Deliverable D2.3
Trust Model and Trust Management Approaches

Document Summary Information

Grant Agreement No	871780	**Acronym**	MonB5G
Full Title	Distributed Management of Network Slices in beyond 5G		
Start Date	01/11/2019	**Duration**	36 months
Project URL	https://www.monb5g.eu/		
Deliverable	D2.3 Trust Model and Trust Management Approaches		
Work Package	WP2		
Contractual due date	M12	**Actual submission date**	14/11/2020
Nature	Report	**Dissemination Level**	Public
Lead Beneficiary	AALTO		
Responsible Author	Muhammad Zubair Farooqi (AALTO), Aiman NAIT ABBOU (AALTO)		
Contributions from	Adlen Ksentin, Bouziane Brik, Sabra Ben Saad (EURECOM), Cao-Thanh Phan (BCOM), George Giourgis (EBOS), George Tsolis (CTXS), Tarik Taleb, Muhammad Zubair Farooqi, Mohammed Boukhalfa, Chafika Benzaid (Aalto)		

Disclaimer

The content of the publication herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the MonB5G consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the MonB5G Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or om ission herein.

Without derogating from the generality of the foregoing neither the MonB5G Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

Executive Summary

This deliverable describes the trust modelling and trust management approaches in 5G networks, with an emphasize on how to enable trustworthy deployment and management of cross-domain 5G network slices.

Trust is a concept that has been considered as a key foundation for decision making in different disciplines, including philosophy, sociology, psychology, economics, law as well as computer science. It symbolizes a relationship in which an entity, often called the trustor, relies on someone or something, called the trustee, based on a given criterion. Meanwhile, a decision to believe in someone (or something) is a decision to embrace the risk that the trustee may fail in upholding the promise to do what the trustor expects he/it to do. Thus, we need to consider the trust decisions, the implications of these trust decisions and information on the trustworthiness of others in order to take informed decisions in a social and technological environment such as 5G networks.

The 5G networks are expected to be highly distributed, multi-actor and service-based which results in heterogeneous untrusted environment. The variety of stakeholders (e.g., users, mobile network operators, service providers, and infrastructure providers) may have diverse business plans and often conflicting objectives. These diverse network entities involved in a 5G network ecosystem broaden its trust surface and calls for novel solutions to provision a secure and trusted environment for slice deployment and management.

MonB5G aims to provide a novel platform for autonomic deployment and management of a massive number of network slices in a 5G environment. To this end, MonB5G platform will heavily leverage distribution of operations, zero-touch management cross multiple technology domains (e.g., Radio Access Network, Core Network, Cloud), and data-driven distributed AI-based mechanisms. The rich 5G ecosystem in which MonB5G platform will operate poses significant security and privacy threats. A malicious service provider could abuse its access privileges to disclose confidential data. Technology domain providers might try to hide their under-performance or not provide accurate and complete data out of malice or to avoid associated overheads. Slice owners might fake SLA violations to consume more resources. A vulnerable Virtual Network Function (VNF) might manipulate the received packets before forwarding them to the next VNF in the service function chain. AI systems can be influenced to make wrong decisions or leak confidential information. The common denominator in the aforementioned threat models is the lack of trust between the involved stakeholders and network entities. To empower a trusted environment for deploying and managing network slices, MonB5G will devise new trust approaches based on Blockchain and integrate a “Trust Management Module” to derive and assess trust levels among involved parties as well as their reputation level.

This document takes a step forward towards building such a trusted environment. For the sake of uniformity and to minimize the potential of misunderstandings, we first define the trust terminology used in the document. After that, we thoroughly review the state of the art in trust modelling, covering both human and machine aspects and particularly focusing trust modelling between machines, especially ones connected over

telecommunication networks including the trust in physical and virtual networks. We then conduct an extensive study of the trust dimensions in 5G networks in general and network slicing in particular, identifying the trust requirements and the appropriate measures to establish and maintain trust for each dimension.

Finally, we introduce MonB5G's trust management vision, where we (i) elaborate the MonB5G's trust model considering both trust among stakeholders and trust between network entities involved in MonB5G's ecosystem; (ii) present the adopted trust formalism for empowering trustworthy distributed decisions in MonB5G platform. We promote the use of computational trust modelling concept for formalizing the trust between the distributed AI agents involved in Analytics Engine (AE) and the Decision Engine (DE) components; and (iii) propose novel approaches leveraging the potential of Blockchain and smart contacts to enable trustworthy deployment and management of network slices using MonB5G platform. The proposed approaches support:

1) ***trustworthy slice brokering architecture***, which allows the slice provider to securely compose end-to-end network slices while leasing resources from different infrastructure providers for each technological domain. The proposed trust architecture: (i) validates all the transactions via a Blockchain, by checking the public keys of the slice provider, resources providers, and their signature in the transactions. The blockchain (owned by the slice provider) is used to generate and negociate contracts between the slice provider and the resource providers; (ii) adds reputation value assigned by a third-tier entity, namely *resource provider trust*, for each resource provider involved in a Blockchain transaction. The assigned reputation value is a function of the fulfilled SLAs.
2) ***trustworthy SLA compliance monitoring and arbirtration architecture***, which aims, on one hand, to manage the life-cycle of SLAs established between the vertical and the slice provider and between the slice provider and the resource providers and, on the other hand, to build the reputation of resource providers. The proposed architecture includes (i) a *monitoring system* to monitor the Key Performance Indicators (KPIs) as specified in the established SLAs; and (ii) a *smart contract* which contains all the signed SLAs and related information (e.g., validity period, target performance level, price, etc.). It is used to check the violation of SLAs based on monitoring information, report the SLA violation to the *resource provider trust* entity, publish in the blockchain the information on resource providers that failed to meet the SLA, and automatically compensate the vertical and charge the resource provider in case of violation.
3) ***robust and accurate monitoring data collection system***, which allows to protect the monitoring data from manipulation. In fact, ensuring the integrity of the data is critical to foster trust in decisions taken by MonB5G platform's entities, particularly the Analytics Engine (AE) and the Decision Engine (DE). The proposed system introduces a learning pipeline with blockchain-based trustworthy data. the pipeline comprises four components, namely: (i) a *Data Collector* which collects data from various sources; (ii) a *Feature Extractor* which extract features relevant to learning task from the raw data; (iii) *ML Algorithm and Model* which use the extracted data for training and inference, respectively; and (iv) a *Data Integrity Module* which maintains and assesses the integrity of data used by the three aforementioned components using blockchain's smart contracts.

The outcomes of this deliverable will be leveraged in the design and development of the “Trust Management Module” and the security architecture of MonB5G. The first and final version of the security-related architectural elements (i.e., Trust Management Module and Security Orchestrator) of MonB5G platform will be presented in D2.1 and D2.2, dedicated to first and final specification of the zero-touch slice management and orchestration architecture to be delivered by MonB5G.

TABLE OF CONTENTS

List of Figures

List of Tables

Abbreviations

ACME	Automated Certificate Management Environment
AF	Application Function
APIs	Application Programming Interfaces
CA	Certificate Authorities
CDM	Continuous Diagnostics and Mitigation
CN	Core Network
CSP	Communication Service Provider
(DAI)	Distributed Artificial Intelligence
HSM	Hardware Security Module
MBB	Mobile Broad Band
MEAO	Mobile Edge Application Orchestrator
MEP	MEC Platform
MITM	Man-In-The-Middle
NEF	Network Exposure Function
NFVI	Network Function Virtualization Infrastructure
NSI	Network Slice Instances
NSMF	Network Slice Management Function
PA	Policy administrator
PaaS	Platform as a service
PE	Policy engine
PEP	Policy enforcement point
PKI	Public Key Infrastructure
PoW	Proof-of-Work
PRB	Physical Resource Blocks
RAN	Radio Access Network
RNIS	Radio Network Information Service
RO	Resource Orchestrator
RRH	Remote Radio Head
RRU	Remote Radio Unit
SaaS	Software as a Service
SBA	Service Based Architecture
SCEF	Service Capability Exposure Function
SIEM	Security information and event management

SLA	service level agreement
SO	Slice Orchestrator
DSC	Domain-slice Contract
DSD	Domain-slice Deployment
DSDC	Domain-slice Deployment Costs
TA	Trust Algorithm
TEE	Trusted Execution Environments
TPM	Trusted Platform Module
TLS	Transport Layer Security
UPF	User Plane Function
VNF	Virtual Network Function
ZT	Zero Trust
ZTA	Zero Trust Architecture
ZTM	Zero Trust Management

1. Introduction

1.1 Scope

This is the public deliverable of the MonB5G project's Work Package 2 (WP2) describing the current status and potential new approaches to model and manage trust in 5G ecosystem. This deliverable includes the state of the art on trust modelling, the different dimensions of trust in 5G network systems, the requirements and the appropriate control mechanisms needed to establish trust in the composition of network slices across multiple domains, and novel approaches based on blockchain to enable trustworthy deployment and management of network slices using MonB5G platform.

1.2 Target Audience

The target audience of this deliverable are stakeholders related to trust and security in 5G technologies and infrastructure. The deliverable describes the technologies that are used to build and enhance the trust factor between the components of 5G networks.

1.3 Structure

The main structure of this deliverable can be summarized as follows:

- Section 2 describes the trust terminology used in the deliverable;
- Section 3 presents the state of the art in trust modelling, covering human trust, trust in technology, machine trust, trust in 4G and specifically 5G Networks;
- Section 4 contains an analysis of the Zero Trust Management (ZTM) concept, the trust dimensions in 5G Networks, and security measures needed to establish and maintain trust for each dimension;
- Section 5 describes the composition of trustworthy cross-domain slices with its trust requirements;
- Section 6 introduces novel blockchain-based trust management approaches to foster trustworthy deployment and management of network slices using MonB5G platform;
- Section 7 concludes this deliverable.

2. Trust Terminology

Trust is a concept that has been considered in different disciplines, including philosophy, sociology, psychology, economics, law as well as computer science. As a consequence, various trust terminologies have been proposed, with a narrow focus on discipline-bounded perspectives [1]. Although the definitions of trust vary across disciplines, they all share the common idea that trust is "a relationship in which an entity, often called the trustor, depends on someone or something, called the trustee, based on a given criterion" [2].

For the sake of uniformity and to minimize the potential of misunderstandings, we provide in this section the trust terminology used in the deliverable:

- **Trust[1]:** a confidence in the reliability, truth, or ability of someone or something;
- **Trustor:** a person or thing that has trust in someone or something else;
- **Trustee:** the person or thing in which the trustor has trust;
- **Trustworthiness:** the property of being reliable, truthful and capable;
- **Trust Model:** a basis for understanding and analyzing the role played by trust (in a socio-technical system), and using qualitative and where appropriate quantitative measures of trust and trustworthiness;
- **Zero Trust (ZT)[1]:** a cybersecurity paradigm based on the assumption of mistrust; that is, everyone can be a threat and the network is hostile. The key tenets of ZT is to never trust, always verify, enforce least privilege- access, and maintain dynamic risk-based access policies;
- **Zero Trust Architecture (ZTA)[1]:** an enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement.

3. Trust Modelling – State of the Art

"Trust is a social good to be protected just as much as the air we breathe or the water we drink. When it is damaged, the community as a whole suffers; and, when it is destroyed, societies falter and collapse…Trust and integrity are precious resources, easily squandered, hard to regain." [3]

Trust is an integral component of our everyday life, as it inherently dictates the risk of loss, of what people entrust unto others. The concept of trust will be explored in this section, firstly trust as applicable between human beings, and how it affects their attitudes and behaviours. Secondly as applicable to technology, including human-machine trust, machine-machine trust, and trust in machine decision making processes. The main aim of this section is to utilize the wealth of knowledge of human behaviour, history of human-machine interactions, its trust issues and risks, in order to reach the basis of the trust model that will be responsible for securing the **MonB5G** platform.

3.1 Human Trust

3.1.1 TRUST DEFINITIONS

Trust has many academic definitions, among the ones relevant to our purpose as defined by Merriam-Webster[1] are:

1. a: **assured reliance** on the **character**, **ability**, **strength**, or **truth** of **someone** or **something;**

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[1] https://www.merriam-webster.com/dictionary/trust

b: one in which **confidence** is placed.

2. **dependence** on something **future** or **contingent**.

3. a: a property **interest held** by one person for the **benefit** of **another**;

b: a combination of firms or corporations formed by a **legal agreement**, especially: one that **reduces** or **threatens** to **reduce competition.**

4. a: CARE, CUSTODY

Physicians **evoke** their patient’s **trust**.

b (1): a **charge** or **duty imposed** in **faith** or **confidence** or as a **condition** of some **relationship;**

(2): something **committed** or **entrusted** to one to be **used** or **cared** for in the **interest** of **another.**

3.1.2 HUMAN TRUST PILLARS

From these aforementioned definitions, we can extract the four most applicable pillars of any trust outline, as we can see in Figure 1:

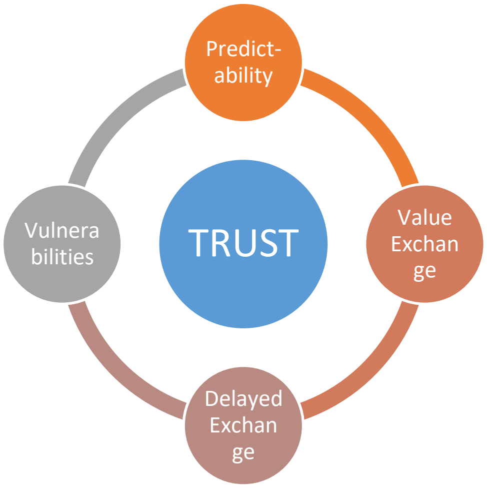

Figure 1: Components of Human Trust.

1. Predictability

Trust enables the prediction of what others will do and in what situations to some extent. Thus, through trust, we can create safe conditions.

2. Value Exchange

Trust always involves making a certain value exchange between people. Assuming that full knowledge of all conditions and situations will not be possible, trust’s value exchange could mean exchange of their intent and the things that they offer one another.

3. Delayed Exchange

Trust usually means giving something now, with future expectation for reciprocation, possibly with unknown value, and undefined time.

4. Vulnerabilities

Trust means giving other people or machines the opportunity to take advantage of your weaknesses and vulnerabilities, but trusting that they will not do this.

3.1.3 TRUST IN GENERAL

It is evident from the various trust definitions presented in section 3.1.1 that trust is essential to our everyday life, but it is always a probable risk. This risk arises when we entrust other people or machines for a certain exchange, but for some reason they fail to accomplish the expected exchange, which will in turn affect the future trust condition of that person/machine. Apart from basic human betrayal of trust, or betrayal of contracts where the expected value is not exchanged, we place far more relevant trust in our machines that we rely on every day. For instance, having either your computer or your car simply failing to switch on when you want it to (and trust it to) can be sometimes attributed to hardware failures, but other times could reflect greater dangers, as compromised security.

That is why trust components will always be the foundation of any security, whether it is human-human, human-machine or machine-machine, and accordingly, whether it is contractual, software or hardware. To bridge the gap between creating trust and security, we shall briefly explore and define the concept of trust modeling in the remainder of this section.

1. Able / Ability

By showing ability, a person's environment starts to trust someone's actions. A certain level of expertise is expected, and if they do not show that they have that expertise, others will have less trust. Thus, demonstrating competencies will inspire others and increase trust.

2. Believe / Believability

By acting with integrity, people show that they are honest and will not harm others' trust in them. People expect that others behave in accordance with certain standards and values necessary to accomplish the tasks at hand which need their mutual trust.

3. Connected / Connectedness

By being genuinely interested in their environment, groups and colleagues, as well as maintaining good communication, will be beneficial for a team's cooperation to accomplish tasks.

4. Dependable / Dependability

By showing others that one is dependable, will lead to a positive response from their environment. This will elicit consistent respect from their environment and will ensure that collaboratively they all deliver on their promises, within the time that was agreed.

One of the most widely used (human) trust models is "The ABCD Trust Model" designed by Ken Blanchard [4]. The foundation of this model is giving and receiving trust. As shown in Figure 2, the ABCD trust model comprises four key components, namely:

By implementing what has been discussed above, an individual as well as teams can work on building a good and long-lasting relationships of trust with their environment, which will in turn serve to continuous collaborative accomplishment of mutual tasks.

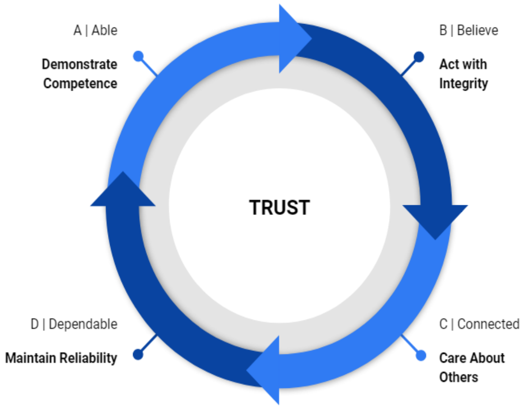

Figure 2: Key Components of Blanchard's ABCD Trust Model.

This concludes our brief overview of human trust modeling. In the next subsection, we will explore the basis of trust modeling in technology, in order to combine the findings to construct the basis of our MonB5G Trust Model components in the forthcoming sections 4-6.

3.1.4 TRUST IN TECHNOLOGY

The first exploration of trust in relation to technology, with the intent to implement through a **Computational Trust Model** [5] was the thesis by **Stephen Paul Marsh**. Marsh's model is one of the first works which proposed a formal treatment integrating different trust concepts. According to Marsh, the most notable early contributions to understanding trust have largely come from the areas of sociology, social psychology and philosophy, more specifically in work carried out by Diego Gambetta [6].

Many attempts have been made to represent trust mathematically and a number of computational trust models have been proposed, many of which have been compiled in a recent ACM Computing Survey [50]. But for our purposes, we mainly focus on Gambetta's definition of trust; which states that to trust someone or that someone is trustworthy, implicitly means that the probability that they will perform an action that is beneficial or at least not detrimental to us, is high enough for us to consider engaging in some form of cooperation [6]. These mathematical trust models have emerged mainly for risk management mechanisms in online communications, among other applications. The main *goal* of a **computational trust model** is to assist users with **decision making**.

An analogy of trust modeling between (human) societies and an agent-based computational model (artificial societies**)** is **phone networks**. It describes the phone network as an artificial society consisting of many **nodes**, each of them endowed with some **intelligence** and having the capability to decide **how to route traffic** (phone calls, data, etc.). Within this analogy, since the network nodes work with each other, this means that there is indeed trust, even if it is limited. For example, 'does this node trust this other node *enough* to send a message?'. The other prominent example is the first major virtual **collapse of the internet** back in 1988, which was caused by excessive laxity, where the infamous '**Morris Worm**' took advantage of various '**trusted host**' connections.[1]

Marsh proposes a novel formalisation of trust modeling through artificial agents, that are rational, intelligent and trusting. His model is further inspired by human society, where trust is distributed through **Multi-Agent Systems** (MAS), or **Distributed Artificial Intelligence (DAI)**, in one structure, that is the **Artificial Society**. Comparatively, one of **MonB5G's** core design objectives is to completely decentralize the main management's system through the distributed and data-driven components, namely the **Monitoring System** (**MS**), **Decision Engine** (**DE**), and **Anlaytics Engine** (**AE**). This design is tailored for beyond 5G network requirements, and will be able to cope with associated inherent vulnerabilities and efficiency needs. Particularly analogous to Marsh's **DAI**, it is **MonB5G's DEs,** which provide judgement of the behaviour of the other agents, based on AI-driven mechanisms.

- **Distributed Artificial Intelligence**

At the time of Marsh's innovative approach to trust modeling, DAI was a novel research field progressively growing in applicability and relevance, both to Artificial Intelligence and to computing in general. In short, it involves concepts of distribution, intelligence, society, independence, graceful degradation, and localised decision making.

In essence, DAIs novelty (at the time of its inception) was autonomy and independence, whilst at the same time, keeping cooperation, collaboration and coordination between the different DAIs. This makes them a tool for the study of the implementation of a trust model, as with the DEs in MonB5G. Below are Marsh's assumptions for his computational model, and Table 1 shows a summary of his equation descriptions, representations and value ranges.

- **Assumptions for DAI in Trust Models**

1. Agents are assumed to be *(pseudo-) intelligent*. Since in groups of agents, intelligent behaviour must include observations of others who may affect the agent. Therefore, trust presents an agent with an extra capability in that direction.
2. Agents are assumed to be *(pseudo-) rational*. For rational agents, a goal would be the implementation of rational trust. Trust as confidence supplies this viewpoint.
3. Agents are generally assumed to be *cooperative*. When cooperation may be necessary, there is a choice about who to cooperate with.
4. Agents are *distributed*. Trust is a societal concept, and distributed agents with non-random interactions between them are a society where trust can be observed in interactions within such artificial societies.
5. Agents are generally *independent*. Within a society of independent agents, its behaviour can be readily investigated and observed, and anomalies detected.

- **Marsh's Trust Model Formulas [5]**

Where variables and notations are defined as:

[1] https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

- x *and* y *are two different agents.*
- T_x is the basic trust of agent x.
- x trusts y in situation α.

Marsh distinguished three different aspects of trust that are formalized as follows:

- **Basic Trust:** $-1 \leq T_x < +1$
- **General Trust**: $-1 \leq T_x(y) < +1$
- **Situational Trust:** $T_x(y, \alpha)$

Table 1: Summary of Notation [5].

Description	Representation	Value Range
Situations	$\alpha, \beta, \cdots$	
Agents	$a, b, c, \cdots$	
Set of agents	A	
Societies of agents	$S_1, S_2 \cdots S_n \in A$	
Knowledge (e.g., x knows y)	$K_x(y)$	True/False
Importance (e.g., of α to x)	$I_x(\alpha)$	[0, +1]
Utility (e.g., of α to x)	$U_x(\alpha)$	[−1, +1]
Basic Trust (e.g., of x)	T_x	[−1, +1)
General Trust (e.g., of x in y)	$T_x(y)$	[−1, +1)
Situational Trust (e.g., of x in y for α)	$T_x(y, \alpha)$	[−1, +1)

3.2 Machine Trust

In the previous section, we presented the general concept and models of trust, both between humans and between humans and machines (trust in technology). In this section, we outline the state-of-the-art in modelling trust between machines, especially ones connected over telecommunication networks.

3.2.1 TRUST IN M2M/IOT

Due to the ubiquity of fixed and mobile networking infrastructure and the extension of the Internet to not only interconnect computer networks, but also things interacting with each other in Machine-to-Machine/Internet of Things (M2M/IoT) fashion, there has been a resurgence of academic research in the domain of trust modelling of these interactions during the last few years. In that context, trust refers to the faithfulness in the identification of machines/devices for communication and further involves th e reputation-building between the machines/devices and the infrastructure, leading to a way to make the network secure, while preserving its privacy.

The work in [7] proposes a M2M trust model that introduces two trust metrics: (1) pairwise similarity-based feedback credibility and (2) threshold-controlled trust propagation. They demonstrate that their trust computation model can effectively constrain malicious nodes to gain direct trusts from dishonest feedback ratings by leveraging feedback credibility. Furthermore, their threshold-controlled trust propagation mechanism can successfully block the trust propagation from good nodes to malicious nodes.

[8] proposes a secure trust evaluation method in which privacy of trust values and relevant weights are preserved. The proposed method is constructed based on an information theoretic framework for modeling trust and two approaches that propagate trust in a network, i.e., multipath and referral chain techniques. This utilizes secure multiparty computation to provide protocols by which the nodes in a network will be able to evaluate their trust values in a secure fashion. An application of this method in the context of network routing protocols is also presented.

The more recent [9] survey analyses extensive research literature on security, privacy and trust in the M2M/IoT context. Trust modelling and trust management approaches are specifically classified, based on the categories shown in Figure 3.

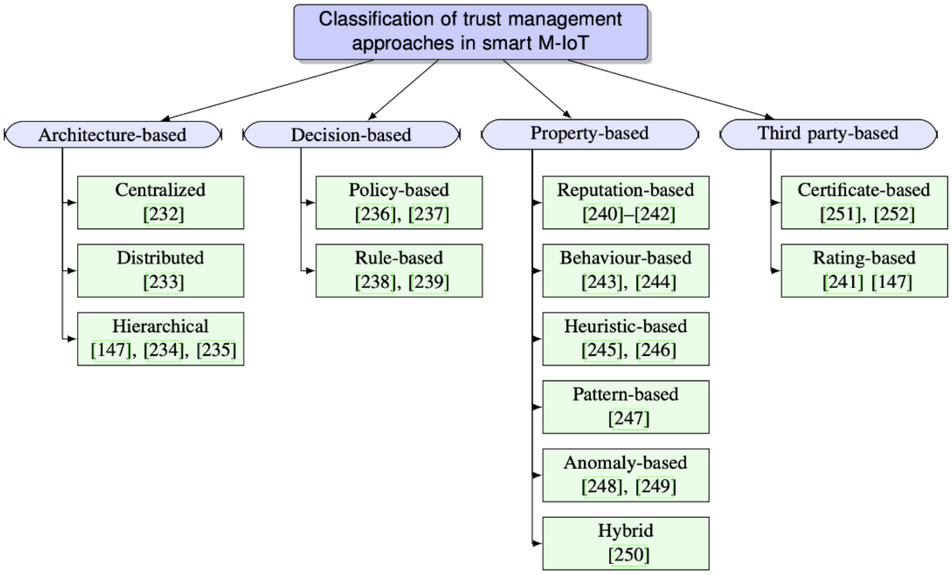
Classification of trust management approaches in smart M-IoT
Architecture-based
Centralized [232]
Distributed [233]
Hierarchical [147], [234], [235]
Decision-based
Policy-based [236], [237]
Rule-based [238], [239]
Property-based
Reputation-based [240]–[242]
Behaviour-based [243], [244]
Heuristic-based [245], [246]
Pattern-based [247]
Anomaly-based [248], [249]
Hybrid [250]
Third party-based
Certificate-based [251], [252]
Rating-based [241] [147]

Figure 3: Classification of trust management approaches in M2M/IoT [sharma_arxiv_2020].

Please refer to Section VII of [9] for the definition of each of these categories and corresponding trust models, as well as to Table VIII for an overview of the corresponding work referenced by the survey.

3.2.2 TRUST IN PHYSICAL AND VIRTUAL NETWORKS

In the previous subsection, we provided references to literature related to the trust modelling and management of machines/things/devices that interact with each other through global communications networks. But how did the computational trust model (see section 3.1.4) actually evolve when we transitioned from centralized systems to distributed computing and, subsequently, to virtualized & cloud computing?

Trust in networks is established through strong confidentiality, integrity and availability guarantees that are ascertained by corresponding measures in the appropriate OSI Reference Model layers (ITU-T X.200 - ISO/IEC 7498 and, particularly, ITU-T X.800 - ISO/IEC 7498-2 Security Architecture). At a high-level, measures involve:

- **Ascertaining data integrity** via error checking/correction and frame/packet re-transmission mechanisms, implemented in the data link, network and/or transport layers, depending on the network medium and whether reliable data transmission is required by the application;
- **Strengthening availability** by offering multiple redundant network paths between any two points and implementing robust routing protocols (implemented in the network layer);
- **Ensuring the confidentiality** of data by applying encryption schemes which, depending on the security requirements of the network medium and application, can be in the data link, network or transport layer;
- **Authentication** of peer entity or data origin;
- **Access control** to resources accessed via the network.

Standardization of these measures for the TCP/IP protocol stack is covered by IETF technical standards, BCPs and RFCs, specifically the Security Area (https://www.ietf.org/topics/security). Important protocols include:

- Transport Layer Security (TLS): https://datatracker.ietf.org/wg/tls; the latest stable version being TLS 1.3.
- Automated Certificate Management Environment (ACME): RFC 8555 (https://tools.ietf.org/html/rfc8555).

The reason we highlight two protocols is that they correspond to two major pillars of trust in networks: i) Strong cryptographic algorithms that ascertain the integrity and confidentiality of data transmission, combined with ii) Public Key Infrastructure (PKI) that binds public keys used for encryption with respective identities of entities and is used to authenticate connection peers or data origins. The binding is established through a process of registration and issuance of (ITU-T X.509) certificates by Certificate Authorities (CA), which form chains of trust, since a CA certificate can be signed by another CA, up to the top-level "Root" CAs. It is not a surprise that many attacks to network security are conducted by compromising this chain of trust between CAs. Even though TLS is ubiquitous, ACME is relatively new and aims to streamline issuing of secure certificates.

Another important aspect of trust management in networking is dividing networks between trusted and untrusted and applying access controls and security measures in the boundaries between them. This is the model applied by enterprises that secure their corporate perimeters with traditional network controls. However, the introduction of virtual networks, hosting providers and cloud infrastructure, as well as the adoption of PaaS & SaaS services, extends the network perimeter beyond the offices and data centres of an enterprise. Albeit virtual networks by themselves don't fundamentally change the trust model of networks, other than the introduction of new actors (hosting & cloud providers) and multi-tenancy aspects, the expanded network perimeter requires new approaches, which involve adopting micro-segmentation and zero-trust approaches. Zero-trust management is elaborated further in section 4.4, while the relevant positions of major cloud vendors are outlined in Microsoft Zero Trust Networking[1] and Google BeyondProd[2].

3.2.3 TRUST IN PREVIOUS MOBILE NETWORK GENERATIONS

A trust model has been implicitly embedded in mobile telecommunication systems since the first-generation analogue implementations. But per the [10] published towards the end of 5G-PPP Phase 1, there is no explicit and complete trust model documented for 3G and 4G networks. This introduced challenges in the 5G context, where new actors are entering the value chain, new types of services and devices, etc. Also, the trust model applied in the inter-operator networks, designed for a small number of large national operators, was considered problematic, causing concerns of e.g. impersonation on signalling interchange networks. Second, virtualization and management aspects are largely left outside the scope of [11], which is not sustainable for 5G, which depends heavily on orchestration aspects. Third, for mission critical services (health, transport, industrial automation, etc.), an entirely new threat and risk landscape applies. The damage done by cyber-attacks to safety (potential loss of life) goes way beyond the impact on the "mobile broadband" type services that are the norm in 3G/4G networks.

3.2.4 TRUST IN 5G NETWORKS

As we mentioned above, there is a need for robust and effective trust modelling and trust management in 5G networks, since they are multi-tenant, heterogeneous and service-based systems. The white paper [10] provides an update on early efforts to that direction, summarizing the activities of many 5G-PPP Phase 1 projects (i.e., 5G-ENSURE, 5G-Ex, 5G-NORMA, CHARISMA, COGNET, SONATA, SPEED-5G, SELFNET and VirtuWind).

Most of the work on trust modelling in 5G-PPP projects so far was done as part of 5G-ENSURE. Relevant project deliverables include Deliverable 2.2: Trust model (draft)[3] and Deliverable D2.5: Trust model (final)[4].

One of the goals of 5G-ENSURE was to make trust assumptions an explicit part of the architecture. Per Section 6 of the abovementioned white paper, 5G has been developed with two levels of trust models that are embedded into the 5G architecture:

- The first level of the trust model is in respect to stakeholders. Characteristics of this aspect of the trust model are: i) to evaluate the stakeholder's trustworthiness in the network, ii) to measure the security strength of stakeholder's network and services, iii) to quantify the stakeholder behaviour in the network, and iv) to migrate the risks and vulnerability autonomously through interactions between stakeholders. Trust thus becomes an essential aspect of 5G architecture stakeholders to act dependably, reliably and securely within a specified service level agreement (SLA) and policies.
- The second level of the trust model relates to network entities, e.g. software-defined mobile networking controller/coordinator/orchestrator, physical and virtual network functions, etc. Similarly to the above, characteristics of the network entities trust model are: i) to evaluate the network entity's trustworthiness in the network, ii) to measure the strength level of security mechanism used in the network entities, iii) to quantify the network entities behaviour in the network, and iv) to migrate the risks and vulnerabilities

[1] https://www.microsoft.com/security/blog/2020/06/15/zero-trust-part-1-networking/

[2]https://cloud.google.com/blog/products/identity-security/beyondprod-whitepaper-discusses-cloud-native-security-at-google

[3] http://5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.2-TrustModel.pdf

[4] http://5gensure.eu/files/5g-ensured25-trust-model-final-v22-inc-historypdf

autonomously through interactions between network entities.

In 5G, machine trust models will be needed to support trust decisions over the selection of physical and virtualised assets and provisioning of (virtualized) infrastructure and applications. Machine trust models can be used in this context to provide quantified estimates of trustworthiness, and so enable automated decisions to accept or avoid specific interactions or dependencies.

As noted above, such estimates of trustworthiness may also be useful to provide decision support for human users, e.g. by using trust models to calculate the reliability of different network services, and providing feedback on this to a human through their UE devices.

Trust and trustworthiness by design models aim to capture the relationships between the architecture of a system and the types of risks that may be present. This in turn provides a basis for identifying and analysing the trust decisions that may need to be taken by system components and stakeholders.

Ultimately, a decision to trust (in a system, stakeholder or component) is equivalent to accepting one or more risks. The alternatives are to avoid the risk (i.e., distrust and disengagement), transfer the risk (e.g., by making other stakeholders responsible for that risk through the terms of use, or by insuring against the risk so an insurance company pays for any damage caused), or to reduce the risk by introducing security measures. Consequently, trust(worthiness) by design models tend to start from the premise that risks can be reduced by using security controls, and the purpose of the model is usually to identify where this might be needed, and decide when it is appropriate.

Trust (as opposed to trustworthiness) comes into these models in two ways:

- as one of the two possible risk management responses (along with distrust) where the risk cannot be transferred, and security controls would be disproportionate or cannot be used at all; and
- as a property of (at least human) participants that allows them to engage in the system, whose loss could represent a source of risks to the system (if one considers users to be part of the system).

Among others, major purposes these types of models can serve are to:

1. Enable design-time analysis of trust and trustworthiness in a vertical 5G application ecosystem, which can be used to support decisions about the design or configuration of security features.

2. Capture the (system-related) context for trust decisions by humans or automata, within which quantitative trust models can be used to assess specific concerns at run time.

Such models could also be used to provide a tangible measure of the effect of 5G security enablers on the trustworthiness (and where appropriate trust) in 5G networks. They may also be used to identify where additional security enablers might be needed, so consideration can be given to adding these to 5G Security Technical Roadmap.

In 5G, there will be more stakeholders involved in the delivery of any service, due to the opportunities created by virtualisation technology to create multiple virtual networks each of which may serve specific communities or applications. There will be also more recognition of who trusts whom to do what, driven at least in part by the need to manage risks associated with the complex and application-dependent interdependencies if the opportunities of virtualisation are to be seized.

It is not straightforward to enumerate the stakeholders and trust relationships in a 5G network. One side effect of virtualization is that the relatively static roles found in 4G networks are much more fluid, and services can be composed from other services in more complex ways. This leads to a more complex (and more application dependent) set of stakeholders and relationships. The 5G trust model should recognize a set of roles that stakeholders might take, based on the 4G actor model above plus some new roles such as Virtual Infrastructure Providers, Virtualized Network Function providers, Vertical Application Service Providers, etc. However, the relationships between these actors will not be fixed, but should be flexible enough to capture different configurations that may be found in different scenarios and value chains.

It is anticipated that stakeholders will want to define their roles and responsibilities to each other via SLAs, given that these responsibilities may vary depending on the scenario. To formulate such agreements, it will then be important to capture expectations and the ways in which things could go wrong.

Other more recent projects that are active in the area of 5G trust modelling and management are:

- INSPIRE-5Gplus[1]

As noticeable from the abstract, vision and concept, they propose an "automated end-to-end smart network and service security management framework that empowers not only protection but also trustworthiness and liability in managing 5G network infrastructures across network slices that span multiple domains". The verticals they target are "ranging from autonomous and connected cars to Critical Industry 4.0".

- 5GZORRO[2]

As noticeable from the abstract, vision and architecture, they propose a "zero-touch service, network and security management in multi-stakeholder environments, making use of smart contracts based on Distributed Ledgers and Distributed AI Technologies". Per the abstract & architecture, they focus on slice orchestration as well. On the other hand, they don't focus on specific vertical industries, please see use cases.

4. Trust Dimensions in 5G Networks

4.1 Overview

The previous section 3.2 outlined the motivations for trust management in telecommunications. Assuring trust gained a lot of interest since commerce was enabled on the internet, in order to assess the level of confidence that a customer can have on an online store. It relates to the attestation mechanisms in place to communicate if the involved parties can be trusted. Since telecommunication networks are adapted to new services and gain other functionalities, trust concepts have been incorporated into them.

In contrast to previous mobile network generations, 5G has a business approach in which generic services such as Mobile Broad Band (MBB) evolve into unique and differentiated services. This permits to address a

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

[2] https://5g-ppp.eu/5gzorro/, https://www.5gzorro.eu

richer set of customers, offer different QoS to sell services that go beyond pure connectivity and, in this way, create new value chains [12].

The quest at this moment is how to ensure trust in the mobile network as a whole, as well as between its elements. Moreover, with the elements outside of it that interact with the network.

4.2 New Requirements in 5G

An important remark for 5G is that, as mobile networks evolve:

(i) the number of internal components increase;

(ii) the protocols that are used change, are improved and increase in number and use cases;

(iii) the chain of software development speeds up, due to the characteristics of software (open source);

(iv) the inclusion of new stakeholders from diverse provenances makes difficult to map their interactions and have attestation of their credibility; and

(v) the realization becomes more virtualized, leading to requirements regarding the applicability of hardware-based trust assessment to a virtualised infrastructure and the integrity and privacy of virtual instances hosted on multi-tenant platforms [13].

As a consequence, mobile networks are more opened up, making the ecosystem more complex; with a greater attack surface compared with its predecessors, because of the addition of more network functions and because of the use of virtualized elements; and with more actors and stakeholders playing a role, having multiple interactions which have to be trouble-free, mapped and trusted [12].

For instance, these new qualities and requirements have an impact on the security and privacy of this technology. Lessons learned from previous standards provide a futuristic mindset, so the security considerations seek to anticipate to future security challenges. Due to its tight relationship with cloud technologies, 5G is going to use security mechanisms that are already in use by IT systems, closing even more the gap between IT and TT.

Attack surface is braider, not only because of the increasing number of devices and network functions, but also because of the rising amount of services. These services will require control plane and exploding amount of user traffic, transferred at a higher speed. Due to these characteristics, the window opportunity to stop a menace is smaller. Linked to the attack surface, there are risks about the provenance of equipment and developers of the network functions. Trust issues are important to be considered, as will be shown in the next section.

4.3 Trust Considerations in 5G

From a point of view of the attestation of trust, there are four dimensions to take into account [14]:

1. **Trust stack on entities**: a chain founded on a root of trust. This way, we can assure (i) the provenance of the data; (ii) the identity and integrity of the source of the data; and (iii) the integrity of the data itself. The chain of trust can be founded by the use of Trusted Platform Module (TPM). Other part of the problem is the trust on where the entities are instantiated, that is, the underlying infrastructure.

The idea is to have attestation of the nodes in the NFVI in order to have trust in the NFV environment. For this, a Trust Manager is added in MANO, outside the NFVI [15].

2. **End-to-end trust**: After each entity has its own assured trust stack, it is necessary to evolve into the problem of how to communicate this trust with other entities that are involved in the end-to-end service. An attestation server is needed for this purpose, in order to enforce the trust policy and to maintain trust relationships. These trust relationships can relate to the machines where the code is executed (at infrastructure level) or related to slices that need to communicate between them (at a service level).
3. **Supply chain integrity**: This refers to the trust of all software and hardware that are used to realize the end-to-end services in 5G. This is difficult to assure since a lot of actors are involved, at different levels of the architecture. An alternative is to annotate or notarize the data between entities, by coupling it with the underlying chain of trust. Since each component has its own manager, not only for the service, but to manage the trust, synchronization is needed between Trust Manager and the other managers [13].
4. **Dynamic trust**: Trust changes through time, it is not static. Thus, it is necessary to consider feedback loops in order to re-evaluate trust conditions and assure that the trust policies are valid. Beyond conditions, evaluation process must consider the cost and consequences of continuous trust assessment in terms of processing capacity, calculation time and latency.

Trust is a complex topic, since trust models are not only between users and network operators, but also between network operators and service providers. Service providers range from providers of sim cards, IoT devices or even machine learning models and artificial intelligence based services. This broadens the scope of the trust relationship.

Several strategies can be envisioned to realize these four dimensions. Notarization schemes and certificates of provenance as a way to assure the integrity of the systems that are used; the usage of an on-chip root of trust in order to have assurance of the identity of the used elements and the correct attestation of all the chain of components. Several technologies are envisioned to provide these requirements, as the Zero Trust paradigm, which will be addressed in the next section.

4.4 Zero-Trust Management

The objective for all Communication Service Provider (CSP) is to offer services that are trusted by its customers. The most trustful the services are, the more likely those customers will continue purchasing services, and at the same time, attracting new customers. Building that trust requires optimized security operations from the source device up to the cloud edge and the core network. Three conditions help to build this trust: insight, scalability and adaptiveness [16]:

- **Insight**: refers to the self-knowledge of the security posture of the CSP, in order to know how ready the CSP is in order to respond to attacks. It considers the preparation of 'playbooks' not only as response mechanisms, but also as part of new service creation and deployment.
- **Scalability**: refers to the capacity of the CSP to respond to attacks and add resources as needed to defend its network and its customers. Automation is needed in order to perform the prevention – detection – response – recover life cycle. Tools as artificial intelligence are necessary to deduce an adequate response.

- **Adaptiveness**: refers to the usage of security management strategies that suit each of the inner domains of a network. In our case, each component of the 5G system (RAN, edge, CN, DN) has its own requirements, SLA and security constraints which must be controlled and verified. The security manager adapts to the type of component, detects threats earlier and deploy the suitable countermeasure.

A way to fulfil these conditions and gain customer trust is by using the Zero Trust paradigm.

Zero Trust (ZT) is the term for an evolving set of cybersecurity paradigms that move network defenses from static, network-based perimeters to focus on users, assets, and resources [17]. This approach is born from the fact that there is no single, easily identified perimeter for a network. Perimeter security is insufficient because it does not properly address internal threats. Actually, an intentional act, a misunderstanding of the functioning or an implementation error are likely to damage the protected resource. ZT focuses on the protection of the resource, and not on the network segment containing it, since the resource's location in the network is no longer considered to be a primary safety criterion.

In addition, there is no default trust for any entity. Actually, before establishing a session with the resource, it is necessary to firstly verify the user, his device and the targeted application using a secure authentication method, and secondly to provide secure access control mechanism for defining and restricting access rights. ZT relies on continuous analysis and risk evaluation of internal assets to maintain or deploy further protections to mitigate risks.

The principles of ZT architecture are:

- Data sources are considered resources in the same manner as services and applications. For example, devices that send data to aggregators or storage devices, systems that send instructions to actuators, etc. are included as resources.
- All communication should be done in the safest way regardless the location of the device in the network.
- Access to a resource is granted on a per-subject session basis, with as few privileges as possible to accomplish the task at hand.
- Access to resources is determined by a dynamic policy, which includes the observable state of the requester and the requesting assets, and other possible behavioural and environmental attributes.
- The security status of resources should be continuously monitored and verified, corrective action must be taken to maintain the proper level of security, and denial of access may be instated if this cannot be reached.
- Authentication and authorization are required before granting access to resources. Moreover, according to the security policy, re-authentication and re-authorization can be requested following a change in the state of the resource, its behaviour or its environment.
- Continuous monitoring of resources, traffic and network infrastructure, to collect data to improve policy creation and enforcement.

Addressing the issues and enabling the realization of this concept involves applying the Zero Trust Architecture (ZTA), which is presented in Figure 1.

The key components in this architecture are:

- Policy engine (PE): provides the final decision to allow or deny access to a resource for a given subject.

The PE makes the decision using policy and environmental-external sources of information.

- Policy administrator (PA): responsible for issuing credentials/tokens to grant access to a resource, under decision issued by the PE. Via these credentials/tokens, permissions can be revoked and this way, cut the communication path between a subject and object.
- Policy enforcement point (PEP) responsible for enabling, monitoring and terminating connections between a subject and objects, according to instructions received from the PA, which is in the control plane. This is possible because the PEP is in the data plane.

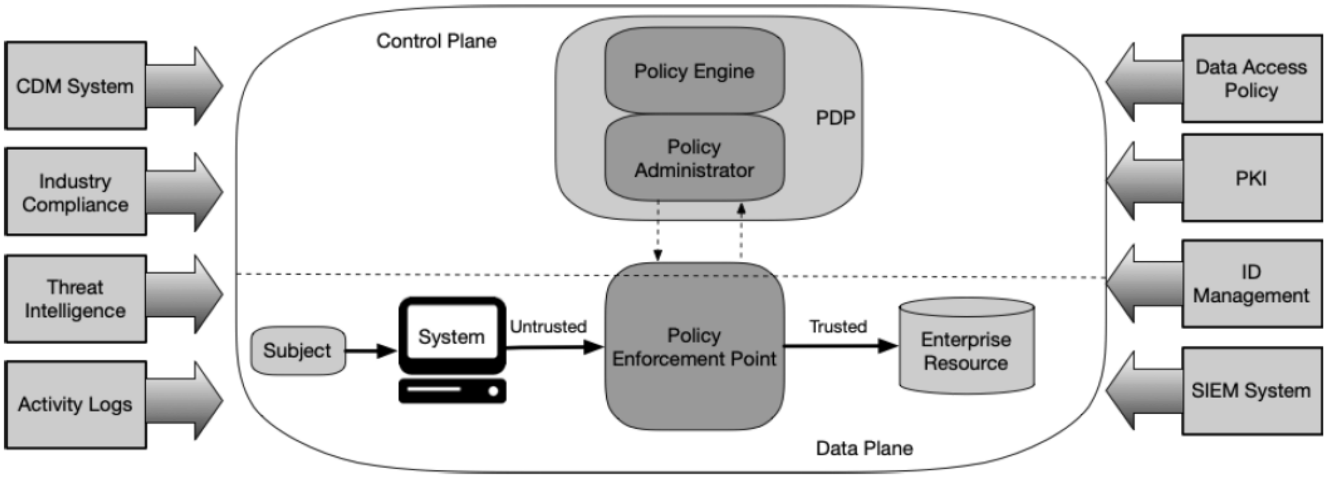

Figure 4: Core Zero Trust Logical Component, from [17]

In addition to these components implementing a ZTA, a suite of data sources feed the policy engine with input and policy rules used to make access decisions. These data sources can be either local or external to the enterprise, and as shown in Figure 4 the following can be highlighted:

- the *Continuous Diagnostics and Mitigation (CDM) system*, which keeps the settings, software and description of the managed equipment up to date. It informs the PE of this information for the devices that have access to the services;
- *Industry compliance system*, which provides regulatory criteria that the PE should ensure the compliance with when defining policy rules;
- *Threat intelligence*, which updates the PE with discovered threats and vulnerabilities;
- *Data access policies*, which enclose attributes, rules and policies about access to data, applications and services;
- *Enterprise public key infrastructure*, which is in charge of generating certificates to subjects and resources;
- *ID management system*, which manages information about subjects such as identities, roles, and assigned assets;
- *Network and system activity logs and Security information and event management (SIEM) systems*, which improve asset protection by updating access rules based on the security information collected.

The PE uses the Trust Algorithm (TA) in its process to decide on granting or denying access to resources. The inputs for the TA are not limited by the information about client, device, service and policy provided by the above data sources, it can also include environmental parameters as well as behavioural attributes. Environmental attributes comprise location and time, while behavioural attributes indicate the reason and the method.

The management of these pieces of information varies from CSP to CSP, according to its interest and type of business service offer. This reflects on the weight that each data source has on the TA. The algorithm that operates on those inputs varies according to the access control problem that wants to be addressed by the CSP. According to [17], two methods can be used to implement a TA:

- **Criteria-based vs score-based**: Criteria-based allows an access to resource if the required conditions are met. Score-based uses weights to the information sources and computes a confidence level. If that level is superior to a threshold, the access is allowed.
- **Singular vs contextual**: Singular TA treats each request as a new one, this means that no history of subject or object are used to take a decision. A contextual TA takes into account the history of the entities when evaluating the access request. In consequence, the PE has to keep state information and enables it to detect unusual behavior of the requests. In [1], the author proposed to use the method *Kipling* to define access rules to resources. This method consists of answering six questions (who, what, when, where, why, how) to determine the conditions of access to a resource for a subject. As a consequence, trusted traffic is whitelisted and the exposed attack surface is reduced.

Contextual TAs are desired, however, a balance of security, usability and cost-effectiveness must be reached in order to create the TA. After its implementation, it is recommended to have a testing and tuning phase in order to verify how the TA behaves. At the end, it is important that, since the entities that interact in the network are dynamic, the TA must be reevaluated in a timely matter, in order to assess whether the trust threshold – score – conditions still hold in order to preserve (or revoke) access to resources.

4.5 Trust between Entities

Multiple trust dimensions need to be considered by a Trust Management System (TMS) in order to establish trust between network entities involved in a 5G and beyond network ecosystem [18]:

4.5.1 TRUST IN COMMUNICATION

The means of contact between the communicating entities may be susceptible to a range of different threats, such as spoofing, DDoS, Man-In-The-Middle (MITM), message replay, eavesdropping and even manipulation [19]. Efficient and secure information sharing is therefore essential to guarantee the accessibility of services while avoiding data leakage and confidentiality. Authentication, authorization, and encrypted transmission services are necessary for this reason. The authentication mechanisms ensure that contact between valid entities is made. It should be remembered that 5G expands the confidence paradigm to cover service providers, as opposed to 4G and previous generations as seen in the Figure 5. As a consequence, 5G implements a modern security mechanism that enables an end-user system to conduct not just a primary encryption for network connection but also a secondary services access authentication [20]. In order to ensure compliance with privacy standards and to avoid the risks of sensitive information leakage and manipulation, control messages or user data should be exchanged via encrypted and integrity-protected channels. In addition, interfaces used to consume and provide services must also be protected. Indeed, the key role played by the Application Programming Interfaces (APIs) in integrating and orchestrating services makes them an ideal target for attackers [21]. By 2022, API abuses are expected by Gartner[1] to be the most-frequent attack vector. Such abuses may involve identity theft, DDoS and MITM. The API security can be enabled through the implementation of various security measures, including authentication (e.g., using OAuth2.0, JWT tokens), authorization (e.g., using Role Based Access Control, Attribute Based Access Control), communication encryption (e.g., using Transport Layer Security (TLS)), input validation, and throttling/rate limiting [21].

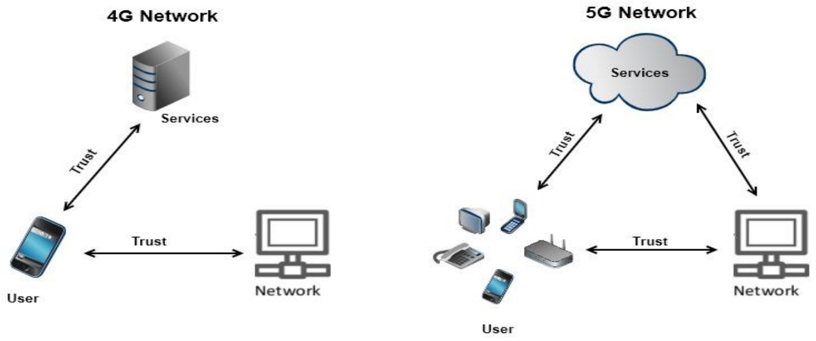

Figure 5 : 4G vs 5G Trust Model.

4.5.2 TRUST IN VNF

The virtualization of network services poses new protection issues given its potential for the provision, scaling, mobility and cost-effectiveness of network infrastructure production and implementation. Evidently, a malicious or infected VNF may escalate privilege, escape isolation, expose and exploit data, distribute malware and conduct DoS attacks. For example, a harmful VNF can manipulate obtained packets prior to transmission to the next VNF in the service function chain or restrict resource access to co-located VNFs by extenuating common resources. Mechanisms are thus essential to construct and evaluate the trustworthiness of VNFs during their lifetime [22]. During on-boarding and eventual instantiation of the VNF, the validation and certification of the VNF package must be done. The validation is an authenticity and integrity process to ensure that the origin of the VNF package is from a trusted supplier and that its content has not been breached. A VNF should be certified by performing quality and security checks to ensure that the VNF software performs up to standards and is not vulnerable. The confirmation of the VNF instance identity and the monitoring of its results and actions during its lifetime is therefore crucial to creating trust amongst instantiated VNFs.

4.5.3 TRUST IN NFV INFRASTRUCTURE

This collection of physical processing, storage and network tools is the NFV Infrastructure (NFVI) and virtualization framework that generates the virtual environment in which the VNF is deployed. Since VNFs may perform dynamically time critical functions, its virtualized hosting architecture is important. Nonetheless, dangerous, and/or malicious NFVI may present serious safety dangers for hosted VNFs, such as isolation failure and introspection attacks. A compromised hypervisor may violate the confidentiality,

[1] Gartner, "How to Butild an Effective API Security Strategy," Dec. 2017.

integrity and/or availability of co-resident VNFs if a malicious VNF endangers isolation [23]. In addition, a malicious hypervisor with introspection capabilities could access, inject and/or change operating status information (i.e., code + data) associated with VNF. A NFVI should ensure its own security, as well as its ability to meet the safety and performance requirements of hosted VNFs to be trusted. Secured boot is a prerequisite to ascertaining the hypervisor and VNF integrity at load time. Measured boot (i.e., the load time integrity status) and the hardware-based roots of trust (e.g., the Hardware Security Module (HSM), Trusted Platform Module (TPM)) are a prerequisite to remote platform certification. The capacity of an NFVI to provide an isolated and trusted environment in which vital software components can be executed is necessary to avoid introspection threat. Trusted Execution Environments (TEE) are hardware-based solutions to accomplish this aim. As the NFVI can span several geographic areas, the location assertion is essential to meet the operating location rules. In fact, certain VNFs may just have to work at a specific location, geographic or logical. For instance, VNFs for lawfully interception are allowed to operate only in the country that issued the. Furthermore, NFVI should ensure the availability of resources needed to satisfy the performance requirements of the hosted services in compliance with the Service Level Agreement (SLA).

4.5.4 TRUST IN MANO

Due to the central position of NFV management and orchestration (NFV-MANO) modules (i.e., NFVO, VNFM, VIM), their compromise may endanger the security and operation of the whole network [24]. For example, a compromised or impersonated NFVO could carry out malicious actions on VIM that contribute to the depletion of resources resulting in DoS attacks. In order to build confidence in MANO modules, it is important to guarantee their resiliency, reliability and availability. To avoid masquerade attacks, mechanisms to verify the identity and integrity of MANO components are essential. Moreover, MANO components require continuous evaluation of their activities and their resistance to security threats in order to trust in their actions. Finally, to satisfy availability and geographical restriction requirements, adequate redundancy procedures are needed [24] .

4.5.5 TRUST IN AI/ML

AI is necessary for integrating cognitive and self-managing capacities into 5G and beyond networks, allowing fully autonomous networks that can meet the stringent bandwidth and reliability requirements. Nevertheless, the implementation of AI systems poses questions regarding reliability, safely, security, and accountability. At the one side, the AI systems are vulnerable to many adversarial threats [25,26], which may cause them to learn incorrect patterns, make wrong decisions or leak sensitive data. On the other side, the field specialists (e.g., telecommunications operators, verticals) require assurances to trust the decisions made by the AI system. Therefore, AI will inadvertently become harmful without enforcing its trustworthiness, which endangers not only the performance expectations of 5G and beyond networks but also the lives of people. To inspire trust in its decisions, an AI system must be able to explain its reasoning. For example, a telecommunication operator needs to clarify the decision reached by an AI-driven network optimization solution that has failed to satisfy the high-latency criteria. An explainable AI investigates what, how and why a decision was made, which allows to implement accountable, reliable and transparent AI systems. Data processing must be performed in accordance with privacy legislation by the AI systems. The attestation of robustness and resiliency of AI/ML models for adversary attacks is another essential criterion for empowering trustworthy AI.

4.5.6 TRUST IN DATA

AI is a crucial enabler to empower autonomous self-management capabilities in 5G and beyond networks. Nevertheless, the ability of AI in achieving those capabilities is highly contingent on the quality of the underlying data. Indeed, manipulated and inaccurate data may greatly affect the quality of strategic and intelligence decision-making processes. For example, incorrect historical traces of a user's location will contribute to wrong forecasting of his next position, which may mislead the caching service to make the correct decision on whether and where the user's content will be cached beforehand. The trust of data therefore needs to be assured. Many factors help to create trust in data, including data quality, data provenance and data security. The data quality refers to data that is appropriate for use by data consumers [27]. Accuracy, completeness, timeliness, validity and consistency are the main criteria used to measure the quality of data. The conformity with the necessary data quality must be assessed and tracked across the whole data life-cycle in order to maximize data trsutworthiness. The data origin promotes confidence in data by tracking their source and derivation history. The purpose of data security is to protect data from tampering by carrying out integrity checks.

The main security threats discussed above as well as the potential measures to establish trust between network entities involved in a 5G ecosystem are summarized in Table 2.

Table 2: Summary of trust dimensions between entities in 5G ecosystem, the related security threats and the potential measures.

Trust Dimension	**Potential Security Threats**	**Potential Security Measures to Build Trust**
Communication	• Spoofing • DDOS • MITM • Message reply • Eavesdropping • API abuses	• Authentication and authorization controls • Encrypted transmission services (e.g., TLS) • Throttling/rate limiting APIs usage
VNF	• Privilege escalation • Escape isolation • Data exposure and exploitation • Malware dissemination • DDoS attacks	• VNF software validation (authenticity and integrity) • VNF software certification (Quality and security tests) • VNF instance identity assurance • VNF instance’s behaviour and performance monitoring
NFV Infrastructure	• Isolation failure • Introspection attacks	• Secured boot • Measured boot • Hardware-based roots of trust (e.g., HSM, TPM) • TEE
MANO	• Impersonation	• Identify and integrity mechanisms

	• DDOS (resource depletion)	• Continuous assessment of MANO's activities and resiliency to attacks • Redundancy procedures
AI/ML	• Incorrect patterns learning • Wrong decision making • Sensitive data leakage	• Explainable AI • Privacy-preserving AI/ML • AI/ML models resilient to adversarial attacks
Data	• Manipulated and inaccurate data	• Data quality (accuracy, completeness, timeliness, validity, consistency) • Data provenance (Track its sources and derivation history) • Data security (integrity checks)

5. Trustworthy Cross-domain Slice Composition

The previous section discussed the trust considerations and dimensions in 5G networks. In this section, we focus particularly on trust in network slicing. The requirements and the appropriate control mechanisms that are needed to establish trust in the composition of network slices across multiple domains will be presented.

5.1 Trust in Network Slicing

In order to develop trust in the composition of network slices between multiple domains along with its possible multiple stakeholders, some key points can be taken into account:

- **API security**: This element takes into account how APIs are consumed (exposed). It does not only relate to the consumption from the trusted entities from a single provider in the Service Based Architecture (SBA), but how another Communication Service Provider (CSP) can consume APIs from other domains/CSP/stakeholders. Efforts into this initiative are supported by the TM Forum [28]. Likewise, in [29], GSMA presents the efforts of 3GPP to offer horizontal APIs thanks to the inherent functionalities of the Network Exposure Function (NEF) and Service Capability Exposure Function (SCEF). These functions permit to securely expose and discover the services and capabilities provided by 3GPP network interfaces.
- **Traceability of operations**: Trust involves also the confidence on the service requests and the resources that are assigned. Blockchain is a technology that could be used to ensure that operations between stakeholders are tracked and not changed. Moreover, it can be used as a mechanism to keep track of what are the resources that are assigned to network slices.
- **Identity management**: 5G and network slicing rely on a cloud native approach. Trust and verification will be the key security enablers. For this, CSPs will need to assure the confidentiality, integrity and availability of their data as it is transmitted, stored or processed by third parties in the service chain that leverages on shared resources in the cloud. Identity management capabilities for both users and infrastructure components will be a major requirement in order to build trust [48]. An identity

management system, which exploits blockchain technology, presents an advantage over traditional authentication and authorization methods since it establishes trust between the parties and guarantees the authenticity of data and certificates without revealing the actual data, thus preserving privacy.

- **Continuous evaluation of trust**: Trust can change through time. Stakeholders can experience certain failures or security breaches that can jeopardize the services that they provide. It is necessary to establish multi-dimensional criteria to represent the credibility of providers under a concrete context [30]. In order to evaluate trust, it is more useful to have its quantification. For it, basic criteria such as confidentiality, integrity, availability and reliability can be used in order to build a ranking. This quantification can be used to accept or deny interactions between stakeholders, based on the minimal trust level that is desired [31].

5.2 Trust Requirement on the Slice Composition

A network slice is a composite element that exploits the services offered by its constituent network slice subnets to provide end-to-end communication services. For instance, a 5G core network slice usually relies on three network slice subnets, such as an access network NSSI (Network Slice Subnet Instance), a serving network NSSI, and an Internet protocol network NSSI. The NSSI members of the same NSI can communicate with each other to exchange data, delegate a service or chain a sequence of actions to achieve an end-to-end service.

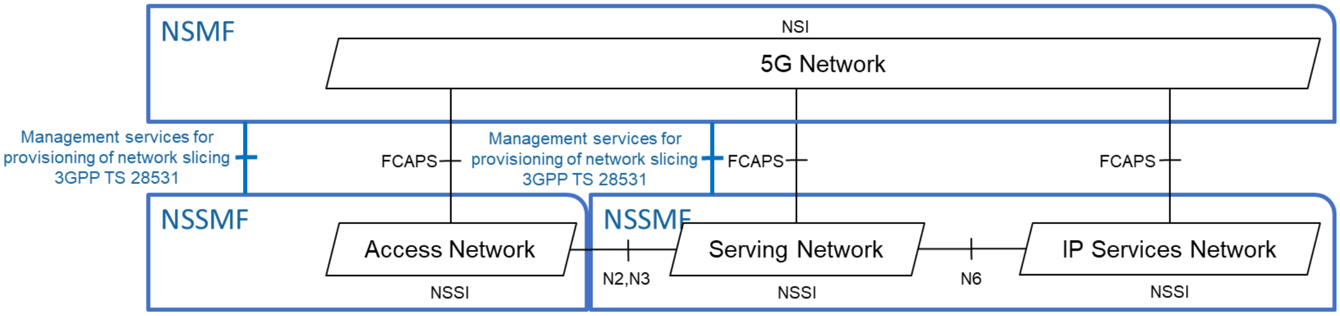
NSMF
NSI
5G Network
Management services for provisioning of network slicing 3GPP TS 28531
FCAPS
Management services for provisioning of network slicing 3GPP TS 28531
FCAPS
FCAPS
NSSMF
Access Network
NSSI
NSSMF
N2,N3
Serving Network
NSSI
N6
IP Services Network
NSSI

Figure 6: A 5G network slice made up of three slice sub-networks provided by 2 different Network Slice Subnet Management Functions.

There is a manager that controls each object class, for example in Figure 6, Network Slice Management Function (NSMF) for network slices, Network Slice Subnet Management Function (NSSMF) for slice subnets [33] The manager includes a logic for orchestrating object instances and optimizing the underlying resources used, and it and exposes interfaces to provide access to these objects. For instance, on a NSSI request made by the NSMF, the internal logic of NSSMF translates the requirements of the request into suitable amounts of resources and network functions, the latter performs the NSSI functions. We can reiterate this model of interaction between managers on the one hand, and between the objects provided by them on the other. The NSMF interacts with the NFVO via the reference point Os-ma-Nfvo for the management of network services, and a Network Service (NS) may expose FCAPS (Fault, Configuration, Accounting, Performance, Security) features to NSSI via the EM. The ETSI MANO specifications [34] [35] [36] link the information models of network services to the virtualized resources used to deploy VNFs and describe the interfaces between the corresponding managers via the reference points Or-Vnfm, Or-Vi, Vnfm-Vi. In addition, the NS [37] information model allows the nesting of one NS in another to delegate part of the functions, this makes lateral communications between the NFVOs possible.

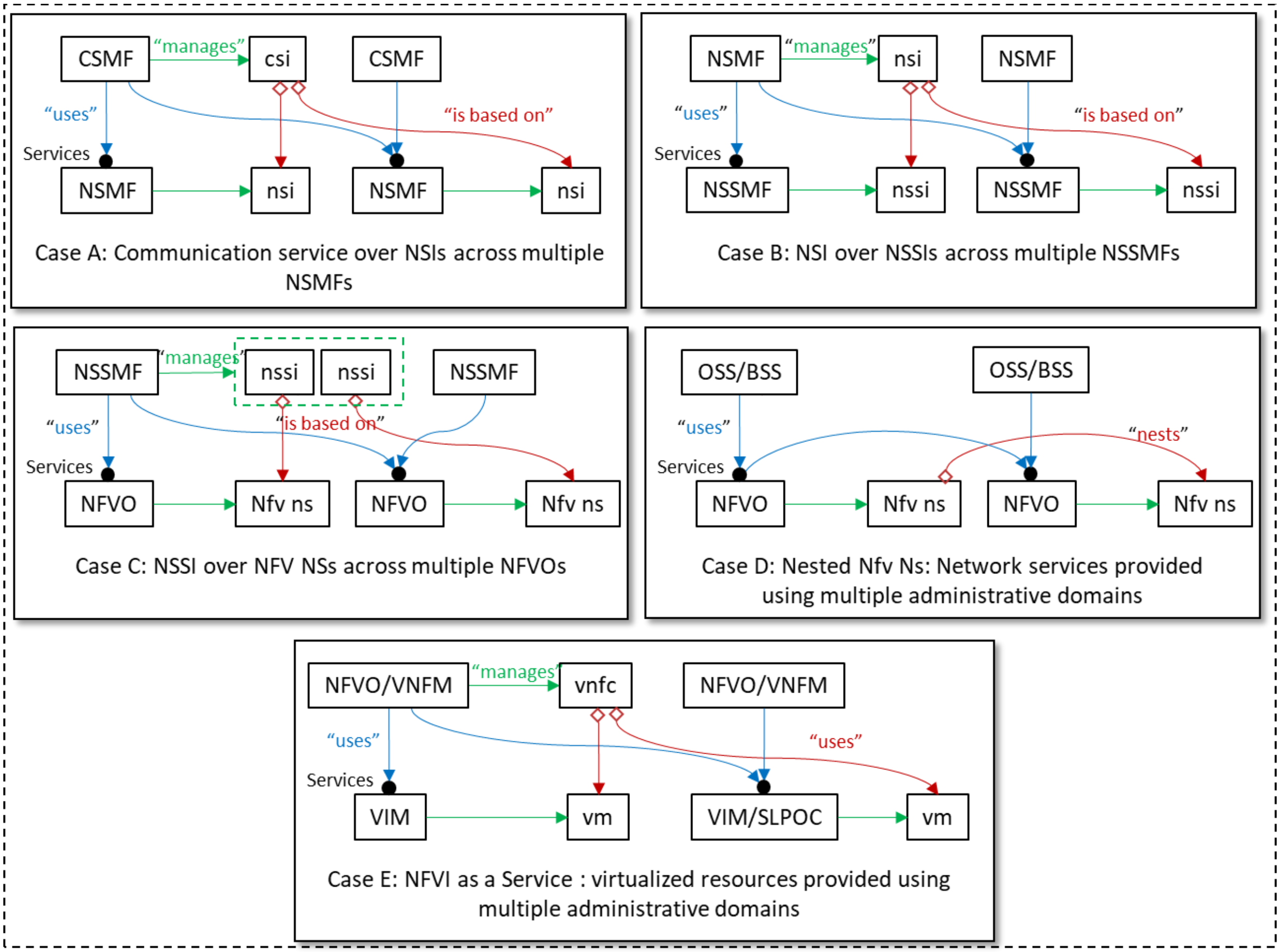
CSMF
"manages"
csi
CSMF
"uses"
"is based on"
Services
NSMF
nsi
NSMF
nsi
Case A: Communication service over NSIs across multiple NSMFs
NSMF
"manages"
nsi
NSMF
"uses"
"is based on"
Services
NSSMF
nssi
NSSMF
nssi
Case B: NSI over NSSIs across multiple NSSMFs
NSSMF
"manages"
nssi
nssi
NSSMF
"uses"
"is based on"
Services
NFVO
Nfv ns
NFVO
Nfv ns
Case C: NSSI over NFV NSs across multiple NFVOs
OSS/BSS
OSS/BSS
"uses"
"nests"
Services
NFVO
Nfv ns
NFVO
Nfv ns
Case D: Nested Nfv Ns: Network services provided using multiple administrative domains
NFVO/VNFM
"manages"
vnfc
NFVO/VNFM
"uses"
"uses"
Services
VIM
vm
VIM/SLPOC
vm
Case E: NFVI as a Service : virtualized resources provided using multiple administrative domains

Figure 7: Network slice composition use cases for services offering across multiple domains.

Managers/orchestrators and managed objects may belong to different domains, and the characteristics of a domain are multiple, they may be administrative, geographical or follow different policies. Therefore, it is necessary to select a trust model and use the appropriate control mechanisms aforementioned to establish trust before approving a subject to use a service or access data.

For the network slice composition, we identify three types of interactions where the subject and the resource (i.e., service, application or data) can be in separate domains and a trust model needs to be instantiated:

1) Manager to Manager

Case A of Figure 7 corresponds to the scenario where the Communication Service and Management Function (CSMF) manages network slice instances (NSI) across multiple NSMF to provide a communication service. According to[38] , this corresponds to the options 1 and 2 of NSI creation across multiple operators.

As for Case B, the NSMF must rely on two NSSMFs to generate network slice sub-networks capable of meeting the constraints that the customer has issued for the creation of a network slice.

Another scenario is the network slice subnet composition across operators as shown in the case C,where the NSSMF realizes its NSSI using network services offered by orchestrators administrated by different operators.

Case D is similar to Case C, where an NSSI is realized using the network services of several operators, but the network services are nested under a composite, which is the sole one visible by the NSSMF. This correspond to the use case “Network Services provided using multiple administrative domains” according to [49].

The last case E of federation is the NFVIaaS use case as described in [49], where the NFV orchestrator (NFVO) utilizes some amount of virtualized resources offered by an external VIM.

2) Composite to Component

After agreement, the component can grant the composite limited management capabilities and access to selected management data. Several composite cases are illustrated in Figure 7, such as the dependency between a communication service and its NSIs hosted by another operator in case A, or the aggregation of several NSIs to form an NSI in case B. Similarly, cases C and D show an external NFVO sharing a subset of network services in its catalog with the local NFVO or NSSMF to build a more complete and feature-rich network service or slice subnetwork. In use case E, a network service instance deployed on an external VIM must be able to rely on the isolation of the NFVO's resources to ensure the confidentiality, integrity and availability of its applications and data.

3) Component to Component

Components that are intended to collaborate with each other to construct a composite object must be certain of their exchange of services and data. In Figure 7, the Serving Network NSSI should be able to rely on services and data delivered by its adjacent NSSIs (Access Network, IP Services) regardless of their location at the NSSMF.

Figure 8 shows the delegation or federation relationship between managers to provide objects as services and the composition and dependency relationships between managed objects. At these points of interaction, credential-based trust management is most appropriate for authenticating and authorizing a manager or managed object to grant it the right to consume a service or resource shared by another manager or managed object.

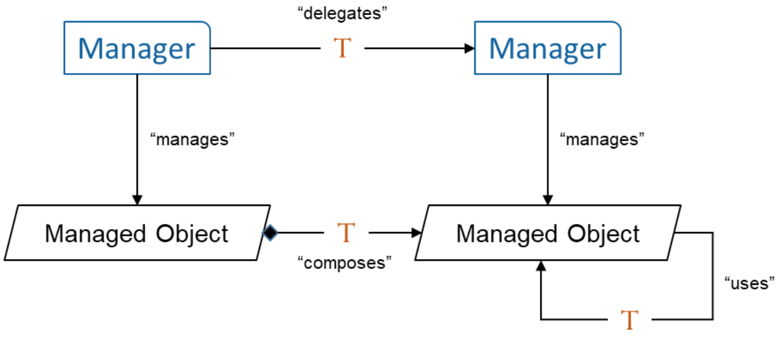

Figure 8: Trust requirement on the composition of managed objects.

5.3 MEC Slicing Security

When Slicing ETSI MEC-based Edge Computing [39], we may envision two ways of deployments of the main component which is the MEC Platform (MEP):

- In the case of MEP multi-tenancy, the MEP and User Plane Function (UPF) are already deployed by the Infrastructure owner. The MEP is shared among the Network Slices.
- In case of In-slice deployment model, the MEP is deployed as VNF along with the MEC application at the edge NFVI. Unlike the multi-tenancy model, the Mobile Edge Application Orchestrator (MEAO) requests the instantiation of both the MEP and MEC application at the same time. The NFVO deploys both, and ensures that there is a virtual link between them.

A major Network Slicing requirement is traffic isolation and security enforcement. Each NS should not be able to access the traffic or other information of other slices.

Two challenges thus arise with respect to MEC slicing: (i) The traffic redirection mechanism should ensure that a network slice cannot specify a traffic redirection policy for traffic it does not "own"; (ii) a network slice should not be able to use MEC services in a way that it gets unauthorized access to information on other running network slices, or consume MEC services not available for it. In the following, we propose solutions to overcome these issues.

5.3.1 TRAFFIC REDIRECTION

An Application Descriptor (AppD) may include appTrafficRule elements, which specify the characteristics of the traffic to offload to the MEC application via a traffic filter. Also, the MEC application provider may add appDNSRule elements, which, combined with appTrafficRule ones, allow traffic offloading using DNS domains. If a slice owner encodes in the AppD DNS rules for domains it does not own, or use a traffic filter that matches traffic flows of another running network slice, this may introduce significant security threats. A malicious application instance can (i) intercept traffic flows it is not supposed to have access to, causing confidentiality breaches, and (ii) perform ''black hole'' or other DoS attacks by diverting and dropping UE traffic destined for victim MEC instances.

We argue for augmenting the MEC NSSMF with security and access control functionality so that it can check that each MEC application has the necessary permissions to request traffic redirection as indicated in its

AppD. To mitigate these threats and offer sufficient protection to MEC slice instances, Public Key Infrastructure (PKI) technologies can be used. In particular, we propose the use of a trusted third party, which may coincide with the network operator and which can guarantee that the slice owner has the appropriate permissions to indicate specific DNS entries and traffic filters in the AppD. This necessitates extending the AppD with a field where a signature of the trusted third party over the set of appDNSRule and appTrafficRule entries will be placed.

5.3.2 *MEC SERVICES: RNIS AND LOCATION SERVICE*

Another important issue for MEC slicing is related to MEC services that expose privacy-sensitive information about the UEs of a slice, such as their (coarse) location or channel quality. Depending on the considered use case, access to this type of information should be restricted only to the slice's MEC applications. To this end, we propose two solutions, which depend on the considered deployment scenario (multi-tenancy vs. in-slice).

In the case of multi-tenancy, the MEC Platform (MEP) should check the identifier of the MEC application, and whether the latter can have access to the specific MEC service. Furthermore, it should check which are the users that the MEC application can request information about. We propose that along with any MEC service request, the Single Network Slice Selection Assistance Information (S-NSSAI) identifier of the slice where the requesting MEC application belongs is included. The Radio Network Information Service (RNIS) and location APIs should be modified to integrate the S-NSSAI of the UE in addition to the UE identifier, allowing to restrict applications to access only information on UEs of their slice. The proposed solutions improve the MEP, by allowing it to obtain more information on the network slices along with their associated users and authorizations. The MEP will be S-NSSAI-aware, in order to know to which network slice an application or set of UEs belong to, and maintain a mapping of MEC services to the slices authorized to access them and the respective permissions.

The solution is slightly different for in-slice deployment. It is not the MEP that should implement the access control mechanism, as it belongs itself to the slice. We propose in this case to rely on the RAN controller. That is, when the MEP discovers the RAN controller in charge of the zone, it includes its S-NSSAI with the request. The RAN controller can be considered a 5G Application Function (AF), which can access the Network Slice Selection Function (NSSF) via the NEF to check which are the users with this S-NSSAI, and filter accordingly the information provided to the MEP.

6. MonB5G Trust Management Vision

This section aims at presenting the MonB5G's vision of trust modeling and management approaches. MonB5G's trust vision is driven by the identified MonB5G's stakeholders and their roles from T2.1 (to be documented in D2.2), the 1st release of the MonB5G zero-touch slice management and orchestration architecture from T2.2 (to be documented in D2.1), and the thorough review of the state-of-art in trust modeling and extensive study of the trust dimensions in 5G networks in general and network slicing in particular conducted in the previous sections.

6.1 MonB5G Trust Model

The MonB5G's trust model we are proposing in T2.4 is driven by the different stakeholders and network entities involved in MonB5G ecosystem. In what follows, the MonB5G's trust model will be elaborated considering both trust among stakeholders and trust between network entities.

6.1.1 TRUST BETWEEN STAKEHOLDERS

T2.1 identified the various stakeholders' roles involved in MonB5G ecosystem (see Figure 9). The details on stakeholders and their roles is out of scope of this deliverable and will be documented in D2.2. In the current deliverable, we focus on the trust relationships between stakeholders.

The relationships between these actors should be flexible enough to capture different configurations that may be found in different scenarios and value chains while being trustworthy.

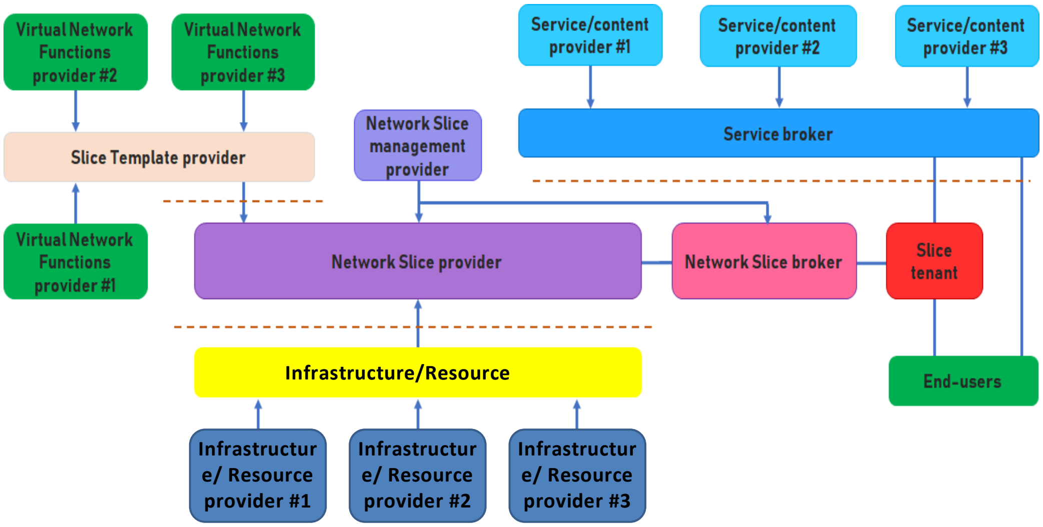
Virtual Network Functions provider #2
Virtual Network Functions provider #3
Service/content provider #1
Service/content provider #2
Service/content provider #3
Network Slice management provider
Slice Template provider
Service broker
Virtual Network Functions provider #1
Network Slice provider
Network Slice broker
Slice tenant
Infrastructure/Resource
End-users
Infrastructur e/ Resource provider #1
Infrastructur e/ Resource provider #2
Infrastructur e/ Resource provider #3

Figure 9: Overall MonB5G's business model.

In MonB5G, the trust among stakeholders is established according to the contracts signed between them. The roles and responsabilities of each stakeholder involved in the contract are specified as SLA and SSLA (Security SLA) that each party commits to deliver. A stakeholder should provide the assurance that the necessary capabilities and measures are enabled to meet the agreed SLAs and SSLAs. For instance, the infrastructure provider should ensure the availability of resources needed to satisfy the performance requirements of the hosted services in compliance with SLA. A network slice provider should ensure that the appropriate isolation level is achieved in order to prevent cross-slice atacks.

The fulfillement of agreed SLAs/SSLAs or their violations allow to define the reputation and the trust level of entities involved in composition, monitoring and dynamic management of network slices. MonB5G will provide a trust management module (TMM) which will maintain a set of historical information of the interactions of the various stakeholders, based on which it will be capable of deriving trust and reputation metrics. This information will include (secure) performance ratings (e.g., E2E KPIs, per technological domain performance indicators), history of SLA compliance and will act as a trustworthy KPI Scoreboard. The reputation and trust levels computed by the TMM are used to securely compose end-to-end network slices while outsourcing resources from different infrastructure providers for each technological domain. Section

6.3 will elaborate the trust management approaches proposed by MonB5G. The approaches advocate the use of **Blockchain** and **smart contracts** to enable secure and automated domain-slice resource auctions as well as automated SLA arbitration and compensations.

6.1.2 TRUST BETWEEN NETWORK ENTITIES

Building trustworthy MonB5G platform is intertwined with guaranteeing that adequate security measures are put in place to resist security incidents. The composition, management and orchestration of network slices involve different entities across multiple domains, including MANO (NFVO, VNFM, VIM), VNFs, NFVI, NSMF, NSSMF as identified in section 5.2. To empower self-managing capabilities in MonB5G, the managing entities (i.e., AE and DE) will rely on distributed AI/ML models and monitoring data collected by the MS. Thus, assessing the security risks stemming from each entity and deploying the adequate security measures is paramount to foster trust between involved entities.

In section 4.5, we identified the different trust dimensions, the related security threats and the potential countermeasures to foster trust in a self-managed virtualized environment such MonB5G platform. An NFVI should deploy mechanisms to prevent introspection attacks and isolation failures. VNF software has to be valid and certified and a safe boot should be guaranteed for a VNF instance. Besides, it is important to verify the identity and integrity of management entities (e.g., MANO, NSMF, NSSMF) as well as their reliability and availability in order to avoid impersonation and DDoS attacks. Communication channels and APIs that links all these components together has to be efficient and secure. Thus, it is essential to guarantee the accessibility of services while avoiding data leakage and protect the confidentiality. To this end, authentication, authorization, and encrypted transmission services are necessary. To adopt the "never trust, always verify" principle underlying the Zero Trust paradigm in MonB5G, explicit authentication and authorization of each access request is required. The key role played by AI/ML techniques in enabling the analytics and decision functions of AE and DE components, respectively, requires to build explainable, privacy-preserving and resilient AI/ML models. In MonB5G, a particular attention will be paid to how to build distributed AI/ML models that can resist adversarial attacks. The decisions taken by the AI models incorporated in AE and DE components and the derivation of the reputation and trust levels are highly contingent on the quality of data (e.g., KPIs) collected by the monitoring system (MS). Indeed, ensuring the integrity of collected data and their provenance from legitimate sources is paramount to foster trust in decisions taking by MonB5G management platform. To support the decentralized nature of MonB5G platform, we will investigate the potential of blockchain to devise mechanisms for ensuring data integrity and authentication of data sources. Section 6.3 will elaborate the trust management approaches proposed by MonB5G.

6.2 Trust Formalism for Trustworthy Distributed Decisions

MonB5G's core objective is to provide a zero-touch fully decentralized network slicing management system by introducing distributed and data-driven components, namely MS, AE and DE across technological domains. Figure 10 depicts MonB5G vision of a decentralized management system for network slicing. The three components are deployed on different entities that take part in the management process, such as OSS/BSS, network slice owner, MANO, network slice manager, and the VNF.

The AEs and DEs will leverage modern DAI techniques, including federated learning and multi-agent deep reinforcement learning, to empower autonomous distributed slice LCM capabilities. The DAI techniques allow distributed learning and decision making while sharing the learned knowledge between agents, hence significantly reducing the learning overheads while increasing the accuracy. However, a key issue facing collaborative/federated learning tasks is the problem of the trustworthiness of the agents involved in the task. As aforementioned in section 4.4.5, AI systems are vulnerable to many adversarial threats [25,26], which may cause them to learn incorrect patterns and make wrong decisions. In fact, a malicious agent involved in a federated learning (e.g., AI Agent 2 in Figure 10) may poison the parameter updates to be sent to the centralized element. For instance, a malicious agent can manipulate its local parameters in order to fool the model into taking randomized VNF migration decisions. Thus, a **formalism to model the trust** between distributed AI agents **is essential** to foster confidence in AE/DE decisions.

In MonB5G, we advocate the **use of the computational trust modelling** concept introduced in Section 3.1.4 for formalizing the trust between the distributed AI agents involved in DEs and AEs components. The formalism can be embedded in an AI agent, enabling it to make trust-based decisions and provide judgement on the behaviour of other agents.

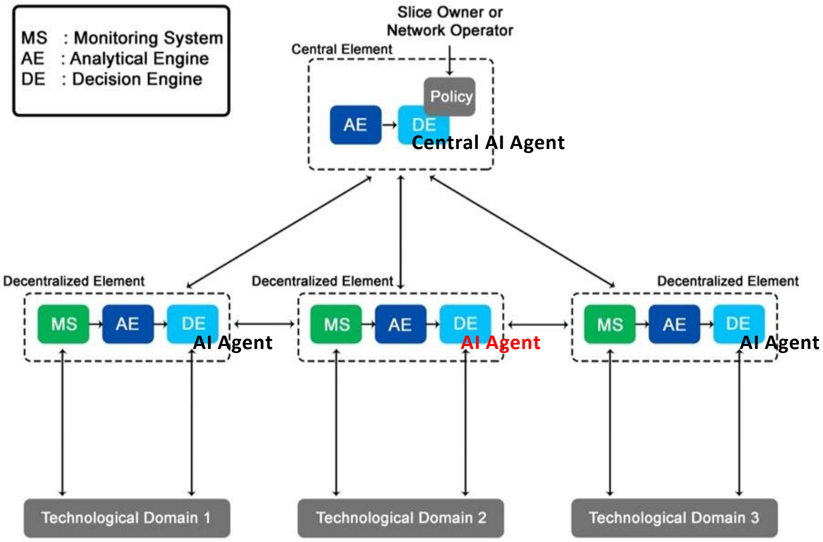

Figure 10: MonB5G vision of a decentralized management system for network slicing.

6.3 Trust Management Approaches

This section will present some approaches we are proposing to enable trustworthy deployment and management of network slices using MonB5G platform. The presented approaches leverage the potential of Blockchain to (i) incorporate trust in brokering architecture, allowing the slice provider to securely create end-to-end network slices while outsourcing resources from different infrastructure providers; (ii) devise a trust architecture to manage the SLAs between the vertical/slice owner, the slice provider and the infrastructure provider; (iii) ascertain the integrity of data and their provenance from legitimate sources, in order to foster trust in decisions and actions taken by the main three entities (i.e., MS, AE, DE) composing the MonB5G's decentralized management system of network slicing.

6.3.1 BLOCKHAIN OVERVIEW

Blockchain technology [44] was originally developed for use in Bitcoin to provide fully-distributed and secure transactions between anonymous participants without the need for a centralized entity. Blockchain is a distributed chain of blocks (ledger) that can be considered as a database of digital deals. Once a new block is created, it should be validated by peers before being added to the chain. This validation process is known as Proof-of-Work (PoW), which makes the system secure. Also, by adding a new block to the chain, it is not possible to change its content or remove it (immutability). The Blockchain's intrinsic features of decentralization, security, immutability, transparency and auditability allow it to play the role of a distributed trust authority.

Based on Blockchain's application, we distinguish two types:

- Permissionless Blockchain: This is also known as a public Blockchain network, where every user is allowed to create transactions and add them to the ledger in a fully decentralized and anonymous fashion. Furthermore, any node can act as a miner to verify transactions. An example of this type is Bitcoin.

- Permissioned Blockchain: This is also known as a private Blockchain network, where users are not free to join the network, consult transactions, or add new ones. These networks are centralized (e.g., organization, government, etc.).

A key feature introduced by Blockchain is the use of smart contracts. To recall a smart contract, based on Nick Szabo [46] taken from the original publication, is an agreement between several parties in the form of computer code. They are distributed and therefore stored in a public database that cannot be modified such as a blockchain. They allow trusted transactions to be carried out automatically without having to resort to a third party, so not depending on anyone, and automated transactions occur when one or more contract conditions are met.

For more information on the Blockchain concept, the reader may refer to [45].

6.3.2 NETWORK SLICE DEPLOYMENT

6.3.2.1 INTRODUCTION

In 5G and beyond, the network slice provider is separated from a resource provider, which could be a network provider (for the RAN and transport network) or a cloud provider (for VNF deployment, including the CN functions). The network slice provider is the interface between the vertical (or the network slice owner) and the infrastructure provider. The network slice provider leases resources from the infrastructure provider, to create and provide an end-to-end network slice to the vertical.

It is commonly accepted that a network slice is composed of domain-slices that belong to different technological domains, which may be part of the same or different administrative domains. For example, a RAN domain-sliceis dedicated physical Resource Blocks (pRB) [40] and dedicated eNB functions, which can be virtualized (in the form of VNFs) [41], while a Core Network (CN) domain-slice is exclusively composed by VNFs along with their computation resources (CPU, storage, memory). Stitched together, via specific interfaces [42], domain-slices will compose an end-to-end network slice that fulfills the requirements of the requested 5G service [43]. Accordingly, the resources composing a network slice could be provided by a single resource provider (i.e., all the domain-slices are provided by the same operator or domain), or from different resource providers (or administrative domains); in the latter case, we refer to a multi-domain end-to-end slice [44].

In this context, the network slice provider needs to select carefully the resources from the infrastructures providers, on one hand, to reduce the cost and make a profit, and, on the other hand, to ensure the necessary resources for a specific slice to respect the Service Level Agreement (SLA) which will be signed with the vertical or slice owner. Indeed, it is important that all the agreed transactions between these three actors, i.e., the vertical, the slice provider and the infrastructures providers, need to be transcribed into SLA, and monitored.

In this section, we will devise a novel brokering architecture based on Blockchain and featuring Trust Management, allowing the slice provider to securely build an end-to-end network slice while leasing resources from different infrastructure providers for each technological domain. The proposed trust architecture: (i) validates all the transactions via a Blockchain, by checking the public keys of the slice provider, resources providers, and their signature in the transactions; (ii) adds trust value assigned by a third-tier entity for each resource provider involved in a Blockchain transaction.

6.3.2.2 TRUST PROCEDURE FOR END-TO-END NETWORK SLICE NEGOTIATION AND CREATION

6.3.2.2.1 SYSTEM OVERVIEW

Figure 11 shows the proposed trust procedure that allows negotiating and deploying an end-to-end network slice. The proposed procedure is composed of the vertical (or slice owner), slice provider, infrastructure/resource providers, and a third-tier entity that creates and maintains the reputation of the infrastructure/resource provider, namely resource provider trust. The Blockchain layer is owned by the slice provider and is used to generate and negotiate contracts between the slice provider and the resource providers.

The negotiation between the slice provider and the resource providers is done per domain-slice. The sub-entity at the slice provider in charge of this negotiation is the resources broker. In this context, we envision a domain-slice deployment brokering mechanism as a series of small contracts. Each contract has a unique identifier and some data fields and can perform actions such as creating a new contract or updating the state of the Blockchain. Contract actions are triggered by on-chain data updates (i.e., the creation of a new contract). Each domain-slice generates a contract. The inter-domain end-to-end slice is ready for the deployment once all the contracts regarding its domain-slices are negotiated and finalized.

The vertical or the slice owner requests the creation of a network slice using a template or a blueprint. This template may contain high-level information. The slice provider will translate the template to specific slice resource requirements, such as the number and types of domain-slices, PNFs, VNFs, CPU, I/O, memory, storage, etc. The domain-slice components are translated to resources of a Technological Domain (TD). A TD can be a computing resource domain (such as CPU, I/O), a storage domain, a radio domain (eNB, Central Unit - CU, Distributed Unit - DU, Remote Radio Head - RRH / Remote Radio Unit - RRU), and transport domain (e.g., VLAN, VPN). We assume that a slice is composed by several TDs, noted as NS = $\{TD_1,TD_2,TD_3,\cdots ,TD_n\}$. For each TD, the slice provider describes the needed resources according to the slice type. For instance, in the case of the computing resource domain, they could include the number of CPUs, VM instances, etc. For the radio domain, resources could be related to the functional split type, the MAC scheduler algorithm, the number of Physical Resource Blocks (PRB), and others. Transport domain resources, on the other hand, may include the type of a link (bandwidth, latency), number of VLANs, front haul link capacity, VPN links, QoS, etc. We define R(TDi) = {p_1,p_2,p_3,...,p_n}, as the set of parameters requested by TD_i.

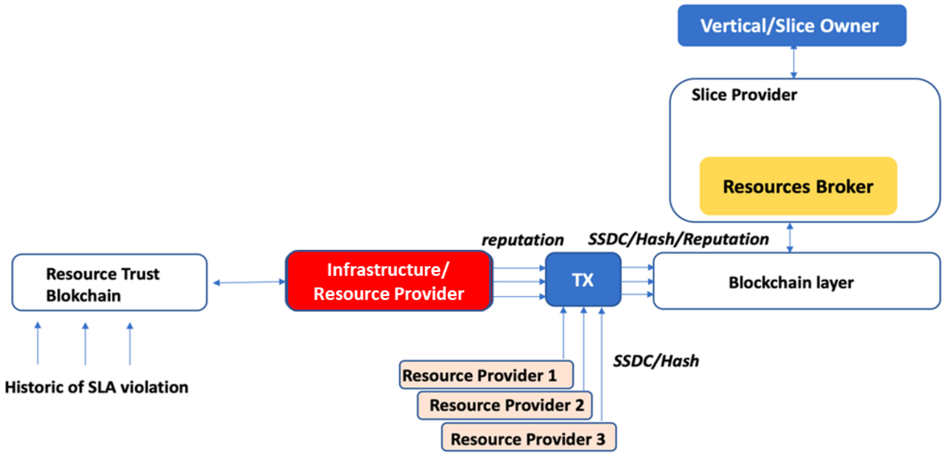

Figure 11: MonB5G Trust procedure for end-to-end network slice creation.

6.3.2.2.2 DOMAIN-SLICE BROKERING

Once each domain-slice is described in terms of resources (i.e., R(TD_i)), the request for each domain-slice is sent to the Blockchain layer. Each domain-slice will generate a contract to be negotiated. Once the query for a domain-slice arrives at the Blockchain layer, a Domain-slice Contract (DSC) is created and published. This contract specifies the necessary resources needed by the domain-slice (i.e., R(TDi)) and the duration of the domain-slice. The different resource providers are notified of the new DSC. Here, all the DSCs are visible on the Blockchain. The resource providers respond by publishing Domain-slice Deployment Costs (DSDC), which specify the cost that the resource providers are willing to charge for providing the necessary resources for each component of the domain-slice R(TDi). The resource provider trust module records the trust value of the corresponding resource in the DSDC as appended information in the blockchain layer. The original DSC collects all the related DSDC and arbitrates according to specific objectives (e.g., cheapest, best in terms of quality, or other criteria). All other contracts are terminated, and the winning contract is used to deploy the domain-slice components. All related information about the domain-slice deployment is recorded in the Blockchain managed by the slice provider. Relevant information on the different interfaces allowing to access to the domain-slices, such as the stitching interface (the Resource Orchestrator (RO) interfaces and their description), are compiled in a Domain-slice Deployment (DSD) document.

6.3.2.2.3 DEPLOYMENT

Once the resources are negotiated and transcribed in SLAs. Indeed, SLAs have to be established, on one hand, between the slice provider and the vertical; on the other hand, between the slice provider and each infrastructure/resource provider. Details on how the SLA is established using a Trust procedure will be described in section 6.2.

Once everything is settled, the Slice Orchestrator (SO) handling the Life Cycle Management (LCM) of the deployed network slices, will use the RO interfaces indicated in each SSD to: (i) instantiate and create the domain-slice; (ii) stitch the domain-slice with the other domain-slices to build the end-to-end network slice. Note that each resource provider uses its domain RO to manage and orchestrate its resources. The resourc e provider exposes interfaces to allow other ROs or the SO to interact with the local RO.

6.3.2.2.4 RESOURCE PROVIDER REPUTATION

The resource provider trust module relies on the precedent experiences with the infrastructure/resource provider, and particularly on the respect of the SLA signed with a slice provider. To this aim, the infrastructure/resource provider trust module monitors all the SLA signed between a slice provider and a n infrastructure/resource provider. According to the monitored information on SLA, a Rep(i) of the resource provider is maintained and updated. The Rep(i), and hence the trust of the infrastructure/resource provider, is a function of the respected SLA by the infrastructure/resource provider i. The reputation of a infrastructure/resource provider increases if a signed SLA by the infrastructure/resource provider is respected, and decreases otherwise.

$$\begin{cases} Rep(i) = \min(Rep_{max}, Rep(i) + \Delta R) \text{ if the SLA is respected} \\ Rep(i) = \max\,(Rep_{min}, Rep(i) + \alpha.\Delta R) \text{ if the SLA is not respected} \end{cases} \quad (1)$$

Where ΔR is the reputation increase step, α ΔR is the reputation decrease step, *Rep_{max}* is the maximum value of the reputation, and *Rep_{min}* is the minimum value of the reputation.

Details on how the SLA is monitored will be introduced in the next section.

6.3.3 SLA MANAGEMENT

6.3.3.1 INTRODUCTION

As introduced in section 6.3.1, SLAs have to be established between the vertical and the slice provider, and between the slice provider and the resource providers. Generally speaking, SLAs are contracts between consumers and a service provider. An SLA specifies what customers can expect from a service provider. The SLA is used to check whether a defined service is delivered as contracted and the management of violations via the degradation of Quality of Service (QoS). An SLA defines QoS requirements, e.g. bandwidth, throughput, and latency, without specifying the technology to be used in order to deliver a particular service. SLAs include general information, such as the parties, the service fee, the validity period, and the compensation value used in the case of an SLA violation when the performance levels are not met. In 5G, SLA should reflect the QoS as related to the pre-defined type of slices, i.e., mMTC, eMBB, and uRLLC.

The established SLA needs to be managed and monitored in order to ensure that the service is well functioning, and hence build the reputation of the resource providers. In this section, we will introduce a Trust management architecture to manage the SLAs between the above-mentioned entities. The proposed architecture is linked with the one introduced in 11, in order to build the reputation of the resource providers, which is used when a resource provider replies to a domain-slice creation request.

6.3.3.2 TRUST MANAGEMENT PROCEDURE

The proposed trust management architecture has two objectives: (i) manage the life-cycle of the SLA; (ii) build the reputation or trust of the resource providers. The proposed procedure is illustrated in Figure 12. Three elements are new by report to Figure 11, the monitoring system, the smart contract, and a Resource Trust AI-enabled Blockchain. The monitoring system is a third-tier trusted entity, which monitors the KPI as specified in the SLA established between the vertical and the slice provider, and between the slice provider and the infrastructure/resource providers. The monitoring information will be used to verify if an SLA is violated. In future extension of this procedure, we will address the case of a Trust architecture for monitoring as all the entities need to trust the monitoring solution, which should be not attacked and altered. The smart contract will contain all the signed SLAs, and related information such as validity period, targe t performance level, price, compensation value, and relevant information. It stores the addresses of slice provider, vertical, resource providers, monitoring system and resource provider trust. It is used to check the account balance, to transfer funds, to report SLA violation to the resource provider trust, and to allow only authorized addresses to interact with the smart contract.

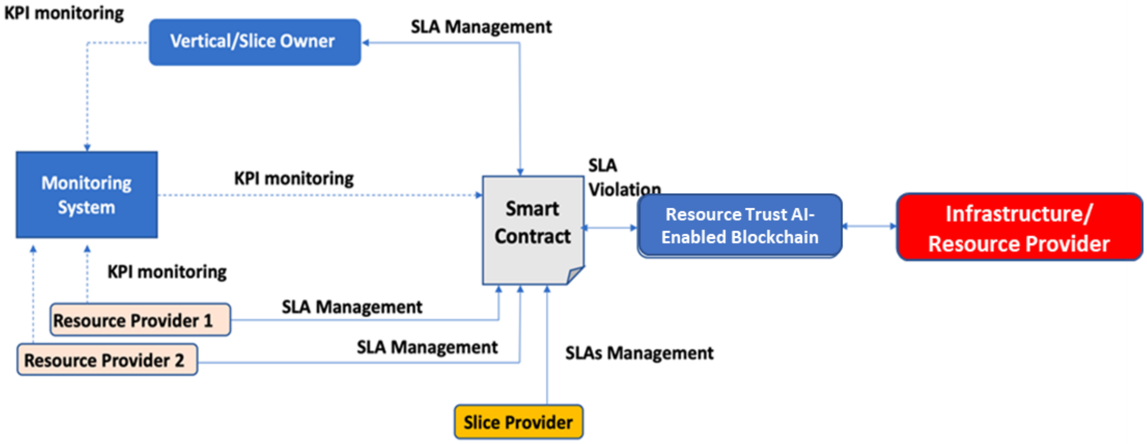

Figure 12: MonB5G SLA Management trust procedure.

In the proposed architecture, the smart contract is managed by the slice provider, and according to the monitoring information obtained from the monitoring system, it checks if one of the involved entities is violating the SLA. Moreover, it is used to automatically give compensation to the vertical if th e service is not satisfactory and finds which infrastructure/resource provider has failed to support the SLA. The concerned infrastructure/resource provider will be charged automatically to pay penalties to the service provider in this case. It is worth noting that the compensation and penalties to pay are committed by all parties when the SLA is signed. To this aim, the smart contract includes functions that calculate the number of detected violations in an interval, also it is used to verify if the compensation interval has ended. At the end of the life cycle of SLA, the compensation is paid, based on the number of the violation. Finally, a compensation function is called to transfer the compensation value for the vertical address stored from the slice provider, and for the slice provider address from the resource providers which violated the SLA.

On the other hand, at the end of the session, the smart contract publishes in the Resource Trust AI-enabled Blockchain, owned by the third-tier party in charge of building reputation of the infrastructure/resource providers, information regarding the infrastructure/resource providers that violated the SLA. This information will be used by the Resource Trust module to update the reputation value (equation 1).

6.3.4 ROBUST AND ACCURATE MONITORING DATA COLLECTION

As described previously, 5G network slicing combines many actors distributed through different technological and administrative domains. In such decentralized untrusted environment, the efficiency of AI-driven self-managing services will depend on data gathered from a variety of sources (e.g., users, services, network) across multiple domains [25]. Thus, ascertaining the integrity of data and their provenance from legitimate sources is paramount to promote trust in data and decisions relying on them.

In this section, we will explore the potential of AI-enabled Blockchain to collect trusted immutable data from authenticated distributed sources.

6.3.4.1 AUTHENTICATION OF THE DATA SOURCES

Authentication is a fundamental step in the security to verify and confirm the identification. In the autonomous network environment, Zero Trust Model (ZTM) is considered among entities, which requires strong authentication mechanisms to ensure that data source is genuine and check legitimacy between untrusted services.

In a 5G environment, a large amount of data circulates through the multi-layer distributed architecture. This huge data collected coming from various sources aiming to enhance orchestration and optimization, training machine learning models, as well as resource monitoring. The network slicing architecture requires wide data gathering at different levels (e.g., VNF, domain-slice, E2E).

From MonB5G vision, data is collected locally in each technical domain and exchanged between the three engines (i.e., MS, AE and DE). The MS periodically transmits monitoring information to the AE that processes the data and provides the required analysis output to the DE. In addition, the data is transmitted from the local domains to the E2E domain.

The fully autonomous network will leverage AI-driven mechanisms, specifically the distributed AI and Federated learning, this promising ML technique enables distributed training using the local dataset to a device or domain and shares only the model parameters while keeping the data where it is generated. Although this approach may support data privacy, the update parameters exchanged need to be authenticated and protected.

These large data sources may represent a potential risk to the slice orchestration and monitoring. As stated in Section 6, the nature of distributed slice network environments comes with additional security threats, such as data forging and APIs abuse, that will need to be avoided by means of suitable mechanisms such as strong authentication. However, authentication remains a challenge that has not yet been widely addressed in 5G management and slicing orchestration.

Software modules and network enablers are currently based on traditional authentication mechanisms, APIs provide authentication based on Password, Trusted Third Party (e.g., OAuth), or tokens. These mechanisms are still based on centralized authentication while moving to decentralized environments. Thus, new innovative data protection solutions are required to ensure secure and efficient data source authentication over the untrusted decentralized environments. Recently, many researchers have been working on integrating AI-enabled Blockchain to prevent the poisoning attacks in various domains such as IoT, edge computing, and healthcare [47]. Indeed, this vision can be achieved due to the wide range of interesting features that AI-enabled Blockchain offers such as decentralization, privacy, immutability, and traceability [26].

In contrast to the conventional database management systems, which often use a centralized server to perform access authentication and security mechanisms, AI-enabled Blockchain can implement decentralized access validation based on the computing power of all legitimate network participants. To control access to data resources, AI-enabled Blockchain miners can check whether the requester meets the corresponding access control policy. Instead of relying on external PKI, AI-enabled Blockchain can authenticate automatically access, detect threats and discard malicious access from the networks autonomously without revealing client information; and potentially reduces network complexity without the need for other complex cryptographic primitives between network services. In addition, it eliminates single point failure bottlenecks and improves significantly system trust [47].

In the previous 5G scenarios contributions, AI-enabled Blockchain has been used to build a trusted authentication architecture for cloud radio access networks and address effectively network access authentication with trusted agreement among service providers and IoT users. Furthermore, it has been utilized as an authentication solution for SDN-based 5G networks to eliminate the unnecessary re-authentication in repeated handover among heterogeneous cells. This integration of AI-enabled Blockchain in SDN is thus promising to remove intermediaries for authentication. At the VNF level, AI-enabled Blockchain can perform data auditing and monitoring of system state during the network communication. Moreover, to guarantee secure and private transactions between the network slice provider and the resource provider for 5G services, Blockchain is employed to build a brokering mechanism in network slicing [47].

6.3.4.2 INTEGRITY PROTECTION OF THE DATA GENERATED BY MS/AE/DE

The main three entities (i.e., MS, AE, DE) composing the MonB5G's decentralized management system of network slicing heavily rely on data-driven, AI/ML-based techniques. Thus, protecting the data used by those MS, AE and DE from manipulation and ensuring their integrity is critical to foster trust in decisions taken by those entities.

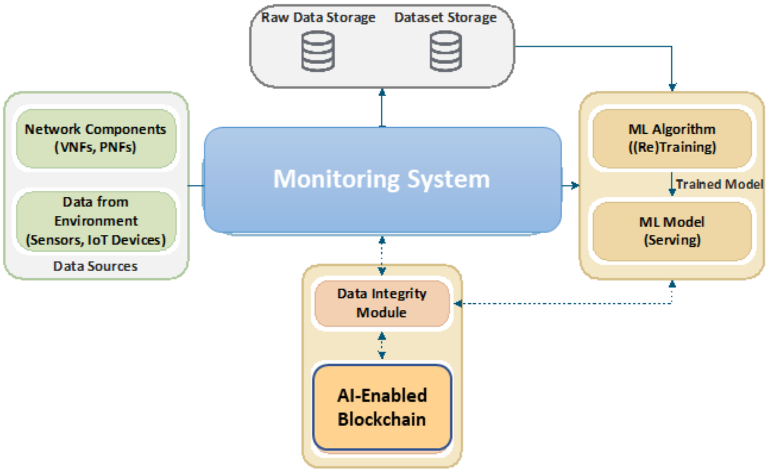

Figure 13: Learning Pipeline with Blockchain-based Trustworthy Data [18].

Different enablers can be leveraged to enforce the integrity of data. Traditionally, cryptographic mechanisms such as Message Authentication Codes (MAC) and digital signatures have been used to achieve data integrity protection. However, a major challenge with those mechanisms is their reliance on trust in a third party for public/private key generation. Consequently, if the key generator is compromised, the whole system is compromised [45]. Recently, AI-enabled Blockchain is poised as an ideal alternative to develop advanced methods for guaranteeing data integrity in an exposed environment without relying on a trusted third party.

Indeed, it can be used to enable data integrity assurance. Furthermore, its immutability property can be leveraged to maintain comprehensive audit trails of all events and changes related to data, allowing to ascertain their provenance from trusted sources [18].

In what follow, we will introduce a learning pipeline with AI-enabled Blockchain-based trustworthy data. As depicted in Figure 13, the pipeline comprises four components, namely: (1) a Monitoring System (MS) that performs both Data Collectoion and Feature Extraction from the raw data; (2) a Data Integrity Module which maintains and assesses the integrity of data using AI-enabled Blockchain's smart contracts; and (3) ML Algorithm and Model which use the extracted data for training and inference, respectively.

For each collected raw data file, the Data Collector allocates a unique identifier (ID), records its hash and ID in the blockchain leveraging the hashing service provided by the Data Integrity Module, and stores the file in the raw data storage. It is worth mentioning that given the huge amount of data that can be gathered from the network, only the raw data hashes are stored in the blockchain, which enhances the blockchain's scalability and performance. The Data Extractor can either get the raw data file from the storage (during training phase) or receive it in real-time from the Data Collector (during the inference phase). In both cases, the Data Extractor uses the Integrity Checking Service provided by the Data Integrity Module to assess the integrity of the raw data file. After proving its integrity, the raw data file is used by the Feature Extractor to extract the relevant feature vectors. Once extracted, the set of feature vectors is split into multiple chunks. For each chunk, the Feature Extractor allocates a unique ID, records its hash alongside its ID and the ID of the raw data file from which it has been extracted in the blockchain using the hashing service provided by the Data Integrity Module, and stores the chunk to the dataset storage. The rationale behind breaking data down into chunks is to prevent losing the whole data in case of data integrity breaches; only the altered chunks will be lost. Similar to raw data files, the ML Algorithm (during the training phase) or the ML Model (during the inference phase) conducts an integrity check before using the chunks. It is worth noting that the interaction with the AI-enabled Blockchain is performed through a smart contract including functions to add and retrieve hashes.

7. Conclusions and Next Steps

In this deliverable, we provided a comprehensive review of the state of the art in trust modelling, covering both human and machine aspects. A particular attention was paid to work on modelling trust between machines, especially ones connected over telecommunication networks including the trust in physical and virtual networks. We discussed the lack of a complete trust model in 3G/4G networks and how it becomes a challenge in introducing trust in 5G context. The contributions on modelling and managing trust in 5G from previous and ongoing 5G-PPP projects has been investigated.

To meet MonB5G's aim of providing advanced models for trustworthy deployment and management of cross-domain 5G network slices, and using the insights we gained from the state of the art analysis, we conducted an extensive study of the trust dimensions in 5G networks and the security measures needed to establish and maintain trust for each dimension. A particular attention is then paid to trust in network slicing. In fact, the requirements and the appropriate control mechanisms that are needed to establish trust in the composition of network slices across multiple domains were discussed.

Finally, we introduced MonB5G's trust management vision, which encompasses the MonB5G's trust model considering both trust among stakeholders and trust between network entities involved in MonB5G's ecosystem; the use of computational trust modelling concept for formalizing the trust between the distributed AI agents involved in DEs and AEs components; and novel approaches leveraging the potential of AI-enabled Blockchain and smart contacts to enable trustworthy deployment and management of network slices using MonB5G platform. The proposed approaches support (i) trustworthy slice brokering architecture; (ii) SLA compliance monitoring and arbirtration; and (iii) robust and accurate monitoring data collection.

The outcomes of this deliverable will be leveraged in the design and development of the Trust Management Module and the security architecture of MonB5G. The first and final version of the security-related architectural elements (i.e., Trust Management Module and Security Orchestrator) of MonB5G platform will be presented in D2.1 and D2.2, dedicated to first and final specification of the zero-touch slice management and orchestration architecture to be delivered by MonB5G.

8. References

[1] P. P. Li. Towards an Interdisciplinary Conceptualization of Trust: A Typological Approach. Management and Organization Review, Vol. 3, Issue 3, pp. 421-445, 2007.

[2] J.-H. Cho, K. Chan, and S. Adali. A Survey on Trust Modelling. ACM Computing Survey, vol. 48, no. 2, Oct. 2015.

[3] S. Bok. Lying: Moral Choice in Public and Private Life. Harvester Press, 1978.

[4] K. H. Blanchard, C. Olmstead, and M. C. Lawrence. Trust Works! : Four Keys to Building Lasting Relationships. 2013.

[5] S. P. Marsh. Formalising Trust as a Computational Concept. PhD Thesis, University of Stirling, 1994.

[6] D. Gambetta. Trust: Making and Breaking Cooperative Relations. Oxford: Basil Blackwell, 1988.

[7] L. Liu, M. Loper, Y. Ozkaya, A. Yasar, and E. Yigitoglu. Machine to Machine Trust in the IoT Era. In Proc. of the 18th International Conference on Trust in Agent Societies (TRUST'16), Volume 1578, pp. 18 – 29, May 2016.

[8] M. G. Raeini and M. Nojoumian. Secure Trust Evaluation Using Multipath and Referral Chain Methods. In proc. of the 15th International Workshop on Security and Trust Management (STM 2019), pp. 124 – 139, Luxembourg, Sept. 2019.

[9] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim. Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey. IEEE Access, Vol. 8, 167123 – 167163, 2020.

[10] 5G PPP Security WG. White Paper; 5G PPP Phase1 Security Landscape. June 2017.

[11] 3GPP TS 33.401. 3GPP System Architecture Evolution (SAE); Security architecture. July 2020.

[12] S. Bhattiprolu. 5G Trust Model: Recommendations and Best Practices for CSPs. In Proc. of RSA Conference, 2020. http://www.rsaconference.com/usa/agenda/5g-trust-model-recommendations-and-best-practices-for-csps (accessed Apr. 11, 2020).

[13] M. De Benedictis and A. Lioy. On the establishment of trust in the cloud-based ETSI NFV framework. In Proc. of 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 280–285, Nov. 2017.

[14] S. Holtmanns, I. Oliver, Y. Miche, A. Kalliola, G. Limonta, and G. Peinado. 5G Security – Complex Challenges. in Wiley 5G Ref, American Cancer Society, pp. 1–15, 2019.

[15] ETSI. ETSI GR NFV-SEC 003 V1.2.1, Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance. 2016. (accessed Mar. 05, 2018).

[16] G. Reddig. The triangle of trust: What security means to 5G operations. Nokia, 2020. https://www.nokia.com/blog/the-triangle-of-trust-what-security-means-to-5g-operations/ (accessed Jul. 14, 2020).

[17]S. Rose, O. Borchert, S. Mitchell, and S. Connelly. Zero Trust Architecture. National Institute of Standards and Technology, NIST Special Publication (SP) 800-207, Aug. 2020. doi: https://doi.org/10.6028/NIST.SP.800-207.

[18] C. Benzaid, T. Taleb, and M. Z. Farooqi. Trust in 5G and Beyond Networks. IEEE Network Magazine (Conditional acceptance).

[19] ENISA. ENISA Threat Landscape for 5G Networks; Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G). Nov. 2019.

[20]. 3GPP TS 33.501. Security Architecture and Procedures for 5G System(Release 16). March 2020.

[21] C. Benzaid and T. Taleb. ZSM Security: Threat Surface and Best Practices. IEEE Network Magazine, vol. 34, no. 3, pp. 124 – 133, May/June 2020.

[22] ETSI GS NFV-SEC 003. Network Functions Virtualisation (NFV);NFV Security; Security and Trust Guidance. Dec. 2014.

[23] S. Lal, T. Taleb, and A. Dutta. Nfv: Security threats and best practices. IEEE Communications Magazine, vol. 55, no. 8, pp. 211 – 217, Aug.2017

[24] M. Pattaranantakul, R. He, A. Meddahi, and Z. Zhang. Secmano: To-wards network functions virtualization (nfv) based security managementand orchestration. In Proc. of the 2016 IEEE Trustcom/BigDataSE/ISPA, pp. 598–605, 2016.

[25] C. Benzaid and T. Taleb. AI-driven Zero Touch Network and ServiceManagement in 5G and Beyond: Challenges and Research Directions. IEEE Network Magazine, vol. 34, no. 2, pp. 186 – 194, March/April2020.

[26] C. Benzaid and T. Taleb. AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?. IEEE Network Magazine, doi: 10.1109/MNET.011.2000088.

[27] R. Y. Wang and D. M. Strong. Beyond Accuracy: What Data QualityMeans to Data Consumers. Journal of Management Information Systems, vol. 12, no. 4, pp. 5 – 33, March 1996.

[28] TM Forum. Open Digital Architecture & Open API Manifesto. TM Forum, 2020. https://www.tmforum.org/oda/open-digital-architecture-open-api-manifesto/ (accessed Aug. 05, 2020).

[29] GSMA. The 5G Guide. 2019. https://www.gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf (accessed Jul. 15, 2020).

[30] W. Li, L. Ping, Q. Qiu, and Q. Zhang. Research on Trust Management Strategies in Cloud Computing Environment. Journal of Computational Information Systems, vol. 8, no. 4, pp. 1757 – 1763, 2012.

[31] S. Dey, V. K. Solanki, and S. K. Sen. SVM – A Way to Measure the Trust Ability of a Cloud Service based on Rank. In Proc. of the International Conference on Communications and Cyber Physical Engineering (ICCCE 2018), pp. 105 – 113, Springer Singapore, 2019.

[32] Palo Alto Networks. Simplify Zero Trust Implementation Using A Five-Step Methodology. May 2019. [Online]. Available: https://www.paloaltonetworks.com/resources/whitepapers/simplify-zero-trust-implementation-with-a-five-step-methodology.

[33] 3GPP. 3GPP TS 28.530 – Management and orchestration; Concepts, use cases and requirements. 3GPP, 2020.

[34] ETSI. ETSI GS NFV-IFA 005: Or-Vi reference point - Interface and Information Model Specification. ETSI, 2020.

[35] ETSI GS NFV-IFA 013. Os-Ma-nfvo reference point - Interface and Information Model Specification. ETSI, 2020.

[36] ETSI GS NFV-MAN 001 V1.1.1. Network Functions Virtualisation (NFV); Management and Orchestration. ETSI, 2014.

[37] ETSI GS NFV-IFA 014. Network Service Templates Specification. ETSI, 2019.

[38] 3GPP TR 28.801 v15.1.0. Study on management and orchestration of network slicing for next generation network. 3GPP, 2018.

[39] ETSI MEC 003 V2.1.1. Multi-access Edge Computing (MEC); Framework and Reference Architecture. ETSI, 2019.

[40] A. Ksentini and N. Nikaein. Towards Enforcing Network Slicing on RAN: Flexibility and Resources Abstraction. *IEEE Communications Magazine*, Special Issue on Agile Radio Resource Management Techniques for 5G New Radio, June 2017.

[41] A. Ksentini, P. A. Frangoudis, A. PC, and N. Nikaein. Providing Low Latency Guarantees for Slicing-Ready 5G System via Two-Level MAC Scheduling. IEEE Network, Vol. 32, Issue 6, pp. 116 – 123, Nov./Dec. 2018.

[42] I. Afolabi, A. Ksentini, M. Bagaa, T. Taleb, M. Corici, and A. Nakao. Towards 5G Network Slicing over Multiple-domains. *IEICE Transactions on Communications*, Vol. E100-B, No. 11, pp. 1992–2006, Nov. 2017.

[43] K. Katsalis, N. Nikaein, E. Schiller, A. Ksentini, and T. Braun. Network Slices Toward 5G Communications: Slicing the LTE Network. IEEE Communications Magazine, Vol. 55, Issue 8, pp. 146 – 154, 2017.

[44] Q. Feng, D. He, S. Zeadally, M. K. Khan, N. Kumar. A survey on Privacy Protection in Blockchain System. *Journal of Network and Computer Applications, Vol. 126, pp. 45 – 58,* 2019.

[45] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka. Security Services using Blockchains: A State of the Art Survey. IEEE Communications Surveys and Tutorials, Vol. 21, No. 1, pp. 858 – 880, Firstquarter 2018.

[46]https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[47] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne. Blockchain for 5G and Beyond Networks: A State of the Art Survey. Journal of Network and Computer Applications, Vol. 166, Sept. 2020.

[48] RSA, “The Role of Security in Trustworthy Cloud Computing,” 2009. http://www.klcconsulting.net/security_resources/cloud/Cloud_Security_WP-2009-02-by-RSA-EMC.pdf (accessed Mar. 03, 2019).

[49] ETSI, “ETSI MEC 003 V2.1.1, Multi-access Edge Computing (MEC); Framework and Reference Architecture.” 2019.

[50] D. De Siqueira Braga, M. Niemann, B. Hellingrath, F. B. De Lima Neto. “Survey on Computational Trust and Reputation Models.” ACM Computing Surveys, Vol. 51, No. 5, Article 101, Nov. 2018