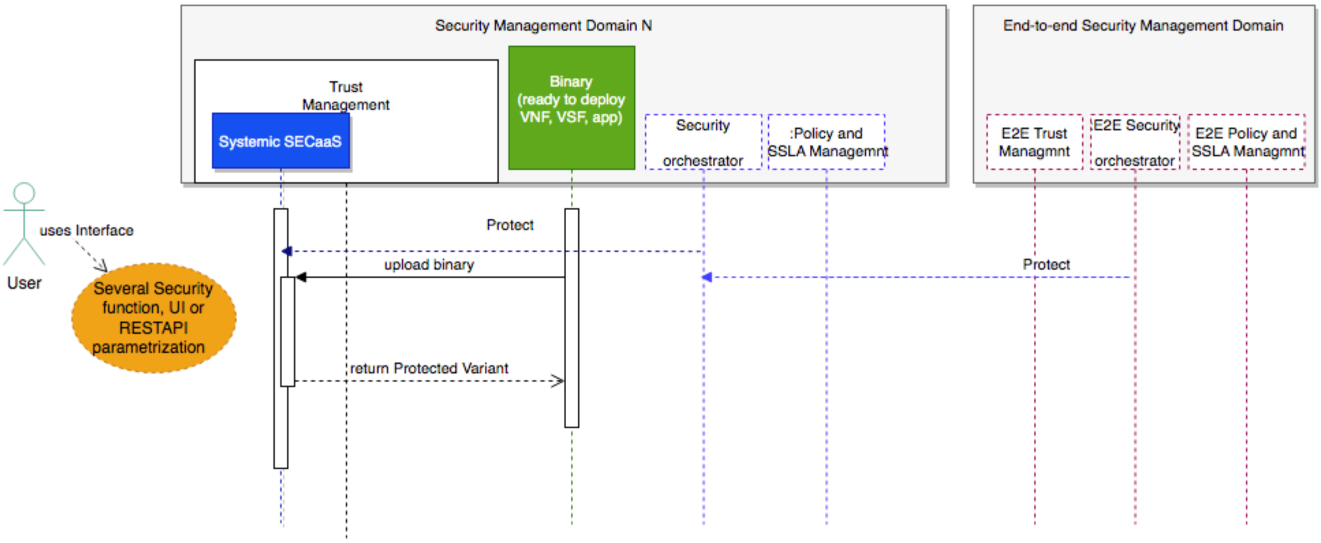

Security Management Domain N
Trust Management
Systemic SECaaS
Binary (ready to deploy VNF, VSF, app)
Security orchestrator
:Policy and SSLA Managemnt
End-to-end Security Management Domain
E2E Trust Managmnt
E2E Security orchestrator
E2E Policy and SSLA Managmnt
User
uses Interface
Several Security function, UI or RESTAPI parametrization
Protect
upload binary
return Protected Variant
Protect

Figure 9: Systemic SECaaS sequence diagram.

Trustworthiness attributes implemented by the enabler

The Table 4 below presents the Trustworthiness attributes implemented by the enabler.

Trustworthiness Attribute	Trustworthiness Metric (TM) and KPI	Evidence	Related Trust SLA Attribute
Code is confidential at cold storage (stored software image). Binary text section encryption.	TM: Encryption strength (AES 256) KPIs: -Easy deployment of the key -Easy wrapping of the code	Metadata from Systemic (attesting the enforcement)	**Cyber Security**
Code is protected in confidentiality (partially-obfuscation)	No TM: Obfuscation is a non-standardized activity. KPIs: -Easy protection set-up -Assessed conversion (i.e., efficiency/performance loss ratio)	Metadata from Systemic (attesting the enforcement)	**Cyber Security**

Trustworthiness Attribute	Trustworthiness Metric (TM) and KPI	Evidence	Related Trust SLA Attribute
Code authentication at load. (Implementation using TPM, using TEE, without hardware anchoring)	TM: Asymmetric encryption strength. -Software deployment workflow (e.g., need for hardware provisions) -Easy deployment of the public key -Easy protection set-up	Measurement, verification by verifier for TPM based scheme Metadata from Systemic self-authentication scheme	**Cyber Security**
Code integrity is checked during execution	TM: Memory page integrity periodic verification KPI: -Surface or scope of the check (partial or full program footprint in memory) -Frequency of the checks -Easy protection setup	Metadata from Systemic, attesting the enforcement	**Cyber Security**
Code is licensed (i.e., used with right)	No TM: DRM is a non-standardized activity. The strength of the use right enforcement varies with the technology used. KPIs: -Easy protection and activation workflow -Easy workflow for software activation method -Assessed conversion ratio (i.e.,solidity of the enforcement and performance loss)	Code will not launch in environments or conditions not fulfilling the rights verification.	**Cyber Security**
Code is geolocated (executes at a specific machine)	No TM: Software geolocation is a non-standardized activity. The strength of the platform binding varies with the technology used. KPIs: -Easy protection and activation workflow of the hosting machine (provisioning of secret). -Assessed strength ratio (i.e., solidity of the binding between the code and the machine)	Code will not launch in one machine or a set of machines which is/are not provisioned for that execution.	**Geolocation**
Code integrity by use of TEE	TM: Encryption strength of the program page (used by TEE)	Natively, it is not possible to know if the code runs inside a TEE	**Cyber Security**

Table 4: Systemic VNF Wrapper Trustworthiness attributes.

4.2.2 Proof Of Transit (PoT)

Description:

Proof of Transit (PoT) as it is described in D4.1 provides a cryptographic mechanism to verify that network traffic is crossing over a specific list of network nodes. Also, when we refer to Ordered PoT or oPoT, we are considering that the data path must follow a specific order. The trust foundation of this tool is provided by the result of the calculation aggregating the information of each node to centralized controller that generates the information needed to evaluate if the data path is compliant with the expected one.

Enabler in HLA big picture

The integration approach is shown in Figure 10 at a high level. The oPoT Controller, considered part of the Trust Management component, interacts with the Security Orchestrator and Policy & SSLA Management in order to define the specific list of nodes (i.e., the topology) and request the enforcement of the data path verification. After this, the policy framework defines the configuration and the oPoT enforcement is activated through the oPoT controller over each of the nodes (agents) in the network. Each agent starts to report telemetry information. The metrics collected by the oPoT controller are shared with the Trust and Reputation Manager in order to make the trust level calculations.

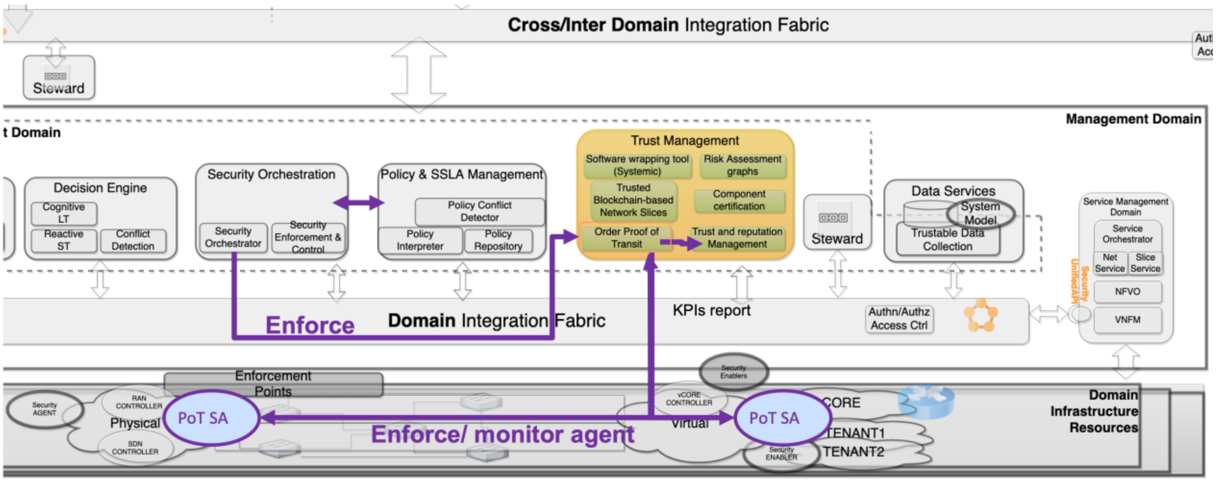


Figure 10: Proof of Transit insertion in the HLA

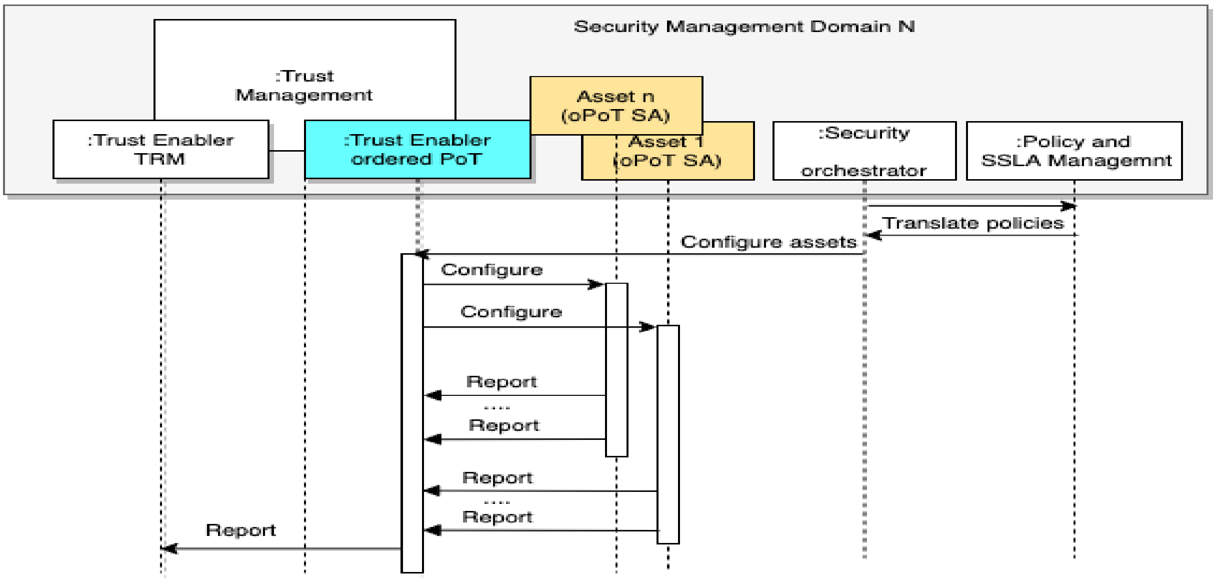


Figure 11: Proof of Transit Sequence diagram.

Figure 11 presents the sequence diagram. When the Security Orchestrator requests the configuration of the trust measurement for data paths in one Domain, the oPoT Controller triggers a configuration for each of the nodes or assets that it has been defined for the data path. Each asset has a Security Agent (SA) that makes validations and reports the values calculated to the oPoT Controller periodically. This report is detailed in D4.1, but includes metrics for Trust calculation. This information is delivered to the TRM component in case of failures (verification error), alerting that the path has been altered and the trust scores for the domain must be updated.

Trustworthiness attributes implemented by the enabler

The Table 5 below presents the Trustworthiness attributes implemented by the enabler.

Trustworthiness Attribute	Trustworthiness metric and KPI	Evidence	Related Trust SLA Attribute
Geolocation of data in transit	List of specific nodes where traffic is crossing over. KPI: nodes IP list includes the ones expected	Validation status with timestamp associated to each node.	Geolocation

Table 5: Proof of Transit Trustworthiness attributes.

4.2.3 Component certification tool (CCT)

Description: D4.1

CCT evaluates trustworthiness properties of a component and publishes a certified list of them for the end user or an automatic SSLA Management process to be able to select the appropriate chain of components to deliver a service. The trustworthiness properties are published under the format of a certificate.

Enabler in HLA big picture

CCT can be viewed either as a standalone tool or as a component in the chain of VNF or slice Management. Its objective is to analyse the integrity and security attributes of a VNF or another digital object such as a slice, and to produce a Digital Trustworthy Certificate embedding all the security attributes of the object. These properties are described according to an ontology, enabling any management tool to poll and sort the VNF according to their security properties. This is a step in the VNF orchestration and chaining, for the central Security Orchestration or Trust Orchestration to select the adequate chain of VNF to provide a service according to Security Service Level Agreement (SSLA) or Trust Services Level Agreement (TSLA).

Figure 12 below shows how the CCT can be either used standalone with a direct interaction with the NFVO from the Management domain, or used in the context of the HLA through the link between the Trust Management and the Security Orchestration. In case of the use of Service Level Agreement concept to handle Trust, according to the architecture, this may be handled by a single tool within the SSLA Management.

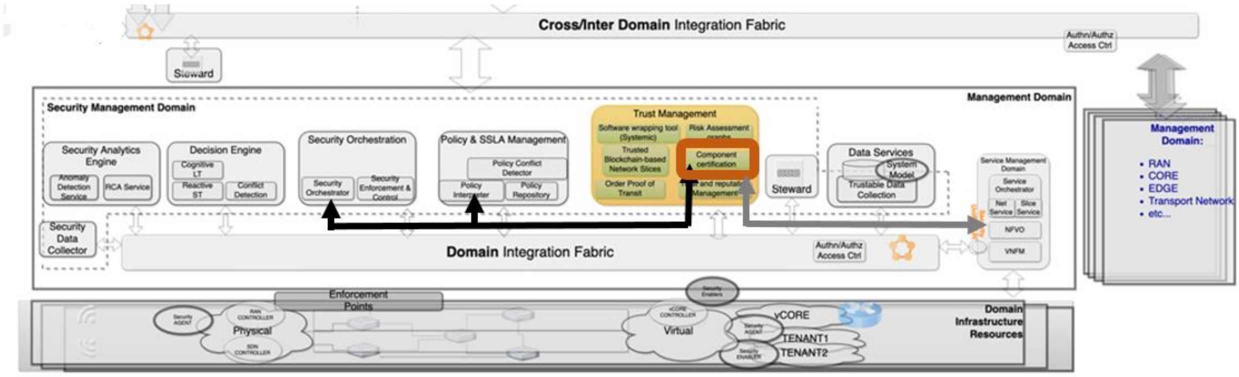


Figure 12: CCT in the HLA big picture.

UML sequence diagram

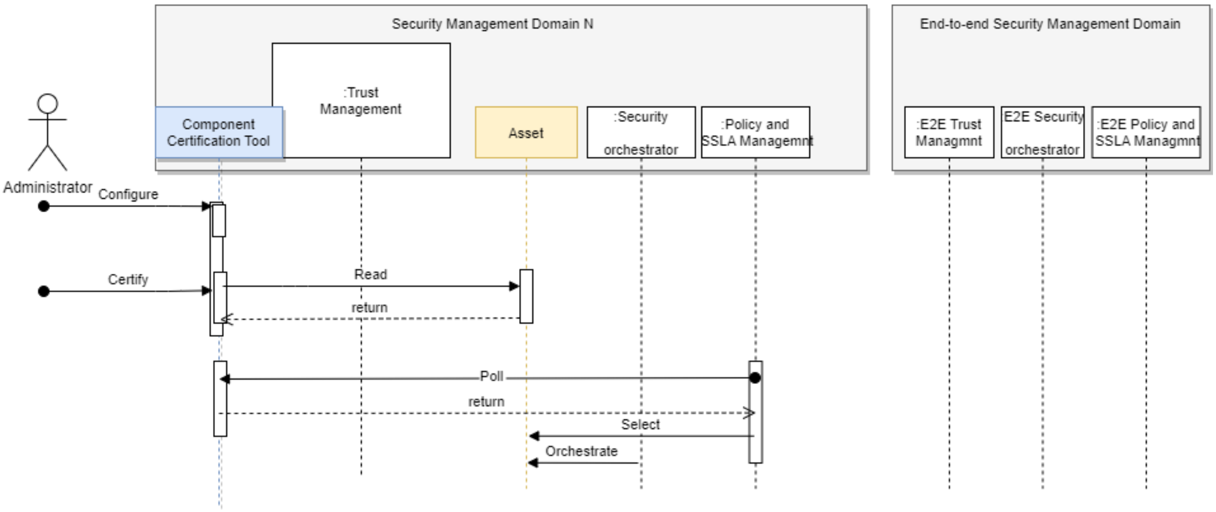

Security Management Domain N
End-to-end Security Management Domain
:Trust Management
Component Certification Tool
Asset
:Security orchestrator
:Policy and SSLA Managemnt
:E2E Trust Managmnt
E2E Security orchestrator
:E2E Policy and SSLA Managmnt
Administrator
Configure
Certify
Read
return
Poll
return
Select
Orchestrate

Figure 13: CCT Sequence diagram.

The unitary sequence diagram for the CCT is shown in Figure 13. An administrator configures the Trust Attributes to be considered in the certification. This depends on the asset to be certified, a VNF, a slice, etc. Then the certification itself is launched. The CCT checks the Trust attributes of the Asset and returns whether they are fulfilled or not. The certificate is then calculated embedding all the results of the CCT control towards the different attributes. A digital signature is appended to guarantee the declaration.

When a service is required to the Policy and SSLA Management, it polls the Component Certification Tool's repository to find within the list of certificates the one corresponding to the most appropriate component or asset according to the security properties listed in the certificates. Then it passes its selection to the Security Orchestrator for it to orchestrate the service.

Trustworthiness attributes implemented by the enabler

The Table 6 below presents the Trustworthiness attributes which could be supported by the enabler.

Trustworthiness Attribute	Trustworthiness metric and KPI	Evidence	Related Trust SLA Attribute
Verified code May relate to Tamper resistant	Integrity check certificate time-stamped and signed by an authenticated and trusted entity	Time tagged run time verification of the code	Cyber Security May relate to Data protection

Trustworthiness Attribute	Trustworthiness metric and KPI	Evidence	Related Trust SLA Attribute
issuer	to guaranty that the code has been verified. KPI: freshness of the integrity verification messages.		
Policy Management	takes two values: Fully policy based VNF or Not policy based VNF	Manual	Usability
Integrity	No modification has been performed on the code of the VNF or on its control flow.	Needs an integrity routine to report	Cyber Security
Secure boot and secure crash	Integrity and source check certificate	Certificate	Cyber Security
Data protection and Privacy	Ensures that the VNF uses protection mechanisms such as secure data storage, access control, etc.	Manual	Data protection and privacy
Patch Management	Date of the last update	Version of the last patch	Maintainability
Migration operations	takes values: No live migration supported Live migration supported Migration partially supported Other migration mechanisms	Manual	Portability
Location awareness	This property describes dependencies of the VNF or some of its components on a position in the topology or geography.	Manual	Portability Geolocation

Table 6: Component Certification Tool Trustworthiness attributes.

4.2.4 e-reputation management (eTRM)

Description: D4.1

The TRM service, inside the Trust Management block, is in charge of assigning trust and reputation values to the corresponding monitored 5G entities, for instance, VNF like Access and Mobility Management Functions (AMFs), User Plane Functions (UPFs) or Authentication Server Functions (AUSFs), nodes, infrastructure, etc., using historical data and monitoring data. To provide the resulting scores to security management entities and end users in 5G virtualized networks, enablers should periodically publish their current status/information in Kafka. Then, TRM will collect data from Kafka and compute the Trust Score of the given entity.

Overall enabler description and interactions within the HLA (High-Level Architecture)

Figure 14 shows the interaction of the eTRM enabler, embedded inside the security management domain. Its purpose is to ensure softwarized and SDN based networks are reliable and trustable. The TRM enabler will interact, through the Integration Fabric mostly via pub/sub services, with the entities from which it has to obtain data (to calculate the trust value), such as SSLAs and Security Data Collector as well as with E2E Trust Manager and with the Blockchain (Steward). The latter is required to calculate the requested trust value, as it is obtained from the execution of a Smart Contract. The enabler's obtained values, as well as the computed trust scores will be stored in a database for further historical post-processing.

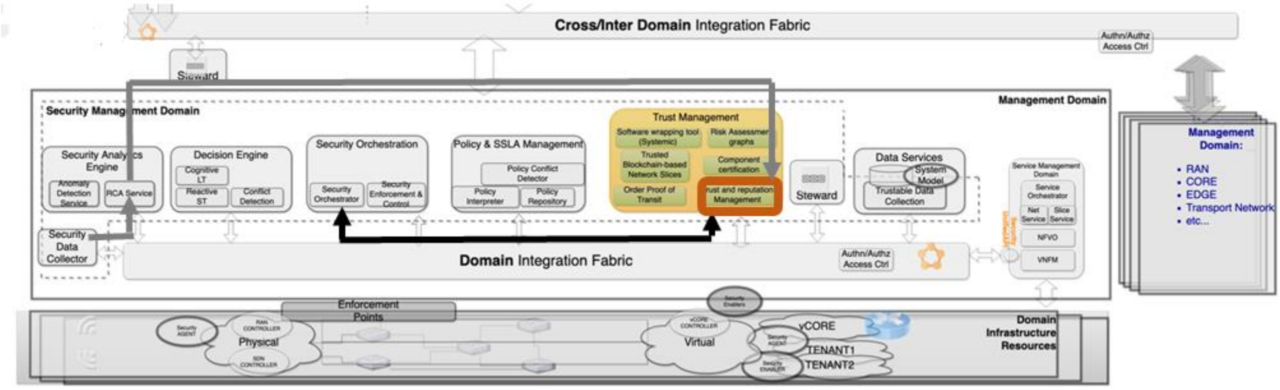


Figure 14: eTRM enabler within the HLA.

UML sequence diagram

Figure 15 shows the corresponding sequence diagram concerning the eTRM. The eTRM depends on the Root Cause Analysis enabler, as the RCA enabler provided it with the updated network topology in the shape of network graph updated with the fault probabilities computed by means of Machine Learning (ML). In turn, it sends that information to the eTRM which will convert those probability values to reputation ones to be send to the Security orchestration.

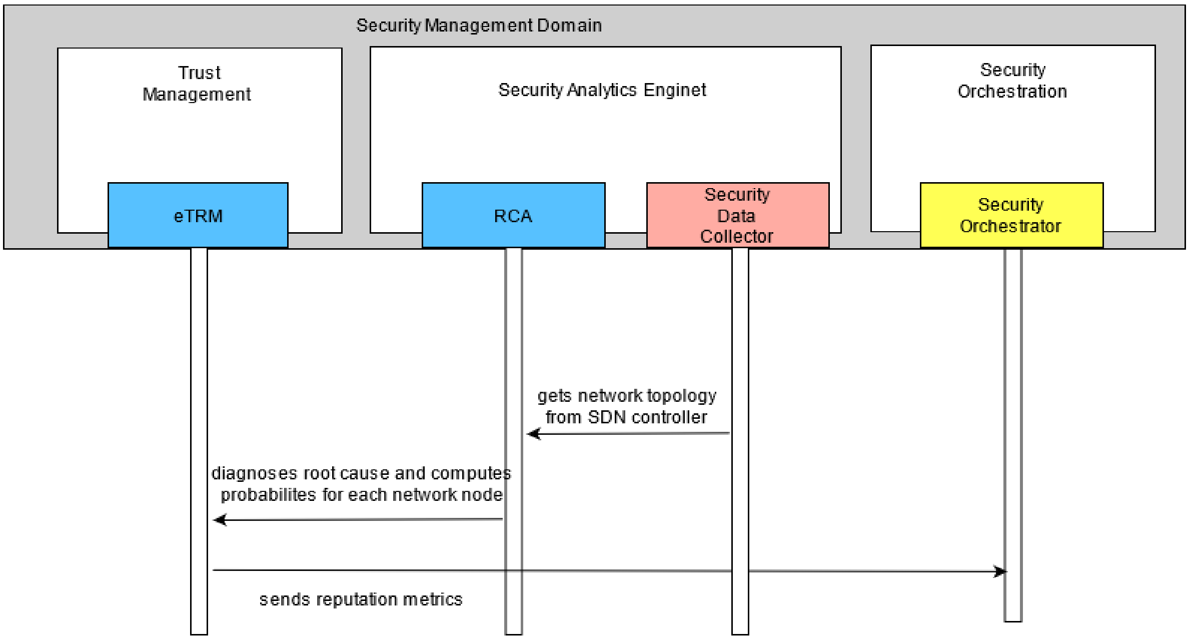

Security Management Domain
Trust Management
Security Analytics Enginet
Security Orchestration
eTRM
RCA
Security Data Collector
Security Orchestrator
gets network topology from SDN controller
diagnoses root cause and computes probabilites for each network node
sends reputation metrics

Figure 15: Sequence diagram for the enabler eTRM.

Trustworthiness attributes implemented by the enabler

Table 7 below presents the Trustworthiness attributes implemented by the eTRM enabler.

Trustworthiness Attribute	Trustworthiness metric and KPI	Evidence	Related Trust SLA Attribute
VNF security	Trust Score Security Service Level Agreement (SSLA) enforcement The reputation values and the probability of fault values are known security and resilience indicators	Data available in any accepted peer.	Data Integrity
Data protection	No Trustworthiness metric	The exposed topological information is only exchanged between RCA and eTRM and security data collector	Data Integrity

Table 7: e-reputation management Trustworthiness attributes.

4.2.5 Trusted Blockchain-based Network Slices (TBNS)

Description:

As described in D4.1 [17], the Trusted Blockchain-based network Slices (TBNS) provides a collaborative solution to deploy and manage Network Slice resources across different domains. The use of Permissioned Distributed Ledger (PDL) technologies such as Blockchain allows to share, store and distribute information among multiple peers (i.e., nodes) in an automatic, transparent, reliable and immutable way.

Enabler in HLA big picture

As illustrated in Figure 16, the TBNS enabler is placed in all the domains because of its use of the Blockchain technology. Its purpose is to ensure the shared knowledge of all the Network Slice Templates available in the different domains in order to compose an E2E Network Slice with them as described in [17].

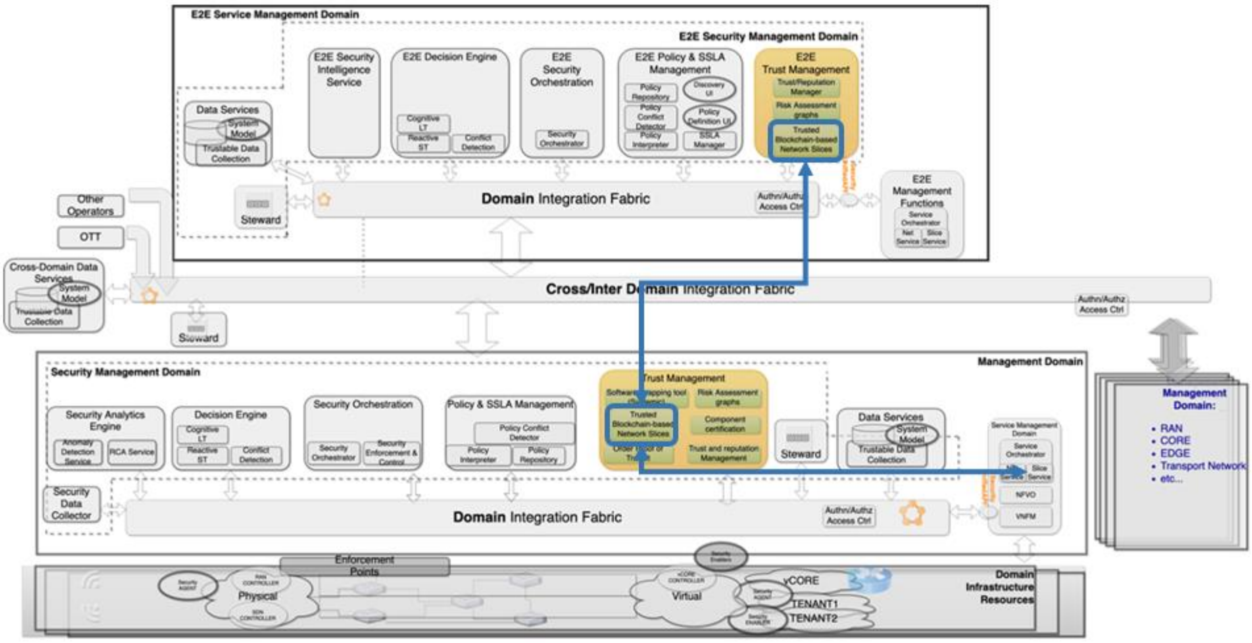


Figure 16: TBNS enabler within the HLA.

UML sequence diagram

Figure 17 shows the basic work-flow of how the multiple TBNS peers interact among them. When a request to deploy an E2E Network Slice (i.e., based on one or more domain Network Slice Templates (NSTs) arrives in the E2E domain, the TBNS in that domain distributes a Blockchain event to all the other peers (the TBNSs in the lower SMDs). Then, only the owner of each domain NST takes the specific event and manages it by requesting its local Network Slice Manager/MANO to deploy the corresponding NST. And once done, the domain TBNS is informed about the deployment result. Finally, the domain TBNS generates a new event to be distributed to all the Blockchain peers in order to store the updated information regarding each NST deployment involved in the requested E2E Network Slice.

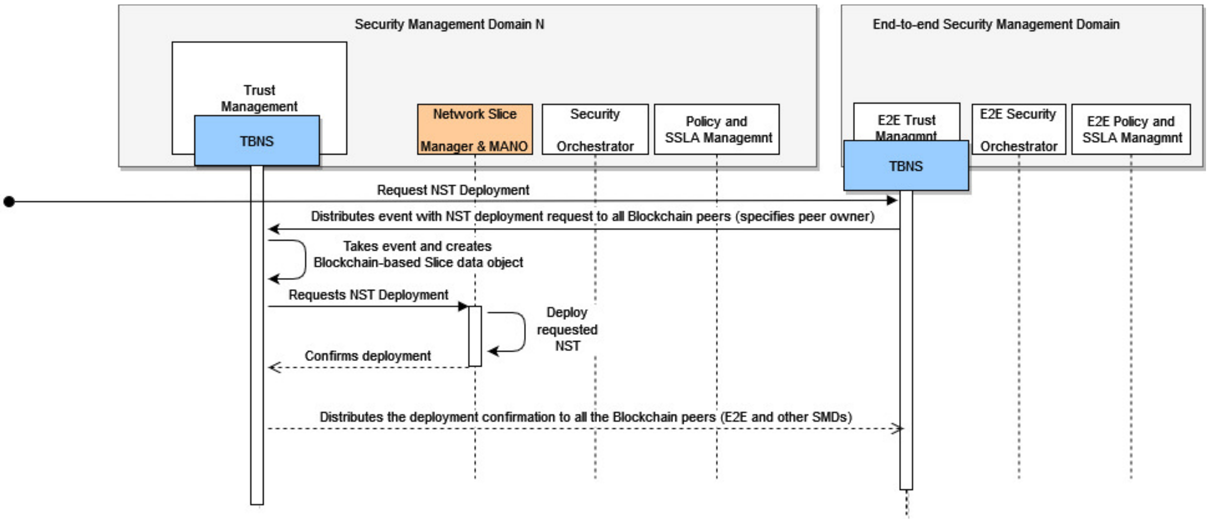

Security Management Domain N
Trust Management
TBNS
Network Slice Manager & MANO
Security Orchestrator
Policy and SSLA Managemnt
End-to-end Security Management Domain
E2E Trust Managmnt
TBNS
E2E Security Orchestrator
E2E Policy and SSLA Managmnt
Request NST Deployment
Distributes event with NST deployment request to all Blockchain peers (specifies peer owner)
Takes event and creates Blockchain-based Slice data object
Requests NST Deployment
Deploy requested NST
Confirms deployment
Distributes the deployment confirmation to all the Blockchain peers (E2E and other SMDs)

Figure 17: TBNS Interaction within the HLA.

Trustworthiness attributes implemented by the enabler

The Table 8 below presents the Trustworthiness attributes implemented by the enabler.

Trustworthiness Attribute	Trustworthiness metric and KPI	Evidence	Related Trust SLA Attribute
Transparency	No TM: Transparency is one of the main characteristics of Blockchain.	Data available in any accepted peer.	Data Integrity
Resistance against tampering	No TM: Data tampering is one of the main characteristics of Blockchain.	The linkage based on hash values between one block of data and the previous one.	Data Integrity
Data stored by consensus	No TM: Consensus protocols are one of the main tools Blockchain needs to work.	Based on the initial Blockchain configuration where the consensus is selected.	Data Integrity Data protection

Table 8: TBNS enabler Trustworthiness attributes.

4.2.6 Risk Assessment Graphs (RAGs)

Enabler in HLA big picture

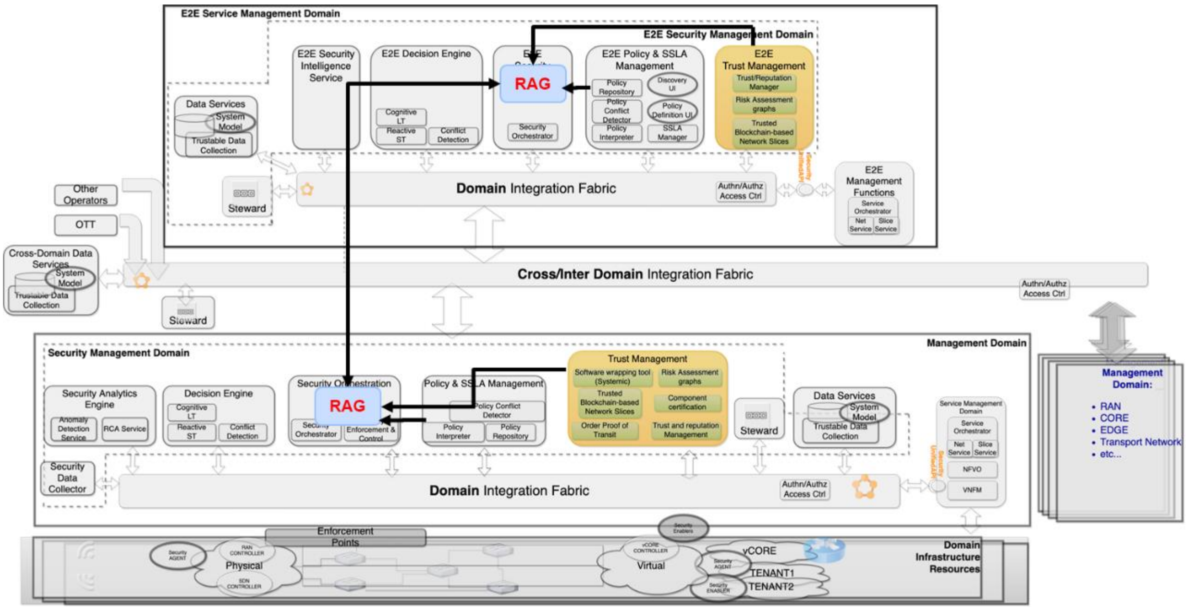


Figure 18: RAG enabler within the HLA

Figure 18 presents the description of the RAG enabler within the HLA:

- RAG – RAG: hierarchical interaction between several vision of topologies.
- RAG – Trust Management: collection of targeted security levels per sub-domain.
- RAG – Security Orchestrator: optimized placement strategy (for Vertical's VNF and counter measures) with respect to Policy, SSLA and trust management constraints.
- RAG – Policy and SSLA management: topology of connectivity between components and available countermeasures at this level of topology.

UML sequence diagram

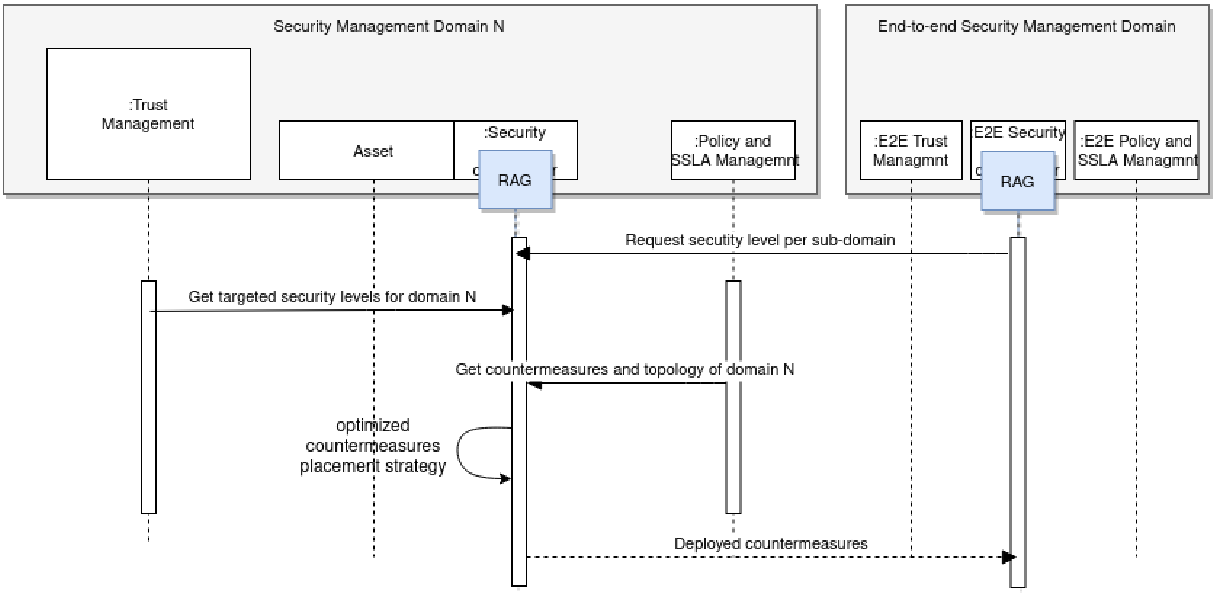

Security Management Domain N
End-to-end Security Management Domain
:Trust Management
Asset
:Security
RAG
:Policy and SSLA Managemnt
:E2E Trust Managmnt
E2E Security
RAG
:E2E Policy and SSLA Managmnt
Request secutity level per sub-domain
Get targeted security levels for domain N
Get countermeasures and topology of domain N
optimized countermeasures placement strategy
Deployed countermeasures

Figure 19: Sequence diagram for the enabler RAG.

Figure 19 presents the sequence diagram for the RAG enabler. At end-to-end level, a request may be initiated to poll the security level at the sub-domain level. Within a domain, the Trust Management gets targeted security levels from RAG. The Policy and SSLA Management on its side gets countermeasures and topology of the domain. RAG computes optimized countermeasures placement strategy and advertises the deployed countermeasures to the end-to-end Management Domain.

Trustworthiness attributes implemented by the enabler

Table 9 below presents the Trustworthiness attributes implemented by the enabler.

Trustworthiness Attribute	Trustworthiness metric and KPI	Evidence	Related Trust SLA Attribute
Network topology verification	Mean Time to Resolve	Time to deliver the topology verification	Network Management
Service composition	Mean Time to Resolve	Time to serve one user request for secure end-to-end service creation	Service Management

Table 9: Risk Assessment Graph Trustworthiness attributes.

4.2.7 Trust Reputation Manager (TRM)

Description: D4.1 The Trust and Reputation Manager mechanism has been designed and implemented to calculate the trust score of a cloud infrastructure, specifically the services and domains deployed on it, based on multiple values for both the infrastructure and the services. This trust score computation and value is stored as a transaction into the DLT deployed for that end by means of Smart Contracts. In this way, the trust values of the enablers and domains involved in the infrastructure remain immutable and can be access when required.

Enabler in HLA big picture

TRM is a WP4 enabler, as it computes and provides a trust score value of the entities belonging to the infrastructure. Figure 20 shows the integration of the TRM into the Trust Management functional block. The TRM will retrieve enabler's information provided through the Integration Fabric in order to compute a given entity trust score. Then, any enabler can directly request a trust score value from a given entity to the TRM. All this enabler information and computation of the trust score are stored as transactions in the Blockchain deployed for this purpose.

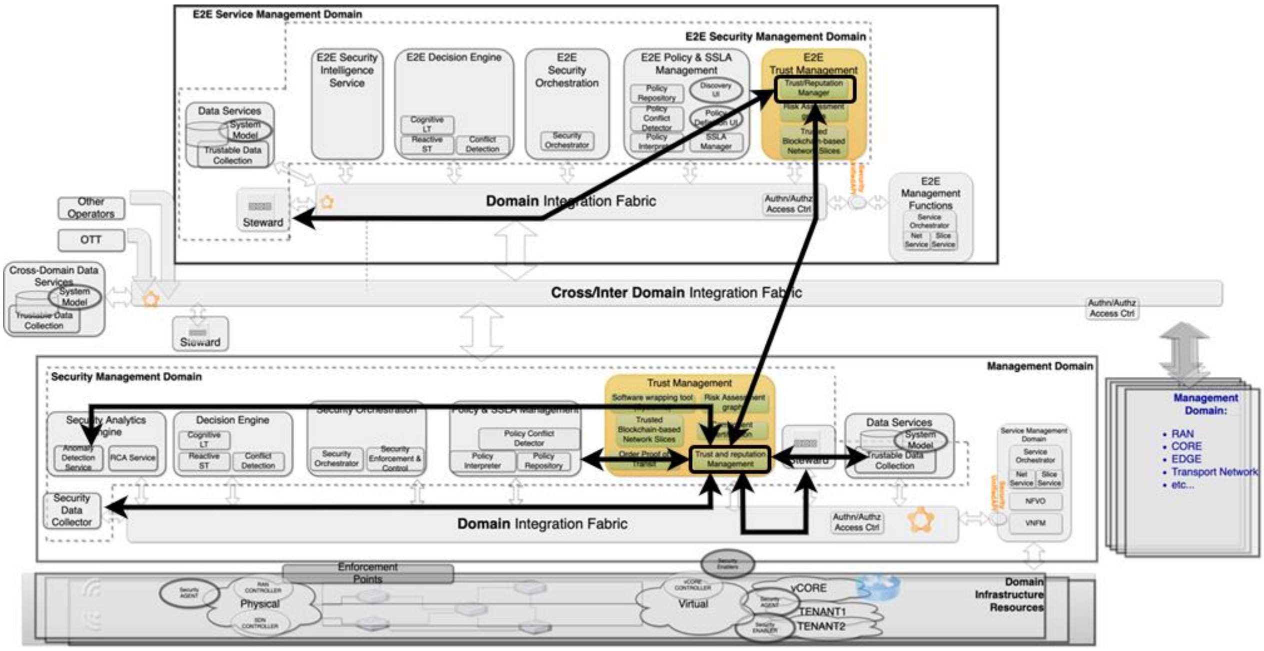


Figure 20: TRM enabler within the HLA.

UML sequence diagram

Figure 21 shows TRM sequence diagram:

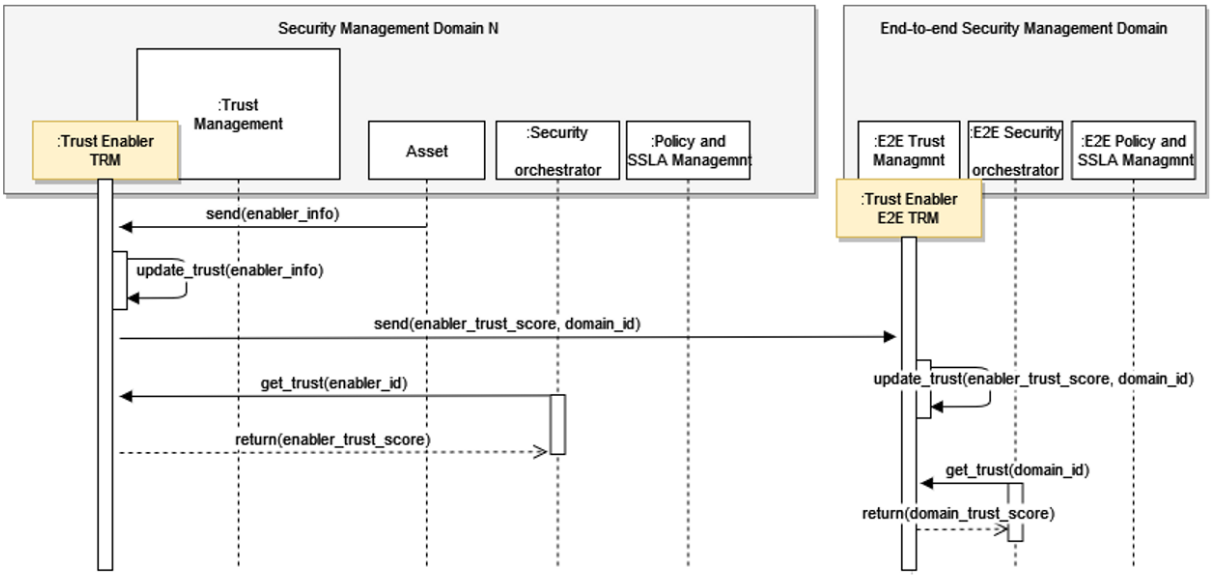

Security Management Domain N
:Trust Management
:Trust Enabler TRM
Asset
:Security orchestrator
:Policy and SSLA Managemnt
End-to-end Security Management Domain
:E2E Trust Managmnt
:E2E Security orchestrator
:E2E Policy and SSLA Managmnt
:Trust Enabler E2E TRM
send(enabler_info)
update_trust(enabler_info)
send(enabler_trust_score, domain_id)
get_trust(enabler_id)
return(enabler_trust_score)
update_trust(enabler_trust_score, domain_id)
get_trust(domain_id)
return(domain_trust_score)

Figure 21: Sequence diagram of the TRM enabler.

To provide the trust scores of the different enablers to security management entities and other end users in INSPIRE-5GPlus deployment, enablers should first publish relevant information through the Integration Fabric, using a publication/subscription mechanism that allows the TRM to subscribe to these publications. Then, the TRM receives the subscribed data through the Fabric. All this gathered information is fed into the computation of trust function in order to compute an updated trust value. After that, the enablers' obtained values, together with the computed trust scores are stored in a Blockchain for further historical post-processing. Finally, any interested enabler may request the value of trust of a given 5G entity. For that end, the TRM relies on an API Rest also provided through the Integration Fabric to allow enablers to make direct requests. It is important to note, that the TRM also provides each enabler's updated trust score to the E2E TRM which will compute, partially based on that enabler trust score, the total domain trust score. This domain trust score can be later provided to other domains that wish to deploy similar entities.

Trustworthiness attributes implemented by the enabler

Table 10 below presents the Trustworthiness attributes implemented by the enabler.

Trustworthiness Attribute	Trustworthiness metric and KPI	Evidence	Related Trust SLA Attribute
High reputation source: Received data has been produced by high reputation node or software	Centralized third party High reputation score. Reputation ranking method. KPI: enabler trust score and/or domain trust score. Value between [0,1].	Score from the TRM	Data protection
Freshness: Received data freshness	Trustable time-stamp – KPI: freshness of the data	Time-stamp	Data protection

	Age of the data (from its generation)		

Table 10: Trust Reputation manager Trustworthiness attributes.

4.2.8 Behavioural profile

Description: D4.2 in the sections below.

a. Description of problems and challenges

This enabler was not previously described in D4.1, thus, in the following sections there will be not only an introduction but a more extensive and detailed explanation of the enabler and its capabilities.

In the race for the connectivity, we have more and more devices that are connected to the Internet, invading our daily life. This fact has been specially emphasized since the appearance of the IoT. Whereas in 2019 the number of connected devices reached the 26.66 billion, some predictions expect a high growth in the next years, reaching the 74.44 billions of devices in 2025 [1]. In particular, one of the most well-known attacks was the Mirai IoT Botnet [2], in October 2016, when millions of IoT devices (e.g., cameras or digital video recorders) were compromised with the aim of executing a distributed denial of service (DDoS) attack against platforms such as Spotify or Amazon. This caused the interruption of services and therefore significant monetary losses. This attack has been evolved through a large number of variations.

To address such security concerns, there is a need to define approaches to reduce the attack surface of the interconnected devices. Beyond the use of traditional cryptographic and access control techniques, the security aspects of interconnected systems should be properly managed through a governance approach to ensure that systems behave as expected. However, the specification and enforcement of such aspects can be challenging in environments where a huge number of devices have the ability to communicate with each other and, sometimes, without the explicit consent of their owners. To address this issue, the Manufacturer Usage Description (MUD) [3] is an Internet Engineering Task Force (IETF) standard aimed to define the intended behaviour of the device through Access Control Lists (ACLs), in order to restrict the communication to/from a certain device. MUD defines an architecture for obtaining MUD files wherein those policies are specified by using the Yet Another Next Generation (YANG) and JavaScript Object Notation (JSON) standards. While MUD was recently standardised (March 2019), it has received a strong interest from the research community and standardisation entities worldwide. The USA National Institute of Standards and Technology (NIST) has also recommended MUD files to complement security credentials in order to reduce the attack surface [4]. In this sense, some authors [5][6] have patented two different usages of MUD files. On the one hand, MUD files are used to deliver policy requirements for a device joining the network, and then translated to network access specific policies. On the other hand, MUD files are collected during the bootstrapping process (in this case, while Extensible Authentication Protocol (EAP) is running) in order to obtain the security policies before the device has access to the network. They also explain that it is possible to obtain the correct MUD file without the MUD URL, through other content included in the authentication request. In other cases, authors [7] go a step forward, developing a method for automatically generating the MUD file from traces of the network, and checking later the compatibility of these policies with the organizational policy.

MUD is focused on the definition of network access control policies. Therefore, these restrictions can be straightforwardly enforced through the Software-Defined Networking (SDN) paradigm, as already proposed in [8]. However, beyond aspects of the network level, the MUD semantics does not provide the possibility of defining security properties to provide a more fine-grained approach that determines how IoT devices should communicate.

As we can observe, one of the main limitations of MUD file are the poor expressiveness they have, since they are only able to specify access control policies at network level. These types of policies are insufficient to establish enough countermeasures. In addition, the generation of the MUD file is still based on the manufacturer recommendations or in minor observations about the traffic, instead of being based on an objective security assessment process. Finally, there is no integration between the different phases of the MUD file management for a general environment.

b. Description of the solution

As reviewed, MUD file presents a wide used format to specify the behaviour of a system or component with the aim of limiting the attack surface of an ICT system. It provides a standardized way to express that behaviour, so it can be shared among the different stakeholders involved in the life-cycle of the ICT system.

Trying to cope with the limits of the MUD, this enabler links the security evaluation and certification methodology developed in the ARMOUR project [9] with the specification of policies using the MUD file, leading to its objective generation, based on real results, and extending the usage of MUD files to express configuration policies aiming to lead with encountered flaws. In addition, the MUD model has been extended to provide a higher expressiveness, allowing to specify different types of policies (e.g., channel protection, authorization, network access and data protection).

On the one hand, the derivation of security policies from the assessment ensures an objective and verified treatment process, whereas on the other hand, the generation of a behaviour profile from the assessment process during the manufacturing copes with the difficulty of secure a system without a risk measure reference once it is installed in the real network in which it will be operating.

Finally, this enabler also integrates the enforcement of the extended profiles within the bootstrapping of a device using Extensible Authentication Protocol with Authentication, Authorization and Accounting (EAP-AAA), in a way the configuration is enforced before the device has access to the network. This approach guarantees the security not only of the device, but also of the whole network. As the MUD model has been extended, new enforcement mechanisms arise as a need. Towards this end, this enabler considers the usage of Concise Binary Object Representation (CBOR) web tokens to enforce authorization, SDNs to enforce network access, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for data protection and direct configuration for channel protection.

c. In addition to extending the MUD model with flexible policy language to express additional aspects such as privacy, channel protection or SDN, the resultant approach introduces the use of DLT (Blockchain) technologies to share device information across different authorized users and devices. This allows the application of accountability and data provenance in IoT scenarios that combined with Ciphertext-Policy Attribute-Based Encryption (CP-ABE) schemes, which uses an attribute-based policy to encrypt data, so that only devices or users satisfying this policy will decrypt such data, can increase the characteristics of privacy-preservation. Current status and future developments
d. TRL4: Proof of concept development available and validated at a low scale. Interfaces specification

MUD does not provide interfaces for this project.

Enabler Behavioural profile in HLA big picture

Figure 22 presents the Behavioural profile enabler (MUD) within the HLA big picture. The idea behind this mechanism is to collect the standard MUD file. For that, an external device willing to access the network previously sends its associated MUD Uniform Resource Locator (URL), which has been in turn received at the MUD Manager, which is part of the security orchestrator, to restrict the device communications. The MUD Manager obtains through the Integration Fabric both the MUD file and the MUD file signature from the MUD File Server using the received MUD URL.

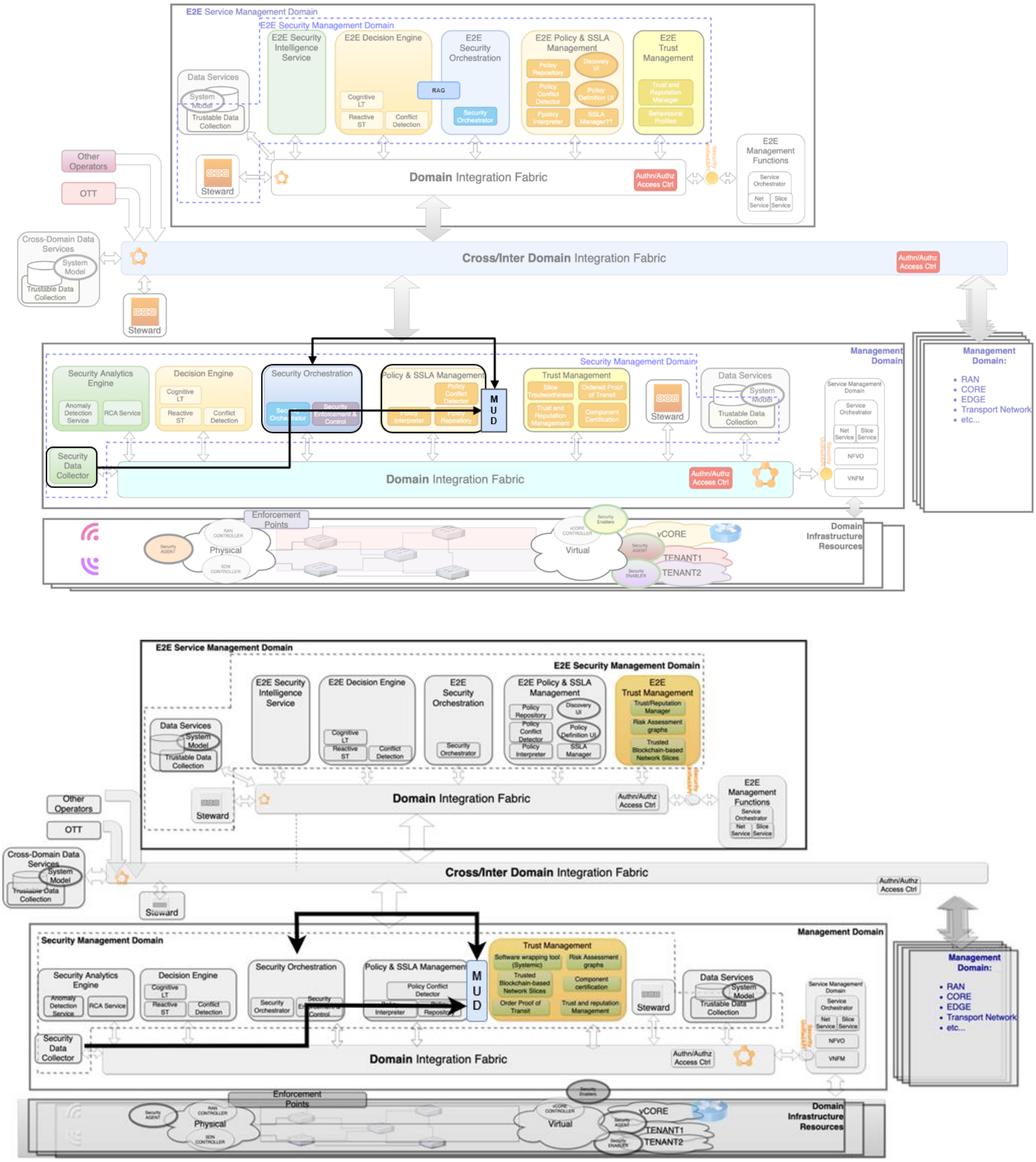


Figure 22: MUD (Behavioural Profile) file within the HLA.

UML sequence diagram

Figure 23 shows MUD sequence diagram:

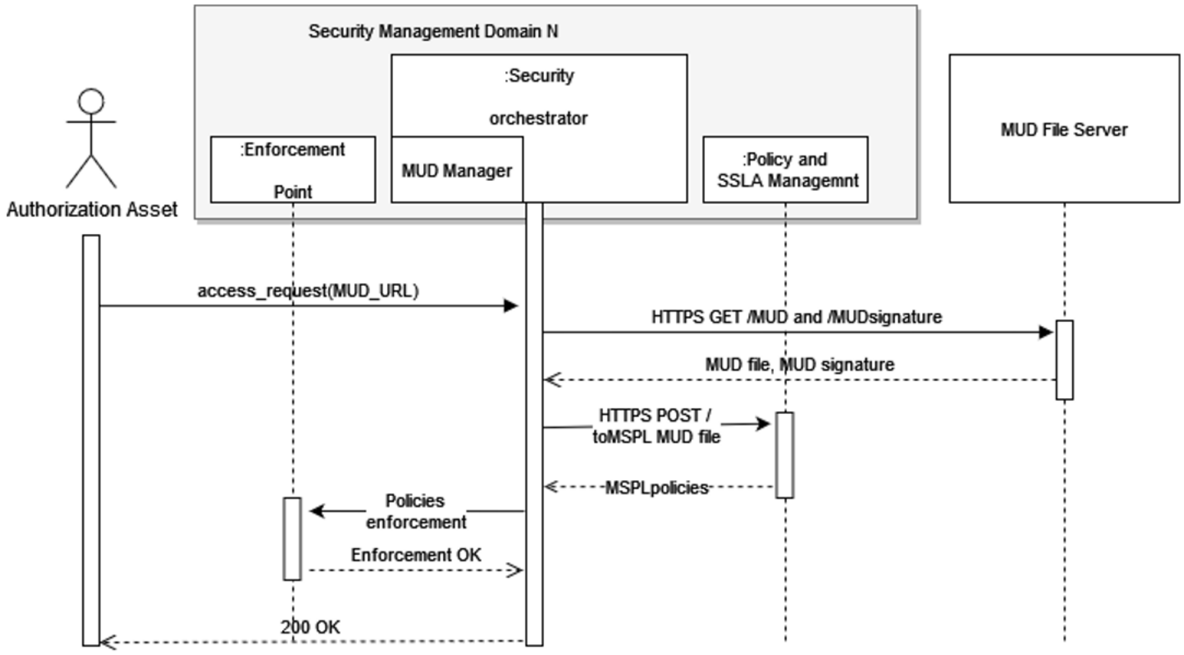


Figure 23: MUD sequence diagram.

In the first place, we assume that an external device willing to access the network sends its associated MUD URL, which has been in turn received at the MUD Manager (as part of the security orchestrator) through an Authorization Asset to restrict the device communications. The MUD Manager asks through the Integration Fabric for both the MUD file and the MUD file signature to the MUD File Server using the MUD URL.

Then, a Policy Interpreter translates MUD policies to MSPL intermediate language. Finally, The Security Orchestrator enforces the new configuration.

Trustworthiness attributes implemented by the enabler

The Table 11 below presents the Trustworthiness attributes implemented by the enabler.

Trustworthiness Attribute	Trustworthiness metric and KPI	Evidence	Related Trust SLA Attribute
Known issuer: Received data was issued from known source and is integrated from its issuance	X509 certificate of the issuer is verified. Received data is verified at receipt before being used. Verification checks that the received data was issued by a known source and integrated from its issuance by use of authentication mechanism).	Verified certificate test boolean	Data protection

Table 11: Behavioural profile Trustworthiness attributes.

4.2.9 DiscØvery

Description: MS8

DiscØvery is a network security analysis tool for IoT and 5G systems and networks. DiscØvery uses a domain-specific language to express systems based on their unique requirements. Models created by DiscØvery are dynamic and evolve based on input by users or software agents. A security engineer will be able to define assets of the system that protect, identify threats and vulnerabilities, get security insights on how to improve security and privacy, in a software-aided analysis. The aims of the software aided security analysis are to 1) augment the expertise of a security analyst; 2) detect network and system threats in complex distributed environments; 3) remotely and automatically identify hardware, software, and even policy-related vulnerabilities; 4) provision of tailored reports (DiscØvery's cyber-insights), which are suggestions based on the unique characteristics of a system; 5) holistic visualization of the complete threat landscape, including the people, the systems, the networks, and the associated policies.

Enabler in HLA big picture

As shown in Figure 24 DiscØvery is an enabler of the E2E Policy and SSLA Management of the INSPIRE-5Gplus HLA. However, DiscØvery's modeling language supports the use of concepts that express trust and risk. The trust and risk concepts can enhance the automated security analysis process of the enabler with additional insights related to improving trust and mitigating risk.

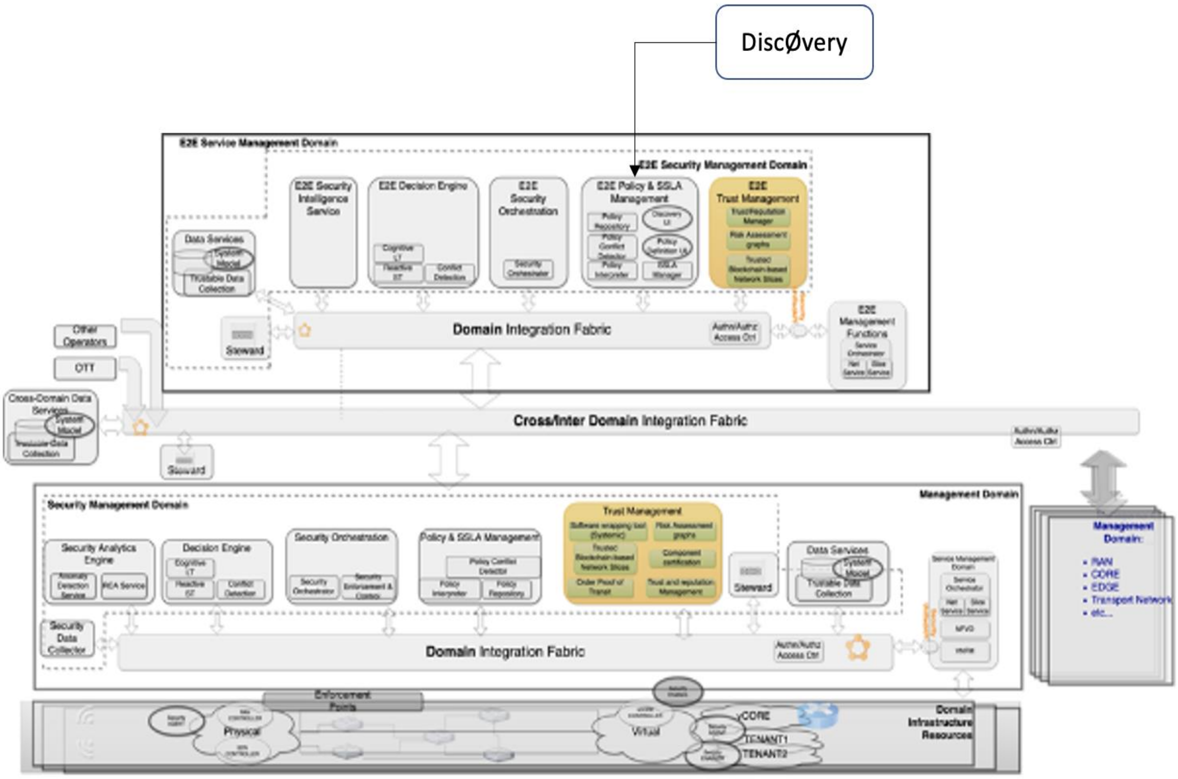


Figure 24: DiscØvery in the HLA

UML sequence diagram

Figure 25: DiscØvery sequence diagram. shows DiscØvery sequence diagram. DiscØvery gathers system data from the assets of the network and analyses them to provide cyber security insights. The cyber security insights are used to produce the final of security posture report of network.

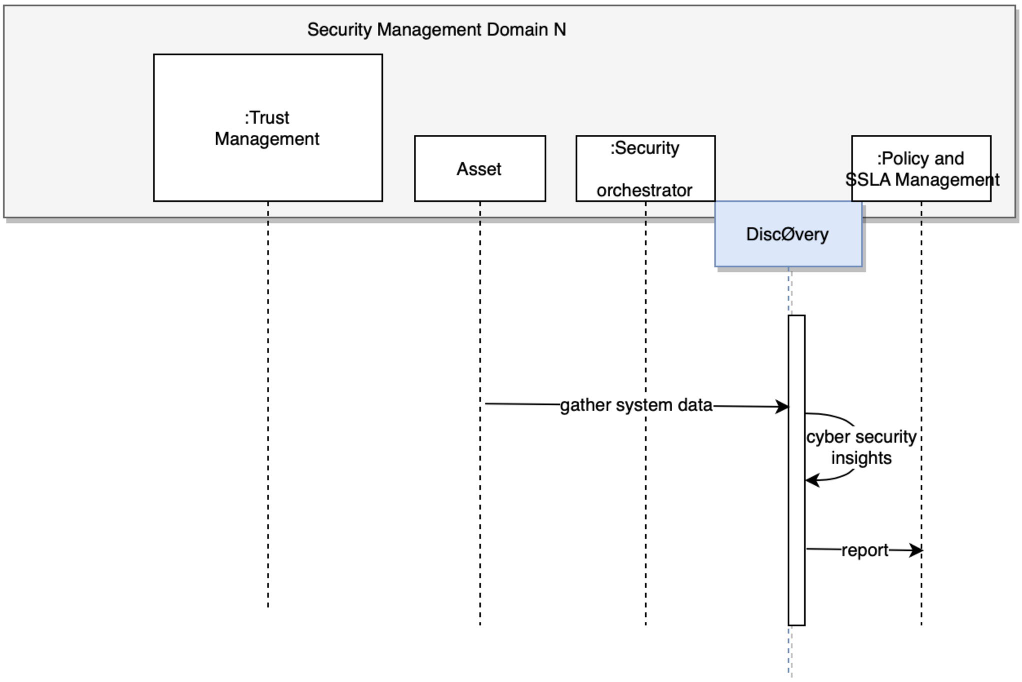


Figure 25: DiscØvery sequence diagram.

Trustworthiness attributes implemented by the enabler

The Table 12 below presents the Trustworthiness attributes implemented by the enabler.

Trustworthiness Attribute	Trustworthiness metric and KPI	Evidence	Related Trust SLA Attribute
Network Topology verification	Identify which network assets are trusted and do not introduce additional risk to the network.	DiscØvery's cyber-security insights that provide suggestions to improve trust and reduce risk.	Network Management

Table 12: DiscØvery Trustworthiness attributes.

4.2.10 General Mapping between the Trust enablers and key TSLA

First, within the list of Trust enablers, a wide spectrum of TSLA is covered. In Table 13 below, parenthesis are indicated when the enabler covers part of the Trustworthiness attributes that are already listed in the Top-down approach. Also, all the key TSLA are covered by one or more Trust enablers. Other main TSLA are mentioned in the table, reporting the main tendency of the Trust enablers.

Enabler WP4	Data Protection	Isolation	Geo-location	Network Management	Cyber-security	VNF security	Service Management
Systemic VNF Wrapper (TAGES)	(x)					x	

Proof of Transit (TID)			x	x			
Component Certification Tool (TSG)	(x)	(x)				x	
eTRM Reputation Management (ORA)	(x)					x	
TBBNS Network Slice Manager (CTTC)							x
RAG Risk Assessment Graph (ORA)				x			x
Trust Reputation Manager (UMU)	(x)					x	
Behavorial profile (UMU)	(x)					x	
DiscØvery (CLS)				x			
Other enablers (not T4.2)							
Manifest (ORA)	(x)	(x)	(x)	x			x
Deep Attest protocol (ORA)			x			x	
RCA (MI)					x		

Table 13: General mapping between Trust enablers and Key TSLAs.

Nevertheless, few gaps are revealed between the top-down approach and the bottom-up approach. In order to ease further work, Table 14 recapitulates the discrepancies revealed by the bottom-up approach. Table 14 is organised by TSLA. For each Trustworthiness Attribute which has not already been listed in the synthetic Table 2 of TSLA, Table 14 analyses if the Trustworthiness Attributes is either:

- Additional TSLA: meaning that the Trustworthiness Attribute hangs on a Trust Attribute which is not part of the Key TSLA,
- Complementary; the Trustworthiness Attribute relates to one key TSLA but is not listed yet. It is complementary to the initial list.
- Similar; the Trustworthiness Attribute is similar to a Trustworthiness Attribute already listed in Table 2.

Trust SLA Attribute	Trustworthiness Attribute	Enabler	Status	Comment
Cyber Security	Code is confidential at cold storage	Systemic VNF Wrapper	Additional TSLA	
Cyber Security	Code is protected in confidentiality	Systemic VNF Wrapper	Additional TSLA	
Cyber Security	Code authentication at load	Systemic VNF Wrapper	Additional TSLA	
Cyber Security	Code integrity is checked during execution	Systemic VNF Wrapper	Additional TSLA	
Cyber Security	Code is licensed	Systemic VNF Wrapper	Additional TSLA	
Cyber Security	Code integrity by use of TEE	Systemic VNF Wrapper	Additional TSLA	
Cyber Security	Verified code	CCT	Additional TSLA	May be related to Data

Trust SLA Attribute	Trustworthiness Attribute	Enabler	Status	Comment
				Protection/Tamper resistant issuer
Cyber Security	Integrity	CCT	Similar	Similar to Systemic Code integrity is checked during execution
Cyber Security	Secure boot and secure crash	CCT	Additional TSLA	
Data protection	Data stored by consensus	TBNS	Complementary	
Data protection and privacy	Data protection and privacy	CCT	Similar To be detailed	Very generic attribute
Data integrity	VNF Security	e-TRM	Similar	Within Data Protection and Privacy
Data integrity	Transparency	TBNS	Complementary	
Data integrity	Resistance against tampering	TBNS	Similar	Similar to Cybersecurity code related attributes
Usability	Policy Management	CCT	Additional TSLA	
Maintainability	Patch Management	CCT	Additional TSLA	
Portability	Migration operation	CCT	Additional TSLA	
Portability	Location awareness	CCT	Similar	Relates to Geolocation TSLA
Network Management	Network topology verification	RAG DiscØvery	Additional TSLA	
Service Management	Service composition	RAG	Additional TSLA	

Table 14: Gap analysis between the top-down and the bottom-up approach.

5 Case study of Trust Management on the Demos

The following sections present a short description on how Trust Management is illustrated in Demo 1 to 3.

KPIs defined in the project's milestone document MS9 have been taken into account in the design of the Trust Management in the demonstration. TSLA management relates to SSLA Management KPI since it can be viewed as an extension of it.

5.1 Key TSLAs management in Demo 1

The demo 1 aims showcasing security closed-loops across interconnected domains and one E2E management Domain. To that end, the demo showcases the setup of two slices with SSLA (Security SLA) including associated TSLA to be addressed in a multi-domain 5G network. This demo incorporates several trust enablers that are part of the HLA Trust Management components and allow monitoring the TSLA mainly based on a trust score attribute of the 5G components and security enablers, computed using information provided by INSPIRE-5GPlus enablers (not exclusively WP4 enablers).

Multiple enablers and domains are triggered to deploy both SSLA from the E2E Management domain. Security orchestrator in each domain collects the trust and reputation score before deploying the slices, according to the TSLA defined. This information is requested and provided by the Domain TRM. Once the service is deployed and active, if any kind of attacks happen, the enabler that makes the detection also alerts the TRM. In view of this alert, TRM re-evaluates and decreases the trust score attribute for the vulnerable asset that has been attacked and the service until the problem is solved (e.g., until a 5G component is redeployed with a more trusted version and complies with the TSLA) and increases the reputation of the enabler which detected the attack. This information is in turn shared with the E2E Trust Manager from each domain, that will directly propagate the updated value to each TRM that uses the involved enabler at the SMD.

5.1.1 Data protection

This demo involves the following Trust-worthiness attributes associated with Data protection:

- High reputation source: The Domain TRM calculates a Trust reputation score KPI. The demo uses a cryptomining attack that compromises the 5G service resources, detected by the Smart Traffic Analysis enabler (see D3.3), and as a consequence the service Trust score is reduced, until the problem is solved.
- Data integrity and confidentiality in transit: The cipher suite selected for the channel protections, using the I2NSF IPsec and DTLS enablers (see D3.1), provides the evidence for the TSLA data protection attribute.

5.1.2 Isolation

The pervasive use of the Security Orchestrator with Open-Source MANO, jointly with OpenStack services in different domains, achieves an effective isolation. These service level and process level trust-worthiness attributes are not integrated in the demo with the TRM, but are used to guarantee an effective isolation.

5.1.3 Geolocation

Geolocation of the data in transit trust-worthiness attribute is achieved, with the support of the Ordered Proof of Transit enabler (see section 4.4.2). This enabler reports to the TRM periodically the list of IP addresses (Geolocation) involved in the IPsec slice. It includes as evidence the cryptographic validation calculations of the path for the IP addressed involved.

5.2 Key TSLAs management in Demo 2

Demo 2 presents on-demand trustworthiness establishment. In a security or safety critical scenario, there is a need to get a higher trustworthiness on the situation analysis elements. Elements below will be completed after the upcoming face-to-face meeting organised in the next month.

5.2.1 Data protection

Together CCT and Systemic can be used as defined in Use Case R (UCR) to confirm the correctness (integrity) of the code involved in the situation report generation and transmission.

5.2.2 Isolation

Demo 2 mainly explores how to guarantee the isolation property.

5.2.3 Geolocation

As this deliverable is written, several options are investigated to implement geolocation. One of those is to add the **geolocation** of the software which delivers the situational report (as this code shall run exclusively in trusted platform).

5.3 Key TSLAs management in Demo 3

The relevance of Demo 3 for trust related enablers stems from the utilization of Systemic as a VNF integrity monitoring enabler for Moving Target Defence (MTD) paradigm in virtualized network environment. In that regard, Systemic usage in Demo 3 provides the capability to convey VNF integrity alerts to OptSFC-MOTDEC complex for deciding and optimizing MTD operations developed in WP3 activities. With such information, the MTD framework works out a self-healing of the network (ignoring the corrupted platform) by using the IP address of the platform hosting the issuer (i.e., running the protected VNF embedding Systemic routine triggering the integrity alert). Therefore, the solution brings both the geolocation and the type of attack (code tampering) incident in the network into the MTD scenario as part of Demo 3.

5.3.1 Data protection

In Demo 3, Systemic is utilized to verify the integrity of a network service in order to identify whether it is tampered or not (i.e., an attack is in progress). This monitoring information regarding data protection aspect allows the MTD based protection to act and defend the assets in the demo scenario.

5.3.2 Isolation

Demo 3 does not explore how to guarantee the isolation property. However, it focuses on an end-to-end slice perspective for security. Moreover, if isolation aspect is relevant for a use case, MTD may consider slice isolation during its control of security enforcement actions.

5.3.3 Geolocation

Similar to Demo 2, several options are possible to implement geolocation in Demo 3. One approach can be to embed the geolocation of the integrity-protected software using the trusted platform capabilities. That information can be used to pinpoint of the attack on the integrity, which can then be used to decide on the specific MTD action (e.g., to which platform to migrate the key services in the protected slice). However, Demo 3 does not integrate geolocation information at the moment.

6 Directions for further works on Trust Management

6.1 Trust Management between Security Management and Liability Management

6.1.1 First considerations on the principles of Trust Management

Trust Management is situated between the two adjacent concepts of Security Management and Liability Management. Security Management corresponds to a well-acknowledged need to secure data and assets in the cyber-space. Security standards and technologies present a wide spectrum in the research and innovation fields, as well as in the digital industry. With 5G, where telecommunications, Information Technologies and Data are converging in a context of multi-tenants, multi-operators, multi-domains, the concept of Liability seems gaining in importance. It becomes necessary to trace the responsibilities between the different players when it comes to guarantee a Quality of Service. Therefore, an accountability framework shall support the Liability concept.

In the middle of both security and liability, Trust helps catching the end-user subjective perception of a service, developing different aspects of the relation between the service consumer and the service provider, behind whom a plurality of service operators contributes. Figure 26 shows a big picture of Trust Management with its dependencies with Security and Liability Management, and the relation with a multiplicity of operators.

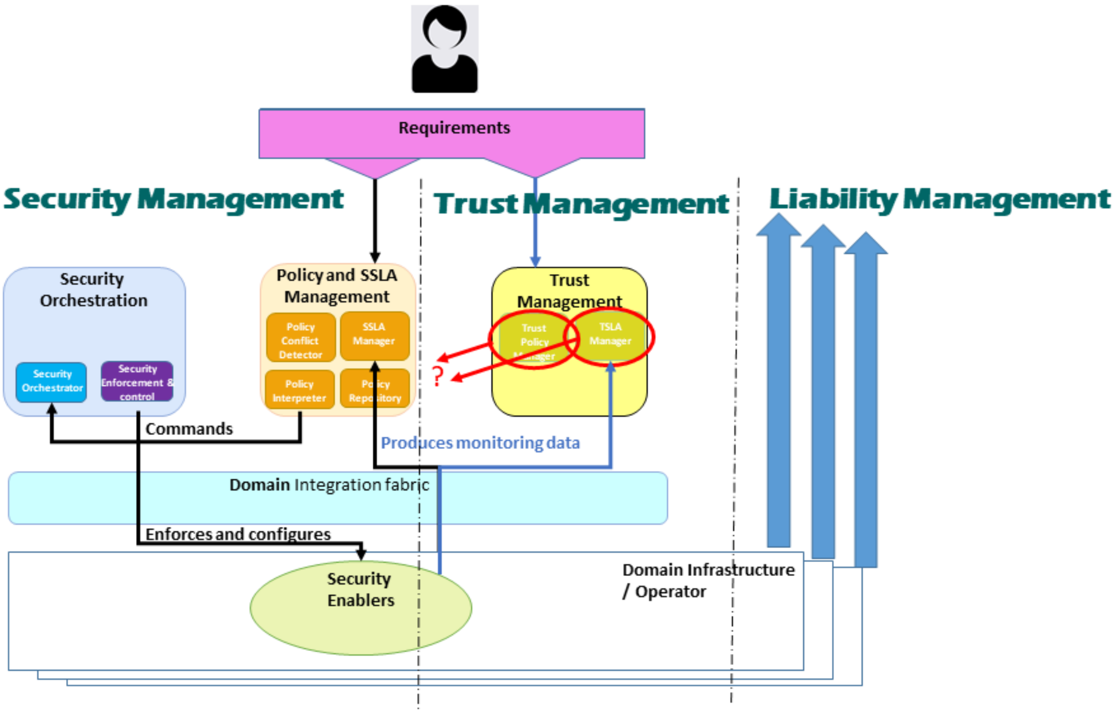


Figure 26: Trust Management further works big picture.

6.1.2 Considerations on the technical assets of the HLA

In technical terms, D2.2 [16] defines the respective roles of Security Orchestration, Policy and SSLA Management, and Trust Management. As far, Trust Management is more a wide set of Trust enablers than a full mechanism to manage it from end user requirements to TSLA monitoring and management at run-time. There is a need to consolidate the architecture of Trust Management. The following paragraphs give an argumentation to augment Trust Management with two sub-functions: a Trust Policy Manager and a TSLA Manager; in deep cooperation with symmetric functions used for Security.

The **Security Orchestration** has been studied through several European projects as described in [16], and the mechanisms to translate a policy into an enforceable chain of enablers begin to be well described. Such a mechanism is needed to deploy the Trust enablers necessary to enforce Trust Management.

Similarly, for **Policy Management**, several projects describe the refinement made to catch end-user security requirements into a High-Level Security Policy Language and then in a Medium-level Security Policy Language, which is then translated into technical configuration according to the chosen list of enablers to enforce the policy. Same design shall apply to transform end-user Trust requirements into a Trust Policy to be taken in charge by the Security Orchestrator. Security Policy Management and Trust Policy Management shall probably converge in common parsers after a first treatment which may be specific to Trust and its language.

Service Level Agreement not only helps to write the contract between the service consumer and the service provider, but also translate into policies to deploy and enforce technical enablers. These enablers may monitor not only Security SLA, but also the respect of the Trust SLA at run-time. On the other hand, T**SLA Management** shall be driven by Zero-Touch Management principles designed by a closed-loop to decide for mitigation actions in case the contract is not fulfilled. This closed loop should be the same for mitigation of a non-respect of the SSLA and of a TSLA violation.

This leads to an architectural dilemma whether Trust Management should be apart from Security Management or not.

Trust catches a much more subjective perception than security and involves perceptions which are out of the “pure” security technical field. Nevertheless, when the end user expresses their needs, they may not perceive the difference between technically-grounded attributes and subjective attributes. As can be seen with the description of the key TSLA described in section 3, some ambiguity persists on the nature of the attributes, some Trust attributes corresponding exactly to technical security attributes. This leads to envisage a common interface to catch the end user requirements, and a close format for the expression of SSLA and TSLA.

In terms of policy management, it appears that some Trust Attributes refer to Security Attributes and lead to the enforcement of Security enablers. This means that there is an overlap between Trust Policy Management and Security Policy Management. In many cases, concatenation and consistency of both security policy and trust policy shall be worked out by means of the Policy Conflict Detector. At the end, both policies shall be orchestrated by the same Security/Trust Orchestrator.

The Management of TSLA at run-time, involving the monitoring of a list of both Security and Trust enablers may be handled separately from SSLA to focus on TSLA concepts. Nevertheless, since both SSLA and TSLA may poll the same monitoring data, they may both read them in a common Repository or Data Analytics Engine.

6.2 Trust Management towards societal concerns

The state of the art proposed in section 2 shows that the Trust concept goes beyond the simple “Trust in technologies” considerations analysed in [4]. Trust shall precise the contract between the service consumer and the service provider, their-selves offering a single interface to the service consumer when plethora of operators contribute to the service provision. Section 6.1.1 discusses the relation between Trust and the close concepts of Security and Liability. Trust is probably the place where to take into account the societal criteria on which the consumers put more and more emphasis in the selection of their provider.

Labels reveal a well-adopted way to advertise for a certain claim guaranteeing either ethics in the production or trade process, quality of the raw material used, a geographical area of production, a specific or genuine manufacturing process, etc. Maybe they provide a good way to simplify the expression of personal requirements for the biggest number of users. Nevertheless, verticals may still need finer criteria to express their needs. Therefore, developing languages to express requirements and Trust Service Level Agreements remains a proficient direction.

6.2.1 Ethical considerations

Multiple ethical considerations also lead the choice of a service consumer in the adoption of it. Just to give few examples to illustrate the importance of it, several among others are mentioned here: fair balance between women and men, respect of the minorities and the people, respect of the childhood, respect of the gender diversity and preferences, social status and compensation of the workers, animal welfare, dialogue with the concerned parties, digital equity, accounting for negative externalities, etc.

These criteria may enter into consideration when discriminating between different services. As far and as they are listed above, they seem too generic. In the same way, putting a criterion on the respect of data privacy or liberty of expression could look a priori too generic. Works undertaken about data privacy show that such a field can be better clarified by different law and regulations, and then translated into technical criteria and attributes. Further works could be conducted on the ethics underneath a commercial product or service.

6.2.2 Ecological considerations

As climate change consequences reveal themselves closer and closer, when data production and consumption are from day to day more ubiquitous and voluminous, driving up energy consumption, it appears that important regulations need to be acknowledged toward green and sustainable society. The invasion of Ukraine by Russia and the ethical considerations about whether Europe should proceed to commercial restrictions against Russian hydrocarbons shows again the dependency of Europe on raw material extracted from abroad and paves the way to better balance world-wide exchanges in the goal of fostering autonomy, liberty and peace of the people. Again, this may lead to redefining the priorities in terms of energy consumption and associated usages.

A key factor for this is not only to reduce the volume of data, but also to reduce the expectations on its availability online, and its criticality. Including such TSLAs, Trust Management could serve this ecological project to bring both individuals and operators to invent the ecological design of the future.

7 Conclusions

Although Trust is a concept developed since more than a tenth of years, it remains still flexible according to the context and the editor, or organisation, or service provider using it. This matter of fact probably relies on the fact that, as a concept, it stays at the crossing of subjective considerations and technical, objective imperatives.

Nevertheless, this deliverable inherits from an IT technical background, where the distinction between Trust and Trustworthiness helps setting the limits between a subjective world and a technical domain. As both are described by means of Attributes, Trust Attributes are finally mapped in the technical world by Trustworthiness Attributes corresponding to the controls monitored by technical Trust enablers.

The deliverable identifies a few main key Trust Attributes or related Trust Service Level Agreement (TSLA) and presents how they are used and illustrated in the project's Demos.

Two approaches are confronted and consolidated in this deliverable. First a top-down approach starts from a theoretical analysis of three key Trust Attributes or Trust Service Level Agreements (TSLA). From the state of the art, the technical means to manage these TLSA are detailed through Trustworthiness Attributes to detail the technical measures which are followed and guaranteed. Then, a bottom-up approach reviews all the technical Trust enablers to understand which Trustworthiness Attributes they map and support at design-time as well as for run-time monitoring. Gaps are identified and listed in this deliverable. Some Attributes are similar to the ones already identified, some are complementary, others are related to TSLA which are not developed yet in this deliverable.

Additional future works can be envisaged to serve the concept of Trust. First at architectural level, following the model of SSLA management which paved the way, it seems necessary to first define a language to express Trust requirements, to be technically translated into Trust policies implemented by a chain of Trust enablers. A single Security and Trust Orchestrator would be the central tool to orchestrate and deploy Trust policies as well as Security policies. Dedicated enablers may take in charge TSLA Management to guarantee their respect during the whole service life-cycle. A careful design should apply to the relationship between the TSLA and the SSLA Management. Second, Trust concept is opened to wider fields than purely technical ones and should be distinguished from the concept of IT Security. Since it helps at grounding the relationship between a service consumer and a service provider, the expression of Trust contract shall include a variety of fields that are pregnant in the aware consumers decision to buy a service. As more and more people and citizen reach digital concerns, our societies shall bring to public knowledge ethical and ecological considerations in the description of digital services.

References

[1] INSPIRE-5GPLUS D4.1: Trust mechanisms for 5G environments

[2] Networld 2020 - Strategic Research and Innovation Agenda 2021-27 (Sept 2020) Section 4.1 Evolution of Networks and Services p.56

[3] J.-H. Cho, K. Chan, and S. Adali, ''A survey on trust modeling,'' ACM Comput. Surv., vol. 48, no. 2, 2015, Art. no. 28.

[4] McKnight, D. H., Carter, M., Thatcher, J. B. & Clay, P. F. 2011. Trust in a specific technology: An investigation of its components and measures. ACM Trans. Manage. Inf. Syst., 2, 1-25

[5] 3GPP. (2017). TS 22.261: 3GPP Service Requirements for the 5G; System; Stage 1. http://www.3gpp.org/news-events/3gpp-news/1786-5g_reqs_sa1

[6] ITU-T Recommendation G.1000 "Communications quality of service: A framework and definitions"

[7] 5G-ENSURE. (2017). Deliverable D2.5: Trust Model (Final). http://www.5gensure.eu/deliverables

[8] ETSI. (2004). GS NFV-SEC 003: Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance. http://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/003/01.01.01_60/gs_NFV-SEC003v010101p.pdf

[9] NIST Special Publication 800-39

[10] Arfaoui G., Bisson P., Blom R., Borgaonkar R., Englund H., Félix E., Klaedtke F., Kumar Nakarmi P., Näslund M., O'Hanlon P., Papay J., Suomalainen J., Surridge M., Wary J.-P., and Zahariev A., A Security Architecture for 5G Networks IEEE Access Volume, Electronic ISSN: 2169-3536, 2018 April 17th. https://ieeexplore.ieee.org/document/8340149/

[11] Cheshire, C. 2011. Online trust, trustworthiness, or assurance? Daedalus, 140, 49-58.

[12] Li J., Mao B., Liang Z., Zhang Z., Trust and Trustworthiness: What they are and how to achieve them, SPT-IoT 2021: The fifth Workshop on Secuity, Privacy and Trust in the Internet of Things

[13] The Continuous Audit Metrics Catalog, Version 1.0, Cloud Security Alliance, https://cloudsecurityalliance.org/research/working-groups/continuous-audit-metrics/

[14] ETSI EG 202 009-3 V1.3.1 (2015-07) Quality of ICT services; Part 3: Template for Service Level Agreements (SLA)

[15] INSPIRE-5GPlus D2.1: 5G Security: Current Status and Future Trends

[16] INSPIRE-5GPlus D2.2: Initial Report on Security Use Cases, Enablers and Mechanisms for Liability-aware Trustable Smart 5G Security

[17] INSPIRE-5GPlus D4.1: Trust mechanisms for 5G environments

[19] Kotulski, Z., Nowak, T., Sepczuk, M., Tunia, M., Artych, R., Bocianiak, K., Osko, T. and Wary, J.P., 2017, September. On end-to-end approach for slice isolation in 5G networks. Fundamental challenges. In 2017 Federated conference on computer science and information systems (FedCSIS) (pp. 783-792). IEEE.

[20] NIST Cybersecurity framework https://www.nist.gov/cyberframework

[21] ISO 27000 series - https://www.iso.org/standard/73906.html ; http://www.27000.org/

[22] ENISA's (CSIRT) Maturity Framework 2022 - https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework

[23] NFV Security in 5G - Challenges and Best Practices - https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices

[24] LF AI & Data Trusted AI Committee. https://lfaidata.foundation/projects/trusted-ai/

[25] Newsha Emaminejad, Alexa Maria North, and Reza Akhavian. Trust in AI and Implications for the AEC Research: A Literature Analysis. *ASCE International Conference on Computing in Civil Engineering (i3CE)*, 2021. https://arxiv.org/abs/2203.03847

[26] Kha Dinh Duy, Taehyun Noh, Siwon Huh, and Hojoon Lee. Confidential Machine Learning Computation in Untrusted Environments: A Systems Security Perspective. *IEEE Access*, vol. 9, pp. 168656-168677, 2021. doi: 10.1109/ACCESS.2021.3136889.

[27] T. Hunt, Z. Zhu, Y. Xu, S. Peter, and E. Witchel. Ryoan: A distributed sandbox for untrusted computation on secret data. *12th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pp. 533-549, 2016.

[28] R. Kunkel, D. L. Quoc, F. Gregor, S. Arnautov, P. Bhatotia, and C. Fetzer. TensorSCONE: A secure TensorFlow framework using Intel SGX. arXiv:1902.04413, 2019.

[29] O. Ohrimenko, F. Schuster, C. Fournet, A. Mehta, S. Nowozin, K. Vaswani, and M. Costa. Oblivious multi-party machine learning on trusted processors. *25th USENIX Security Symposium (USENIX* Security*)*, pp. 619-636, 2016.

[30] INSPIRE-5GPlus white paper (2022). Evolution of 5G Cyber Threats and Security Solutions DOI:10.5281/zenodo.6457557

[31] INSPIRE-5GPlus D2.3: Final report on Advanced 5G Security Use Cases

[32] INSPIRE-5GPlus D5.1: 5G security test cases