Sustainable Trust

v1.0

www.ngmn.org

WE MAKE BETTER CONNECTIONS

SUSTAINABLE TRUST

by NGMN Alliance

Version:	1.0
Date:	26-July-2021
Document Type:	Final Deliverable (approved)
Confidentiality Class:	P - Public

Project:	Security Competence Team
Editor / Submitter:	**Stan Wong (Hong Kong Telecom)**
Contributors:	**Stan Wong (Hong Kong Telecom), Minpeng Qi (China Mobile), Colin Blanchard (BT), Sheeba Mary (Lenovo), Andreas Kunz (Lenovo), Peter E. Yee (Akayla), Douglas W. Varney (UScellular)**
Approved by / Date:	**NGMN Board, 20th July 2021**

NGMN e. V.
Großer Hasenpfad 30 • 60598 Frankfurt • Germany
Phone +49 69/9 07 49 98-0 • Fax +49 69/9 07 49 98-41

Abstract

A Trust Model has implicitly existed since the first generation (1G) analogue mobile system and evolved to the fifth generation (5G) mobile system. The telecommunication system trust model has evolved from one with a simple trust relationship between a subscriber and a mobile network operator (MNO), from static network elements to dynamic network functions, and from traditional business-to-customer (B2C) to business-to-business (B2B), with multi-stakeholders involved. MNOs face a complex trust relationship in relation to the modern telecommunication business. Therefore, the telecommunication industry requires a trust model with sustainability that can harmonize the standards developing organizations (SDOs) system design principles and evaluate the overall system functional elements at runtime. In this paper, a sustainable trust model is presented to resolve the complexity of the trust relationship between stakeholders and network functions in future generation(s) of telecommunications systems.

Contents

1 INTRODUCTION

The telecommunication system is entering into a critical period of replacement from one generation to another, transforming the physical network elements to virtualized function entities, converting aggregated systems to a disaggregation of resources, from macro-management to micromanagement of system control, combining different fields of technologies and shifting from static to dynamic on-demand resources with the goals of network flexibility, services agility, and fast deployment.

Under this generational replacement, the telecommunication industry has been also confronting an important issue of software products in the infrastructure at runtime. In particular, the greatest area of concern is the volatility of the software products' trustworthiness in operation, the liability of the software products under varying geo-political policies, local regulation, and precise implementation of specifications.

With those concerns, there are some issues from technology innovation and cyber-attacks that affect the volatility of trust in real-time. Notably, cyber-attacks have different forms, which can maliciously disable network functions, steal data, or use a compromised network function to act as a launching point for other attacks. More importantly, the vast varieties of attacks could consequently ruin a company's reputation. Even though SDOs have put great effort to develop the security framework to prevent runtime attacks, those issues of the runtime attacks still have not been totally resolved due to differences between network deployments. Currently, the 3rd Generation Partnership Project (3GPP) uses the Trust Computing Base (TCB) and Trusted Platform Module (TPM) to enforce the behaviours between network entities. Each interface has a specific protocol and design of the protocol in order to achieve the desired behaviours. 3GPP took the static approach to design the entire telecommunication security that uses the best effort in designing the behaviour and analysing the potential key attack issues as a design defence principle. Nonetheless, every actual deployment of networks and the defence mechanism ends up differently. Even if the deployment network follows 3GPP specification, there is still a number of entities' implementations and configurations that are different. Therefore, a real-time, dynamic approach to network security would work complementally with the 3GPP static approach. Also, we need a real-time, evolutionary system to prevent insider attacks, and in the same context to drive the company to increase the external trustworthiness and internal awareness. Moreover, this real-time, evolutionary system should be able to give a dynamic evaluation of the network elements' trustworthiness and obtain a measurement of the volatility of trust through interactions.

In this paper, we explore a method to illustrate a future generation telecommunication sustainable trust model, which can harmonize the current and future development of the SDOs trust models and embrace runtime trust volatility while the telecommunication system moves towards the softwarisation of the network functions.

Scope of the document

This is a document to define the Sustainable Trust of telecommunication systems. It is based on the 3GPP Trust Model with the enhancement of a dynamic, real-time evaluation approach and high adaptability to develop a future trust model from 3GPP. This document focuses on delivering a 5G trust model and definition of network entities' interactions, which can be identified as a foundation for Sustainable Trust.

2 SUSTAINABLE TRUST OVERVIEW

In this section, an overview of Sustainable Trust is presented, starting with the four fundamental elements that are based on the fundamental elements of a human fundamental trust relationship and followed by the four layers of a trust acquisition architecture formulation. Basically, the sustainable trust model uses the same methodology as when humans formulate a trust relationship. Trust is established based on interactions and using those interactions as a medium to collect evidence for evaluating the trustworthiness of an object or another human. An interaction has an important role in the sustainable trust model for extracting an object or human's behaviour. These extracted behaviours can be categorised into static behaviour or dynamic behaviour. Static behaviour is designed by the protocol, the different types of protocol algorithms, and the network entities' relationships. Typically, an SDO would provide the design of interaction sequences and implementation guidelines. Dynamic behaviour is based on the runtime activities and represents the quality of implementation and deployment.

Figure 1 illustrates Sustainable Trust which can be extracted from a static approach (left half) and a dynamic approach (right half). The static approach is based on the SDO TCB trust model approach, e.g., 3GPP trust model [1]. This approach does not give a real-time status of the deployed network trustworthiness. Therefore, the telecommunication industry requires a dynamic approach that is based on the deployed mobile network real-time analytics. These real-time analytics should provide a dynamic approach to evaluate any trust relationship in the network.

Furthermore, Figure 1 also shows the relationship of four fundamental elements (i.e., benevolence, integrity, competence and predictability) for formulating a Sustainable Trust

using four systems; design methodologies system design, quantification of interaction relationships, and knowledge-based management of interaction relationships. When these fundamental elements, via their interactions, positive evidence, we can conclude that if it is a trustworthy object, company, or human being. This positive evidence must be derived from many different types of interaction and the interactions must be quantified on a trustworthiness index. Then we can analyse the interactions of every event over a time interval. On the other hand, the trustworthiness index can also indicate that some interactions serve as negative evidence.

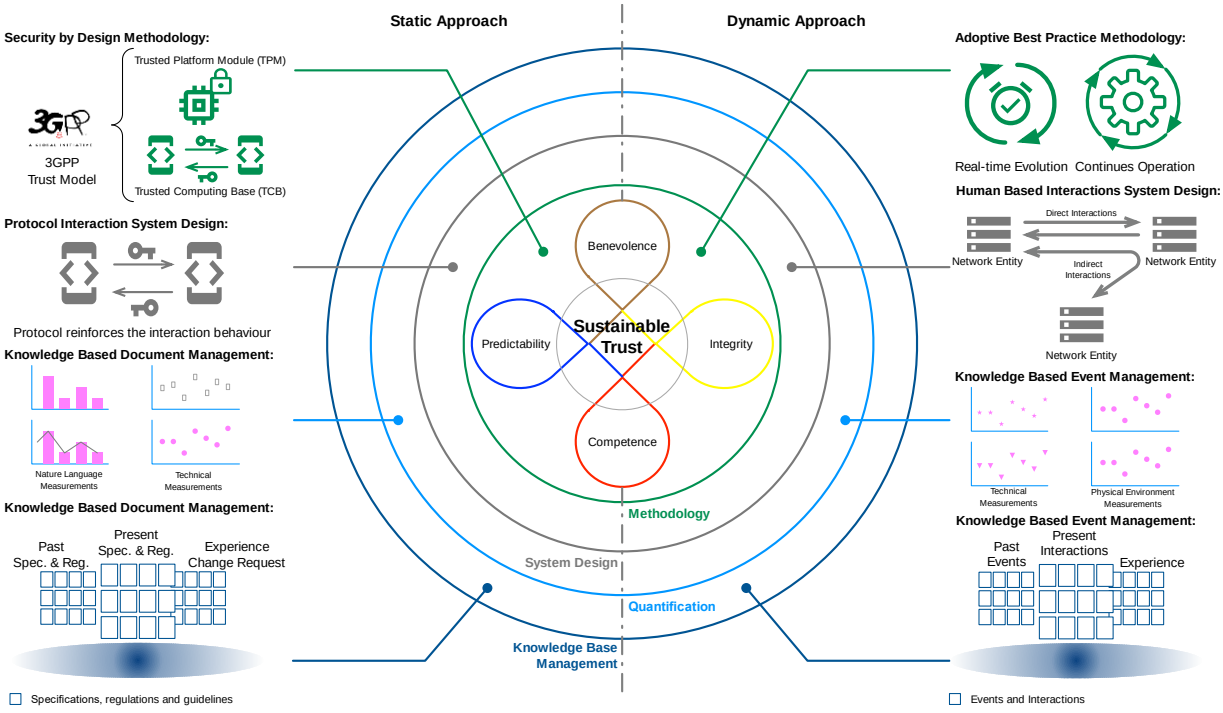

Figure 1: Sustainable Trust

2.1 Four Trust Model Fundamental Elements

There are 4 fundamental elements of Trust node: Benevolence, Integrity, Competence and Predictability.

Benevolence can be referred to the genuine positive attitude, give and support for the need of others and always having a positive response to others. An example of positive benevolence is a network entity implementation deployable on various hardware or network environments, which has high adaptability and anticipated variability in network deployment environments. This network entity implementation also anticipates the network technology evolutions and has ability to adapt automatically without any manual configurations or modification. Basically,

the network entity was implemented with a high degree of flexibility and design with substantial consideration. This analogy can also be applied to stakeholder scenarios.

Integrity can be represented by making a good faith agreement, informing the truth, and delivering on promises. An example of positive Integrity is a network entity implementation that is exactly the same as its product description, and in particular the runtime behaviour fulfils the same product description. This general example can also be applied to stakeholder scenarios.

Competence can be interpreted into the willingness to use their capability to support others. For example, a network entity has built-in extra functionality to cover other network entities' insufficient capability. Another example is the stakeholder's eagerness to share their knowledge and have a high willingness to collaborate with the others.

Predictability can be referred to the ease in consistently forecasting in every situation. For example, a network entity's functional behaviour can be effortlessly estimated with positive outcome with confidence. Also, the network entity's functional behaviour can be easily anticipated with the common knowledge and reasoning on a future event.

Each of these four fundamental elements of trust have unique properties to assist a system to obtain sensible judgment under actual observation.

2.2 Trust Acquisition

Nowadays, we often design a system with security considerations and embedded security features as the foundation of the entire system. A system trust model is often used as a secured system design methodology. Basically, a trust model can be used to reinforce the behaviours between entities or objects, by means of a common interaction criteria or scheme for the entire system. This set of rules is formulated as an overall system design principle to protect the system and prevent attacks.

Although the entire system is often considered to be designed perfectly securely, it is well-known that attack methods evolve based on system implementation defects and deployment loopholes. Hence, Security-By-Design (SBD) is represented as a static approach and Adaptive Best Practice (ABP) is represented as a dynamic approach which aims to adjust the system through changes to the defence mechanisms during its operation. These two approaches are the foundation for designing a secured system. Moreover, Figure 1 shows a logical illustration of sustainable trust system requirements.

Design Methodology – Figure 1 shows the two types of Design Methodologies: a static SBD and dynamic ABP. These two methodologies can ensure the foundational design that is embedded in the system security considerations and can adjust the system to prevent attacks during its operation.

System Design – refers to a pair of specific entities or objects that rely on a protocol for exchanging signalling or messages for function invocations. This communication protocol

could help the system design behaviour and the behaviour could be controlled by security mechanism e.g., key length and encryption algorithm etc. On the other hand, these predefined protocol interactions, level of security mechanisms, and any other information correlated on the interfaces could characterize the normal and abnormal behaviours.

Quantification – refers to an observation of system's internal and external behaviour by analysing the interaction relationship between network entities, or objects and stakeholders, and transforming the interaction relationships to an index. Then the index can be used to identify or measure the trustworthiness using artificial intelligence algorithms. Therefore, when an event occurs, the trustworthiness index can be obtained via those entities, or objects and stakeholder's interactions.

Knowledge Base Management – extracting the overall trustworthiness from the past events, current interactions, and aggregated past events' experience requires the support of a knowledge base management platform. Also, this provides the opportunity to incorporate and manage prior knowledge from SDOs.

3 WHAT IS TRUST MODEL

The fifth generation (5G) telecommunication system is focused on deploying a flexible network and service agility using virtualization, containerization and softwarisation technologies. Hence a 5G system faces many complex trust issues owing to the different roles of network entities, network services, and stakeholders. For most network entities the starting point is to follow the SDO trust model to embed security considerations into the implementation and reinforce the interaction behaviour in between network entities. But it is critical to also require prevention of any attacks arising from human error, implementation flaws, and deployment loopholes that happen in operations.

It is very difficult to find a sensible judgment of the network functions amongst runtime behaviour and the stakeholder's behaviour, and to trust referents under the complex 5G services or its complex business relationships. Moreover, those sensible judgments of trust referents in 5G cannot directly obtain the quantified forms of those trust referents from the system. With reference to the common understanding of trust referents, the fundamental trust elements can give a sensible formulation of the network entity's and stakeholder's trustworthy behaviour in 5G.

Indeed, envisioning the trust model in delivering a secure, multi-tenancy and multi-network slice service in 5G, an interaction relationship model should be formulated to evaluate the trustworthiness of network entities and stakeholders. In fact, a trust model [2] has been implicitly embedded into mobile telecommunication systems since the first generation (1G) analogue telecommunication system. In each generation of the telecommunication system, the trust model has been evolved. Throughout the evolution of the trust model, the roles of the stakeholders have changed. In the second generation (2G), the trust relationship was set between user (subscriber) and network (operators). Moreover, the third generation (3G) was

extended to deliver multimedia and internet services which enhanced the direct trust relationship from user and network to an indirect trust relationship between the user and the service via the network. Furthermore, 4G was enriched from multimedia and internet services to high-speed content delivery services. The 4G Trust Model stayed unchanged but it increased the network speed which provided more novel business opportunities. The evolution of telecommunication system trust models from 2G to 4G is shown in Figures 2 and 3.

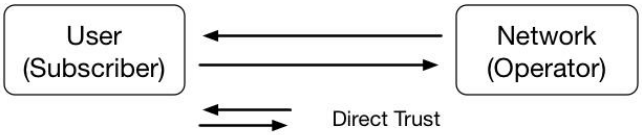

Figure 2: 2G Telecommunication System Trust Model [2]

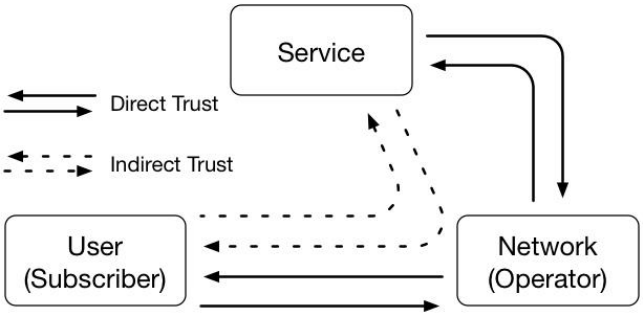

Figure 3: 3G and 4G Telecommunication System Trust Model [2]

Generally, an SDO uses two trusted methods to design a trusted environment of a system or platform. These trusted methods are Trusted Computing Base (TCB) and Trusted Platform Module (TPM).

3.1 Trusted Computing Base

TCB is a method that holds the overall security policies, enforcing a unified security policy across the entire system. This method also assists to design the system with embedded security, and to resolve the key security issues and potential vulnerabilities in between network entities or objects. A typical TCB exemplar can be found in the telecommunication standard is 3GPP's Authentication and Key Agreement (AKA) protocol. It provides an authentication procedure in a specific sequential manner, and an exchange of message in a particular order to enforce the network interface behaviour in order to protect the network entities. Usually, these specific protocol policies are implicitly embedded for the protection of network entity and interfaces.

3.2 Trusted Platform Module

TPM is a method that sets a platform with Root of Trust for Measurement (RTM) and enables the network entities or system with configuration to be reliably chronicled [3]. This method also assists to design the system based on the integrity measurement with sequential interactions in between software components under the predefined platform behaviour. A typical exemplar is Subscriber Identification Module (SIM) that stores the root key as a TPM. All software components are restricted to interact with a specific and predefined software component.

4 FUNCTIONALITY OF THE 5G TRUST MODEL

Network entities trust relationships can easily be found in any telecommunication systems. 3GPP defined 5G security architecture and the context can be used in between network entities as a reference to identify the trust relationship in between network entities. Therefore, the domain defined in 3GPP 5G security architecture could be used to explain different trust relationships [4], as shown in Figure 4. The architecture differentiates between three stratums, the application stratum for application security features, the home stratum/serving stratum for UE authentication and security between network functions, the transport stratum for UE access and the security between access network and serving network functions.

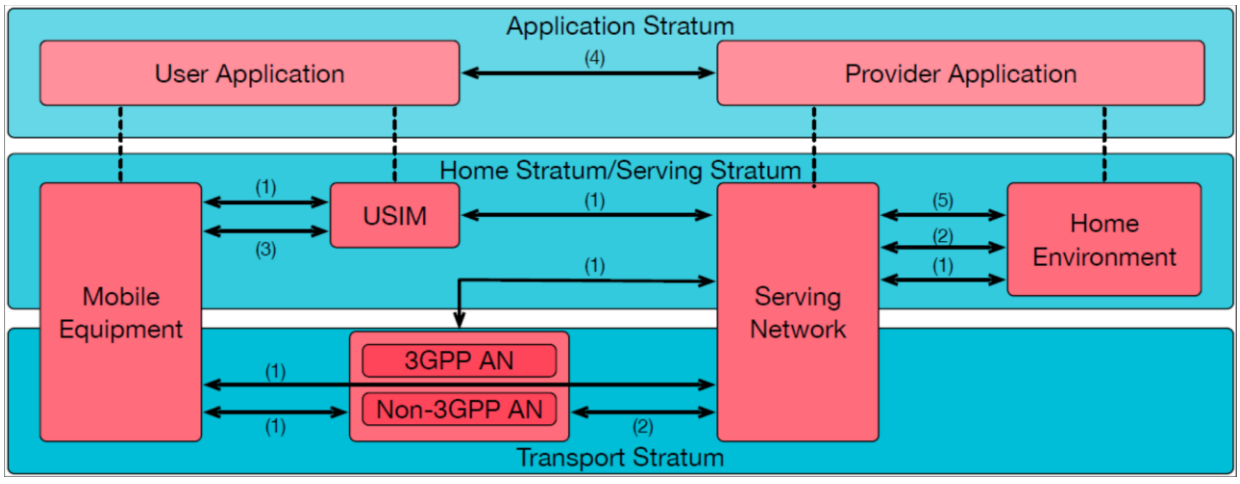

Figure 4: 5G Security Architecture

Within these three stratums, 6 security domains are defined in order to build the relevant trust between applications, mobile equipment, USIM, access network, serving network and home network:

1) **Network access security:** After the authentication of the UE with the network, the UE sets up the access stratum security, including 3GPP Access and Non-3GPP Access, i.e., the serving network provisions the security context to the access network. This enables

the trust of the access network to the UE also for subsequent procedures e.g., handover, where the key material is changed towards the new Radio Access Network (RAN) node.

2) **Network domain security:** Network nodes are set up with a secure connection between each other and pre-provisioned with certificates in order to ensure the trust between them, so that signalling data and user plane data can be exchanged securely.
3) **User domain security:** provides a set of security features so that the user can access mobile equipment in a secure way, e.g., with entering the USIM PIN at phone boot-up.
4) **Application domain security:** User applications and provider applications can exchange messages securely. For some operator provided applications e.g., IMS services, the applications trust each other based on an authentication procedure and a resulting key exchange.
5) **SBA domain security:** This new security domain compared to 4G provides secure communication between the network functions in the serving network domain and home network domain. Trust between the network functions is achieved with mutual authentication with TLS and HTTPS and server-side and client-side certificates or with network domain security.
6) **Visibility and configurability of security:** This feature provides feedback to the user whether certain security features are enabled or not, i.e., the user can trust that the communication is secured on various layers.

Further the procedures that are carried out between the different functions and entities in the network establish the following trust relationships as shown in Figure 5:

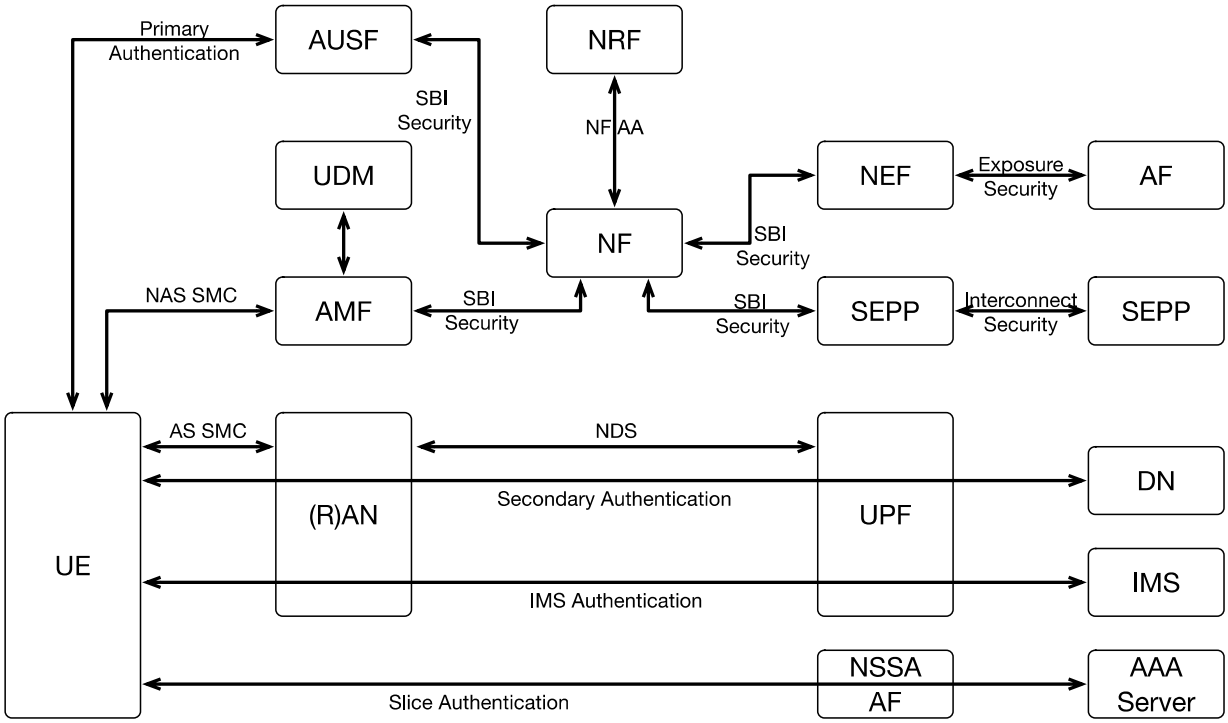

Figure 5: Trust Relationships between Network Functions and Entities

Several trust relationships are illustrated as follows:

- **UE – AUSF:** The UE and the AUSF perform the primary authentication (EAP-AKA' or 5G-AKA) in order to build up the trust relationship and the resulting key material. The authentication is performed in the home network, only after successful authentication is the serving network viewed as trusted and receives the UE profile.
- **UE – AMF:** The UE and the Access and Mobility Management Function (AMF) perform the Non-Access Stratum (NAS) Security Mode Command (SMC) procedure in order to generate keys for a trusted NAS communication.
- **UE – (R)AN:** The UE and the (R)AN perform the AS SMC procedure in order to generate the key material for securing the communication over the radio interface. After a handover, the new (R)AN nodes can trust the UE once the new key is provided from the old (R)AN node and there is no key mismatch.
- **UE – DN:** The UE can authenticate with an AAA-Server in a Data Network with the secondary authentication procedure. After the successful secondary authentication. i.e. the UE is trusted by the data network, the serving network provides the UE access to the data network.
- **UE – AAA-S:** In order to access certain slices, the UE may authenticate with an (external) AAA-Server via a Network Slice Authentication and Authorization Function (NSSAF). Once the UE is authenticated and trusted, the serving network grants access to the network slice.
- **UE – IMS:** The application client in the UE authenticates with an operator service, e.g., IMS. After authentication the client is trusted and can access the service.
- **(R)AN – UPF:** As an example, the (R)AN node and the UPF are using network domain security (NDS) for trusting each other and protecting the communication between them.
- **AMF – NF:** Two network functions use SBI security for authentication and authorization and a trusted communication.
- **NF – NRF:** Each NF authenticates mutually with the NRF via transport layer protection solution, client credentials assertion-based authentication or implicit based on NDS/IP or physical security. Once the NF is authenticated by the NRF, it can get authorized by the NRF for service access at a service producer.
- **UDM – AMF:** After primary authentication, the AUSF provides the authentication result to the UDM so that the UDM can trust subsequent AMF requests.
- **NEF – AS:** For secure service exposure to 3rd party application functions, the NEF and AF perform authentication based on client and server certificates using TLS. The NEF then trusts the requests from the AF on NF events and capabilities.
- **SEPP – SEPP:** SEPPs perform mutual authentication and negotiation of cipher suites with each other using certificates for authentication. SEPPs differentiate the certificates of peer SEPPs with intermediate SEPPs performing message modifications.

5 TRUST DEFINITION

Every trust model requires a definition of trust. The Sustainable Trust Model is not an exception; it aims to use SDO trust models as a foundation and has the ability to adapt the future evolution of trust models from SDOs. Moreover, sustainable trust should have an ability to evolve based on the runtime environment. Therefore, the fundamental Sustainable Trust definition is based on the collection of evidence regarding the runtime relationship between stakeholders or network entities. There are several attributes of trust: reliability, visibility, sensitivity, reputation, utility, availability, risk, vulnerability, quality of service (QoS), and quality of experience (QoE), that would affect the network entity's and stakeholder's trustworthiness indices.

The Sustainable Trust Models also define direct and indirect trust relationships in between network entities and between stakeholders.

5.1 Direct Trust Interactions

Direct trust is fundamentally based on the direct communication, direct interactions, and service behaviour in between two entities. For instance, a direct trust relationship exists between network entities. For the current network entities, the reference of direct trust is formed on the needs of exchanging request and response of signalling or data traffic. For example, 3GPP 5G core network entity AMF has a direct trust relationship with Session Management Function (SMF). The AMF directly interacts with SMF based on the Packet Data Unit (PDU) Session ID received from the NAS message. Figure 6 illustrates the direct trust relationship in between AMF and SMF.

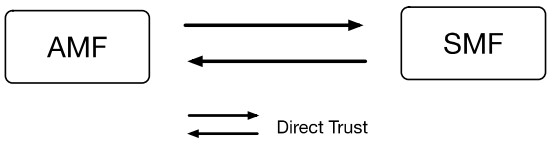

Figure 6: AMF and SMF Direct Relationship

Another example of direct trust based on the stakeholders, a direct trust relationship exists between end-user and tenant or tenant and MNO. In mobile networks, the reference of direct trust is formed on the identity of the subscriber. Subscribers have a strong direct trust relationship with the Home Public Land Mobile Network (HPLMN) operators.

5.2 Indirect Trust Interactions

Indirect trust is derived from the service behaviour and the recommendation passed through one or more intermediate network entities or stakeholders. For instance, an indirect trust relationship can be specifically referred to the 3GPP 5G core control plane network entities. The indirect trust relationship can be found in between PCF and UPF, with the intermediate network entity being an SMF. Typically, trust relationship would be initiated from a SMF request to obtain the policy rules from PCF and convey those obtained policy rules to handle and forward packets

by the UPF. Figure 7 illustrates the direct trust relationship in between PCF and SMF and indirect trust relationship in between PCF and UPF.

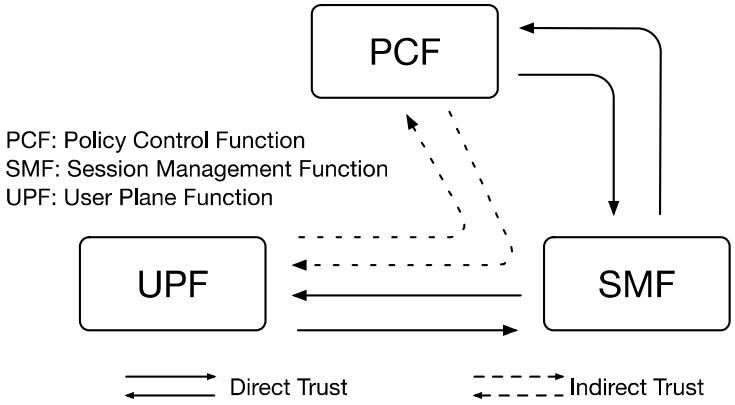

Figure 7: An Indirect Trust Relationship

Another indirect trust relationship example can be referred between stakeholders, tenants, and infrastructure providers (InP) from the tenant's point of view, in which they do not have SLAs. In current mobile networks, the reference of indirect trust is formed on the identity of the subscriber, but the indirect relationship would be defined via mobile virtual network operator (MVNO) to MNO. However, the indirect trust reference would dynamically rely on the identity of the subscriber, tenant, MNO, and various types of InP.

6 NETWORK FUNCTION TRUST MODEL

Virtualization, containerization and softwarisation provides flexibility in terms of network infrastructure resulting in agility to deploy network functions and services. Disaggregation of network functions and services decouple the software from hardware and allow network functions to be split into multiple locations. Therefore, commodity hardware and openness of software would evolve the development and operation (DevOps), and continuous integration and continuous delivery (CI/CD) processes of the future generation network.

Typically, before the network is ready for production, a vulnerability assessment would be conducted to identify or classify all security risks which give a state of the installed software trustworthiness to the operating network. However, after the network is in operation, there is no mechanism to ensure the network function or service's security risk and trustworthiness. Software reliability at runtime is a big issue of software supply chain and the deployment of network service chain. Particularly, companies might not apply code review process properly, and some of the network functions are relied on open-source community and the project leader to ensure the quality. Therefore, a reliable software or network function implementation is highly important, which enables building trust. Furthermore, ETSI Network Function Virtualization (NFV) has already proposed a framework to formulate a chain of trust via network entities interfaces interaction [5].

There are several characteristics of the network entities trust model they involved: (i) evaluation of the network entity's trustworthiness in the network, (ii) measurement of the strength level of security mechanism used in the network entities, (iii) quantification of the network entities' behaviour in the network, and (iv) mitigation of the risks and vulnerabilities autonomously through interactions between network entities.

6.1 NFV Main Network Functions Trust Model

NFV is a mobile network resources information management platform. It sets to manage the physical and virtualized resources information in order to orchestrate the resources that would be based on traffic and service resources on demand. Under the NFV architecture, there are three main entities that interwork in a specific way. The NFV Orchestrator (NFVO) is responsible to govern the entire resources and arrange the network resources to produce a desired effect. The Virtualized Infrastructure Manager (VIM) is responsible to control or administrate the NFV infrastructure (NFVI) compute, storage and network resources within an administrative domain. The Virtual Network Function Manager (VNFM) is responsible to manage and organize lifecycle of virtual network functions (VNFs) within the administrative demand. However, those main network entities might have various level of quality. Also, those network entities may have poor quality implementing, potentially resulting in runtime errors or buffer overflow bugs that cause irregular behaviour within the network entity. Furthermore, these irregular behaviours might also affect the interactions, message exchange and the trustworthiness of the network entities software at the runtime.

Figure 8 shows the direct trust relationships in between NFVO and VNFM, VNFM and VIM, and VIM and NFVO. Indirect trust interactions are in between NFVO and VIM via VNFM. The NFVO directly interacts with the VNFM, when it requires executing of workflows in adding or removing VNF instances. The NFVO directly interacts with the VIM, when there simply is a request of virtualized infrastructure management information or other virtualized resource optimization executions. The VNFM also directly interacts with the VIM, when there is an execution of scaling or keep alive message exchange. Moreover, the indirect interactions from the NFVO to the VIM via VNFM also could be based on the service optimization or scaling executions.

However, implementation might subsume all functionalities into one single entity, then the trust model would be in between function invocations.

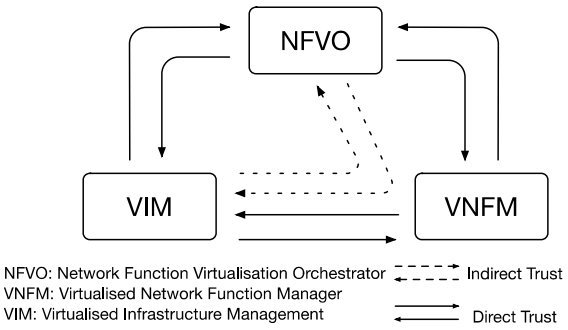

Figure 8: NFV MANO Main Entities Trust Model

6.2 RAN Function Trust Model

The RAN function trust model can be classified into two sub-trust models, the RAN internal trust model and RAN external trust model as shown in Figure 9 and 10 respectively.

The RAN internal trust model deals with the interactions and trust evaluations within a RAN (i.e., between various gNB internal functions such as gNB-CU-CP, gNB-CU-UP and gNB-DU that together form a disaggregated gNB). A gNB may consist of a gNB-CU-CP, multiple gNB-CU-UPs and multiple gNB-DUs. The gNB-CU-CP can derive direct trust with the gNB-CU-UP(s) (for interactions over E1 interface) and gNB-DUs (for interactions over F1-Control plane interface). Similarly, the gNB-CU-UP can derive direct trust with the gNB-DU (for F1-User plane interface). In general, the gNB-CU-CP selects the appropriate gNB-CU-UP(s) for the UE requested services as defined in [4]. To provide different sets of services simultaneously for a UE, a gNB-CU-CP can select one or more gNB-CU-UPs but establishes a common user plane security. The sustainable trust computation can have significant impact to the disaggregated gNB, especially for the user plane as the user plane security terminates in the gNB. For example, the gNB-CU-CP can consider the associated gNB-CU-UP's trust level/trust index to adopt dynamic measures to ensure user plane security accordingly.

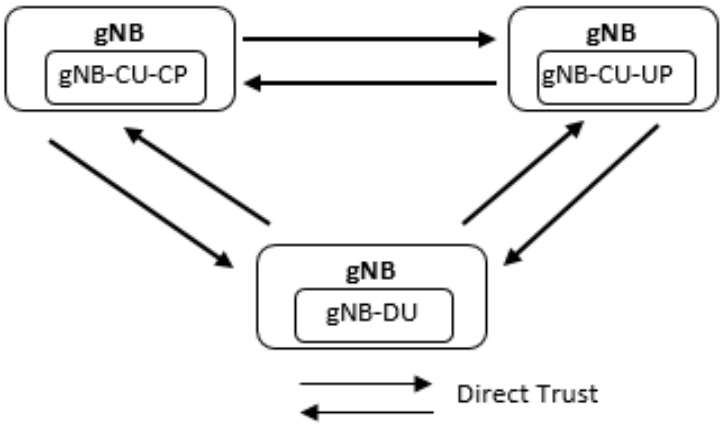

Figure 9: 5G RAN Function Internal Trust Model

The RAN external trust model deals with the interactions of RAN (e.g., gNB) with UE(s) and other core network functions (example., AMF, SMF and UPF). RAN can ideally compute either direct trust, indirect trust or both direct and indirect with any associated network function accordingly based on the involved protocols and network node's operational relationship. For example, the RAN can compute direct trust for the interactions with the AMF, which terminates the RAN Control plane interface (i.e., N2). The indirect trust can be computed by the RAN for indirect interactions with SMF, which manages the session and initiates AN specific SM information to RAN (sent via AMF over N2). Furthermore, the RAN can compute both direct and indirect trust for the interactions with UPF, i.e., a direct trust can be derived for the user plane interface (over N3) and an indirect trust can be derived for the control plane signalling (i.e., sent via AMF and SMF over N2 and N4) respectively.

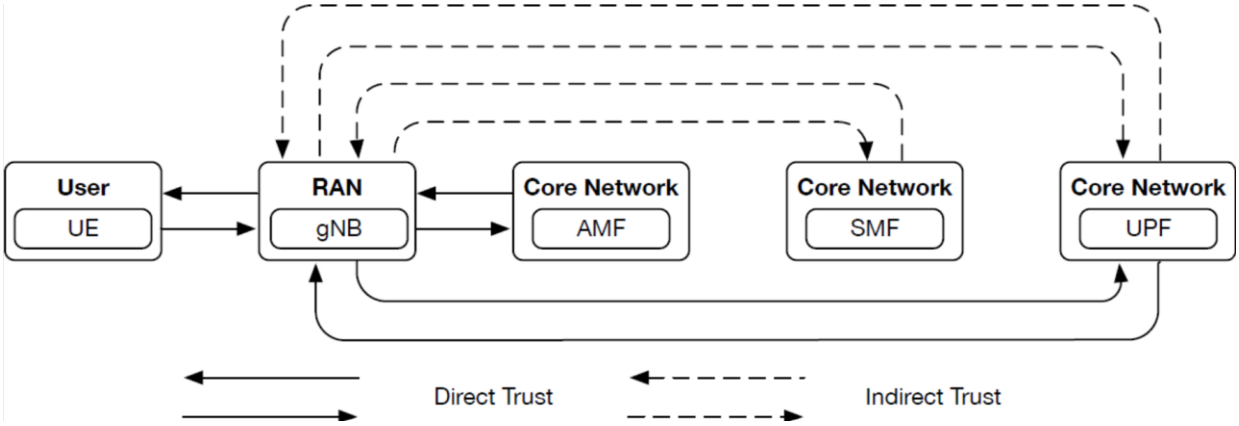

Figure 10: 5G RAN Function External Trust Model

7 STAKEHOLDER TRUST MODEL

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 which is illustrated in Figure 11. The characteristics of the stakeholders' trust model are: (i) evaluation of the stakeholder's trustworthiness in the network, (ii) measurement of the security strength of stakeholder's network and services, (iii) quantification of the stakeholder behaviour in the network, and (iv) mitigation of the risks and vulnerability autonomously through interactions between stakeholders. 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.

The stakeholders are end-users, customers, subscribers, tenants, MNOs, service providers and infrastructure providers, etc. Furthermore, the 5G trust models are useful in gauging the security level of a telecommunication system in real time and capturing the level of trustworthiness index.

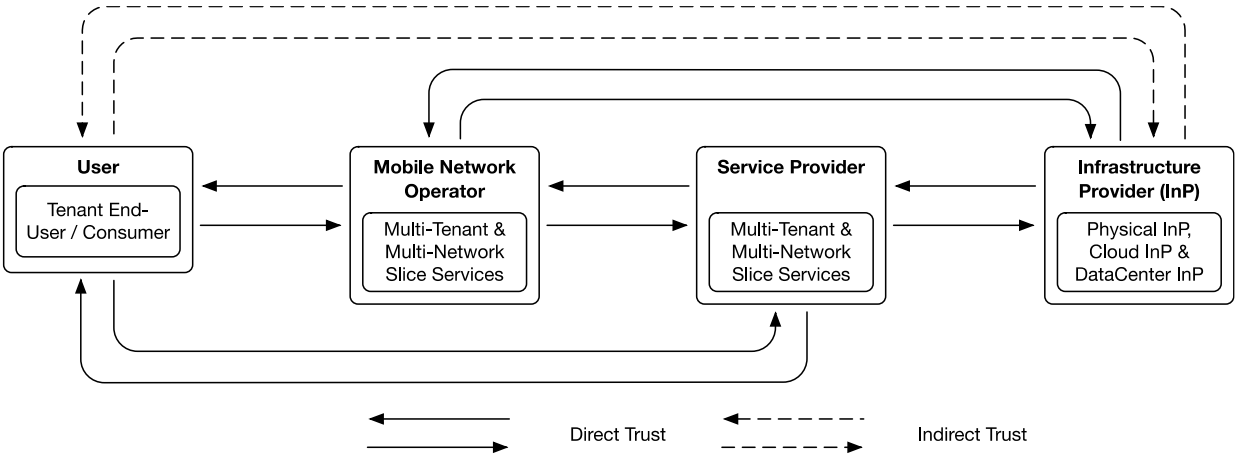

Figure 11: 5G Stakeholder Trust Model

8 TRUST MEASUREMENT AND DIFFERENTIATION

Telecommunication systems have many sources of contextual information available to be extracted that can help to derive the trustworthiness of network entities and stakeholders. Identifying and differentiating trust metrics would facilitate determining trustworthiness. However, algorithms might require to be developed for analysing the collected data. In this section, a simple approach for identifying the trust metric that would help to determine the basic parameters or attributes for trustworthiness index is introduced. This metric could be formulated from a single dimensional array to multi-dimensional arrays and also those dimensions could be formulated with different attributes. The National Institute of Standard and Technology (NIST) has provided a security measurement metric for general purpose of system security and analysed a common process needs: one shall identify what should be measured, then organize the involved variable, and design the collected index ranges. For example, the trustworthiness index related to any end-user can be computed by the network functions of an operator network or service provider based on the identity of the subscriber and interaction relationships. The use of digital identity with service specific verifiable credentials can enable computation of an accurate real-time and accurate trustworthiness index during the direct and indirect trust derivation for any end-user. Figure 12 provides a few examples of potential parameters that can be collected or used to obtain trust value. These examples could be extended based on the same principle as long as those parameters feed with the derived expert algorithm. Moreover, this principle can be simply applied on the security association's key length. It is well-known that a security association with longer key length delivers stronger security association, therefore, the measurement of key length can be interpreted as an element of representation of security mechanism strength in between two network entities, which can use to drive the trustworthiness of the network entry trust behaviour. A graphical representation can be found in Figure 13.

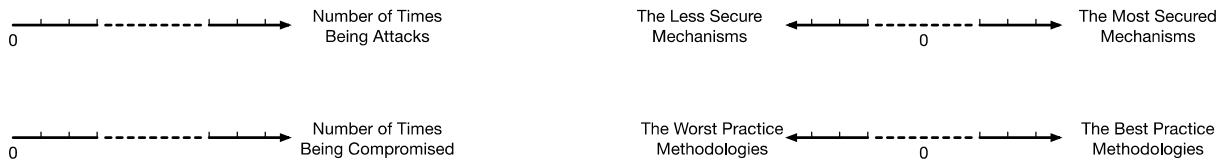

Figure 12: Exemplar of Trust Measurement and Differentiation

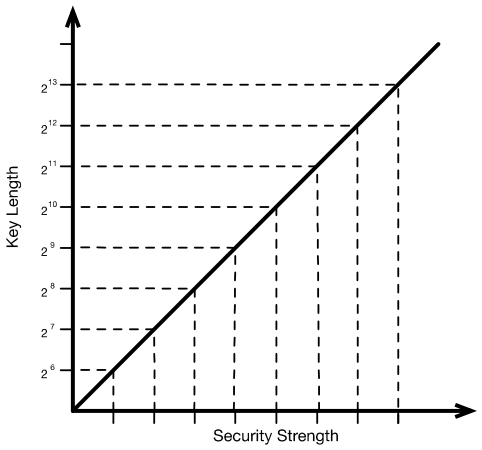

Figure 13: Exemplar of Trust Measurement of Security Association Key Lengths

9 KNOWLEDGE-BASED MANAGEMENT IN TRUST

Knowledge-based management (KBM) is often referred to the gathering of data, transformation of data to useful information, and organizing the past and present information to knowledge. Trust model applies the KBM approach to formulate an entity, object or stakeholder's trust paragon of virtue. By quantifying the trust model fundamental elements (See Section 2.1) and formulating the necessary trust measurements (See Section 6), the KBM processes would generate trust knowledge, and transfer the trust knowledge in creating a better understanding of entity, object and stakeholder trustworthiness.

In a trust model, the KBM is divided into two categories (a document/text-based approach and event-based approaches) to extract the trustworthiness of network entities, services and business stakeholders. For instance, in the text-based approach, a document has been submitted to SDO would trigger an evaluation process. This process can be used to detect the content similarity and identify the quality of the document's content from the past documents. The current submitted document could use these detection and identification processes to obtain the current trustworthiness of the stakeholder and who submitted the document, enabling an ultimately increase in the quality of the SDO documents quality. Furthermore, the detection and identification processes could use natural language process on the submitted documents. For an event-based approach, an interaction would trigger different types of events. Those events are distinguished into past events and current events, then the current event is combined or aggregated aggregate with past event as a relationship experience to obtain the current trustworthiness of an entity, service or stakeholder. Furthermore, basically, those obtained trust relationships can be represented by a graph theory, and different interaction relationships could also be represented by directed graphs and undirected graphs.

Moreover, telecommunication systems are constantly evolving. Trust-KBM can differentiate the level and type of knowledge, which definitely would increase the overall sustainability and the

level of overall system protection. The obtained trust knowledge could also assist the system to formulate self-evolution.

10 CONCLUSION

A Sustainable Trust Model should be able to adapt any changes and facilitate any evolution of those trust models. It should give a complementary to all SDO trust models and be able to co-exist with those trust models. However, the design of a sustainable trust model is reliant on the real-time evaluations approach of trustworthiness which currently the telecommunication systems are lacking. Further, this sustainable trust model should also have a flexible capability to maintain and influence the behaviour of network entities, services implementation, and integration with different telecommunication systems. Last but not the least, the behaviour of stakeholders should also be influenced by the sustainable trust model and keep delivering the right and precise service to other stakeholders.

A Sustainable Trust Model is a practical framework that complements an SDO static trust model approach. It could help the MNO to secure a flexible network under a virtualisation environment, increase the entire network runtime reliability and reduce the risk of runtime error. Besides, the Sustainable Trust Model puts an embedded behaviour validation in the entities, objects or stakeholders which is very similar to a peer-review process. Moreover, it enforces the good service or software quality, and ensures the vendor to put thorough testing on the service or software. This White Paper also provides an advanced approach of a real-time evaluation of future generation telecommunication systems which is based on the run-time trustworthiness of the network entities, services or stakeholders. An artificial intelligence knowledge-based management can be used to handle the event and text-based approaches for obtaining trustworthiness.

In the future generation network, a Sustainable Trust Model will give a confident environment to the network infrastructure design that is based on the SBD and ABP. Basically, it helps the MNO to tackle and resolve the run-time trustworthiness issue of the network entities and increases the virtualised network infrastructure visibility. The Sustainable Trust Model is not restricted to future generation networks, it is also recommended to be introduced to legacy networks where possible.

LIST OF ABBREVIATIONS

1G	1st Generation
3GPP	3rd Generation Partnership Project
5G	5th Generation
AAA-S	Authentication, Authorization and Accounting Server
ABP	Adaptive Best Practice
AF	Application Function
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
AN	Access Network
AS	Application Server
AUSF	Authentication Server Function
B2B	Business-to-Business
B2C	Business-to-Customer
CU	Central Unit
CP	Control Plane
DN	Distinguished Name
DU	Distributed Unit
EAP	Extensible Authentication Protocol
gNB	Next generation NodeB
HTTPS	HyperText Transfer Protocol Secure
KBM	Knowledge-based management
ID	Identifier
IMS	IP Multimedia Subsystem
InP	Infrastructure Provider
IP	Internet Protocol
MNO	Mobile Network Operator
NAS	Non-Access-Stratum
NDS	Network Domain Security
NEF	Network Exposure Function
NF	Network Function
NFV	Network Function Virtualization
NFVO	NFV Orchestrator
NRF	Network Repository Function
PCF	Policy Control Function
PIN	Personal Identification Number
RAN	Radio Access Network
SBD	Security-By-Design
SBI	Service Based Interface
SDO	Standards Developing Organisation
SEPP	Security Edge Protection Proxy

SM	Session Management
SMC	Security Mode Command
SMF	Session Management Function
TCB	Trust Computing Base
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDM	Unified Data Management
UE	User Equipment
UP	User Plane
UPF	User Plane Function
USIM	UMTS Subscriber Identity Module
VIM	Virtualized Infrastructure Manager
VNF	Virtual Network Function
VNFM	Virtual Network Function Manager

REFERENCES

[1] https://www.3gpp.org/news-events/1975-sec_5g

[2] Stan Wong, "The Fifth Generation (5G) Trust Model", IEEE WCNC 2018

[3] Shane Balfe, Eimear Gallery, Chris J. Mitchell and Kenneth G. "Challenges for Trusted Computing", Paterson Information Security Group, Royal Holloway, University of London

[4] 3GPP TS 38.401 C16.4.0 "'Security architecture and procedures for 5G system", (Release 16), Jan 2021

[5] ETSI GR NFV-SEC 007 V1.1.1 (2017-10), Network Function Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments"

[6] https://downdetector.com

APPENDIX

Cloud Service Provider Operation

Typically, a service provider sells services to a customer and the customer has to find out which service provider is more reliable and provides good quality of service. However, there is very limited information available of service provider's performance to the public. Therefore, Sustainable Trust Model is one of the methods to increase the visibility of service in the future. Figure 14 shows a vision of how Sustainable Trust Model applies on cloud service provider's services to increase the cloud service visibility and real-time trustworthiness evaluation. In the Real-time Service Outage example, we provide an existing service for system evaluation. In Figure 14, we combine the real-time service outage monitoring concept into the Sustainable Trust Model from a cloud customer purchasing a cloud service to the operation, and the knowledge-based management based on events.

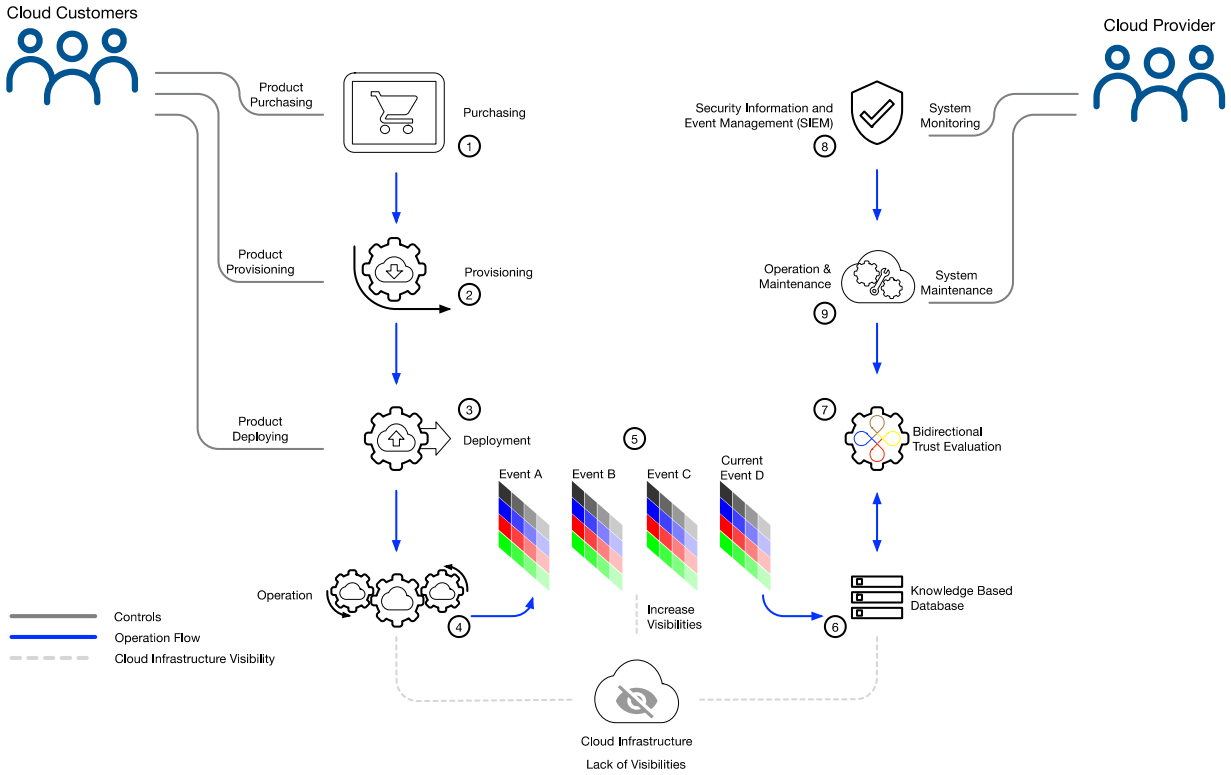

Figure 14: Cloud Infrastructure Operation with Trust Evaluation

A Real-time Service Outage Platform

This is a web platform [6] for providing a real-time outage information as a service provider evaluation for the public to gain trustworthiness of those services that are provided by the

service provider. It also has a graphical illustration which services are provided and the period of time of failure. It also has other types of services evaluations on the website. The graphical indication provides the service trustworthiness from the graph of real-time outage, which in this way provides a service evaluation.

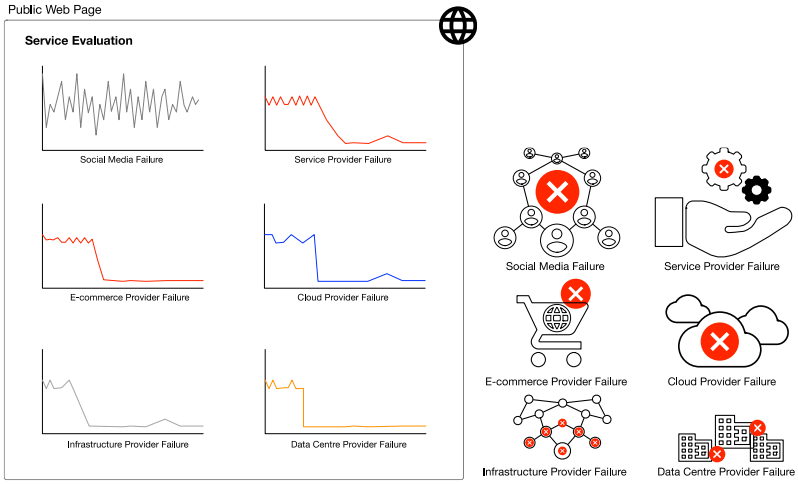

Figure 15: An Illustration of A Real-time Service Outage Web Platform