



Deliverable D2.2

Trust model (draft)

Project name	5G Enablers for Network and System Security and Resilience	
Short name	5G-ENSURE	
Grant agreement	671562	
Call	H2020-ICT-2014-2	
Delivery date	v1.0: 2016-08-25; v1.1: 2016-11-22	
Lead beneficiary	IT Innovation	Stephen Phillips: scp@it-innovation.soton.ac.uk
Authors	IT Innovation: Stephen C. Phillips, Gianluca Correndo, Mike Surridge Orange: José Manuel Sanchez Vilchez, Ghada Arfaoui Nixu: Seppo Heikkinen VTT: Marja Liinasuo, Pekka Ruuska EAB: Christian Schaefer, Mats Näslund Oxford: Ravishankar Borgaonkar, Piers O'Hanlon TASE: Gorka Lendrino, Carla Salas TIIT: Pier Luigi Zaccone, Luciana Costa	

Executive summary

Trust is a response to risk. A decision to trust someone (or something) is a decision to accept the risk that they will not perform as expected. To manage risk in a socio-technical system such as a mobile network we need to understand what trust decisions are being made, the consequences of those trust decisions and we need information on the trustworthiness of other parties in order to make better decisions.

New business models and new domains of operation in 5G networks facilitated by network function virtualisation and software defined networking bring increased dynamicity compared to 4G and an increase in the number of stakeholders and associated trust relationships. New relationships bring new risks that must be understood and controlled and in a system as complex as 5G this implies the need for a trust model which can model the system, highlight potential risks and demonstrate the effect of adding controls or changing the design.

This document takes the first steps towards such a trust model. Firstly we discuss and define terminology. This is essential, as in common speech terminology can be quite muddled but in trust modelling we must be precise. We then review the state of the art in trust modelling, firstly looking at human trust factors (as humans are essential components of 5G network scenarios), understanding how humans make decisions on whether to trust or not when dealing with other humans and when dealing with machines. Secondly we review work on machine trust: machines of course only follow the instructions given to them through their software code by humans, but we review what the options are and the indicators for trustworthiness of other entities, whether they are humans or machines. Finally we look at trust and trustworthiness by design techniques which we recommend for use both during the design of 5G and when changing the design of a 5G deployment by adding or removing elements.

To understand 5G networks we must first understand 4G networks, and this is what is covered in the next chapter, looking first at the actors and business models of 4G (including where they touch on satellite services) and then extracting the trust aspects of the 4G network. Following this we review how the actors and business models are expected to change as we move to 5G, bringing in new domains and new opportunities for operators (both terrestrial and satellite). Here we also review the majority of the 5G use cases identified by 5G-ENSURE in an earlier document, identifying the entities involved and the trust issues in each one.

The final chapter brings all this information together to firstly discuss privacy aspects, then analyse the relationships between 4G stakeholders (demonstrating surprising complexity even there) and finally lay out a proposed approach for the work in 5G-ENSURE which will culminate in a machine understandable trust model able to assist stakeholders in managing risk.

As this document is a “draft” trust model, the next steps to be done are set out alongside the conclusions.

Foreword

This document was originally entitled 'Trust model ("U2Ut and M2Mt")' and was to have been followed by a second deliverable 'Trust model ("M2Ut")' at PM18. In early analysis of the 5G trust models it became clear that the separation of the user to user and machine to machine trust aspects from the machine to user trust model was not useful and it was decided that this document should be retitled 'Trust model (draft)' and to follow it with 'Trust model (final)': both documents encompassing all user and machine combinations.

The document has been written in cooperation with the writing of D2.3 'Risk assessment, mitigation and requirements (draft)'. It is informed by D2.1 'Use cases' and, along with the risk analysis, feeds into the work on architecture currently proceeding and to be reported in D2.4. Of course, the trust model also informs the work underway in WP3 in the Trust and the Privacy tasks.

Contents

1	Introduction.....	6
2	Terminology.....	6
3	State of the Art in Trust Modelling	10
3.1	Human Trust.....	10
3.1.1	Human to human trust.....	10
3.1.2	Trust in technology	12
3.1.3	Human trust and 5G.....	13
3.2	Machine Trust	14
3.2.1	Trust decisions	14
3.2.2	Trust models in Wireless Communication Networks.....	15
3.2.3	Computational Trust models.....	16
3.2.4	Trust models in Virtual networks	21
3.2.5	Machine trust and 5G	21
3.3	Trust and Trustworthiness by Design Models.....	22
3.3.1	General features and 5G	22
3.3.2	Zero Trust Model	22
3.3.3	System trustworthiness modelling	23
4	Trust in 4G Networks	25
4.1	Actors and Business Models	26
4.1.1	Overview	26
4.1.2	4G Satellite Business Models.....	27
4.2	Trust.....	28
4.2.1	Historical analysis	28
4.2.2	Current trust model	29
5	Trust in 5G Networks	32
5.1	Actors and Business Models	32
5.1.1	New domains for 5G	35
5.1.2	Potential of 5G new domains: Business models powered by network performance, data and slicing	37
5.1.3	Trust considerations in 5G	38
5.1.4	5G Satellite Business Models.....	39
5.1.5	Summary of 5G actors.....	41
5.2	Use Case Analysis	42

5.2.1	Satellite Identity Management for 5G Access (UC1.3)	42
5.2.2	MNO Identity Management Service (UC 1.4)	43
5.2.3	Device Identity Privacy (UC 2.1)	44
5.2.4	Subscriber Identity Privacy (UC 2.2)	44
5.2.5	Trust in Authentication of IoT Devices in 5G (UC 3.1)	45
5.2.6	Trust in Network-Based Key Management for End-to-End Security (UC 3.2)	46
5.2.7	Virtualized Core Networks, and Network Slicing (UC 5.1)	47
5.2.8	Adding a 5G node to a virtualized core network (UC 5.2)	47
5.2.9	Reactive traffic routing in a virtualized core network (UC 5.3)	47
5.2.10	Verification of the virtualized node and the virtualization platform (UC 5.4)	48
5.2.11	Control and Monitoring of Slice by a Service Provider (UC 5.5)	48
5.2.12	Integrated Satellite and Terrestrial Systems Security Monitor (UC 5.6)	48
5.2.13	Satellite-Capable eNB (UC 8.1)	49
5.2.14	Trust in alternative roaming (UC 9.1)	49
5.2.15	Privacy in context-aware services (UC 9.2)	50
5.2.16	Trust in network elements (UC 9.3)	50
5.2.17	Trust in botnet mitigation (UC 10.1)	51
5.2.18	Privacy Violation Mitigation (UC 10.2)	51
5.2.19	SIM-based and/or Device-based Anonymization (UC 10.3)	51
5.2.20	Trust in Lawful Interception in dynamic 5G Network (UC 11.1)	52
5.2.21	Trust in End-to-End Encryption for Device-to-Device Communications (UC 11.2)	53
5.2.22	Summary	54
6	Trust Model	54
6.1	The Role of Privacy	54
6.2	Proposed Approach	55
6.2.1	Trust model requirements	55
6.2.2	In whom (or what) does a trustor trust?	56
6.2.3	For what does a trustor trust?	59
6.2.4	How much should a trustor trust?	63
6.2.5	How much does a trustor trust?	65
7	Conclusions and Next Steps	66
8	References	67

1 Introduction

The characteristics of the 5G use cases are quite different from any previous generation network, which implies that the 5G trust model must be carefully analysed and defined. The trust model used in networks up to and including 4G has been relatively static over the last 20 years, involving actors such as the user/subscriber and two network operators (home and serving). However, we note that even in this seemingly simple case, the actors and trust relationships are complex and the complete trust model for 4G has never been defined.

A 5G trust model is required to assist in the design and operation of 5G networks. The security enablers and architecture being developed in the project need to enable and facilitate trust in the dynamic 5G environment, taking into account human and machine factors.

Due to the dependency between deliverables of 5G-ENSURE (specifically Trust Model, Threats/Requirements, and Security Architecture), the project has adopted the approach of working in two iterative cycles. Initial “drafts” of the three corresponding reports are produced at the “half-time” point of the project. These drafts will then be refined into “final” versions near the end of the project.

This “draft” document takes a first step towards defining the actors and business models for 5G and the trust and liability model between these actors, supporting the identified business use cases. The chapters on the “State of the Art in Trust Modelling” and “Trust in 4G Networks” are not expected to need updating. The chapter on “Trust in 5G Networks” is preliminary: the set of 5G actors may be refined, the analysis of use cases will be extended to include (at least) all the use cases from 5G-ENSURE D2.1 “Use Cases” and the analysis of all the use cases will be taken to the next level of detail. The “Trust Model” chapter is preliminary and at this stage outlines the approach and dependencies.

2 Terminology

Trust as a concept is of interest in many different research disciplines including psychology, sociology, economics, and even law, as well as in IT. Each discipline has its own understanding of the word ‘trust’, and inevitably over time, each understanding has become specialised to address the needs of its research community. Consequently the word is often used in a narrow technical sense, e.g. the OASIS standard ‘WS-Trust’ [WS-Trust] has nothing to do with trust in a human or social sense, but relates to the verification of remote assertions from different sources in IT systems. Unfortunately, such narrow definitions may also limit the scope of research into trust, and lead to models that fail to capture all its relevant dimensions. They certainly make it difficult to communicate the results of research with other research communities or with the general public.

To avoid these problems of ‘jargonised’ terminology, we propose a return to the full meaning of trust as a word in English. The definitive source for this is the Oxford English Dictionary (OED), which gives the following common definition:

Trust: firm belief in the reliability, truth, or ability of someone or something.

The OED goes on to discuss other less common uses, including specialisation to acceptance of a statement as being true. This is closer to the meaning in ‘WS-Trust’ and is more often used in IT research. Even in an IT context, the broad definition is often needed. For example, in the Internet Security Glossary v2 (RFC 4949) [Shirey 2007], trust is defined as “...a feeling of certainty (sometimes based on inconclusive evidence) either

(a) that the system will not fail or (b) that the system meets its specifications (i.e., the system does what it claims to do and does not perform unwanted functions)”, though RFC 4949 then focuses mainly on the role of trust related to security tokens such as X.509 certificates. In 5G-ENSURE, we need to consider trust between different actors as well as between actors and ‘the system’ in a 5G ecosystem, so we recommend that the full, broader general English definition should be used.

We can also then define:

Trustor: a person or thing that has trust in someone or something else.

and

Trustee (or subject): the person or thing in which the trustor has trust.

Given the above definition of trust, it makes sense to look at the same source for the definition of the term ‘trustworthiness’. According to the OED this means ‘the ability to be relied on as honest or truthful’. That doesn’t quite match the full sense of ‘trust’ which may involve belief in things other than honesty or truthfulness. We therefore propose the following slightly different definition in 5G-ENSURE:

Trustworthiness: the property of being reliable, truthful and capable.

This definition initially seems circular, equivalent to ‘being worthy of trust’. That is not quite the case, because trust is a belief, i.e. it is a subjective view held by the one who trusts. However, trustworthiness is a property that could be measured objectively for an actor, system or system component. In fact, RFC 4949 refers to a ‘trustworthy system’ as “A system that not only is trusted, but also warrants that trust because the system's behaviour can be validated in some convincing way, such as through formal analysis or code review”. Again, we need to consider trustworthiness of actors as well as IT systems and components, and allow for the possibility that a system might be trustworthy yet still not be trusted, so we prefer to use the less specific definition in 5G-ENSURE.

The optimum situation is when trust in an entity and the trustworthiness of that entity are in balance. If trust in an IT system is lower than its trustworthiness, the trustor will use the system less than they could safely do (failing to reap the full benefits), or they may take precautions before they start to use it (adding to their costs). If trust is higher than the trustworthiness of the system, the trustor will be exposed to more risk than they think, and may end up coming to some harm.

This raises an important point, that trust is related to the acceptance of risk. (If fact many lawyers would argue that the definition of trust should be in terms of risk, and that trust only exists if the trustor demonstrably accepts a level of risk).

Risk: exposure (of someone or something valued) to danger, harm or loss

In classical risk analysis, including information system risk management based on ISO 27001, a risk exists where there are potential threats, i.e. a threat is a source of risk. Here we need to move away from the strict English definition, which encompasses the notion that a threat is a statement of intent to cause harm or loss. In the context of 5G-ENSURE, it does not matter whether or not intent to cause harm exists or is communicated. The definitions from RFC 4949 are actually more useful:

Threat: a potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.

RFC 4949 makes it clear that threats could be ‘intentional’ (involving attack by a malicious and intelligent entity), or ‘accidental’ (arising from an unintended error or natural disaster). It goes on to define further terms describing the structure of a threat:

Threat action: a realization of a threat, i.e. an occurrence in which system security is assaulted as the result of either an accidental event or an intentional act.

Threat consequence: a security violation that results from a threat action.

Threat agent: a system entity that performs a threat action, or an event that results in a threat action.

Finally, we can add two more definitions that are important in risk analysis:

Threat likelihood: the probability that a threat is realised, i.e. that the threat action will occur.

Threat impact: the level of harm caused by the threat consequence.

In conventional risk analysis based on [ISO 27005] or (more generally) [ISO 31010], the level of risk is determined from a combination of threat likelihood and impact. The correct treatment depends on the level of risk, the main options being to:

- accept the risk (i.e. trust that it won’t arise);
- avoid the risk (by disengaging with the untrusted entity);
- transfer the risk (e.g. by insuring against the risk or reaching an agreement with someone else making them responsible); or
- reduce the risk (by using security measures to reduce the threat likelihood or to mitigate its consequences).

Finally, we can specify what we mean by a trust model:

Trust model: a basis for understanding and analysing the role played by trust (in a socio-technical system), and using qualitative and where appropriate quantitative measures of trust and trustworthiness.

With these definitions, one can consider three basic questions that always arise in any consideration of trust, which should be captured and answerable for a system by using the associated trust model. These are:

- In what does the trustor trust?
- How much should the trustor trust?
- How much does the trustor trust?

The first of these questions is really equivalent to a question about risks, i.e. what risks does the trustor accept? If we want to model this important aspect of trust, we need to model risks. The trust model in 5G-ENSURE should therefore capture the potential risks identified by 5G-ENSURE, including any risks to 5G system components, applications or stakeholders.

One risk often found in remote interactions in IT systems is the risk that someone or something is not who or what it claims to be. This is why RFC 4949 contains so many terms related to trust that are concerned with

the role of trust in establishing identity. Other potential risks include the system or network not achieving the expected level of performance, the trustor's data leaking to some unauthorised party, the input provided by some other entity not being valid or truthful, or another stakeholder of the system acting fraudulently. All these types of risk apply to 5G networks. One of the biggest areas of concern is that part of a 5G-based system might be hacked by a malicious party who then makes it act in a way it should not. Trust in an IT system always involves a measure of trust that system components can resist malicious attempts to compromise their integrity.

The second question is really a question about trustworthiness, i.e. how trustworthy is the entity that the trustor trusts? This should always be qualified as a question with respect to the trustor's expectations of that entity, which of course depends on which risks the trustor accepts. It is possible to produce objective and quantified responses to questions about trustworthiness, in terms of the probability that the trusted entity will fail to meet the trustor's expectations. One way to obtain this is by examining the past performance of the trusted entity – if it met an expectation 90% of the time, then one could claim that its trustworthiness in that respect is 90%. If the trustor doesn't have a lot of experience of interacting with the trusted entity, then they won't be able to formulate such a measure of trustworthiness. This is why trustworthiness is often measured by using reputation systems which aggregate the experience of many trustors. Of course, the trustor then has to decide whether to trust the reputation system. Also, one ought to consider the possibility that the trusted entity's aim is to accumulate a good reputation and wait for the chance to perform that one malicious act, which makes the wait worthwhile. Components in 5G networks inherited from 4G networks will inherently be more trusted than new 5G components which have no "past performance" to be judged upon.

The last question, concerning how much trust a trustor has in someone or something is very difficult to answer. At one level, one can argue that the trustor either trusts an entity or they do not, and if they trust the entity they will accept risks that the entity fails to meet their expectations. At this level one could say trust can be measured by observing the trustor's behaviour. Their trust level will either be 100% or 0% with respect to each risk, depending on whether or not their behaviour indicates they accepted that risk (i.e. the lawyer's definition). This overlooks the fact that trust is a belief, and the strength of the trustor's belief in the trusted entity may be as important as whether they acted on that belief. Unfortunately there is no easy way to measure the strength of an individual's subjective belief. However, it is possible to estimate the strength of belief in a collection of equivalent potential trustors, by examining what proportion of them accept a risk. If 70% do trust an entity, one might argue that in the population of potential trustors, the level of belief in that entity is 70%. This type of approach is often used in trust surveys, which seek to estimate trust levels by asking a group of respondents how they would act in certain situations given certain knowledge. If one is mainly interested in balancing the level of user trust against the trustworthiness of the system they use, this is a useful measure of trust because it allows one to determine how many users will take the risk, and hence how many will reap the benefits of using the system and also (given its trustworthiness level) how many will be harmed.

3 State of the Art in Trust Modelling

3.1 Human Trust

3.1.1 Human to human trust

Our definition of trust, as described above, draws on the most universally accepted understanding of the concept, which has its origins in the notion of trust as it pertains to human-to-human relationships. These notions were subsequently incorporated into conceptualisations of trust between humans and technology-based systems. It therefore makes sense to consider first the findings from previous research regarding the level of trust humans have in IT systems and in other humans or organisations, and the factors that influence this.

Researchers investigating trust from this human perspective have defined trust in many different ways in the literature. Although often conflated with trustworthiness [Cheshire 2011], [Colquitt 2007], which is (in the context of human relationships) a perceived characteristic of the person or thing to be trusted, there is some consensus surrounding the core themes used by researchers to define trust [Lewicki 2006]. The key elements of trust include the trustor having confident expectations about the trustee, and a willingness in the trustor to risk making themselves vulnerable to the actions of others, based on an expectation of a positive outcome [Mayer 1995].

Mayer et al. identify several distinct aspects to the formation of trust by one human in another:

- **ability**: the domain-specific set of skills that enable another to be capable of achieving something as desired by the trustor;
- **benevolence**: the willingness of another to look beyond their own self-interest and genuinely seek the good of the trustor;
- **integrity**: the perception that another meets the criteria which the trustor finds acceptable;
- **risk taking**: that the trustor accepts a risk that adverse consequences may ensue if their trust is misplaced;
- **trust propensity**: the characteristics of the trustor that influence their willingness to trust;
- **context**: though not explicitly highlighted in the model, this includes the dynamically changing perception of the political, social and economic climate and organisational influences, e.g. coming from the trustor's employer; and
- **outcomes**: the result of a trusting behaviour which will cause the trustor to re-evaluate whether trust is warranted in future interactions.

In subsequent research [Schoorman 2007], Mayer acknowledged that this model avoided or neglected several important issues including relationships (e.g. between trusted and untrusted entities), cross-cultural similarities or differences which may reinforce or weaken the propensity to trust another, the effect of reciprocal behaviour (e.g. if my doctor can't recall my name, I may trust them less), and violation and repair effects whereby if trust is breached, whether the trustee apologises and seeks to remedy the situation may effect subsequent trust.

Trust, from the psychological or mental perspective, is also subjective. [Lee 2004] in a review of human trust decisions (actually about technology) define trust as the attitude that an agent will help achieve an individual's goals in a situation characterized by uncertainty and vulnerability. This encompasses the notion of risk taking which forms part of Mayer's model, and the notion that trust is based on an attitude, which is

not based on objective facts. Some argue that trust (or distrust) can only emerge when there are not enough objective facts on which to make fully rational decisions. However, trust can be informed by objective facts such as the qualifications of the trustee (which provide an objective measure of their ability).

Another factor that is relevant is the importance of the decision, i.e. whether there is something important at stake. If it doesn't matter much what the outcome is, i.e. whether the agent proves trustworthy or not, then it could be argued that the required level of trust is low. This should always be seen from the perspective of the trustor. If a stranger asks you to borrow your mobile phone for a period of time, giving the phone to him or her requires a high level of trust that they will not prove to be untrustworthy and fail to return it. Of course, a wealthy person may feel losing a phone is not a big deal, and for them lending their phone to a stranger may require a lower level of trust. The importance of a trust decision is subjective, depending on the attitude of the trustor as well as the potential favourable or unfavourable outcomes from the trustor's perspective. One can certainly argue that higher trust levels are needed when the trustor feels there is more at stake. However, it is also clear that a trustor may be more likely to trust another when there is less at stake. This is a significant point – which interpretation is most useful in the context of 5G-ENSURE? This point will be discussed in Section 6.

[Gambetta 1998] also refers to this combination of risk and subjectivity, based on the definition that “... trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever be able to monitor it) and in a context in which it affects [our] own action.” The term “subjective probability” refers to subjective evaluation by the trustor. Gambetta discusses the fact that even apparently objective facts can only be perceived subjectively when a trust decision is made, and highlights possible reasons why these facts may be open to question by the trustor, e.g. if the trustor and trustee have conflicting interests that may lead to misrepresentation or misinterpretation of their respective qualities. Note also that Gambetta explicitly links trust to the anticipation of some future situation. Trustworthiness will be shown in the future, when events future will have important consequences to the trustor. Until then, the trustor is limited to subjective judgements based on trust.

[Capra 2004] referring to Gambetta also notes that trust is also asymmetric, meaning that two agents need not have similar trust in each other. This refers to the situation when trust-related matters are considered to take place among two people or groups of people. This is partly due to the fact that trust is subjective, so even if the objective facts are symmetric (i.e. both sides are equally trustworthy), subjective perceptions and trust decisions may still differ on each side. Of course, trust may also be asymmetric because the two sides have different characteristics, which may remain evident to each side despite the subjectivity of their mutual assessments. Finally, trust is dynamic as it tends to be reduced if entities are misbehaving or, vice-versa, increased if agents are doing well. Experiences affect trust so that in that sense, trust is not blind.

To sum up, human trust can be described as

- **subjective** as it depends on individual goals and preferences or attitude, that is, is based on something deeply personal;
- **based on evaluation** which involves the awareness of uncertainty of that evaluation;
- related to the **importance** of the potential outcomes for the trustor;
- **oriented towards future**: the future will show the consequences of (justified or misplaced) trust;
- **asymmetric** as it does not have to be mutual;

- **context dependent** so that it is hard to foresee when trust takes place in the future in different situations; and
- **dynamic** in the sense that trust can transfer into distrust or vice versa depending on how the anticipated situation is in accordance with the actual situation.

3.1.2 Trust in technology

Although Mayer et al.'s definition is based around trust between pairs of individuals, it has since been used successfully in other settings including trust within teams, organisations and (importantly here) to trust in technology [Lewicki 2006], [Li 2008]. Despite this, some question whether the characteristics of human trusting beliefs can be applied to trust in technology have been presented [Sollner 2012]. Sollner et al. argue that since technology has no volition (i.e. no choice or will as to whether to behave in particular ways), it cannot be considered as a subject of trust. However, [McKnight 2011] argue that (as in trust between humans), trust in technology exists under contextual conditions involving risk, uncertainty and lack of total user control. Even though technology lacks moral agency (i.e. it doesn't choose whether or not to meet the trustor's expectations), the concept of trust in technology is still relevant. For example, a car has no free will, yet we trust (or don't) that it will work when we want to use it, i.e. that it will start, move and (perhaps most importantly) stop when we issue the appropriate commands. Therefore, trust in technology reflects a trustor's belief in the technology's characteristics that it will function as expected, whilst at the same time accepting vulnerability to system failures even if the trustor considers such failures to be unlikely. This line of reasoning has been used by many researchers to construct definitions of trust in technology to suit their purpose. For example, [Xin 2012] define trust in IT as people's beliefs regarding the trustworthiness of particular IT to perform a task.

Theoretical frameworks of trust in technology have also evolved from models of trust between humans [Li 2008]. The same arguments have surrounded these developments, with some researchers arguing that IT systems can be perceived as social actors mirroring characteristics similar to humans. Such findings have been used by some to argue that models of human-to-human trust and the factors believed to underpin the decision to trust can be applied to explain people's trust in technology [Li 2008], [McKnight 2001]. However, others have warned that trust in technology has a different character. For example, [Dijkstra 1999] found that in some situations people expect computerised systems to be more objective and rational than a human, and are more inclined to trust them than human advisors. In some situations technology can be trusted too much so that even malfunctioning is not perceived as something detrimental [Parasuraman 2007], so that if trust in technology is relatively high, occasional failures do not remarkably reduce trust on it unless the failures are sustained. However, trust in technology may also be more fragile than human-to-human trust [Madhavan 2007]. In some cases it seems this is due to the fact that when users have high expectations that a technology will not fail, they are inclined to overreact when it does fail, leading to a drastic reduction in trust [Dzindolet 2002]. This also works the other way round; technology may also be distrusted so much that every time the technology does not work this conviction is strengthened, irrespective of the reason of the failure (such as inability to use technology or some other reason, not necessarily originating from the technology itself).

One other interesting finding is that where technology plays a role in mediating interactions between humans, trust between humans and trust in technology become coupled in complex ways. For example, if a patient trusts their doctor, and the doctor acts in a way that suggests the technology is not a positive factor in their relationship, the patient may lose trust in the technology [Hooper 2015]. This suggests that to fully capture trust in technology, one should avoid the common practice of considering human actors to be

external to the system. They should be treated as part of the system in which they may or may not trust. This is also a feature of the OPTET approach to trust modelling (see Section 3.3.3).

Technology is routinely used to automate tasks that might otherwise be carried out by humans. In an early analysis [Parasuraman 1997], Parasuraman and Riley noted that humans typically use automation to reduce their workload, and this motive interacts with (subjective) assessments of risk and trustworthiness and leads to different ways of using technology:

- Use: simply the normal, expected way to use technology;
- Misuse: overreliance on automation, trusting it to possess higher qualities than are actually present, which may lead to using technology when it should not be used;
- Disuse: rejection of the technology when its use is appropriate, leading to failures from underutilisation.

Parasuraman and Riley also define the concept of ‘Abuse’ which results if designers or other professionals use technology to automate functions without due regards for the consequences of automation for human performance, and especially without allowing humans the possibility to act according to their responsibilities and capabilities. This happens if the technology constrains the actions that humans can take, or if it prevents humans monitoring a situation for which they are responsible. These lead humans to distrust the automation, especially if they are compelled to use the technology and cannot resort to other solutions. Conversely, if technology is well suited to the task, humans perceive its value and are inclined to trust it [Sollner 2012]. In fact, Sollner et al. identified three main contributors to human decisions to trust in technology:

- Performance: does the technology help the human achieve their goal, producing accurate and reliable results while reducing the mental workload of the user?
- Process: does the technology behave in ways the user understands or at least finds authentic, including providing security features that the user expects it to have?
- Purpose: does the technology do what it is supposed to do, i.e. are the designers and operators benevolent and providing technology in order to help the users?

These ideas are consistent with the earlier work by Parasuraman and Riley showing that human trust in technology is highly subjective, and related to the level of user understanding of the technology as well as what it does. In some sense this reflects the obvious fact that if the ‘trustee’ is a piece of technology, then the trustor is likely to be concerned about its creation and operation as well as its actions, while often having relatively little understanding of how it works.

3.1.3 Human trust and 5G

In some sense, the main goal of 5G-ENSURE with respect to human trust is to address these key points:

- helping 5G system/application designers and operators avoid what Parasuraman and Riley call ‘Abuse’;
- helping 5G system/application users to avoid errors of ‘Misuse’ or ‘Disuse’, by making potential risks and countermeasures more evident;
- providing a basis for stakeholders to communicate their trustworthiness and cement their trust in each other, mediated by their technology.

In the context of 5G technology, there are some specific points that need to be considered. Network technologies are usually not perceivable directly but are perceived via some technical device such as tablet or mobile phone. Being more extensive than the current 4G technology, the 5G technology based network may affect humans in situations and locations the network has not done before. However, the effect is always mediated by the usage of the device and can also be mixed with the trust on the device. This is highly relevant. Some functionalities or services can be more usable in, say, tablet format, and will correspondingly evoke trust only when used via the tablet. Furthermore, the qualities of the device can be mixed with the qualities of the network. In some cases it can be beneficial to 5G from the eminence perspective, as drawbacks such as poor performance can be seen as qualities of the device and the advantages provided by the device can be appraised to be due to 5G. The same applies, of course, also in opposite situations when 5G is blamed due to misunderstanding the situation. As the network and the device produce the effect of using the network together to the user or actor, the point where the effect of 5G starts and the one produced by the device ends is very hard to make.

People are differently aware and knowledgeable about technology. Some issues may be misperceived so that the related problems do not affect trust. The opposite is also possible; some features can be misinterpreted or used in a faulty way, resulting in loss of trust. As a whole, most network users are not professionals so that misunderstandings are probably quite general. Many network related matters are also not visible (perceivable). If you do not have the ability to track in any way whether you are monitored through a network, how can it affect you? The only possibility way it can affect, then, is the knowledge of such a possibility and the attitude towards such a thing. That is why it is important to understand people's attitude towards various things, even if they are not visible, and to prepare to deliver information also about such "invisible" matters and about how negative consequences and the like can be avoided.

Considering trust is subjective, it is important to deliver clear and appropriate information about 5G to enable as realistic trust as possible. Only this way can humans make appropriate trust decisions about the use of 5G technology and features. 5G networks are likely to support safety critical applications, and generate huge amounts of personal data, so the stakes are very high indeed. If trust is lacking the resulting 'disuse' of the technology may lead to serious consequences for individuals, yet too much trust could be equally damaging. Trust is context dependent, subjective and dynamic which means it can be hard to evaluate how much some technical solution will be trusted upon.

3.2 Machine Trust

3.2.1 Trust decisions

In the above discussion, the main concern was whether humans trust other entities (including technological constructs), and whether they do so in an appropriate fashion. Here we consider the orthogonal question of whether a technological construct should trust other entities.

A technological construct (i.e. a machine) can only operate according to a set of instructions that determine and constrain its behaviour. A machine trusts another entity when it follows instructions whose outcome depends on that entity's behaviour. Strictly speaking, the author of the instructions is the one trusting the other entity to behave itself. Machine trust relates to the situation where the author of the instructions recognises the possibility that other entities might not be trustworthy, and includes instructions on how the machine should assess that and alter its behaviour if appropriate.

Machine trust therefore involves a computational procedure to calculate trust in (or strictly speaking, trustworthiness of) other entities, and thus decide what trust assumptions should determine the machine's behaviour. These computational trust (or trustworthiness) models are widely used by various types of automata, and also to provide decision support for human trust decisions, e.g. in reputation systems. Here we will focus on machine trust models used in Wireless communication systems. We categorize them in three: Wireless Sensor Networks, Cognitive Radio Networks, and Mobile Ad Hoc Networks.

3.2.2 Trust models in Wireless Communication Networks

We will follow the following nomenclature, as provided in the survey from [Yu 2010]: The trustor is the entity that trusts another entity, and the subject (or trustee) is the entity to be trusted (both consistent with Section 2 above). A witness is an intermediary entity that interacts with the subject and informs the trustor. Those concepts are depicted in Figure 1.

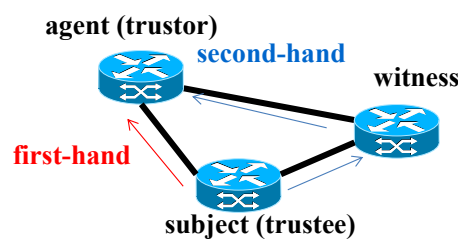


Figure 1. First-hand and second-hand evidence to evaluate trustworthiness

Trust is defined in wireless communication networks in [Yu 2010] as “the expectation by a trustor node about the outcomes of the actions of a subject node based on past experiences. These past experiences may come directly measured from the subject node or they may come given through witness nodes (intermediate nodes)”. In our terms, this is of course a measure of the subject node's trustworthiness, and is used to determine whether the trustor should indeed trust the subject. As discussed above, this assessment may be made in advance by the operator of the trustor node (by configuring the trustor node to always trust the subject node), or left to an algorithm by which the trustor node can make the decision by also using information from the subject and possibly second-hand witnesses. This is the situation we are concerned with here.

Trustworthiness evaluation depends on first-hand evidence containing the experience that a trustor has after having interacted with a subject node. However, when the first-hand information is not available or there is not enough information to evaluate trustworthiness accurately, second-hand information is the only alternative. Second-hand evidence is provided by a given witness node which does have direct interaction with the subject node, the witness is then the only intermediary between the user and the trustor to report evidences.

We analyse the three main categories of wireless communication networks covered in the survey by [Yu 2010], and we discuss their particularities concerning trust(worthiness) and the concrete motivations for establishing trust models.

Wireless Sensor Networks: These types of networks, often abbreviated as WSN or WSN, are distributed networks conceived to monitor physical conditions such as patients' health, or environmental conditions such as temperature or weather [Akyildiz 2001]. Those networks are composed of nodes and sensors, where the sensors capture the environment information and forward it across the nodes towards a special node called gateway, which connects to the remote station extracting the monitored information. Those networks

are fully decentralized so the forwarding decisions may be made based on different criteria but there is no entity dictating the forwarding paths. These types of networks are collaborative because all the network nodes co-operate with each other in order to monitor events and forward this information by reducing cost and consumption.

In this context, trustworthiness estimation is necessary because these network nodes are hardware-constrained so those become easily compromised. A TRM (Trust and Reputation Management System) has the crucial role in this context to determine the credibility of the network nodes for monitoring a given event.

Cognitive Radio Networks: These types of networks, often abbreviated as CRN or CR, are intelligent radio networks that can be programmed and configured dynamically. As defined by FCC in [FCC 2016], CR is “a radio that can change its transmitter parameters based on interaction with the environment in which it operates”.

In these types of networks, the spectrum is managed dynamically by harnessing the available spectrum channels not in used by the primary users and profited by the secondary users to transmit information. Primary users are those who have higher priority to use a given spectrum band while secondary users have lower priority, in such a way that they are not permitted to interfere with primary users. Spectrum sensing is the functional task to sense the unused spectrum bands in a given geographical area and share it, but without interfering with primary users when using this available spectrum. These types of networks are collaborative because the secondary users have to cooperate with each other in order to detect and share the information on the available unused spectrum channels.

In this context, trustworthiness estimation is necessary because the secondary users can be easily compromised, this means in this context that a given node can be controlled to share fraudulent information about a free channel and make the rest of the network utilize this channel when it is not free and so interfere with the primary users.

These types of networks are centralized so there is an entity, which intermediates between any pair of nodes. In this context, first-hand evidence is not an alternative because a given trustor cannot direct interact with the subject node, but only with the central entity.

Mobile Ad Hoc Networks (MANETs): These types of networks, often abbreviated as MANETs (Mobile Ad hoc NETwork), are distributed and self-configurable networks [Taneja 2010].

In this context, nodes cooperate with each other in order to increase throughput. If a node is not the destination of a given packet, it can act as a relay, accepting the packet and forwarding it to neighbouring nodes until it reaches its destination. This is a very similar case to WSN because nodes cooperate with the same purpose. However, and similarly to WSN, nodes are also easily compromised so the forwarding decisions taken by the nodes have to be based on trust, guided by trustworthiness estimation mechanisms.

In these types of networks, like in WSN, a trust model can rely on both first-hand evidence and second-hand evidence because a given trustor can communicate with all the reachable nodes whether directly or through witnesses.

3.2.3 Computational Trust models

As discussed in [Yu 2010], computational models are less complex and easier to implement as algorithms than socio-cognitive models. A trust model is based on two levels of trust:

- individual-level trust: which refers to the trust among nodes;
- system-level trust: which refers to the trust inside the system as a whole, and thus is based on individual-level trust.

A trust model is a first step to help prevent the situation where any kind of misbehaviour on nodes could affect the overall performance of the network. Indeed, the trust model is to help decide where it is necessary to put in security mitigation actions, namely where there is a lack of trustworthiness. Strictly speaking, therefore, the model estimates the trustworthiness of other nodes, providing information about how much trust in them is warranted.

There are two types of misbehaviour, on the one hand, selfishness, where the nodes maximize their gain at the expense of other nodes, and on the other hand, maliciousness, where nodes act to degrade the system or certain nodes with no explicit intention to maximize their gains.

It is worth noting that in practice the computational trust is often based on authenticated identities. In other words, once the entity is authenticated, there is basis for allowing it to perform additional actions or interaction. If a trustor knows that a certain identity is trustworthy enough to perform these actions, then the trustor could be said to be having a direct trust relationship with this entity. If on the other hand, trustor trusts a third party to be able to vouch for other identities, the indirect relationship is formed. As described above, this is an example of second-hand trust. PKI is a well-known example of this, relating to trust in the identity or other assertions based on affirmation from a third party.

A third kind of relationship can be formed through opportunistic trust. Here, there is basically no trust in the entity at the beginning of the interaction aside from trust that the entity remains the same. Thus, it is meaningful to assign reputation score for such an entity. Sometimes this kind of opportunistic approach is also called “resurrecting duckling” security policy model [Stajano 1999]. SSH is an example of a tool, which is often used in an opportunistic fashion and the basic tenet is that you have a cryptographic identifier of which you can claim and prove ownership.

3.2.3.1 Individual-level trust

The goal of an individual-level trust model is to estimate the likelihood of a successful interaction among nodes before is actually established. Strictly speaking, the model provides an estimate of how trustworthy the interacting nodes will be. In this way, ideally, a node can decide whether or not it engages in a given communication with another node. It is free to choose another node, which is the typical case in MANETs or mesh grid networks, where the forwarding is completely distributed, contrariwise to SDN, where the forwarding is dictated from an external entity called the SDN controller, and the switches cannot choose which nodes to send the information.

Figure 2 shows the different phases to evaluate the trustworthiness of a given network node, which are detailed hereafter. These phases are: bootstrapping, evidence space, trust space, interaction decision making, and interaction outcome evaluation.

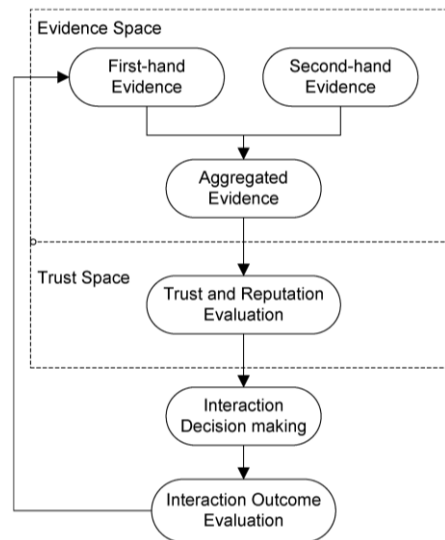


Figure 2. Interaction decision making process procedure in individual-level trust

Bootstrapping phase: This is the phase where the reputation value of a node is calculated. In this phase, the trustor node initializes by setting weight on the information received by the subject. This weight is the reputation value given by the trustor node and it can be adjusted depending on how trustable demonstrate the subject to be. For instance, if a given node turns to be less trustable, its reputation value can be reduced in order to be less influential than their counterparties with respect to making a given forwarding decision. When a new node appears in the network, the trustor can give him a low, neutral or a high reputation value which will have more or less influence when other nodes make decisions.

However, depending on the frequency of interactions between the trustor and the nodes, these weights cannot be reliably calculated.

In the event of few interactions, there is the need to introduce artificial traffic which may lead to an overhead. Indeed, this traffic should be undistinguishable from real traffic to avoid ON-OFF attacks, where the node can behave very well at the beginning to raise its reputation based on this artificial traffic and then behaves very badly with the real traffic which causes a decrease in the performance because the node has influenced the decisions of other nodes. If artificial traffic has the same format as the real one, the node cannot change its behaviour in this manner.

In the event of high interactions, at the beginning the trustor node will give the subject nodes the same weight to take into account them equally, but it will gradually discount data from less trustworthy nodes as their reputation value decreases.

Evidence space: This phase is about representing the past experiences of a trustor with a given subject node. As said before a trustor node can monitor direct information directly from the subject (first-hand) or indirect information directly from a witness node (second-hand). In wireless communication systems, most authors classify the interactions with the subject node with a pair $\langle p, n \rangle$, where p means a positive outcome and n means a negative outcome. How those values p and n are defined depends on the context.

However, one limitation is that a given trustor only takes into account individual interaction outcomes, but it does not consider the entire history of the interactions mainly due to memory constraints (let's recall here that we are considering wireless communication networks where nodes are hardware-constrained). One

intermediate solution is to consider a reasonable time window. However, even considering a time window, all the interactions should not count the same in order to detect behaviour changes on the nodes. One solution for this is to separate the last reputation values from the historical reputation values. This is necessary because a given subject node can change its behaviour such as in an ON-OFF attack. Against this type of attack, computing the reputation value by considering all the interactions with the same weight is not the best approach. This is why in this survey the authors advocate for two different weights as seen in the following equation:

$$R_{Updated} = \rho_1 R_{Historical} + \rho_2 R_{Latest}$$

Indeed, one possible approach to counter ON-OFF attack is to compute the reputation in such a way that is hard to earn but easily to lose. This means to make the weight change dynamically as it an adaptive mechanism that can continuously compute the reputation values and update them with in accordance with behaviour changes on the nodes. For instance, if the latest interaction is negative (n), we set $\rho_1 \ll \rho_2$ in order to give priority to the latest behaviour, if on the contrary, the latest interaction is positive (p), the reputation value gradually increases.

When it comes to considering second-hand evidence, several issues arise. First of all, the evidence may contain false values. When those false values cause trustworthiness to reduce it is called “badmouthing”, and when those false values make trustworthiness increase is called “ballot stuffing”. To this day, no Trust and Reputation mechanism can tackle both ballot stuffing and badmouthing simultaneously without assuming some pattern on the behaviour of the nodes.

Normally, the reputation of the witness node is not considered in the calculation of the reputation value. In this way is taken for granted that the witness information is reliable (Figure 3 in green), so its reputation is maximal. But the reputation of the witness (Figure 3 in red) can be also included in the reputation calculation of the subject to solve ballot stuffing. One way estimate the witness reputation is by means of a deviation test that calculates the deviation between the witness node evidence and the trustor evidence. If this difference is higher than a given threshold, the trustor can consider that evidence of the witness as inaccurate and filter it out. Another option is to assign a lower value of reputation to that node due to this deviation and punish that node.

Another way to circumvent this issue is to deploy trusted trustors on the network to act as witnesses and extract their evidence instead of using any node for this purpose.

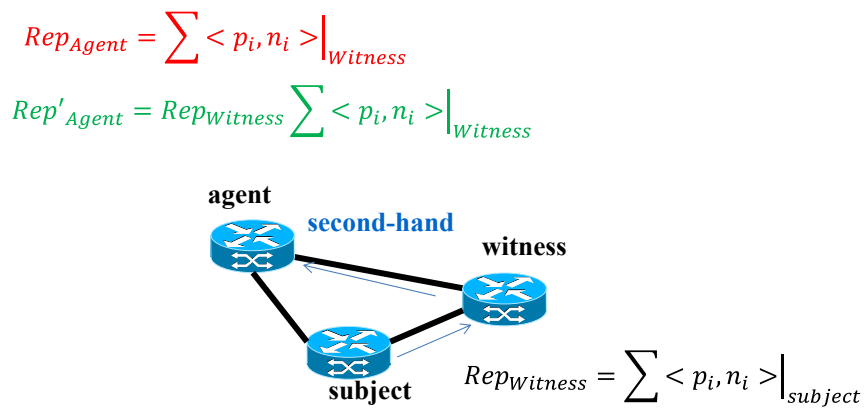


Figure 3. Inclusion of witness reputation in the reputation of subject node

Trust space: This phase is about mapping the aforementioned evidence space $\langle p, n \rangle$ to the trust space, which contains the trustworthiness values of the nodes. This trustworthiness value T is calculated based on the observation values from the evidence space as $\tau = \frac{p+1}{p+n+2}$. This value is normalized, in the typical intervals of $[0,1]$ or $[-1, 1]$.

However, the behaviour of a given node is highly dynamic and this trustworthiness computation does not model the subsequent uncertainty in the evidence space.

Interaction decision making: This phase is where the trust space is used as a basis for deciding the node to interact with. The reputation of a given node can be used in many ways, for instance, a given node can choose the most renowned node to interact with it, or it can discard those less renowned nodes, or it can consider a weighted aggregation coming from several nodes resulting in a pseudo-democratic decision. The methods that make decisions based on trust or reputation models are called trust-aware decision making methods.

There are three types of methods: threshold-based, ranking-based, and weight-based methods.

- Threshold-based: filters out the reported information from untrustworthy nodes.
- Ranking-based: ranks nodes according to their trustworthiness values.
- Weight-based: weights the decisions according to all nodes but considering their reputation values.

The weight-based decision methods are more typical in centralized infrastructures, where one node is the central entity. For instance, in SDN infrastructures, the SDN controller can take evidence from the SDN resources and make the trust-aware forwarding decisions based on the trustworthiness of those SDN resources.

Interaction outcome evaluation and update: Finally, once the node has interacted with a chosen node, the outcome of this interaction is evaluated as positive or negative and the reputation value associated to that chose node is updated to take it into account in the next decision. It can be seen that this step is a feedback to the first phase bootstrapping.

3.2.3.2 *System-level trust*

System-level trust relies on the individual-level trust mechanisms deployed on the network nodes to spread and disseminate the reputation values of each network node to the rest of the nodes. Based on these reputation values, the system-level trust can enact punishment or reward policies on those nodes. Indeed, trust is seen as a social value that is propagated through the network nodes to make better decisions. A system-level trust is a mechanism that disseminates trust among the network nodes and enforces punishment and reward policies in order to ensure the cooperation among nodes. Figure 4 shows a high level description of a system-level trust model, where its basic pillars are the dissemination of trust module and the rewarding and punishment module. The trust and reputation values are given by the trustors that calculate those values as explained in the previous section.

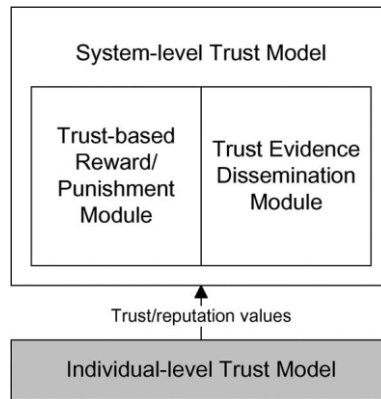


Figure 4. Components of a system-level trust and its relationship with individual-level trust

3.2.4 Trust models in Virtual networks

[Wen 2010] provides a way to estimate trust of a given end-user on the different virtual networks supporting several services. In order to answer to this question, the authors conceived a trust model M2Ut, where the user U trusts a given virtual network (VN) to provide with services S . This trust computation is based on a Bayesian Networks algorithm that propagates trust in a given dependency graph. Figure 5 shows the probabilistic dependency graph of a given VN providing a set of services S .

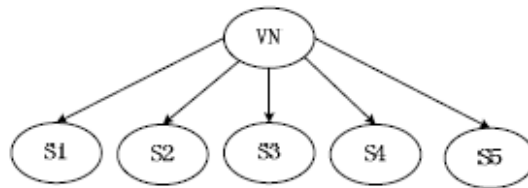


Figure 5. Bayesian Network of a given Virtual network supporting 5 services

A given VN can provide with different services, each of them with a given SLA (Service Level Agreement). An end user has to decide which VN is going to use to access to its requested service. The trust model is used here to evaluate and update the trust between the end users and the VNs.

As far as the computation of the trust model is concerned, there is an entity called TME (Trust Model Engine), which is a trusted and objective entity for computing the trust model. Owing to the high number of VNs in the infrastructure, the authors choose a distributed architecture to build the trust model per domain, where there is a single TME per domain. In each domain, the TME evaluates the trust value of the VNs based on the end users' (EU) ratings.

As shown before, an EU can decide which VN to use to access to a given service. It first queries the trust value assigned so far to that VN to make that decision. After having interacted with the chosen VN the EU can submit a new evaluation in order for the TME to update the trust model, as it was seen in the previous section. The authors consider five levels to evaluate the VN: mediocre, bad, average, good and excellent, but do not detail what those levels depend on.

3.2.5 Machine trust and 5G

In the 5G-ENSURE project, machine trust models will be needed to support trust decisions over the selection of physical and virtualised assets and provisioning of (virtualised) 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.

3.3 Trust and Trustworthiness by Design Models

3.3.1 General features and 5G

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, as discussed in Section 2, 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).

In the context of the 5G-ENSURE project, these types of models can serve several purposes:

- as a means to analyse the 5G-ENSURE security architecture, to determine what risks and trusted dependencies are present (bearing in mind that no system is totally risk free);
- to 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;
- as a framework to 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

Related to the first of these, such models could also be used to provide a tangible measure of the effect of 5G-ENSURE 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 the Technical Roadmap produced by WP3.

3.3.2 Zero Trust Model

The zero-trust architecture approach, which was originally developed for data centres, differs from the perimeter-centric security strategies in that there is no default trust for any entity. Users, devices or applications, also when they reside inside the same network, cannot trust each other unless they are verified by a secure method [Kindervag 2010]. Such architecture may provide ubiquitous security. This is a good example of a trustworthiness by design model, in which the risk (that perimeter security cannot exclude untrustworthy or malicious users or devices) is reduced by using an appropriate control strategy.

While there are security controls on the network boundaries, the security strategy of 4G systems assumes trust inside an operator's network. Since SDN and NFV emerged, this basic trust assumption has become somewhat questionable. The zero-trust approach is a rather extreme but still potential approach to solve this problem. One way to implement zero-trust is segmenting, or micro-segmenting the network to isolated sections where all users, applications and network functions may have limited, specific access rights. The access rights and the security policies can be dynamically changed to reflect any abrupt changes in the environment. Segmenting effectively prevents lateral spread of threats inside a data centre or a SDN. When compared to VPNs or VLANs, segmenting enables control of privileged information and limited threat inspections. However, as the 5G systems are expected to reach end-to-end latencies of less than 10 ms or even as low as 1 ms [NGMN 2015], [5GForum 2015] among several other very strict service requirements, computing resources may not suffice to support zero trust approach simultaneously.

3.3.3 System trustworthiness modelling

The other approach that is relevant to 5G-ENSURE involves creating a model of the system, which can then be analysed to detect potential threats and identify potential countermeasures. The analyst using such a model is then able to improve trustworthiness (by specifying countermeasures to reduce risks), or at least highlight where users or system components may need to trust other parts of the system. This approach is especially useful if the models can capture risks (and trust) in relation to system components involved in threats, and thus provide insights on how the system architecture and design lead to those specific risks being present.

Many methods have been developed to try to identify and analyse threats in ICT-based systems. [Shostack 2014] breaks the threat modelling process down into four stages: system modelling, threat identification, threat addressing, and validation. Threat identification is usually the most difficult step, for which a range of methodologies have been devised. Three broad classes are normally used:

- Asset centric methods: are based on analysing the system to identify assets that contribute to its success, then identifying ways those assets (or their contribution) may be compromised.
- Attacker centric methods: are based on understanding who might attack the system and what means they might be able to use, and then identifying where the system may be vulnerable to those attacks.
- Software centric methods: are based on finding potential vulnerabilities in the software assets in the system, with a view to guiding implementers to avoid introducing them.

Software centric methods are most amenable to automated analysis. For example, Microsoft's Secure Development Lifecycle (SDL) framework [Howard 2009] can be supported by STRIDE [Swiderski 2004] which is a secure software design tool designed to help developers identify and address threats from spoofing, tempering, repudiation, denial of service, information disclosure, and elevation of privilege. The main problem with automated software centric methods is that the vulnerability databases they use are often quite specific, e.g. based on specific known vulnerabilities in specific operating systems, platforms or application software. Ultimately, the goal is to help programmers avoid making errors, and today the most common approach is still based on raising awareness and providing checklists such as the OWASP Top 10 [OWASP 2013] which are used for manual analysis by software developers or in tools like STRIDE or [ThreatModeller 2016] which helps developers identify attack paths based on a library of possible threats. Finally, software centric methods are limited to finding and addressing software vulnerabilities (i.e. programming errors) or their potential consequences. They cannot easily identify or address threats involving

human factors such as social engineering or user error, or threats from inappropriate use of (correctly implemented) system functions.

Attacker centric methods are, not surprisingly, much better at identifying threats from or involving humans. However, these approaches are much more difficult to automate, as they depend on expert knowledge of likely attackers and attack methods. It may also be difficult to decide how various attacks relate to the system being analysed, and hence where security measures could be introduced to counter specific threats. Some tools do exist such as SeaMonster [Meland 2008], and typically use attack trees to help analysts decide how potential system vulnerabilities (which may be software centric) could be used to attack the system. The commercial Nessus tool [Nessus] which can scan a network for potential threats from viruses, malware and hosts communicating with undesirable systems falls into this category as well as the MulVAL tool [Xinming 2006], a logic-based enterprise network security analyser which encodes the network topology and discovered vulnerabilities in Datalog statements to compute and reasons over an attack tree. Both Nessus and MulVAL are used by the PuSAR enabler developed in 5G-ENSURE.

Asset centric methods are the ‘gold standard’ for risk analysis purposes, because they make no assumptions about the nature of the threats that may need to be addressed. These methods include the standardised approach from [ISO 27005], and (if not limited to information systems) [ISO 31010]. Their main drawback is that they depend on an analysis by a security expert with extensive knowledge of the types of threats that could potentially affect the system. Even if that expertise is available, the process (being manual) is usually carried out imperfectly, especially where threats relate to the purpose or function of the system, with which the security expert may be less than familiar. Finally, a manual analysis to identify threats and appropriate responses can take a long time, and is unsuited to agile development using DevOps methods on virtualised platforms [Drissi 2013].

However, in the last decade some efforts have been made to use machine understanding in an attempt to capture information about possible threats and relate this knowledge to the design of a system. [Hogganvik 2006] devised a graphical representation of security threats and risk scenarios, while the Secure Tropos language [Matulevi 2008] also supports modelling of security risks. [Blanco et al 2011] provided a useful review of the early approaches, and concluded that the Security Ontology from Secure Business Austria [Fenz 2009] was the most complete, providing an OWL ontology for modelling system assets, threats and controls based on the German IT Grundschutz specification [IT Grundschutz 2004]. However, this model provides a description rather than a classification of security concepts. It is good for describing security issues in a system, but less useful as a basis for machine reasoning, and as a result it doesn’t provide much assistance (except as a checklist) for threat identification and analysis. This gap was first addressed by one of the 5G-ENSURE partners in the FP7 SERSCIS project [Surridge 2013], which devised a model designed to support a machine inference procedure for identifying which classes of threats affect a given system. The core ontology is shown in Figure 6. Superficially it looks similar to the SBA ontology, but it is based entirely on OWL classes, and has a simpler structure so that fewer facts need be asserted before useful knowledge can be inferred. The ontology is used to support a machine reasoning procedure to decide which types of threats affect a system based on its composition in terms of asset types. Where a threat affects a pattern of interacting assets, a rule base can be used to determine whether the security mechanisms used to protect those assets are sufficient to block or mitigate the threat. In FP7 SERSCIS, the ontology was also used to construct a Bayesian belief graph describing the effect of threats on the behaviour of system assets, which was used to diagnose which threat(s) might be the cause of any run-time misbehaviour.

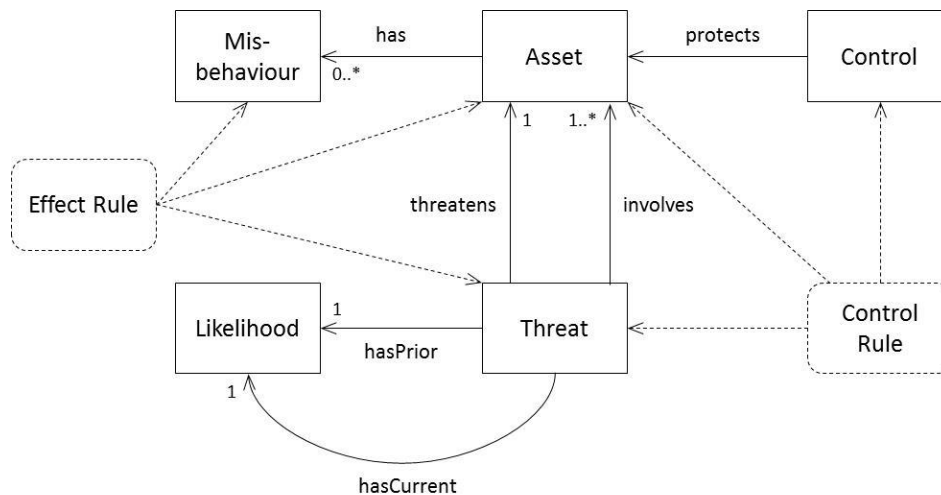


Figure 6. Security Classification Ontology

This approach to automated threat identification and analysis was used and extended by some of the 5G-ENSURE partners in the FP7 OPTET project. This used machine reasoning as part of a framework for managing trust and trustworthiness in advanced Internet-based applications [Gol Mohammadi 2014]. The focus in FP7 OPTET was on ‘trustworthiness by design’, and the ontology was used mainly to support design-time identification and analysis of potential risks [Chakravarthy 2015]. The FP7 OPTET approach includes two features that are highly relevant to 5G-ENSURE:

- the concept of ‘secondary threats’, describing how the disruption of one or more assets could lead to knock-on consequences for other assets; and
- the notion that stakeholders and technology assets form a socio-technical system, and a loss of trust among stakeholders poses a threat to the operation of this system.

Threats are used to describe the potential effect of disruption on stakeholder trust, e.g. if the system provides inaccurate data to a stakeholder, they may lose trust in the system. Such a threat is really a secondary threat, because it is caused by the disruption of technology assets (in this case the fact that data has become inaccurate). Other (primary) threats can be used to model the effect of this loss of trust, e.g. if a stakeholder loses trust in the system they may cease to take actions based on its data.

4 Trust in 4G Networks

There does not seem to exist an explicitly documented and complete trust model for the current (2G-4G) mobile networks, at least not in any of the available technical specifications of 3GPP. In fact, not even in the more academic/research oriented work of the USECA project [USECA 2016] (that ran more or less in parallel to 3G standardization) does trust stand out as a specifically treated subject. This does not mean that an understanding of the current trust model cannot be obtained. By looking at the available security mechanisms and how they have evolved over time (from 2G to 4G) it is quite straightforward to deduce the main components (actors, trust relations, etc.) of the trust model that has been assumed. In addition, in particular with the evolution of 4G, explicit statements about assumed trust can be found in many of the specifications. Though the lack of an explicit trust model is technically unsatisfactory, one has to note that the enormous success of the mobile ecosystem would not have been possible if assumptions about trust between the actors would have been wrong. However, it is also clear that time has caught up with some of

the basic trust assumptions, rendering them questionable today and certainly unsustainable in a future 5G setting.

4.1 Actors and Business Models

4.1.1 Overview

To understand the trust model we must first understand the actors (who trust and are trusted) and the business models (which cause them to interact). The primary actors in the 4G world are:

- Network equipment manufacturers.
- Mobile network operators (taking the role of “home” or “serving” operator). The MNO is commonly also the owner of the infrastructure and is the service provider.
- Interconnect network providers (linking one MNO to another).
- User equipment manufacturers, including USIM manufacturers.
- End users (subscribers).
- Regulators, law enforcement agencies.

Network operators are connected through interconnect providers (transit domains in the terms of TS 23.101 [3GPP 2015]) so that UEs can communicate with UEs connected to another network operator. The trust model on the signalling interconnect networks (mainly older systems using SS7 and MAP) have recently surfaced as a major concern showing how the original trust model between network operators has become questionable over time, something we will return to below. Network operators can take on the role as home operator through the user signing a contract (a subscription) with the network operator. The network operator can also be a serving operator when the subscriber is roaming into the network of a different network operator. One may note that national roaming is usually not possible: as long as the subscriber is in the same country as his/her home operator, only the home operator can provide a serving network. This is however more of a “business model” issue than a technical issue.

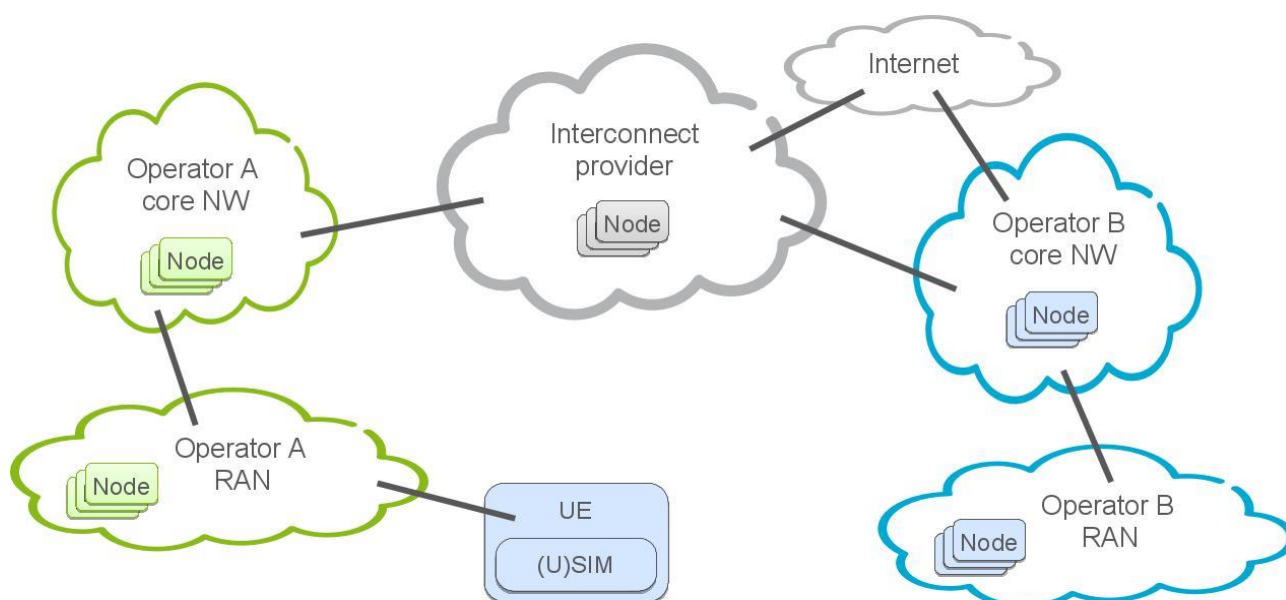


Figure 7: Main Actors in 4G

An additional type of actor are the equipment manufacturers. They produce mobile phones, smartcards (UICC) and network equipment. The network equipment consists of hardware and software elements.

Network hardware manufacturers also provide software for the network but there also exist pure software manufacturers which provide functionality for the network such as charging/billing capabilities. The situation is similar in the mobile phone area where hardware manufacturers exist who also provide software but there are also independent software manufacturers providing functionality for the mobile phone.

All of these actors enable a multitude of business models between users and operators. Considering only the main actors (see Figure 7) a user has a contract with a network operator which enables the user to use services like voice calls, text messages or data. The network operator has contracts with interconnect providers and with other network operators (roaming agreements). In the case of a virtual mobile network operator (VMNO) the network operator only runs the database with customers (HSS) itself and buys the network capacity in bulk from other network operators. Network operators may also have contracts with each other to share hardware, most typically radio base stations.

Taking the additional actors into account, there are also several business models between (network) equipment manufacturers and network operators. The network operator can buy equipment (hardware and/or software) from the manufacturer and run it in its network. Depending on the equipment, the network operator requests that the equipment adheres to standards such as the 3GPP specifications. The network operator can also have a contract with the equipment manufacturer to run the network on behalf of the network operator.

The user can buy a mobile phone from either the network operator having several financing options or from the phone manufacturer either directly or via some distributor. The user gets a smartcard for the phone from the network operator when signing a contract. The network operator itself buys the smartcards from a smartcard vendor, again an equipment manufacturer.

4.1.2 4G Satellite Business Models

Satellite communications are of course used in broadcast networks (e.g. DVB-S, DVB-RCS). The satellite network is used in the forward direction only to provide for instance radio and TV programs sometimes with a return link provided by classical PSTN or xDSL connections. Satellite systems can also be used to feed Content Delivery Networks (CDN) servers and caches thanks to multicasting. Here though we describe the two areas where satellite communications come into the 4G world.

4.1.2.1 *Satellite radio access network (S-RANs)*

Network concepts combining a satellite and a terrestrial component to provide anytime and anywhere connectivity from mobile devices (e.g. vehicular mounted or even handheld) have emerged in the last 10 years.

Satellite systems can be used as a collaborative extension of classical networks (e.g. GSM, GPRS, UMTS) in remote or isolated areas or provision connectivity to specific group of users (the military for instance). The satellite network is used in both forward and return directions to provide services directly to the terminals.

In case of environmental or natural disasters (e.g. Hurricane Katrina), classical access networks have broken down and S-RANs have provided communication access to rescue teams. In these scenarios, satellite systems are essential because disasters are unplanned and can impact large areas for many weeks.

The satellite access network can be reached using different types of satellite links:

- S/L bands (S-UMTS) providing voice and data.

- Ku/Ka bands (DVB-RCS) providing broadband with large capacity and high data rate (e.g. military or medical data).

In case of critical scenarios (e.g. military applications, nuclear power stations) S-RAN can also be used as a backup solution to ensure the lifeline communication services.

4.1.2.2 Satellite backhauling

Satellite systems can be used as a transparent backhauling link connecting several eNBs or even different networks. The satellite network is used in both directions to provide bulk connectivity to a terrestrial network element (e.g. to an eNB or to a local area network).

Satellite backhaul extends the ability to provide voice and data services where topography or distance restricts connection to mobile networks.

4.2 Trust

This section describes the trust model assumed by the security protocols and functions of the 4G network starting with a historical analysis. The trust model further covers the relationships between equipment manufacturers and other actors which mostly relates to how things are implemented (in contrast to what is implemented). The trust model is reverse engineered from the technical specifications of 3GPP.

4.2.1 Historical analysis

In current (2G-4G) networks the main actors are the (mobile) network operators, subscribers (i.e. users) with some User Equipment (UE) and interconnection providers (see Figure 7). At this level a formal domain model can be found in 3GPP TS 23.101 [3GPP 2015] which is reproduced below.

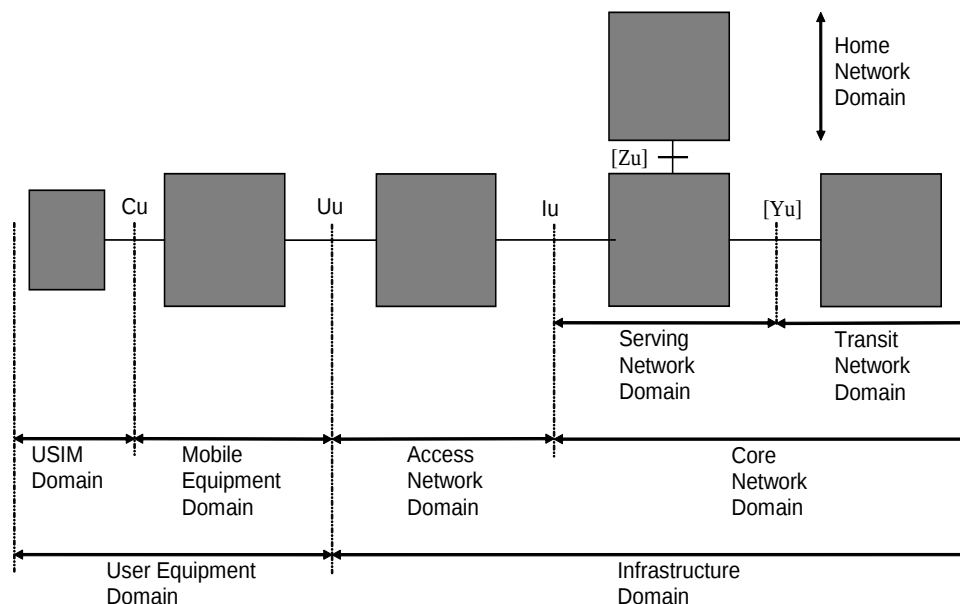


Figure 8. 3GPP TS 23.101 domain model.

The domains of TS 23.101 are therein defined as “highest level of physical grouping” and the partitioning of the network into domains is thus, as such, not trust driven. However, one can already note here that the fact that home, serving and transit domains are separated even though they technically contain similar functionality (and may reside in more or less the same geographical area), implies that the domain

boundaries are not purely physical but also related to business boundaries. This is a consequence of physical and business boundaries determining who has control over assets which is a major factor in trust issues.

Moreover, the presence of some of the domains is directly related to trust. First of all, the separation of the User Equipment domain into the USIM and Mobile Equipment domains is definitely driven by the assignment of critical functionality to the USIM (or more precisely the UICC). Since the USIM resides in a physical location where it can be subject to e.g. tampering it has become necessary to separate it from the rest of the Mobile Equipment (ME), simply because it would have been too costly to make the whole UE tamper resistant. Secondly, we can consider the access network domain. Originally, the separation of the access domain from the core network domain was motivated by the fact that it involves special type of equipment (radio base stations, etc) which have specific technical functionality that cannot be found anywhere else. In addition, the access domain is by necessity geographically distributed since it is the only way to provide coverage and mobility. However, at the time when 2G was defined, these properties did not seem to warrant any special treatment of the access domain from trust point of view. At the time, the threat of tampering with base stations or gaining access to the backhaul transport network was simply not considered realistic.

In 2G networks, communication between the UE (in the user equipment domain) and the base station (in the access domain) was encrypted, and the base station decrypted the data before sending the data on into the core network. In 3G networks, this changed so that the base station just forwarded the encrypted data to the Radio Network Controller (RNC) residing in the core network and therefore the trustworthiness requirements on the access domain were reduced. An additional security feature added in 3G though was that the integrity of signalling data was added and through authentication being made mutual (rather than just the network authenticating the UE). Then, in 4G, it was necessary to move the termination point (user data decryption point) back to the access domain in order to allow the base station to perform header compression and other functions which required access to plaintext data. This was actually one of the key drivers for many of the additional security features that were added such as sophisticated key derivation algorithms, requirements on a “secure environment” inside the base stations and standardization of IP security on the backhaul transport.

4.2.2 Current trust model

User (subscriber)

Generally speaking the subscriber trusts the service provider to correctly provide the services agreed upon in the subscription contract and to do the charging and billing of its service correctly, and this trust is based on experience, reputation and legal framework. The subscriber trusts the service provider to provide services correctly such as phone calls, messaging and data connections based on the same aspects as for charging and billing. Subscribers will have a range of understanding about which service provider(s) and network operators they make use of when using the service. For instance, a subscriber to a VMNO may or may not understand which MNO the VMNO makes use of and may not understand that the reliability or availability of their service is primarily down to the reliability of the MNO’s network (with which they do not have a contract).

Regarding data protection and privacy, one can imagine that a majority of users consider the end-to-end path between themselves and the voice calling party as being “secured”, even though it is clear that all data is in principle available to the operator. This indicates that users trust the operator with rather sensitive information. When mobile broadband started to become useful and popular, surveys showed that users tended to have stronger trust in the security of mobile broadband connections than in their fixed internet

connection at home. The general feeling is that user awareness is increasing and nowadays the majority of users would have similar trust in fixed and mobile Internet connections.

Furthermore, a subscriber trusts that a mobile phone manufacturer's phone is working correctly in the service provider's network to make calls, text or use the data service. In this case the trust decision is based on experience (i.e., a mobile phone just works) and reputation (subscriber's social environment and public perception for example through ratings of phones and networks in magazines). The same holds true for the provider of the mobile operating system: the subscriber trusts, amongst others, that the OS works correctly, implements correctly the basic built in security mechanisms, that it does not contain backdoors and that it correctly receives patches including security related ones. There are most likely still fewer worries about mobile phone malware than PC malware. The consequences of phone malware can be more severe though, as the malware can for instance generate extra costs for the user or use user's bandwidth quota, neither of which are usually an issue in fixed networks.

Phones have begun to contain trusted elements in the phone itself as well, so called "secure elements". This has promoted the idea that the user could use the phone to perform more sensitive operations, such as pairing payment credentials with the phone and using the phone to perform payments. This increases the motivation to prevent the unauthorized use of the phone.

Note that while many security mechanisms' presence is motivated by providing users with trustworthy services, there is also one mechanism which more explicitly is there to communicate a "measurable trust". This is the so-called "ciphering indicator" which is supposed to show the subscriber if the radio link is encrypted or not. This was introduced in 3G but there was also a way for the home operator to disable it and it was rarely implemented in consumer mobile phones. In 4G, the possibility for the user to disable the disabling mechanism was added. Another mechanism which potentially can be seen as trust related is in the usual presentation of the serving network name on the phone's screen.

Service Provider

The Service Provider provides transmission resources to subscribers via the user equipment (e.g. mobile phone). Only the Service Providers have a contractual interface with the subscribers: they sell the service and/or the equipment and bill their subscribers. In many cases, the Service Provider is the same legal entity as the Network Operator.

In the trust relationship with the subscriber several aspects have to be considered. The service provider trusts (to some degree) the subscriber to pay his or her bill but it doesn't trust the subscriber (or the subscriber's phone) to be able to maintain a sufficiently secure credential (such as a password) to authenticate themselves according to the contract. Thus it provides the subscriber a UICC for authentication, which is of course also a usability/convenience aspect.

Network Operator

The Network Operator has a trust relationship with several entities (including the subscriber in the common case of the Network Operator being the same entity as the Service Provider) and can thus be seen as the central entity in the trust model.

The Satellite Network Operator (SNO) or Mobile Network Operator (MNO) owns and is responsible for maintaining, managing, deploying and operating the (satellite) network.

The network operator trusts a roaming partner to authenticate subscribers correctly if they are using an UICC but if the authentication is done using Wi-Fi for example then an IPSec tunnel is used so that the network operator itself can perform the authentication. The root of trust between the roaming partners is a contract, i.e., a roaming agreement. The roaming partner itself then allows a roaming subscriber to use its network as it trusts the corresponding network operator (also known as home network operator) to pay for this service. The network operator and the subscriber also trusts the roaming partner to correctly report network usage. There is no way for the network operator to verify the usage reports originating at a roaming partner and there is no mechanism for the roaming operator to prove the presence of a subscriber.

There are two other entities strongly related to the (satellite) network operator:

- **The interconnection provider** who provides a network linking one network operator to another. The network operator trusts that the interconnect provider connects to other operators so that calls can be made between users with different network operators. The root of trust in this case is a contract between network operator and interconnection provider.
- **The network access provider** who uses the services from one or more Satellite/Mobile Network Operators to provide bulk transmission resources to the Service Providers (SPs) for use by their subscribers.

There do not really exist any (standardized) security mechanisms specifically targeting (dis)trust between network operators sharing the infrastructure. A Service Provider (i.e. a telecommunications company) has a contract with the Network Operator to supply a suitable system capacity with a certain SLA (some QoS guarantees) to be used by its end subscribers. The SP offers pre-paid/post-paid services, needs to ensure that the Network Operator is providing the required SLA towards the Service Provider, and performs some control tasks (such as management of system bandwidth and power to optimize system efficiency, configuration of network components, etc).

The space industry is moving to more open and efficient mission operations enabling multiple missions to share ground and space based resources to reduce mission development and sustainment costs. This additional sharing of network resources (both physical and virtual ones) may raise additional trust and security issues.

Today network operators are basically assumed to fully trust each other, regulated through contract. However, abuse of personal data from dishonest operators is an important threat to these networks. This implicit trust is also built upon the knowledge that the MNOs are nationally regulated entities that have to guarantee certain functional, security/privacy, legal and business-related conditions/regulations to the corresponding national controlling bodies and also legal organizations.

Virtual Mobile Network Operator (VMNO)

The VMNO is a special case of a network operator as it does not own a mobile network and only owns the customer database (in some cases it does not even own a customer database and just rents some space in a network operator's database). Due to this special setup not only the trust model from the network operator applies but also additions with respect to the relationship between a VMNO and its infrastructure provider (i.e., some other network operator). The VMNO trusts the infrastructure provider to run the mobile network and being able to use resources there according to the contract between both. The contract itself might be in place due to the infrastructure provider being forced by regulations to sign such a usage contract.

Equipment Manufacturer

Until recently, equipment manufacturers have been kept largely outside the trust model in the sense that each network operator has simply decided if a certain equipment manufacturer is trustworthy enough, i.e. it has been mainly a business decision and supported by contractual obligations and liabilities on the equipment manufacturer. An exception has been the USIM manufacturers who, due to the specific requirements placed on the USIM/UICC, in practice have been subject to the need to provide more explicit evidence for their trustworthiness, e.g. in the form security certification of their products. In the last few years, similar requirements are starting to appear also on infrastructure manufacturers due to the Security Assurance Methodology (SECAM, [3GPP 2016]) of 3GPP and the associated manufacturer accreditation scheme of GSMA. Part of this work has also been driven due to “political” reasons. As is well known, not all countries in the world trust each other. This, together with the fact that telecom is a nationally regulated sector, has led national regulators to start to put requirements on the way the national network operators procure equipment from equipment manufacturers in other countries.

It is likely that this trend will be extended to the OS software providers and, in general, the networks’ software providers in future. This will require more complex trust decisions to be made in cases where the software provider is different from the hardware provider.

5 Trust in 5G Networks

The previous section reviewed trust in 4G networks. We now move on to looking at the changes expected in 5G networks. First we look at the additional actors and business models to be supported and then review 5G use cases.

5.1 Actors and Business Models

5G is considered a multi-actor mobile network because of the cooperation of several actors in the delivery of services. For instance, an MNO (Mobile Network Operator) can cooperate with a third-party such as an Over-the-top (OTT) provider, or a car manufacturer enterprise, or a city administration to provide a given service.

Role	Business Models	
Asset Provider	XaaS: IaaS, NaaS, PaaS Ability to offer to and operate for a 3rd party provider different network infrastructure capabilities (Infrastructure, Platform, Network) as a Service.	Network Sharing Ability to share Network infrastructure between two or more Operators based on static or dynamic policies (e.g. congestion/excess capacity policies)
Connectivity Provider	Basic Connectivity Best effort IP connectivity in retail (consumer/business) & wholesale/MVNO	Enhanced Connectivity IP connectivity with differentiated feature set (QoS, zero rating, latency, etc..) and enhanced configurability of the different connectivity characteristics.
Partner Service Provider	Operator Offer Enriched by Partner Operator offering to its end customers, based on operator capabilities (connectivity, context, identity etc..) enriched by partner capabilities (content, application, etc..)	Partner Offer Enriched by Operator Partner offer to its end customers enriched by operator network and other value creation capabilities (connectivity, context, identity etc..)

Figure 9. Network operator business models and roles defined by NGMN

The potential benefit of 5G is the synergy among different partners, as seen in the business models defined by the NGMN in [NGMN 2015] and summarized in the Figure 9. These operator-centric business models are presented below. NGMN categorizes the business models into three sets: asset provider, connectivity provider, and partner service provider. These sets differ in what is provided by each actor.

- Asset provider: two types of business models arise in this role: XaaS and network sharing. XaaS is when an operator provides network capabilities to a third party. These network capabilities can be in terms of infrastructure (IaaS), platform (PaaS), or network (NaaS). Network sharing is an operator shares the network infrastructure with another, independent of the implementation or technology used to allow this sharing (i.e. slicing, virtualized network, etc.).
- Connectivity provider: two types of business models arise in this role, called basic connectivity and enhanced connectivity. Basis connectivity is essentially a projection of current 4G business into the future, providing access to consumers or to VMNOs. Enhanced connectivity adds QoS possibilities such as latency and even (self-) configuration options.
- Partner service provider: the business models here are called “operator offer enriched by partner” and “partner offer enriched by operator”. The former case allows enriching a given service provided by an operator (MNO) by the unique capabilities of a third party such as streaming content or specific applications. The latter case is when a 3rd party makes an offer directly to the end customers enriched with the unique capabilities of an operator (e.g. secured VPN service).

On top of the above, one also ought to consider the aspects of infrastructure deployment. When the infrastructure can be implemented using commodity IT hardware (as with NFV), much of it can be deployed in a regular data centre. Thus, a data centre provider could be an actor independent of the actual RAN infrastructure provider. If service providers are able to allocate resources dynamically from whatever infrastructure provider they see fit, the question of location of the actual resources becomes relevant as well. Different regulatory schemes could be applicable in different geographical regions. The location (or lack of certainty in the location) of network function resources can affect user trust as well.

Additional considerations can be given to the certification aspects. Specifically, in the 5G context there can be certification authorities that are used to assure the correct operation of network elements or functions. For instance, different VNFs can be certified, so that the infrastructure provider can have some certainty as to the trustworthiness of the functionality that might be externally introduced into their infrastructure, for instance, by VMNO. It still needs to be determined whether the certification authorities (and relevant testing laboratories) are industry bodies, such as GSMA, or some other entities. The GSMA-based approach seems to be at least adopted in 3GPP when they have been considering the certification aspects of network elements through their Security Assurance Methodology (SECAM).

We identify from the business cases presented above the following business models as critical in terms of trust: XaaS, “Operator offer enriched by partner”, and “Partner offer enriched by operator”. All these aforementioned business models have as common cause that the service delivery relies on the cooperation among several actors. Contrariwise, it is important to notice that the network sharing case is not considered as a multi-actor case. Despite different actors sharing the underlying infrastructure (whether physical or logical), the service delivery is assured separately by each actor’s means so that each actor delivers their services to its clients but no interaction is needed among the actors to deliver the service.

To meet the wide range of use cases defined by NGMN in [NGMN 2015], initially categorized as broadband access in dense areas for pervasive video, broadband access everywhere, higher user mobility for high speed train communications, massive internet of things for sensor networks, extreme real-time communications for tactile internet, lifeline communications for natural disasters, ultra-reliable communications for e-health services, and broadcast-like services for content broadcasting, the NGMN consortium proposed a slicing approach to provide each different service with a unique logical network slice.

A slice, or 5G slice, is defined as “a collection of 5G network functions and specific radio access technology (RAT) settings combined together for a specific use case or business model”. The 5G slicing architecture provides for composing the slices to tailor the network to the particularities of different use cases and their requirements by chaining different network functions, now virtualized thanks to NFV.

For instance, we can define a slice for a remote surgery service (in red in the figure below) and another for broadband access everywhere service (in green).

- The former slice has high resilience and high availability requirements so that this service requires isolated resources to embed the network functions and transport the traffic to avoid any failure propagation affecting the underlying hardware.
- The latter has mobility requirements so that this service requires certain additional mobility management network function.

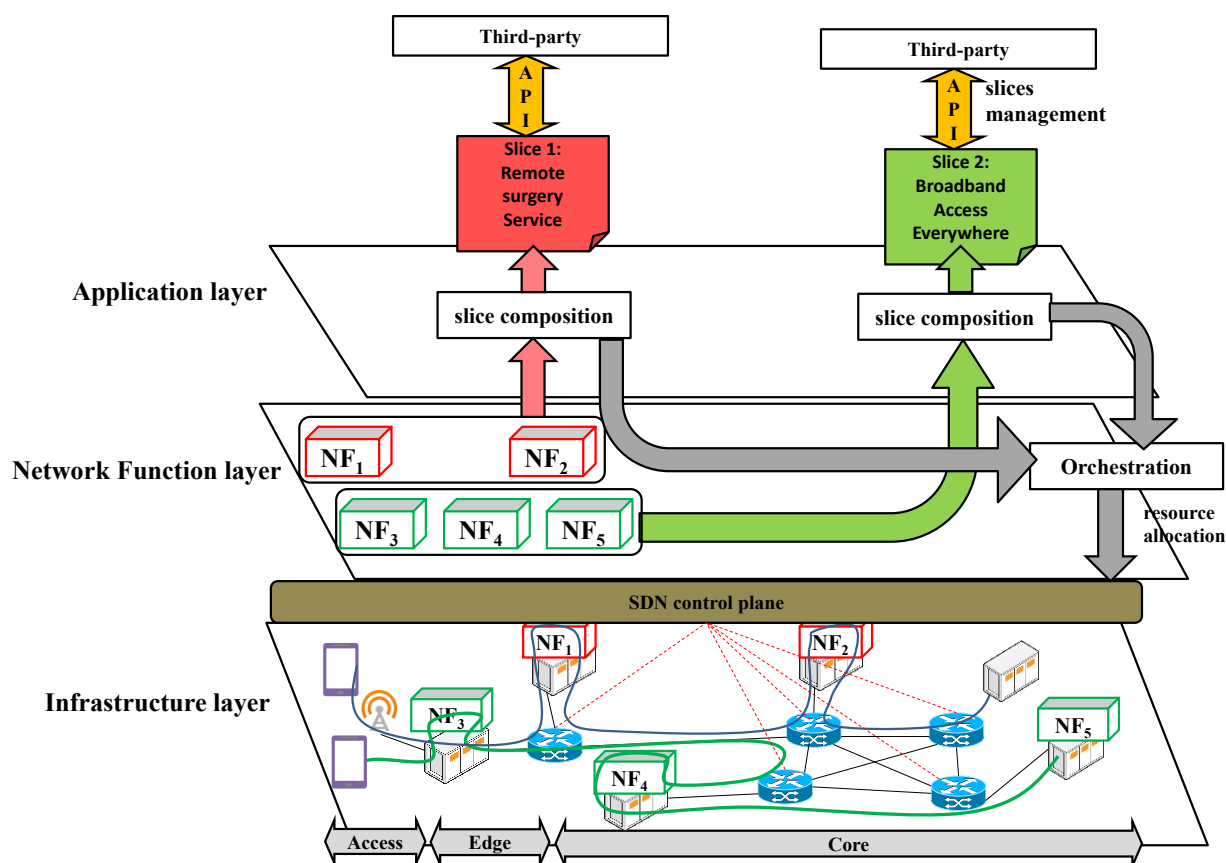


Figure 10. Preliminary 5G slicing architecture

In this multi-actor scenario, where several actors cooperate to ensure an SLA for a given service, trust becomes critical. Trust is the first stone towards the definition of the liability chain in the delivery of a given service. This liability chain is to determine which actor is responsible for a given malfunction impacting the SLA contracted by the end users.

A trust model puts the necessary mechanisms in place to calculate and propagate reputation among actors depending on their performance to maintain their network in an optimal state. This reputation scoring is measured through metrics such as the security mechanisms used by each actor, their rate of unavailability, of their rate of compliance with respect a given SLA, among others. There is no standard regarding the definition of these metrics.

The focus is to define an end-to-end liability chain encompassing all the actors and their resources involved in a given service. Those resources are the physical, logical, and virtual elements involved in the delivery of that service.

5.1.1 New domains for 5G

5G will encompass many indicators pointing to radical changes in mobile communication. They're not only driven by the Internet and telecommunication industry but also by other industries such as automotive, healthcare, industrial networking, manufacturing and logistics, financial and the public sector, who are seeking to reinvent themselves. These kind of industry applications require ultra-reliable and virtual zero latency communication systems.

Minimizing latency and increasing reliability (Figure 11) opens up new business opportunities for the industry, arising from new applications that simply will not work properly if network delays are too high. Latency determines the perception of speed. Real-time functionality demands the lowest possible delay in the network. Reliability creates confidence in users that they can depend on communications even in life-threatening situations.

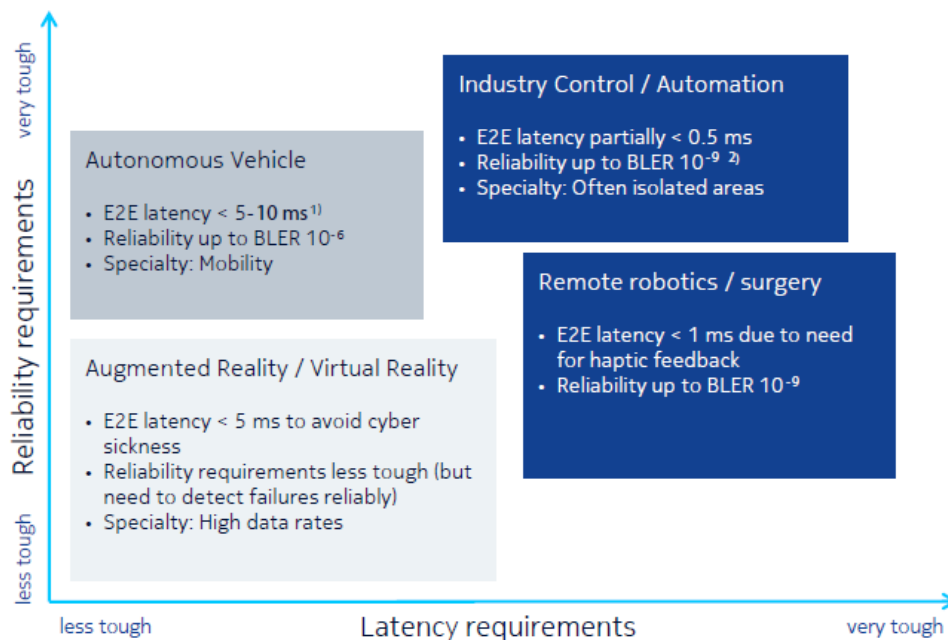


Figure 11. 5G Use cases requiring low latency and/or high reliability

5.1.1.1 Autonomous vehicles

Autonomous vehicles is a hot topic for many industry players from car manufacturers, consumers, and insurance companies to governments. The US Secretary of Transportation has said that driverless cars will be in use all over the world by 2025. The IEEE predicts up to 75% of vehicles will be autonomous in 2040. While the autonomous vehicles developed today rely mostly on on-board sensors and systems, their performance and safety could be vastly improved through 5G communications.

Autonomous vehicles can reduce accidents and improve road utilization as vehicles can be driven closer to each other and more safely than human drivers can achieve. Transportation companies can take advantage of autonomous car fleets. The fleets can be utilized more effectively with fewer accident caused by human error. In addition, real-time, ultra-reliable communications between vehicles, infrastructure and smartphones could enable traffic to flow more smoothly, eliminating traffic jams. Commuting time can be used for other activities with the help of autonomous vehicles. This might save an hour per day for people living and commuting in cities.

The communication system needs to be extremely reliable as it involves human safety. The end-to-end latency requirement needs to be as low as 5-10 ms.

5.1.1.2 Augmented reality / virtual reality

Augmented Reality (AR) enhances a real-world view with graphics. Real-time information is displayed based on the user's location and/or field of vision. Virtual Reality (VR) creates a totally new user experience with the user being in a fully immersive environment. The AR/VR device needs to track user movements

accurately, process the movement and received image, then display the response immediately with end-to-end latency of less than 5 ms.

5.1.1.3 Remote robotics / surgeries

Remotely controlling robots, rovers, devices or avatars in real time can assist in working safely in dangerous places. Hospitals could arrange remote robotic surgery via a customized 5G network as effective as if the surgeon was physically present. For public safety, robots could be sent to work in dangerous situations, such as bomb disposal or firefighting. The system needs to be extremely reliable with block error ratio (BLER) of no more than 10^{-9} and end-to-end latency of less than 1 ms to support the necessary haptic feedback.

Many haptic screens and devices are being developed currently to respond to touch and provide tactile sensations by varying the friction between the user's finger and the screen. This creates an experience of "You feel what you touch (remotely)".

5.1.1.4 Industry control / automation

Industrial networks have stringent requirements because they require fast machine-to-machine communication and ultra-reliable connectivity. A system failure could mean loss of equipment, production, or even loss of life. Time-critical process optimization is a key requirement for factories-of-the-future [5G-PPP FoF]. The need for wireless ultra-reliability and virtual zero latency will be driven by uses that include instant optimization based on real-time monitoring of sensors and the performance of components, collaboration between a new generation of robots, and the introduction of wireless connected wearables and augmented reality on the shop floor.

Machines can receive, analyse and execute tasks much more quickly than humans. Therefore, machine-to-machine communication requires extremely low latency, for example closed-loop control applications for industry automation require less than 1 ms latency.

Indoor traffic control and indoor mobility control of shop floor equipment typically have cycle times around 1-10ms. The highest demands are from actuators and sensors requiring cycle times of less than 1ms with a jitter of less than 1μs. While today's wired systems meet these requirements, 5G will create a unified platform that addresses a wide range of needs from the company supply chain, to inter-enterprise communication, to the control of actuators/sensors on the factory floor. This will reduce administrative costs compared to maintaining multiple systems, eliminate the cost to install wiring and increase flexibility to change production flow in the factory.

5.1.2 Potential of 5G new domains: Business models powered by network performance, data and slicing

5G will be about connecting people and things profitably. These are entirely different business models, yet the flexibility of 5G radio and architecture will enable operators to be profitable in both. In the 5G era operators will be able to monetize three assets (Figure 12):

- *"Connectivity+"*: The new performance level of their networks enables extreme broadband to support uses such as HD and UHD services in the home and on the move, but also virtual reality services that are relevant to the business world. These "Connectivity+" business models provide new opportunities through guaranteed high service levels for end users, as well as for content and other service providers.
- *Information brokering*: The billions of transactional and control data points produced by the network can be used to enable entirely new services that benefit from contextual real-time and non-real-time

data. Operators can broker this information to different industries including providers of augmented reality services, traffic steering systems provided by municipalities, factories and logistical systems and utilities. Real-time big data analytics will play a crucial role in the brokering model.

- “*NaaS*”: Dedicated virtual sub-networks, so-called network slices, can be marketed as “Network as Service” which can have different flavours and provide exactly the functionality that is needed for different industries and their diverse use cases. For example, the functionality and capabilities needed for connecting massive numbers of consumer health sensors are completely different to those required for high quality UHD video delivery to TV sets.

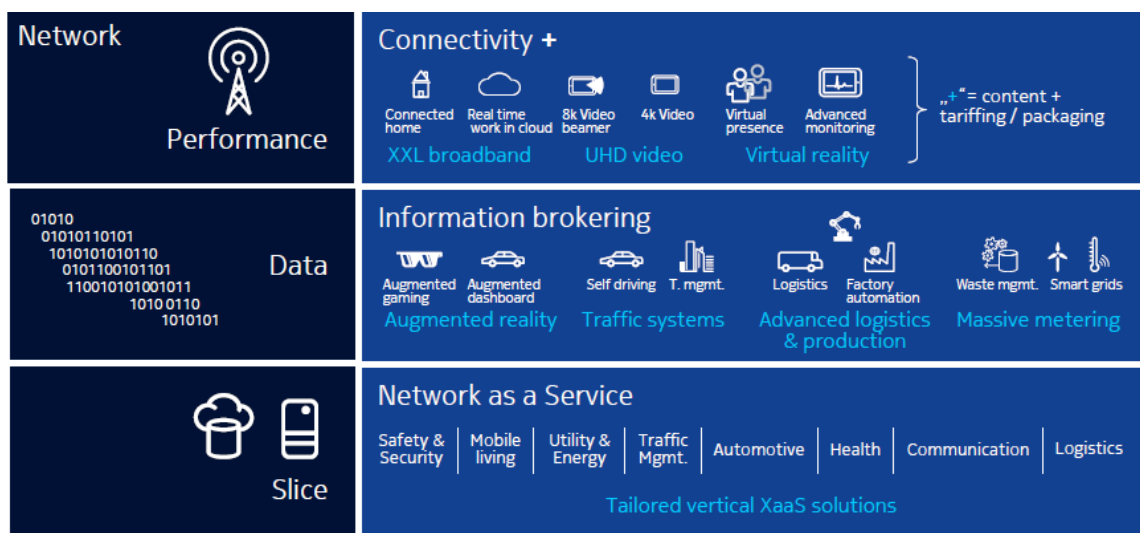


Figure 12. A variety of business models powered by network performance, data and slicing

5.1.3 Trust considerations in 5G

One new possibility for 5G is that due to virtualization a network operator might opt to run parts of its network functions and applications for example on an external cloud infrastructure. One could imagine that for example parts of the subscriber database is run on an external cloud. In this case a new actor is the external cloud provider who is not part of the existing 4G trust model. The external cloud provider might also have data centres in different jurisdictions and it is not always automatically clear in which jurisdiction the virtualized network function is running. Without precaution such as enforcement of geo-location, this also collides with the assumption in the 4G trust model that the network is running within one jurisdiction.

Another new domain for 5G is the possibility to “insource” network functions from third parties in order to enhance the network and/or the services it offers. One could imagine that a content distribution network (CDN) provider integrates caches in a network operator’s network. There it is necessary to ask if the new functionality is not affecting the network in a negative way due to not being compliant to the same technical specification. Another way to extend the network offerings could be that for example a factory is allowed to provide its own identity and authentication mechanism for the devices in the factory and that these devices, authenticated in a non-3GPP way, are then authorized to use, say a slice of the operator’s network. One question arising here is how much the network operator can trust the factory’s authentication mechanism, i.e. avoiding that a weak mechanisms allows unauthorized access.

Common to these use cases is the fact that the operator, of course, always has the option not to use or rely on external parties. However, this may lead to not being able to maximize promises of the 5G eco-system. Thus additional mechanism to sustain these new business and trust models are relevant to study.

5.1.4 5G Satellite Business Models

As far as the satellite Business Model is concerned, the requirements from the 5G network are:

- Access to all types of services.
- Using a single user device able to communicate with different networks.
- Single bill for all services with low cost.
- Reliable wireless access even in case of roaming or failure of one or more networks.

The introduction of Broadband services through the satellite is increasing significantly over the past years and is supposed to continue in that direction over the years to come. Therefore, these models are related to broadband telecommunication systems or telecommunication ground user segments, but may also relate to other systems.

Success comes from the introduction of High Throughput Satellite (HTS) systems with one to several tens of spot beams allowing a great frequency reuse that makes the service more affordable, delivering tens of Gbps in Ku (11/14 GHz) or Ka band (20/30 GHz). Current state of the art Ka band broadband satellite systems provide in the order of 100 Gbps of total capacity with spot width in the range 0.4 – 0.6°.

Current Satellite and Terrestrial communication networks can be complemented or threatened by new High Altitude Pseudo-satellites (HAPS) based services and drones in the short future. HAPS are long-endurance aerostatic or aerodyne platforms in the lower stratosphere, above commercial aviation airspace. Their location, compared to satellites implies shorter paths improving link budgets, which for telecommunication means signal quality or lower power transmission and for observation is translated into ground resolution.

On the other hand, higher altitude than towers provides wider coverage. This zone of stratosphere, although environmentally complex, presents low winds that reduce power consumption, enabling long-endurance missions. Besides, the usage of stratospheric solutions implies shorter time between design and operation phases.

The success of these platforms can be grounded in the increasing of TRL's for systems in the last years, the growing demand of bandwidth and coverage, the fast deployment, the awareness from European regulators (both communications and air traffic) and the improved on-board energy management in modern autonomous aircrafts

5.1.4.1 *Ultra-reliable communications based on hybrid eNBs*

This end-to-end system architecture encompasses the LTE-based Radio Access Network (RAN), the transport network where hybrid eNBs (satellite and dynamic beams) introduces its main research novelties, and the Evolved Packet Core (EPC), also referred to as core network. This model focuses on evolving the Transport Network Architecture (TNA) by combining both satellite and terrestrial transport architectures.

Satellite Backhaul extends the ability to provide voice and data services in disaster areas and temporary hot spots (e.g. sporting events or concerts). The main goal is the ability to offer resilience to cases of link failure. The satellite connectivity adds flexibility to backhauling networks. Also, this model provides offloading capability via satellite to the backhaul network in case of congestion.

The topology management objective is that no nodes in the mesh network are left un-connected, while covering all the needed area. Topology algorithm shall be based on user priority and bandwidth.

5.1.4.2 High data rate networks, broadband, trunking and backhauling

The performance of most "terrestrial based" fixed internet access technologies (e.g. DSL or radio) is distance sensitive. The maximum available bandwidth will decrease as the distance from the access node (e.g. DSLAM, Radio base station) increases. Satellites are a natural environment for high data rate services where their broadcast nature can be fully exploited. Direct-to-Home (DTH) services are very well suited for simple geostationary orbit (GEO) satellite solutions in which neither the satellite configuration nor the coverage have to be modified to match any service evolution.

HAPS can be attractive acting as a ground-based signal repeater in those regions with low terrestrial TV signal quality, improving the terrestrial TV distribution coverage.

The trunking scenario via satellite can also benefit from the good balance between coverage and signal degradation provided by HAPS solutions. In this case, the network architecture could consider the HAPS/drone as an intermediate element between the final user and the satellite, letting users within its coverage area connect via the HAPS and using the satellite for longer-range communications.

For backhauling scenarios, where the cost of introducing satellite would incur an extra charge, the presence of a cheaper component such as a HAPS which increases the instantaneous capacity over a specific area, may complement the pure terrestrial solution. In any case, the cost of introducing this element instead of expanding the terrestrial resources should be carefully studied.

5.1.4.3 Personal communication systems for tactical scenarios

This is one of the most interesting scenarios for the coordination of HAPS and satellites in the same network, and tactical communications are already widely used here. Communication is established using UHF band with omnidirectional antennas that provide very poor quality links for the transmission power (known as the "link budgets") in a limited area of operation, with a radius of tenths to hundreds of kilometres depending on the user terminal transmission power. Low-orbit satellite constellations are normally too complex, expensive and risky to be equipped with a UHF-frequency payload and therefore nations mostly rely on GEO deployments. However, reaching a GEO satellite requires larger radio units and it is at this point where HAPS can be a perfect partner. Deploying a stratospheric platform that could receive the uplink signal with better link and act as an intermediary between the GEO satellite and the targeted user, opens the door to data services for hand-held terminals and world-wide communications and would significantly alleviate the scarce frequency resources that have always been the major issue in the usage of these bands.

5.1.4.4 Mobile broadband

Considering the potential complementation of satellite solution by including HAPS/drone nodes, it is easy to notice that HAPS/drone would not be of much help for vast areas due to its reduced coverage compared to stand-alone satellite solutions. They would certainly be of interest to cover, for example, disaster areas providing mobile broadband communications to the rescue teams or even to the civilian population, or to cover isolated regions such as small islands with complex elevated terrain or desert settlements.

In disaster relief cases, the system architecture must consider that the terrestrial infrastructures can be damaged or even destroyed, which, at the end, is a simplification of the network topology as the HAPS/drone does not need to interact with other ground elements.

For isolated regions, the presence of the HAPS may be sufficient to cover the population's mobile communication needs, and even more if we consider the usage of advanced spot antennas that would allow improvement of the link budget and increase the number of simultaneous users.

5.1.4.5 *Machine to machine communications*

The simplest solution for M2M communications is the usage of GSM networks interconnecting remote locations (individual nodes or centralised sub-networks) with a data centre for information collection and processing. This makes the machine-to-machine use case very similar to the mobile one discussed above.

Also in this case, the evolution of LTE advanced is of the most applicability to allow direct connectivity between the remote location and the HAPS and to ease the integration of the HAPS in the network.

Satellites complement this architecture for locations where the GSM coverage does not reach all the locations. The presence of the HAPS node can expand the capabilities, as the LTE advanced may have difficulties reaching satellites above low Earth orbit (LEO) (and can even have problems for LEO).

5.1.4.6 *High throughput satellite systems hotspots coverage and traffic demand evolutions*

Knowing the long time that it takes for a satellite to become operational, HAPS/drone can be perceived as gap-fillers for new opportunities for the operators to capture clients in the interval while the satellite is being put in place. Other possibilities for HAPS/drone is to cover saturated areas benefiting from the smaller footprint compared to a satellite beam, or even deploying HAPS to areas not usually covered (for example islands, seas and oceans in the summer period).

5.1.4.7 *Novel models under research*

5.1.4.7.1 *Broadband Access via integrated Terrestrial and Satellite systems (BATS)*

BATS proposes a novel architecture that combines satellite and terrestrial service delivery via an Intelligent User Gateway (IUG), dynamically routing each application's traffic to the most appropriate access network, according to its service needs and access link capabilities to optimise the Quality of Experience (QoE). To cope with this integrated scenario, BATS will provide a unified network management framework.

5.1.4.7.2 *Virtualized hybrid satellite-Terrestrial systems for resilient and flexible future networks (VITAL)*

Combination of Terrestrial and Satellite networks by pursuing two key innovation areas, by bringing Network Functions Virtualization (NFV) into the satellite domain and by enabling Software-Defined-Networking (SDN)-based, federated resources management in hybrid SatCom-terrestrial networks.

5.1.5 *Summary of 5G actors*

Based on the reality of 4G network actors and what is planned for 5G (described both above and in the use case analysis below), a detailed list of 5G actors follows. The indented bullet points represent specialisations of the first level bullets and actors who are new in 5G compared to 4G are prefixed with "[5G]".

- Network equipment manufacturer
 - Terrestrial equipment manufacturer
 - [5G] Satellite equipment manufacturer
- Infrastructure Provider
 - [5G] Virtual infrastructure provider (VIP), providing infrastructure as a service (IaaS)
 - [5G] Satellite/HAPS provider
- Network software provider; commonly also the network equipment manufacturer
 - [5G] Virtual network function (VNF) provider
- Interconnect network provider (provides a network linking one network operator to another)

- Mobile Network Operator (MNO) (taking the role of “home” or “serving” operator); commonly also the infrastructure provider
 - Virtual mobile network operator (VMNO) who purchases bulk capacity from MNOs and may (or may not) have their own HSS
 - [5G] Virtual mobile network operator (VMNO) who purchases SDN slices from an Infrastructure Provider
 - [5G] Factory or enterprise owner operating a AAA in a network linked to a (V)MNO
- [5G] Satellite Network Operator; commonly also the satellite/HAPS provider
- [5G] Network access provider (uses the services from one or more Satellite/Mobile Network Operators to provide bulk transmission resources to Service Providers)
- Service Provider; commonly also the (V)MNO
 - [5G] over-the-top (OTT) service provider
- User equipment manufacturer
 - Phone manufacturer
 - USIM manufacturer
 - [5G] Sensor manufacturer
 - [5G] Robot manufacturer
- User equipment software developer/provider
 - User equipment operating system developer/provider
 - User equipment application developer
 - Application store provider
- End user
 - Common phone users (Service Provider subscriber)
 - [5G] Wireless Sensor Network (WSN) owner/operator
 - [5G] Employee of enterprise
- Regulators, law enforcement agencies

The precise relationships between these actors will be defined and clarified as the 5G architecture is determined. Different pairs of actors will require different means to engender trustworthiness. For instance, while an Infrastructure Provider may be convinced to trust some equipment offered by an equipment manufacturer based on its adherence to Common Criteria, the same approach would not be any use for a common phone user’s trust in a user equipment manufacturer’s product.

5.2 Use Case Analysis

In order to provide an indication of the trust issues expected in 5G networks we present here an analysis of 21 of the 31 use cases defined by 5G-ENSURE in D2.1. This is justifiable given the “draft” nature of this document and the remainder of the use cases will be analysed in due course. We have taken care to align the use cases analysed with those analysed and reported on in the risk analysis of D2.3 so that a complete model of the risks and consequences, and specifically the consequences for trust and trustworthiness of the use case subset can be drawn.

5.2.1 Satellite Identity Management for 5G Access (UC1.3)

Summary: This use case works on integrating the envisaged 5G AAA system mechanisms related to user identity with the satellite authentication function using standard interfaces.

This use case explores two identity-management situations involving satellite networks and a dual satellite and terrestrial 5G access: one in which the device attaches to the satellite network to grant access to the satellite resources; the other one in which the 5G device identifies in either the satellite network or the terrestrial network, and then due to coverage issues the 5G device performs a roaming to the other network.

Entities: The entities implicated in this use case are the network operators who manage the satellite and terrestrial network services and resources, the service providers such as a mobile operator who is using these networks and the subscriber/UE who signed up to the mobile operator services in a roaming scenario.

Trust: The network operator needs to trust that the service provider complies with their agreement and the service provider needs to trust that both the satellite and terrestrial network operators are providing correct information. Trust can be broken and responsibilities have to be dissolved in order to pay penalties; depending upon the current legislation, the network operator may have financial and legal prejudice.

From the other perspective, the subscriber needs to trust in his/her mobile operator as part of the direct service agreement and indirectly in the roaming agreement with other operators in order to preserve his privacy. This type of trust can be ensured through technical solutions (e.g. privacy enhancing techniques such as IPSec, encryption schemes such as public key cryptography, certificates signed by a third party certification authority, network usage reporting) as well as roaming agreements between the entities.

Therefore, if these agreements are not honoured the privacy of the subscriber is not guaranteed and the trust can be broken since the risk of a privacy violation is real and may ultimately lead to subscriber revoking his/her subscription.

5.2.2 MNO Identity Management Service (UC 1.4)

Summary: In this use case, the Mobile Network Operator provides an identity management service to a 3rd party service provider on behalf of a user. Consider for instance, a bank is the third party and Bob is a mobile network subscriber and a bank client who signed up to this service. The main idea is to provide the bank with anonymized information about Bob's network context in order to enable the bank to adjust its security policies, hence, it offers and guarantees the same security level of its service (banking service). For instance, the bank may require additional authentication measures if Bob is connected through a public hotspot. Bob's network context information encompasses the access network type, the equipment, the authentication scheme used and the location.

Entities: The entities implicated in this use case are the mobile network operator, a service provider such as a bank and a user who is using the mobile network, the bank service and the new service provided by the network operator.

Trust: In these circumstances, the bank needs to trust that the mobile network operator is providing correct information about Bob. In the same time, Bob needs to trust that the mobile operator is anonymizing his information in order to preserve Bob's privacy. This type of trust can be ensured through technical solutions such as k-anonymization or differential privacy in addition to agreements between the entities. If the user does not any more trust the new service, this will threaten the trust that the user has in the basic network operator service (i.e. telecommunications). If the service provider does not trust any more the quality of the information provided by the mobile network operator services, this may lead to stopping the new service.

5.2.3 Device Identity Privacy (UC 2.1)

Summary: This use case describes a situation where the device identifier (IMEI) can be exposed over the air in case of a network attach procedure of type "Emergency". The IMEI is mostly used to verify whether a call has been made from a specific handset and to detect fraudulent activities. Usually, when the phone is switched on, the IMEI is sent so that the network can verify that the handset requesting cellular services is not a stolen one. The network checks the IMEI number against the Equipment Identity Register (EIR) to see whether the handset is in the blacklist. In current mobile networks (GSM and UMTS and in all networks during an emergency call setup) the IMEI is sent to the network in plain text. This opens the door to device identity disclosure and unauthorized device tracking attacks. Considering that users don't change their mobile very often (i.e., the relation IMSI-IMEI is fixed), passive observation could record the relation between IMSI and IMEI. Intercepting the IMEI sent in clear-text over the air-interface provides some means for an attacker to go around the user identity confidentiality and, as such, weakens the location privacy of the user. In addition device cloning could be possible by using an intercepted IMEI. Moreover, an attacker, by knowing IMSI as well as IMEI, can unblock a stolen mobile phone and make it a legitimate handset in the white market of second hand phones. This is possible by exploiting SS7-MAP vulnerabilities.

Entities: The entities involved in this use case are the subscriber's Home Mobile Network Operator (HMNO), the Serving Mobile Network Operator (SMNO) in a roaming scenario and the user/UE using the mobile network.

Trust: in this use case the user/UE implicitly and unconditionally trusts the network to which it is connected and the MNOs involved. The user has to trust the MNO(s) that it has implemented techniques to detect/avoid the installation/use of fake cell towers. Alternatively the user trust the MNO(s) that it provides privacy enhancing techniques to transfer IMEIs in an encrypted/confidential manner in all situations. This type of trust is now implicit and its basis is a subscription contract. Nevertheless this trust can be ensured through technical solutions in addition to agreements between partners, such as the use of public key-based cryptography.

A false cell tower can pretend to be a legitimate cellular network asking the user to send its IMEI by sending an Identity Request message. 4G specifications mandates that a SIM does not answer Identity request messages asking for any identifier, other than the IMSI, when no encryption context is yet established. This requirement does not avoid IMSI catching, but does prevent the leaking of the other identifiers to IMSI catchers. However, as reported in [Broek 2015] the current 3G or 4G enabled phones and SIM cards used for test also transmit the TMSI and IMEI unprotected when requested. Therefore the trust can be broken since the risk of a privacy violation is real and well documented in current networks, and may ultimately lead to user revoking his/her subscription. Depending upon the local legislation, as a consequence, the mobile network operator may have financial and legal prejudice.

5.2.4 Subscriber Identity Privacy (UC 2.2)

Summary: The use case refers to the user Initial Attach procedure to the 3GPP and non-3GPP network. Due to the current trust model adopted by cellular networks, there are situations when the IMSI needs to be transmitted to the network in clear text through the vulnerable radio access, during the authentication procedure (e.g. EPS-AKA, EAP-AKA). In fact, the current 3GPP system requires a UE to provide its IMSI unencrypted over the air during the initial attach phase. By observing the OTA traffic, a passive attacker can identify a user from on the IMSI. In addition by using a false base station an attacker can overpower the

legitimate cellular network and pretend not to be able to retrieve the user true identity (IMSI) from the temporary one (TMSI, GUTI). In that case, the UE will have to send its IMSI again in clear text.

Knowledge of IMSI allows user tracking also when the user roams to another network. In this scenario, the UE has to provide its IMSI to the serving network for authentication and the IMSI is again stored across the network elements of the roaming network, e.g., in the MME, S-GW, P-GW. This enables the serving network to trace the user.

The IMSI is a valuable information that should not be accessible to anyone except the user Home Network (HN). Its compromise will expose the subscriber to threats like location.

Entities: The entities involved in this use case are the subscriber's Home Mobile Network Operator (HMNO), the Serving Mobile Network Operator (SMNO), the interconnection provider, and the user who is using the mobile network.

Trust: with reference to the permanent identity IMSI, the current trust model is based on the following relationships.

- The UE trusts its HMNO as part of the direct service agreement.
- The HMNO trusts the SMNO as part of the roaming agreement contract and it confers full trust in the SMNO with regards to the IMSI of a subscriber. For authentication, authorisation and billing purposes, the IMSI is exchanged unabated between the serving network (SN) and the home network (HN).
- Both HMNO and SMNO trust their interconnection provider.
- The UE indirectly trusts the SMNO to which it is connected, demanding unconditional trust to the UE in transmitting its IMSI during the access procedure or when explicitly required.

From the above trust model, the SMNO is considered trustworthy by the user, who either accepts or ignores the risk that a compromised third party serving network may pose. The SN may belong to an entrusted third party and the UE/user has little or no way to detect this situation since it trusts it unconditionally. A false cell tower can pretend to be the legitimate cellular network asking the user to send its IMSI.

In current networks there are several vulnerabilities which an adversary may explore to compromise the privacy of the subscriber. This is more critical considering that in today context multiple cellular operators need to interoperate among each other to offer wider coverage to the subscribers, and where an operator that has not set up its own infrastructure needs to establish roaming agreements with third party operators to provide access. Therefore the trust can be broken since the risk of a privacy violation is real and well known in current networks, and may ultimately lead to user revoking his/her subscription. Depending upon the local legislation, as a consequence, the mobile network operator may have financial and legal prejudice.

The types of trust required in this use case can be ensured/guaranteed through technical solutions in addition to agreements between partners, like, for example, the use of encryption schemes based on public key cryptography that can provide the necessary root of trust and the key material in situations where no secret keys are yet shared between UE and the network.

5.2.5 Trust in Authentication of IoT Devices in 5G (UC 3.1)

Summary: As discussed in Section 3.1 trust is necessary in WSN, because IoT devices are hardware-constrained so they may become easily compromised. IoT devices may require specific authentication

mechanisms both due to their hardware-constraints and also for their potential of generating huge peaks of control traffic. A WSN may consist of thousands of devices, which may need immediate authentication in the initialization phase or when they are mobile.

In 5G Systems, alternative approaches to sustain authentication of IoT devices are considered. A WSN may connect to 5G through a specific IoT Gateway, and as well a standard UE may act as a gateway or the IoT devices may connect through trusted or untrusted access points. In these cases the sensor devices may utilize a non-3GPP air-interface, such as Wi-Fi, Bluetooth or ZigBee. Furthermore, even the constrained IoT devices may still be able to use LTE or LTE-M and communicate with standard 5G protocols. For serving the constrained devices 3GPP specified Extended Access Barring (EAB) and Low Access Priority to limit access (and network load) from some UEs. For UEs which can work in power saving mode high latency communication is under specification. Specific group authentication is also under specification in 3GPP, for reducing authentication overhead which may derive from MTC.

In the case that a standard UE or IoT Gateway control authentication of IoT devices, the basic 5G trust model is applied and the gateways are seen as UEs from the network side. Then the IoT network is controlled by the sensor network operator and the IoT devices do not get 5G credentials. However, if M2M communication happens through the 5G network, the trust model changes. This occurs when the IoT devices connect through the LTE, LTE-M air interface or if they are connected through trusted or untrusted Wi-Fi access points. The specific M2M authentication protocols or group authentication may be needed. For untrusted Wi-Fi access 3GPP specified mechanisms that rely on IP security tunnels which should be supported in the UE. However, IPsec is a heavy protocol that creates latencies and shortens battery life in UEs, so it is not a very good solution for MTC.

Entities: MNO, VMNO, WSN operator, subscribers.

Trust: The 5G trust model is based on the 4G model which is explained in Chapter 4. Still in the IoT case, the WSN operator is a new actor functioning either in the User Equipment Domain or the Access Network Domain. There are various potential business models between users of WSN and their operators. A user may own the WSN and the WSN operator may offer the plain IoT gateway or the Access Point or the operator may control the whole system. WSN operators must have contracts with the users and the 5G network operators. The 5G network operator may also take WSN operator's role and control all the gateways treating them as a part of the access network domain. If the IoT devices use LTE or LTE-M no specific gateways are needed. A WSN operator may also offer control of WSN as a service or application which is delivered through a 5G network. Then a user signs a contract with the WSN service provider.

5.2.6 Trust in Network-Based Key Management for End-to-End Security (UC 3.2)

Summary: An encrypted and authenticated IoT Service can be provided for IoT devices through a 5G system although there is no way to share secret keys between endpoints. 5G network may provide a network-enabled key management service which can be used to achieve secure end-to-end service between an IoT device and an IoT backend service. The keys can be provided either for device-specific unicast or group-specific multicast communication. The key management service can be offered by the 5G operator or a third party. The IoT service can be located outside the 5G network, e.g. in the cloud or it can be inside the 5G system. The IoT backend service and the IoT devices should have 5G credentials. 5G should support lawful interception.

Entities: MNO, VMNO, third-party service operator, legal authorities, subscribers.

Trust: The IoT service providers and the owners of IoT devices need to trust the 5G operator. The 5G operator should trust the key management service provider and the operator should trust that lawful interception is not misused. The users and the IoT backend service provider should accept lawful interception.

5.2.7 Virtualized Core Networks, and Network Slicing (UC 5.1)

Summary: This use case focuses on the user plane of an SDN infrastructure. The VMNO and the VIP have an agreement to install a set of slices composing a VCN. One slice serves to xMBB subscribers and the other to mMTC subscribers. The network slices are configured so that commands cannot get accepted to other slices. Trust between the VIP and the VMNO is paramount in this use case, due to the fact that the slices provided by the VIP and exploited by the VMNO to be in turn offered to the subscribers involve three actors. In the event of any kind of service abnormality, responsibilities have to be dissolved in order to pay penalties with respect to the contract among both VMNO and VIP. This multi-partner service and the exposure of virtual resources to third-parties implies that the responsibility towards the subscribers, which has been traditionally always the operator, has to be extended distributed with the same warranties to all the rest of actors/entities involved.

Entities: VIP, VMNO, subscribers.

Trust: Subscribers trust the slice in the sense that those fulfil the SLA requirements for the required service. VIP and VMNO will trust each other what is done through a contract that will dissolve any responsibility and the related penalties to be paid in case of not compliance.

5.2.8 Adding a 5G node to a virtualized core network (UC 5.2)

Summary: UC 5.2 is focused on the control plane of a software-defined infrastructure, where two VMNOs with their own virtual core networks (VCN1 and VCN2) share the same physical infrastructure. This is a multi-slice system, where each slice is deployed over a subset of the physical infrastructure. In this context, a network application that may demand the reconfiguration of the underlying resources underneath a given VCN should not conflict with the current configurations of the rest of existing VCNs. However, the network application must be traceable and validated before those are applied to the SDN controller and eventually to the physical network resources underneath.

Entities: VMNO.

Trust: Trust can be used in this use case to evaluate the level of trust between the network applications associated to each VCN and the SDN controller. Indeed, the SDN controller has to decide if it believes the policies sent by those network applications before it applies them in the resources in the data plane.

On the other way round, the network applications have to trust the SDN controller when it translates those policies into configuration on the data plane, due to the fact that the SDN controller could alter the configuration of the underlying resources belonging to other VCN and thus creating a potential conflict with other slices.

5.2.9 Reactive traffic routing in a virtualized core network (UC 5.3)

Summary: This use case is also focused on the control plane of a software-defined infrastructure, but it focused rather on the reactive forwarding of the network applications. One Virtual Mobile Network Operator (VMNO) has its own core network VCN1 where network traffic is reactively routed by network applications. Subscribers are roaming subscribers attached to VCN1. When subscribers demand access to the physical core network, at the beginning there are any matching flow rules in the data plane components and the network

application is triggered to install those rules. As described in the D2.1, these network applications reconfigure the flow tables of the switches by means of the SDN controller.

Entities: VMNO.

Trust: Trust can be used in this use case to verify that each time the SDN controller reconfigures the switches is on behalf of trusted network applications to prevent any attacker or malicious application is taking control of the SDN controller. Trust can also be used to check that the network applications are legitimate but also the SDN controller is legitimate.

5.2.10 Verification of the virtualized node and the virtualization platform (UC 5.4)

Summary: This use case is focused on the monitoring of the virtualized 5G network and of the virtualization infrastructure. A new MME is virtualized and runs on top of a virtualization platform provided by VIP (Virtualization Infrastructure Provider). The MME is a part of the VCN (Virtual Core Network) and a network slice. There is a certification system for virtualization platforms that issue “level 1 certification” to third party products.

A paramount task here is led by the certification system, where it checks and certifies the integrity of the external VNFs, such is the case of the MME implemented as a VN. This is where trust is so important.

Entities: VIP.

Trust: Trust can be used here to measure the VNF behaviour, because the VNF can send scaling notifications to its VNF Manager that may be influenced by an external attacker controlling that VNF. Another possibility is that the external VNF can be compromised to reprogram the SDN controller to delete all the paths on the data plane, or to inject fraudulent rules on the elements on the data plane.

5.2.11 Control and Monitoring of Slice by a Service Provider (UC 5.5)

Summary: A Service Provider has a contract with a VMNO for the VMNO to supply a suitable sub-slice (or a slice) of the VCN for the Service Provider’s customers to use. The Service Provider needs to be able to monitor the sub-slice to ensure that the VMNO is providing what is required by the contract, and also needs to be able to vary the parameters of the sub-slice within some predefined bounds as the service’s popularity changes. The SP may need more traffic capacity or better QoS at rush hours and the VMNO may or may not provide it.

Entities: VIP, VMNO, SP, subscribers.

Trust: The VMNO and the SP need a SLA that allows SP both to use, monitor and control a sub-slice of the VMNO’s network. Furthermore, at least the VMNO must trust the VIP. And the subscribers should trust the SP, as well as all other participants of the service chain.

5.2.12 Integrated Satellite and Terrestrial Systems Security Monitor (UC 5.6)

Summary: This use case is focused on the monitoring of broadband telecommunication systems or telecommunication ground user segments. Once registered, network components deliver to the security monitoring the indicators collected. Later, security monitoring uses active security analysis with these indicators in order to detect threats.

The Satellite Network Operator connects to the security monitor to check the systems status (e.g. fault management, performance monitoring) and, if needed, responds to the identified threats.

Entities: The entities implicated in this use case are the network operator who manage the satellite network services and resources, the service providers such as a mobile operator who is using these networks and the network components that compile and deliver security and business information to be effectively monitored.

Trust: The satellite network operator needs to trust the information collected by the satellite network components in order to perform the security monitor to check the whole systems status. Many of these components are resource-constrained devices, widely distributed and outside the direct network control so they may become easily compromised or untrusted. These devices may utilize a satellite or 5G air interface.

The service provider (i.e. a telecommunications company) has a contract with the satellite network operator to supply a suitable system capacity with a certain SLA (some QoS guarantees) to be used by its end subscribers. The service provider offers pre-paid/post-paid services and connects to the monitor to ensure that the satellite network operator is providing the required SLA towards the service provider and performs some control tasks (management of system bandwidth and power to optimize system efficiency, configuration of network components...). Trust can be broken and responsibilities have to be dissolved in order to pay penalties; depending upon the current legislation, the network operator may have financial and legal prejudice.

5.2.13 Satellite-Capable eNB (UC 8.1)

Summary: This use case encompasses the LTE-based Radio Access Network (RAN), the transport network (where introduces its main research novelties), and the Evolved Packet Core (EPC), also referred to as core network. This use case focuses on evolving the Transport Network Architecture (TNA) by combining both satellite and terrestrial transport architectures.

The main goal is the ability to offer resilience to cases of link failure. The satellite connectivity adds flexibility to backhauling networks. Also, this use case provides offloading capability via satellite to the backhaul network in case of congestion. The topology management objective is that no nodes in the mesh network are left un-connected, while covering all the needed area. Topology algorithm shall be based on user priority and bandwidth.

Entities: The entities implicated in this use case are the network operators who manage the satellite and terrestrial network services and resources, the service providers such as a mobile operator who is using these networks and the subscriber who signed up to the mobile operator services.

Trust: The network operator needs to trust the information collected by the network components (i.e. eNodeBs) in order to reconfigure the network topology in case of network failure or congestion. The subscriber/UE trusts the network operator that it provides privacy enhancing techniques in cases in which the network topology implies access to different eNodeBs that may demand unconditional trust. This is more critical considering disaster or congestion scenarios where network operator needs to interoperate among each other even if there is no pre-established agreement.

Also, trust can be used in this use case to verify that each time the Topology algorithm reconfigures the network is on behalf of ultra-reliable services to prevent any link failure or congestion (DoS).

5.2.14 Trust in alternative roaming (UC 9.1)

Summary: User is roaming in a visited network. The user is authenticated to the home AAA, once the home network has guarantee that the traffic is originating from a correct entity. The user needs to be sure that all the accounting information related to them is correct.

Entities: Visited network, home network, user.

Trust: The home network should have explicit information about the authenticity of the messages, i.e., it is not enough that the topology of the network would imply any authenticity. Otherwise spoofing of messages can occur and the messages cannot be fully trusted. The home network needs to trust the visited network to provide service to the user. Usually this happens through predefined roaming agreements, although the home network might still not know whether service was really given. If 5G is to provide more dynamic roaming agreement setting (e.g., the business models allow even smaller players to enter the market), where there is no pre-established agreement, then there need to be some external, common source to act as a trust anchor. Ultimately, there needs to be assurance of compensation and liability to motivate the establishment of the trust relationship.

The user also needs to trust the visited network to provide the service they are paying for. They also trust the home network to sort out any disagreements there might be regarding the level of service. Otherwise, user is unjustly billed. Similarly, user could try to make false claims about not using the service. If there are authentic accounting messages that are strongly bound to the identity of the user, then there is concrete evidence of what has happened.

5.2.15 Privacy in context-aware services (UC 9.2)

Summary: Either the visited network or the home network can share context information of the user with the content providers to provide better services. The user issues a privacy policy, which the visited and home network are expected to follow.

Entities: Visited network, home network, user, content provider.

Trust: The user trust that the visited and home network follow the privacy policy of the user regarding the disclosure of context information. Also, content provider should not further disseminate the content information to additional parties, if not explicitly allowed to do so. If the policy is not honoured, then the privacy of the user is endangered. The user trusts societal controls, e.g., regulators, to enforce proper behaviour through sanctions. It is another thing, though, whether these controls can be applied consistently across different entities if, for instance, the visited network resides in a different region.

5.2.16 Trust in network elements (UC 9.3)

Summary: Unauthorized device or network function is installed into the visited network. Due to unpatched vulnerabilities it is able to compromise other nodes inside the network. The home network of the user notices irregular behaviour and notifies the visited network about potential breach.

Entities: Visited network, home network, user.

Trust: The home network ought to be able to trust that traffic coming from other networks is legitimate. In essence, it is expected that the networks are operated with due care and proper physical security measures are followed. Thus, one should not just trust the network boundaries for protection, but also take into account the zero trust concepts presented earlier. If the other network is breached, then the user or other traffic might be spoofed. If the home network does not implicitly trust the traffic coming from the visited network, then the home network might detect the malicious attempts.

5.2.17 Trust in botnet mitigation (UC 10.1)

Summary: The mobile phone of the user is breached and malware is installed. The adversary can remotely control the phone and send premium SMS messages.

Entities: User, phone, home network.

Trust: If the home network provides the anomaly detection capability (perhaps for an added price), then the user trusts the home network to notify (and possibly prevent) the user about any unauthorized actions. Generally, the user might also trust the phone to stay intact (perhaps due to manufacturer branding the phone as secure), but user's own actions can lead to the compromise.

5.2.18 Privacy Violation Mitigation (UC 10.2)

Summary: This use case is focused on the mitigation of privacy violation risks as a result of applications' activities on the users' phones. Mobile devices and the installed applications disclose a large amount of private information both personal and device related information. There are many misbehaving apps, PUAs (Potentially Unwanted Applications), adware and ransomware, and spyware is not so uncommon even in official app stores. Currently the mobile network has no means to protect the user's privacy at the application layer. This exposes the subscriber to threats like location tracking and comprehensive profiling where data about movement, usage, etc., of a subscriber is amassed and linked to his/her identity to enable various attacks at a later time.

Entities: user, UE, mobile network, mobile application, mobile application developer, mobile application store.

Trust: in this scenario the user trusts the application running on her/his device, and indirectly the application developer and the application store. The user assumes that the application behaviour is the legitimate one and also that all permissions requested by the application are necessary for its correct execution and are not used to harm the user's privacy, the device and/or ultimately the network and other network users if the malware propagates.

The trust can be broken since the risk of a privacy violation from malware and misbehaving apps is real, and may lead to, for example, user identity spoofing, user diminishing the use of mobile services (also due to possible device abuse) and, in some cases, user distrusting the MNO as well. For MNOs, such situations can also lead to client churn.

If needed, the type of trust required in this use case can be ensured through technical solutions (e.g. privacy policy configuration and verification implemented on device and on application servers) in addition to application ranking already present on some stores and application security mechanisms provided by the underlying mobile operating system.

5.2.19 SIM-based and/or Device-based Anonymization (UC 10.3)

Summary: This use is focused on the mitigation of privacy violation risks at the source of privacy sensitive information. Mobile devices through the installed applications disclose a large amount of private information both personal and device related information. Currently the mobile network has no means to protect their users' privacy at the application layer. This exposes the subscribers to threats like location tracking and comprehensive profiling where data about movement, usage, etc., of a subscriber is amassed and linked to his/her identity to explore various attacks at a later time.

Entities: app ecosystem (marketplace or service provider and app developer), user/UE, device manufacturer, mobile OS provider.

Trust: in this scenario the user need to trust the entire application ecosystem that is the marketplaces or service provider offering the application and the developer of the application. For the first aspect the level of trustworthiness of the marketplace application provider is based on the security controls put in place to ensure that applications are not infected by malware. In particular the adoption of vetting process, during which each app is tested to ensure that it doesn't crash in any obvious way and that it conforms to all the appropriate application store rules, increases the trustworthy the user have towards marketplace. Also the adoption of analyser tools on the app's binary code, to see whether it makes use of private functionality that is normally off-limits to developers, implicitly contributes in building user's trust in the application developer in terms of compliance to the software development guidelines. Finally, in some cases, security mechanisms like application signing provides to the users a way to verify the integrity of the downloaded application.

In this trust model not only the application ecosystem is relevant but also the trust the user have in the UE both in the device manufacturer for firmware security, and, in particular, on the mobile OS security model in terms of permissions model implemented, vulnerabilities management process and built-in security controls like application isolation in a virtual "sandbox" that the operating system creates for it.

Even with the adoption of security measures in the different part of the trust chain, data leakage occurs very commonly showing that the trust model should be reviewed. Most of the times users ignore applications asking permission to access personal info or they do not pay much care since they might not have much other options if they need to use the application. The risk of this model is that mobile apps can leak information to external sources by sending out device ID (IMEI/EID), contacts, location, etc.

The trust can be broken and may lead to, for example, user diminishing the use of mobile applications (also due to possible device abuse) and, in some cases, distrusting the mobile app ecosystem (app developer, app store) and the MNO as well. For MNOs, such situations can also ultimately lead to client churn.

If needed, the type of trust required in this use case can be ensured/guaranteed through technical solutions (e.g. configurable format preserving anonymization techniques implemented on device) in addition to application security controls already performed by application stores and to security mechanisms built in the mobile OS.

5.2.20 Trust in Lawful Interception in dynamic 5G Network (UC 11.1)

Summary: Lawful Interception is still a requirement imposed to mobile operators through the different mobile network generations. Regardless the target entity, user or service, and the technologies used in the construction of the mobile network (e.g., SDN, NFV or virtualization), a mobile operator should be able to answer any legitimate interception. It is as follows. The Law Enforcement Agency (LEA) identifies a suspected user to be surveyed (e.g., Bob). The LEA retrieves an authorization from the court of justice to perform the interception of the Bob's communications. This authorization is sent to the designated service of the mobile operator. After checking the validity of the authorization, the mobile operator instantiates and activates the LI network function. This latter delivers the required information to the LEA.

Entities: This use case involves four entities: the law enforcement agency that would like to intercept a suspected user communications, the court of justice which delivers the lawful interception authorization, the mobile operator which will perform the interception and end-users (e.g., Bob).

Trust: In this use case, we have two “levels / types” of trust: trust between entities (i.e., LEA, mobile operator and user) and trust within the mobile network (mobile operator, LI function and network infrastructure). Thus, users must trust the mobile operator that it enables the confidentiality and integrity of their communications and will enable only legitimate interception. The LEA must also trust the mobile network that it will deliver correct information (i.e., delivered data are about the designated user and are not corrupted). Within the mobile network, the mobile operator must trust the LI function that it exactly delivers the required information (i.e., data about the designated user) and only and only if it is triggered by the mobile operator (i.e., no one else can initiate an interception). Moreover, the mobile operator needs to trust the infrastructure on which the LI function is running. Note that trust within the mobile network is not only associated to the LI use case but it is network-related.

The first level/type of trust is usually formalized through agreements between the entities. The second can be realized through effective solutions such as attestation of the infrastructure integrity, signature verification and so forth.

If the LEA or the user trust towards the mobile network operator is broken, the mobile network operator may have financial and legal prejudice. If the mobile network operator trust about the LI function is broken, this means that a technical issue has been detected. Therefore, he (i.e., the mobile network operator) should quarantine the LI function till he performs technical tests and fixes the bugs.

5.2.21 Trust in End-to-End Encryption for Device-to-Device Communications (UC 11.2)

Summary: One of the main goals of mobile operators is to ensure the protection of their users’ data that transit through the mobile network. Moreover, in 5G, users’ privacy is fundamental. In this context, a 5G mobile operator can offer a new encryption service to the users. The service would enable two users to have end-to-end encrypted communication. This service should preserve user’s privacy while enabling lawful interception requests. The service is as follows. Alice and Bob are subscribers to the network end-to-end encryption service. Alice is connected to the 5G network (it has been authenticated). Alice, with the help of the network operator, negotiates a session key with Bob. If LEA wants to intercept Alice communications, the LEA, the mobile operator (provider of the encryption service), the court of justice and may be other entities collaborate to retrieve or reconstruct the session key. Only one entity should not be able to retrieve or reconstruct this key. This operation needs at least the cooperation of the LEA, the mobile operator and the court of justice.

Entities: The entities involved in this use case are the same in as the previous one, i.e., the law enforcement agency that would like to intercept a suspected user communications, the court of justice which delivers the lawful interception authorization, the mobile operator which will perform the interception and end-users (e.g., Bob).

Trust: In this use case, similarly to the previous one, users need to trust the mobile operator. Given that the service is developed / offered by the mobile operator and that it is a key-escrow-like service, users need to trust that the mobile operator developed a system that requires at least k agents to retrieve / reconstruct the session key. This kind of trust can be formalized by the contract conducted between the user and the mobile operator as an encryption service provider.

If users trust as regards the encryption service provided by the mobile network is broken, users may stop using this service.

5.2.22 Summary

The use case analysis presented above reveals some interesting challenges for trust in 5G networks.

Additional complexity is introduced through new actors bringing new trust relationships such as that between an application service provider and the MNO (5.2.2), a WSN operator or IoT provider and the access network domain (5.2.5, 5.2.6), a VIP and a VMNO (5.2.7) or satellite operators (5.2.1, 5.2.12, 5.2.13).

Compared to 4G networks, there are new qualities that a trustor relies upon (trusts another entity to provide) such as a defined quality of service (5.2.7, 5.2.11, 5.2.12), and new attack vectors afforded by virtualisation technologies that trustworthy operators must monitor and/or prevent (5.2.10).

Finally, several use cases present ideas about how 5G networks can improve on trust issues which are present in 4G networks, particularly privacy (5.2.15, 5.2.18, 5.2.19) including lawful interception aspects (5.2.20, 5.2.21) but also the users' trust in their network and device (5.2.14, 5.2.16, 5.2.17).

6 Trust Model

6.1 The Role of Privacy

According to [Seigneur 2004], there is an inherent conflict between trust and privacy since the more we trust the system, the more information we risk revealing. For the system, it is required to have measurable trade-off between privacy and trust depending on the nature of services. Seigneur and Jensen propose the use of pseudonymity mechanisms for formation of trust without exposing privacy sensitive information. In the context of mobile networks, related pseudonymity mechanisms are used to protect subscriber privacy.

We describe the interplay between trust and privacy in different domains of the current mobile network architecture. In particular, we refer to the formal domain model as described in Section 5.1.1 and outline risks of each domain with respect to their trust.

In access network domain, the user privacy information is protected using pseudonymity mechanism in the form of TMSI. However, recent attacks [Shaik 2016], [Engel 2014], [Stevens 2014] and incidents [NSA] question whether mechanisms used in the access network domain are sufficient to balance the trade-off between trust and privacy. For example, due to the fact that base stations are treated as trusted elements in 4G networks, compromised base stations pose privacy challenges to mobile subscribers [Shaik 2016]. In addition, the mobile device (in particular the baseband operating system) is trusted during the communication with base stations. Golde's research work raises privacy issues originating from modified baseband software [Golde 2013] in current networks. Research results from [Borgaonkar 2013] and [Golde 2013] demonstrate the need to re-structure the trust properties of elements such as User Equipment and base stations.

In the infrastructure domain, the home and serving networks are trusted domains. A trusted interconnection between these two network domains is necessary for international roaming purposes. However, trust in this interconnection interface raises severe privacy concerns regarding mobile subscribers [Engel 2014]. In addition, trusted access via an API is provided to third parties for certain types of services in the core network domain, for example Home Location Register (HLR) lookup. This implied trust in HLR lookup services also raises privacy questions.

For 5G networks, a new formal domain model based on [3GPP 2015] will be presented in the 5G-ENSURE D2.4 report. In this model, the infrastructure domain will be divided into several sub-domains to support new 5G services. To deliver the services, each trusted domain and sub-domain may not be controlled by a single stakeholder. Hence in order to protect privacy aspects in these trusted domains, anonymity mechanisms such as those described in [Gramaglia 2015] and [Montjoye 2013] are necessary. In particular, these anonymity mechanisms are applicable to subscriber identities and data which could be stored or transmitted in each trusted domain.

Current mobile networks satisfy four fundamental security aspects: authentication, integrity, confidentiality, and availability. However, privacy aspects are not considered from the architectural point of view. With the nature of 5G network services, we believe that new architecture may consider privacy aspects such as unobservability, anonymity, unlinkability, and pseudonymity. These privacy aspects increase the level of trust among different domains as well as between the subscriber and the service provider. Because of lawful interception and regulatory needs, not all privacy properties could be addressed in the architecture. However, as stated in [ETSI], privacy in some trusted 5G network services could be a desirable marketing option.

6.2 Proposed Approach

6.2.1 Trust model requirements

It is not yet feasible to construct a comprehensive trust model for 5G networks. There are several reasons for this, including:

- there is no well-defined trust model in 4G networks, though we have made a start on this in Section 4 and below;
- there is no comprehensive analysis of risks (to which trust is one possible response), as the first draft analysis of risks (D2.3) was prepared in parallel with this report and does not cover all use cases;
- the trust model also depends on the 5G security architecture which has yet to be formulated – it is covered in D4.1 which is due 4 months after this report.

The main purpose of the draft trust model at this stage of the project is therefore to propose how the trust model can be constructed, based on the analysis of the state of the art, the implicit trust model used in 4G networks (as discussed in Section 4), and the ways in which the trust model should be used.

The 5G-ENSURE trust model should allow stakeholders to answer the key questions about trust, as discussed in the definition of the term ‘trust model’ at the end of Section 2:

- In whom (or what) does one trust?
- For what does one trust, i.e. what is it the trustor expects from the thing(s) they choose to trust?
- How much should one trust?
- How much does anyone trust?

However, one can look deeper into these questions by examining the context in which they may be asked. At this stage it seems clear that there are three main cases of interest at different points in the lifecycle of an operating 5G network. These are discussed below.

Verification of the trust and trustworthiness properties of the 5G architecture: to understand how secure the architecture will be, and how this depends on the trustworthiness (and trust) of the stakeholders or their

machine proxies. This can be done by identifying and analysing potential threats to systems based on the 5G-ENSURE secure architecture, and capturing the need for countermeasures. This is something we wish to do during the second half of the 5G-ENSURE project, to track how far the architecture and security enablers devised by 5G-ENSURE help to manage security risks. Of course, this early work on trust models and the related work on risks in D2.3 will inform the design of the other 5G-ENSURE enablers and architecture and should result in risks being reduced.

Identification of risks and trust dependencies during the design of a 5G service proposition: to understand what might go wrong in a specific scenario, e.g. providing a remote surgery service using a network slice with high guaranteed levels of service, or automobiles with built in entertainment services, etc. This can be done by mapping potential threats onto the specific system under consideration, to find out where and how those threats might arise in that system. This is something designers of systems to deliver such a proposition will want to do, so they can determine which risks are likely to be acceptable to users, and which must be mitigated in other ways by introducing security to increase trustworthiness, or by devising business models in which risks are transferred to stakeholders who can cope with the consequences.

During operation of 5G services: to estimate the trustworthiness of system components (including system stakeholders) so decisions can be made over which components to trust. This can be done with respect to the design-time model of threats to that system, by detecting which countermeasures are deployed in the running system, and combining this with evidence from the behaviour of system components to assess their trustworthiness. This is really about using machine trust models as mechanisms for managing the network, or for providing guidance to human users over when and how they can trust the network.

We now consider how the trust model should address each of these points.

6.2.2 In whom (or what) does a trustor trust?

This first question is relatively easy to answer, at least in a naïve fashion. The trustor obviously trusts a subject or trustee, the person or thing that must meet the trustor's expectations if the trustor is to have a favourable outcome (i.e. the one they expect, and in which they are placing their trust). However, as we see from the analysis of trust in 4G networks from Section 4, even in an established architecture it is not immediately obvious who is trusting what. To provide a starting point, the trust relationships described in Section 4 have been analysed. It is immediately apparent that some trust relationships are acknowledged and even in many cases defined in contracts, while others are not, as shown in Figure 13:

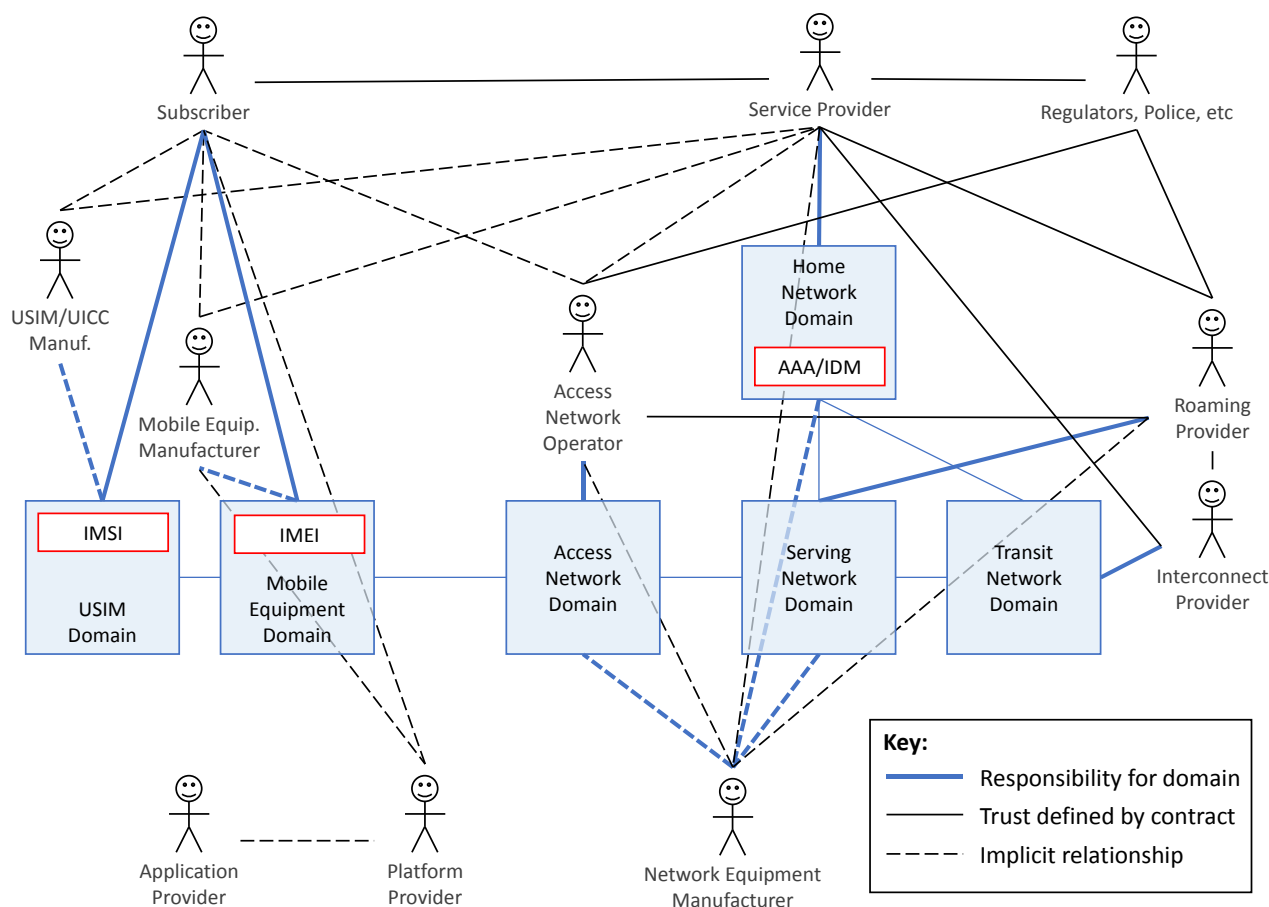


Figure 13. Explicit and Implicit Trust in 4G Networks

Figure 13 is actually a simplified view of trust relationships in 4G networks, as some of the stakeholders have been merged or omitted for clarity, and the domains have not been decomposed into specific components except to show the identity management, AAA and identity key elements related to trust in the subscriber's identity when they use the network.

Focusing on the Subscriber, it is clear that they have a contract with their Service Provider and to some extent this recognises their interdependency and defines what each expects of the other. If both are trustworthy, they will behave in accordance with their contract. If one is untrustworthy, the contract may provide some redress for the other, depending on how the untrustworthy party misbehaved. The fact that there is a contract shows that a trust relationship exists and has been acknowledged even if the parties don't refer to it as such. The terms of the contract also define some of the expected behaviour, e.g. that the service provider will meter the Subscriber's use of the network and bill according to some agreed formula, and that the Subscriber will pay the bill and use only approved equipment to connect to the network, etc. Note, however, that contracts rarely provide a complete specification of a trust relationship, as they only cover aspects over which the parties can agree – usually those that the trustor needs to have formally acknowledged before entering into a relationship, and those for which the trustee is willing to provide compensation if they fail to meet expectations. (Compensation is itself a complex notion, which in some cases is designed to encourage trust rather than to mitigate an adverse outcome).

As noted in Section 4, the Service Provider doesn't actually trust the Subscriber to authenticate themselves. They rely on the IMSI stored in the USIM domain for this, and may also correlate the IMSI and IMEI to help detect spoofing attempts by or against the Subscriber. This means both the Service Provider and the Subscriber are trusting in the manufacturers of the USIM and ME domain equipment. At least in the Subscriber's case there is no contract and possibly no recognition of this implied trust relationship. Other such (usually implicit) dependencies on equipment manufacturers also exist, as shown in the diagram. In most cases, equipment operators are responsible for its behaviour, but manufacturers have some limited responsibility. For example, if a manufacturer supplied equipment knowing it to be defective, they would be considered responsible. In the field of ICT, suppliers usually seek to transfer responsibility for undiscovered defects to the operators via EULA terms.

Some of the other trust relationships are recognised and reflected by the presence of contracts. For example, the Service Provider will have roaming agreements with other providers allowing the Subscriber to connect through their network domains. Both the Service and Roaming Providers will have agreements with providers of interconnection services allowing them to route communications between their domains. The Serving Network Provider (at least) will need an Access Network through which the Subscriber connects, and will have an agreement with whoever operates the Access Network, if they don't do so themselves. Satellite communication networks are usually provided in this way by separate satellite operators, for example. Regulators and law enforcers may also have formal agreements with service providers, e.g. in the UK there is an agreement between mobile network operators and the government specifying what communication data should be retained, and how this may be accessed in certain circumstances. Lawful interception of communication content is usually defined by statute rather than in bilateral agreements.

Diagrams like Figure 13 can be used to describe the trust between stakeholders (humans or organisations run by humans). Where contracts exist these may specify what expectations the trustor has of the trustee, although contracts normally only cover the cases where the trustee accepts some liability should they fail to meet those expectations. However, many trust relationships are implicit and may not even be recognised by the trustor and trustee. And in practice, the primary expectation is that the trustee will provide or operate technology components that behave as they should.

In 5G networks, we expect two things to change:

- 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 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.

At this stage it is difficult even to enumerate the stakeholders and trust relationships in a 5G network. One side effect of virtualisation 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-ENSURE trust model should recognise a set of roles that stakeholders might take, based on the 4G actor model above plus some new roles such as Virtual Infrastructure Providers, Virtualised 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 then reasonable to suppose that stakeholders will want to define their roles and responsibilities to each other via Service Level Agreements, given that these responsibilities may vary depending on the scenario. To formulate such agreements it will be important to capture expectations and the ways in which things could go wrong.

6.2.3 For what does a trustor trust?

6.2.3.1 *Trusts and Risk Acceptance/Avoidance*

As noted in Section 2, trust is really one of the possible responses to a potential risk (risk acceptance), alongside other responses (risk avoidance or distrust, risk transfer, or risk reduction by means of security measures). A trustor is really someone who believes¹ that certain risks will not arise or (if they do) will not cause them undue harm. To capture what the trustor is really assuming, it is necessary to understand what risks are present, and which of those risks the trustor is accepting.

We propose that the 5G-ENSURE trust model should be based on the most comprehensive and rigorous model of risks that can be constructed, following the approach used in the FP7 OPTET project based on machine understandable models, as described in Section 3.3.3. This approach is also well suited to the agile, configurable nature of virtualised 5G networks because it is based on identifying generic types of asset, threats, consequences and countermeasures, and then deriving potential threats in a given situation by mapping knowledge of the generic archetypes onto a specific system configuration. To give a simple example of this, one might identify two generic related asset types:

- Service: an asset that responds to requests by carrying out actions;
- Client: an asset that initiates requests to a Service.

If a Client ‘uses’ a Service, it means that particular Client initiates requests to that particular Service. In many situations the Service needs to know which Stakeholder controls the Client, so its action can be correctly attributed and billed, and so confidential information from the Stakeholder is not released to a third party.

An attacker might seek to impersonate a Client in order to get the service without paying, or to gain access to confidential information. These attacks can be represented as generic threats. In this simple example, the Impersonation threats could be countered if the Service implements client authentication (i.e. verifies the identity of the Client before taking a requested action), and the Client has a verifiable form of identification such as a username/password, or a PKI identity certificate, etc. In a specific system, one might choose to address a risk by implementing such countermeasures. This knowledge can be captured by encoding it as semantic relationships, as shown in Figure 14.

¹ But see Section 6.2.5 below.

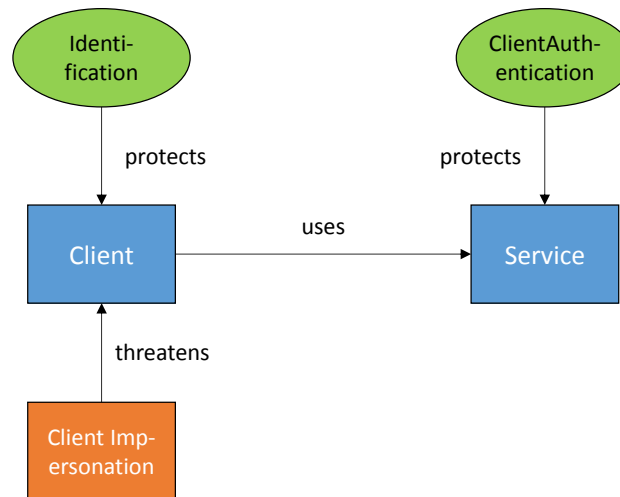


Figure 14. A Machine Understandable Generic Threat

Risk transfer can also be modelled as a form of ‘countermeasure’, which doesn’t prevent the threat but shifts the impact (e.g. to the Service). Whether this makes sense depends on the impact of a threat, e.g. if the threat leads to the disclosure of personal data relating to the Stakeholder controlling the Client, this impact can’t be transferred to the Service. The best the Service Provider can do is to compensate the data subject.

As discussed in Section 3.3.3, the approach developed in OPTET involves capturing patterns like those from Figure 14 in a machine understandable knowledge base, so they can be automatically mapped onto a given system or scenario. Wherever one asset ‘uses’ another in that system or scenario, a potential risk from Impersonation threats must be present. By automating the mapping procedure, one can reliably identify all foreseeable threats (i.e. threats included in the generic knowledge base), and determine countermeasures that could be used to reduce the risk arising from each type of threat. It should then be easy to determine which risks have been reduced or transferred. The remaining risks must then be accepted or avoided by the relevant Stakeholder, i.e. a trust decision must be made whether to use the system (or parts of the system) to which the associated threats apply.

6.2.3.2 Types of threats

As shown in Figure 13, in a 5G (or 4G) network, trust relationships exist between Stakeholders, but in most cases the trustor is trusting technology assets for which the trustee is responsible. Thus the Service Provider trusts the Subscriber to use only compliant equipment, while the Subscriber trusts the Service Provider to protect their data in the Home Network Domain, and to make arrangements for adequate and trustworthy coverage by Access Network Domains. Unfortunately this makes the business of identifying threats quite difficult, because one must consider a wide range of possible ways in which the trustworthiness of the equipment (hardware and software) might fall short of expectations.

It makes sense to distinguish several broad classes of potential threats:

- Malicious stakeholders: threats representing the possibility that one Stakeholder may act against the interests of another;
- Non-malicious actions: threats representing possible adverse consequences caused inadvertently by the action of Stakeholders or their technological proxies, including user errors.

- Malicious attacks: threats representing the possibility that technology operated by a Stakeholder may be subverted by an external attacker, and made to act against the interests of the operator or some other Stakeholder.
- Internal failures: threats representing faults in systems or processes that may arise without external cause, but which may degrade the system to the detriment of one or more Stakeholders.
- External disasters: threats representing damage from non-malicious external causes, such as natural disasters. These threats usually cannot be prevented, but mitigation of the consequences may be possible and in some cases desirable.

To this we should add two more classes of threats:

- Threats to stakeholder trust: representing the effect of adverse experiences on the stakeholder's propensity to continue trusting and using a system.
- Threats from stakeholder distrust: representing the effect on the system should a stakeholder lose trust and withdraw from the system.

Examples of these last two broad classes were found in FP7 OPTET when analysing threats to a proposed Ambient Assisted Living system to support elderly patients. In that case having too many false alarms was identified as potentially reducing the trust of carers, and that distrust may lead to them failing to respond to a genuine alarm. In the context of 5G networks, similar problems might arise if an ad-hoc rural access network provider experienced a high level of attacks from malicious devices, and this led them to withdraw service in an area where no other access networks were operating. From a trust modelling perspective, these last two classes of threat are very significant, because they relate directly to trust decisions and their consequences.

6.2.3.3 Security choices and trade-offs

It will be important to capture trade-offs between security properties of the 5G-ENSURE architecture or supported 5G application scenarios. As noted in Section 6.1, there is an inevitable trade-off between the need for mechanisms to protect privacy and the need to support lawful interception of communications and also lawful access to communications data.

Many privacy concerns can obviously be captured by modelling threats to privacy. These will mostly be concerned with unauthorized access to personal data via management services like HLR lookup services, interception of personal data such as the location of individuals, or propagation of personal data in communication context information that may be accessible to applications. These threats can then be analysed and addressed in a given architecture, scenario or application.

However, other trust issues may exist that conflict with privacy, and these could also be captured in the form of potential threats. For example, subscribers may expect that if their child goes missing, they can be traced by inspecting communication data generated by their interactions with the mobile network. Failure to meet these expectations would be a threat to trust, though not explicitly to privacy. The relevant countermeasure would be to retain communication data generated by some of the technology components in the network.

To do this, one will certainly need additional services that have privileged access to monitor assets involved in transfer of communication content or generation of communication metadata. These services should allow access by authorised agencies to the real-time monitoring streams or to previously stored communication data. Obviously, threats to privacy will then exist representing unauthorized access to these services – in fact making these services highly secure should be a major concern for architects and implementers.

In specific scenarios it may make sense to provide more or less of this monitoring, based on the expectations of users, to minimise potential threats to privacy while ensuring the network behaves in ways its users would consider trustworthy.

6.2.3.4 *Enumeration of threats*

To use this approach, one must find a way to enumerate potential threats representing the possible causes of adverse user experiences. Some of these threats are evident in the analysis of selected use cases described in Section 5.2, but this will only find some of the possible threats even when extended to cover all the use cases from Deliverable D2.1. It is therefore important to understand how such a threat catalogue could be created. It turns out that different sources of information are available for each of the broad classes of threats identified above, and the largest number of threats arise from malicious attacks, where fortunately there is a large corpus available for analysis.

Malicious stakeholder threats: in 5G networks are likely to be covered quite well by the analysis of use cases from D2.1, plus additional scenarios that may be identified during the project. To become a stakeholder in a socio-technical system, one must adopt a legitimate role with respect to that system, so malicious stakeholder threats normally arise where there is a potential conflict of interests, e.g. between the Subscriber's desire to use a service and the Service Provider's requirement that they be paid for the service. A typical threat may involve a Subscriber seeking to defraud the Service Provider to get some services without paying. These types of threats will provide a basis for modelling U2U trust (between stakeholders), and help 5G stakeholders determine what issues should be addressed through service level or subscriber agreements.

Internal failures and non-malicious actions: these types of threats represent error conditions. They arise because they were not foreseen during the development of a system, in the sense that errors that are foreseen are usually eliminated during the system implementation phase. Because the specific bugs or user errors are unforeseen, the most important issue for a threat modeller is to capture their consequences and potential measures to mitigate these consequences. It is relatively easy to classify such threats in those terms, e.g. by considering whether the error leads to a compromise in confidentiality, integrity or availability in the affected system or component.

External disasters: are also relatively easy to classify in terms of their effect on the integrity or availability of the affected system(s) or component(s). From a trust perspective, the most relevant threats are localised threats affecting particular parts of the network, e.g. if a data centre is disrupted by fire or flood. Larger scale disasters producing widespread disruption are less relevant, unless one is analysing a 5G-based network to support emergency responders. This is due to the fact that large scale disasters are rare, few stakeholders would expect non-emergency services to continue working in such a disaster, and that wouldn't be their immediate concern anyway.

Malicious attacks: are very relevant, because malicious external cyber attackers certainly do exist, and have motives that may lead them to attack 5G networking infrastructure or vertical applications. As discussed in Section 3.3.3, it is very difficult to identify potential threats in a given system. However, existing risk analysis methods can be used to compile a knowledge base of generic threats, which can then be mapped onto a given system by using machine reasoning algorithms. The most complete knowledge bases available today focus on software-centric threats, such as the Common Vulnerabilities and Exposures (CVE) database of software vulnerabilities [Mitre-1], and the Common Weakness Enumeration (CWE) taxonomy describing common classes of programming errors that lead to vulnerabilities [Mitre-2]. The Common Attack Pattern Enumeration and Classification (CAPEC) describes common elements used in attacks [Mitre-3], and though

mainly concerned with attacks involving software vulnerabilities, it also provide some analysis from an attacker-centric perspective. As a starting point, we will consider the CAPEC catalogue to identify generic classes of threats that are relevant in 5G networks. Of course, new threats may arise that are specific to 5G networks, so these will also need to be added to the 5G-ENSURE knowledge base as and when they are discovered.

Software centric threats are of course best addressed by eliminating vulnerabilities early in the lifecycle of any ICT-based system, during the design and implementation stages. One should of course address other types of threats at this stage, if possible, e.g. to reduce by design the opportunities for social engineering or malicious abuse of system functionality. The 5G-ENSURE trust (and risk) model should support this process by making it easier to identify common types of threats during design time, so they can be taken into account when devising the system architecture (e.g. using a different design pattern might avoid some risks altogether), and implementing hardware and software components (e.g. by specifying that programmers must check for certain types of security bugs or other weaknesses and if necessary certify that they aren't present up to some ISO 15408 Common Criteria EAL).

The resulting model can then also be used when operating the system at run time, by (a) indicating whether that type of threat is potentially relevant given the architecture and specific configuration of the system at that time, and (b) capturing whether countermeasures were introduced during the design and implementation, ideally by referring to security certification under ISO 15408. There may also be other countermeasures that could be used, e.g. preventing remote access to an asset where it isn't certified to be free of such a vulnerability.

The presence (or absence) of relevant countermeasures then provides a starting point for assessing how trustworthy a system or component is likely to be with respect to threats that are of concern to the trustor. This brings us to the question of how the concepts of trustworthiness (and trust) can be quantified.

6.2.4 How much should a trustor trust?

Estimating the trustworthiness of a system or one of its (technological or human) components is obviously an essential step if trust decisions are to be made on a rational basis. Section 3.2 provides a good overview of how this can be done to support machine trust, i.e. automated trust decisions by technology components. In essence, machine trust models are based on algorithms for computing trustworthiness using information from three sources:

- prior expectations about the trustworthiness of the components;
- first-hand evidence from previous interactions with those components; and
- second-hand evidence based on reports from the interactions of those components with other entities.

A typical algorithm will combine these inputs to get a trustworthiness estimate using something like:

$$T = \frac{p_0 + p_1 + p_2}{(p_0 + n_0) + (p_1 + n_1) + (p_2 + n_2)}$$

where $\langle p_1, n_1 \rangle$ and $\langle p_2, n_2 \rangle$ represent the number of positive and negative outcomes from previous first- and second-hand interactions, and $\langle p_0, n_0 \rangle$ represents an initial expectation that n_0 out of every $(p_0 + n_0)$ interactions will be negative. As noted in Section 3.2, one may need to apply weights to the outcome of each previous interaction, based on how recent it was, and how trustworthy the source is for second-hand reports.

The value of T in the above formulation clearly tends towards the proportion of interactions that produce successful outcomes, i.e. the probability that a randomly chosen interaction is successful. Weighting schemes alter this interpretation slightly, but the idea of using weights is to make T better approximate the *current* likelihood that the *next* interaction *with the trustor* will be successful. The weights are designed to increase the significance of recent over ancient interactions, and adjust for the fact that second-hand reports may be less trustworthy or simply less representative of what would happen in interactions with the trustor.

This interpretation is extremely useful, because it lends itself to a statistical quantification of the models of potential risks (i.e. adverse outcomes) proposed in Section 6.2.3. We can assert that the trustworthiness of a system (or component) with respect to a given threat is the probability that the threat will not arise in the next interaction with the trustor. Once generic threats have been mapped onto a system, one only needs to attach the best estimate of this probability to each (mapped) threat. This goes well beyond the way models of the types proposed in 6.2.3 were used in the OPTET project, but it is fairly clear how the OPTET approach can be extended.

For example, an initial trustworthiness expectation encoded in the pair $\langle p_0, n_0 \rangle$ for each threat could be based on whether or not security measures to reduce the risk from that threat are present. Taking the example from Section 6.2.3.1 above, if a Client does have a means of identification and its Service does use client authentication, then the ratio $p_0/(n_0 + p_0)$ for the threat of that Client being impersonated to that Service should be rather higher than if either measure is absent. The presence of security measures can be thought of as contributing to p_0 rather more than to n_0 . This can easily be combined with contributions representing other factors representing human factors for U2U trust or default settings for M2M trust. Of course, the stronger the security mechanism, the greater the ratio of its contribution to p_0 over $(n_0 + p_0)$ should be. The total contribution to $(p_0 + n_0)$ should reflect the reliability of that ratio, as the higher it is the more interaction reports or other contributions will be needed to shift the value of T .

Of course, a trustor's assessment of trustworthiness is rarely based on a single threat. But a statistical interpretation makes it relatively easy to combine contributions from multiple threats, and understand how the algorithms used reflect assumptions about the system. At this stage we propose a very simple approach, in which overall trustworthiness is the product of threat contributions, i.e.

$$T_A = \prod_i T_i$$

where T_A is the overall trustworthiness of a system or component, T_i is the trustworthiness with respect to threat i , and the index i runs over all the identified threats involving that system or component. This approach is equivalent to assuming that:

- all potential threats are independent of each other, in the sense that the occurrence of one threat is not correlated with the occurrence of any other threat; and
- all threats are equally important to the trustor.

In practice, neither of these assumptions is strictly correct, so the 5G-ENSURE model will need to be refined beyond this simple initial idea. Some threats represent knock-on consequences from the misbehaviour of one asset on other assets with which it interacts. Those threats are clearly not statistically independent of threats representing causes of misbehaviour in the first asset. It is also possible for some primary threats (those representing root causes of disruption) to be correlated, e.g. if they represent malicious attacks that

are likely to be used by the same attacker. OPTET developed an approach for modelling knock-on consequences as ‘secondary threats’, so it should be possible to identify some threats as ‘secondary’ and use a different method for including their trustworthiness estimates in the overall total. The most general approach would be to use a Bayesian network to combine (possibly correlated) trustworthiness values from different threats. This could complement the idea of using Bayesian networks to compare trustworthiness for different systems or components as discussed in Section 3.2.4.

It is also clear that all threats are not considered equally important by a trustor. We know that trustors will most likely rate threats according to their potential impact on the trustor. This suggests that we don’t need to assign an importance factor to every threat, but only to the secondary threats to stakeholder trust representing outcomes that may concern them. The trustworthiness of a system or component with respect to those threats would first need to be assembled by combining contributions from the possible root causes. Then a decision must be made on how to combine the resulting values based on how important each outcome would be to the trustor. One approach used by economists is to compute the expectation value of the overall impact, where the impact is positive for a positive outcome, and has a different negative value for each of the potential adverse outcomes represented by individual threats. This will be explored in the next period, and a suitable formulation included in the updated trust model described in Deliverable D2.5.

6.2.5 How much does a trustor trust?

The hardest thing to quantify in any trust model is this – the question of how much trust exists. As noted in Section 2, trust is actually a trustor’s subjective belief that a trustee (a person or thing) is trustworthy. It is in principle impossible to measure the strength of a subjective belief at the time it is formed and used to make a trust decision. One can only ask people in advance whether they would be trusting in some situation, or infer afterwards from their behaviour whether they did decide to trust. One can also correlate their trust stance with other factors such as their age, gender, cultural background, education or wealth, or features of the situation such as the trustee’s reputation or the trustor’s previous experience of similar situations.

This type of analysis is often used by social scientists to uncover (through correlation) the factors that might lead someone to trust in something. It can also provide a reasonably good prediction of how likely it is that a trustor will do so. This prediction is valid only for a population of potential trustors, for which the observations on which it is based are representative. The prediction is actually for the probability that if someone were chosen at random from that population, they would turn out to be a trustor. That isn’t the same as the probability that a given individual would decide to trust, but it is a reasonable measure of the level of trust in a population of users, which is often what system designers and operators need to know.

If we take this as our measure of trust, how does it relate to the measure of trustworthiness described above, or to the concept of human trust discussed in Section 3.1?

The main advantage of defining our measure of trust in this way is that it can be directly related to the measure of trustworthiness as described above. The trustworthiness measure is the likelihood that a trustee will meet the expectations of a trustor, based on the likelihood that some threat or other will arise to disrupt the experience of the trustor. The trust measure is the likelihood that a trustor would accept that situation. In an ideal world, the level of trust should be high (close to 1.0) if and only if the level of trustworthiness is also high (close to 1.0). This provides a good basis for the designer or operator of a 5G system or application to analyse how trustworthy their system is or will be, and how that relates to a population of potential users.

Evidently, this measure of trust does not support the notion that high levels of risk correspond to a high level of trust. If the trustworthiness of some entity is low, or rather if the trustor perceives it to be low, then the trustor would need a high propensity to trust to go ahead and rely on that entity. Because of that, it is unlikely that many trustors would trust that entity, so the probability that an individual chosen at random would do so is correspondingly low.

Clearly, defining trust as the probability that a randomly chosen trustor will decide to trust decouples it from some of the characteristics we associate with human trust decision processes. It is a measure of the decision outcome not of the internal (and largely unobservable) decision process. If parameters of the decision process are important, they will need to be incorporated into the predictive model that tells us how the likelihood of trust depends on the characteristics of the trustor and their situation.

7 Conclusions and Next Steps

This document provides a thorough review of the state of the art in trust modelling, covering both human and machine aspects as well as trustworthiness by design approaches. We have described the trust aspects of 4G networks through defining the actors and business models and their consequences for trust. We note that there is no formal specification of trust in 4G networks to report on or build upon.

Looking to the future we have documented the new actors and business models expected in 5G networks including the consequences of virtualisation, new domains and tighter integration of satellite and HAPS systems. This is followed by an analysis of the majority of the 5G use cases defined in 5G-ENSURE D2.1 where in each case the entities and trust issues are enumerated.

Taking all this into account we have discussed the role of privacy in 5G and propose an approach to modelling trust in 5G networks, extending the state of the art.

This “draft” trust model document contains a large amount of documentation and analysis. In the “final” version, the 5G use case analysis will be completed and extended to the next level of detail and the entirety will then be combined with further information from various sources to analyse the architecture and potential risks in more detail:

- the CAPEC database [Mitre-3] of known attacks to ensure that a broad range of known malicious attacks is modelled;
- deliverable D2.3 “Risk assessment mitigation and requirements (draft)”;
- deliverable D2.4 “Security architecture (draft)” and 5G architecture documents from elsewhere for details on generic 5G stakeholder roles and technology asset types once they are determined.

The results of the analysis will then be documented in the “Trust Model” chapter and also captured in a machine understandable form. Algorithms will be defined for quantification of trust (and trustworthiness) going beyond the simple ones proposed in this report. All of these results will then feed into the development of security architecture in WP2, also trust enablers in WP3, as well as the specification of the full 5G-ENSURE trust model in Deliverable D2.5 which will include an analysis of the 5G-ENSURE trust enablers.

8 References

- [3GPP 2015] General Universal Mobile Telecommunications System (UMTS) architecture, Online. Last accessed Jan 2016. <http://www.3gpp.org/DynaReport/23101.htm>
- [3GPP 2016] TR 33.916 Security assurance scheme for 3GPP network products for 3GPP network product classes. Online. Last accessed May 2016. http://www.3gpp.org/ftp/Specs/archive/33_series/33.916/33916-110.zip
- [5GForum 2015] 5GForum, "5G Vision, Requirements and Enabling Technologies" retrieved on 11th June, <http://www.5gforum.org/eng/main/main.php>, 2015
- [Akyildiz 2001] I. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: A survey", *Comput. Netw. J.*, vol. 38, no. 4, pp. 393-422, 2002
- [Blanco et al 2011] Blanco, C., Lasheras, J., Fernandez-Medina, E., Valencia-Garcia, R. and Toval, A. 2011. Basis for an integrated security ontology according to a systematic review of existing proposals. *Comput. Stand. Interfaces* 33, 4 (June 2011), 372-388. DOI=10.1016/j.csi.2010.12.002
- [Borgaonkar 2013] R. Borgaonkar, Security Analysis of Femtocell-Enabled Cellular Network Architecture, TU Berlin, dissertation, 2013, https://depositonce.tu-berlin.de/bitstream/11303/3897/1/Dokument_19.pdf
- [Broek 2015] Fabian van den Broek, Roel Verdult, and Joeri de Ruiter. 2015. Defeating IMSI Catchers. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*. ACM, New York, NY, USA, 340-351. DOI=<http://dx.doi.org/10.1145/2810103.2813615>
- [Capra 2004] Capra, L. (2004, October). Engineering human trust in mobile system collaborations. In *ACM SIGSOFT Software Engineering Notes* (Vol. 29, No. 6, pp. 107-116). ACM.
- [Chakravarthy 2015] Chakravarthy, A., Wiegand, S., Chen, X., Nasser, B. and Surridge, M. (2015) Trustworthy Systems Design using Semantic Risk Modelling. *Procs 1st International Conference on Cyber Security for Sustainable Society*, Coventry, UK, 2015, (pp. 49-81). Digital Economy Sustainable Society Network.
- [Cheshire 2011] Cheshire, C. 2011. Online trust, trustworthiness, or assurance? *Daedalus*, 140, 49-58.
- [Colquitt 2007] Colquitt, J. A., Scott, B. A. & Lepine, J. A. 2007. Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. *J Appl Psychol*, 92, 909-27.
- [de Montjoye 2013] de Montjoye, Yves-Alexandre and Hidalgo, César A. and Verleysen, Michel and Blondel, Vincent D., 2013, Unique in the Crowd: The privacy bounds of human mobility, *Scientific Reports*, 3, p1376 <http://dx.doi.org/10.1038/srep01376>
- [Dijkstra 1999] Dijkstra, J. J. 1999. User agreement with incorrect expert system advice. *Behaviour & Information Technology*, 18, 399-411.
- [Drissi 2013] Drissi, S., Houmani, H. and Medromi, H., 2013. Survey: Risk assessment for cloud computing. *International Journal of Advanced Computer Science and Applications*. 4 (12) 2013, 143-148

- [Dzindolet 2002] Dzindolet, M. T., Pierce, L. G., Beck, H. P. & Dawe, L. A. 2002. The perceived utility of human and automated aids in a visual detection task. *Human Factors*, 44, 79-94.
- [Engel 2014] Engel, T., 2014. SS7: Locate. Track. Manipulate. Online. See FTP: <http://events.ccc.de/congress/2014/Fahrplan/system/attachments/2553/original/31c3-ss7-locate-track-manipulate.pdf>.
- [ETSI] ETSI EN 300 175-7 V2.4.0, Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features
- [FCC 2016] Federal Communications Commission. Cognitive Radio for Public Safety. Online. Accessed 23 June 2016. See <https://transition.fcc.gov/pshs/techtopics/techtopic8.html>.
- [Fenz 2009] Fenz, S. and Ekelhart, A. Formalizing information security knowledge". 2009. in International Symposium on Information, Computer, and Communications Security, Sydney, Australia.
- [Gambetta 1998] Gambetta, D. (1998). Can we trust trust? In D. Gambetta (ed) *Trust, Making and Breaking Cooperative Relations*. Basil Blackwell, Oxford, pp. 213–237.
- [Gol Mohammadi 2014] Gol Mohammadi, N., Bandyszak, T., Moffie, M., Chen, X., Weyer, T., Kalogiros, C., Nasser, B. & Surridge, M. Maintaining Trustworthiness of Socio-Technical Systems. *Run-Time Trust, Privacy, and Security in Digital Business*, Springer International Publishing, Eckert, C.; Katsikas, S. & Pernul, G. (Eds.), 2014, 8647, 1-12
- [Golde 2013] Nico Golde, On the impact of modified cellular radio equipment, TU Berlin, dissertation, 2013, https://depositonce.tu-berlin.de/bitstream/11303/4514/1/golde_nico.pdf
- [Gramaglia 2015] Marco Gramaglia and Marco Fiore, On the anonymizability of mobile traffic datasets, *CoRR*, 2015, <http://arxiv.org/abs/1501.00100>
- [Hogganvik 2006] Hogganvik, I. and Stølen, K. 2006. A graphical approach to risk identification, motivated by empirical investigations. In *Proceedings of the 9th international conference on Model Driven Engineering Languages and Systems (MoDELS'06)*, Oscar Nierstrasz, Jon Whittle, David Harel, and Gianna Reggio (Eds.). Springer-Verlag, Berlin, Heidelberg, 574-588. DOI=10.1007/11880240_40
- [Hooper 2015] Hooper, C.J., Pickering, J.B., Prichard, J. and Ashleigh, M., TRust in IT: Factors, metRics, Models, ITaaU TRIFoRM Project Final Report, 10 July 2015. See also <http://www.itutility.ac.uk/2014/10/30/trust-in-it-factors-metrics-models/>
- [Howard 2009] Howard, M., & Lipner, S. (2009). *The security development lifecycle*. O'Reilly Media, Incorporated.
- [ISO 27001] ISO/IEC 27001:2013, Information Technology - Security Techniques - Information Security Management Systems – Requirements.
- [ISO 27005] ISO/IEC 27005:2011, Information technology -- Security techniques -- Information security risk management.
- [ISO 31000] ISO/IEC 31000:2009, Risk management – Principles and guidelines.

[ISO 31010] ISO/IEC 31010:2009, Risk management – Risk assessment techniques.

[IT Grundschatz 2004] IT Grundschatz Manual. 2004. Online. Last accessed Oct 2014. See [http://trygstad.rice.iit.edu:8000/Government%20Documents/Germany\(BSI\)/BSI%20ITGrundshutz%20Manual%202004%20Introduction%20&%20Modules.pdf](http://trygstad.rice.iit.edu:8000/Government%20Documents/Germany(BSI)/BSI%20ITGrundshutz%20Manual%202004%20Introduction%20&%20Modules.pdf).

[Kindervag 2010] J. Kindervag, "Building Security into Your Networks DNA: The Zero Trust Network Architecture," Forrester Research, Tech. Rep., 2010.

[Lee 2004] Lee, J.D., See, K.A. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors*, 50, 2, 194-210.

[Lewicki 2006] Lewicki, R. J., Tomlinson, E. C. & Gillespie, N. 2006. Models of interpersonal trust development: Theoretical approaches, empirical evidence, and future directions. *Journal of Management*, 32, 991-1022.

[Li 2008] Li, X., Hess, T. J. & Valacich, J. S. 2008. Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, 17, 39-71.

[Madhavan 2007] Madhavan, P. & Wiegmann, D. A. 2007. Similarities and differences between humanhuman and human-automation trust: An integrative review. *Theoretical Issues in Ergonomics Science*, 8, 277-301.

[Matulevi 2008] Matulevi, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P. and Genon, N. 2008. Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development. In *Proceedings of the 20th international conference on Advanced Information Systems Engineering (CAISE '08)*. Springer-Verlag, Berlin, Heidelberg, 541-555. DOI=10.1007/978-3-540-69534-9_40 http://dx.doi.org/10.1007/978-3-540-69534-9_40

[Mayer 1995] Mayer, R. C., Davis, J. H. & Schoorman, F. D. 1995. An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20, 709-734.

[McKnight 2001] McKnight, D. H. & Chervany, N. L. 2001. Conceptualizing trust: a typology and ecommerce customer relationships model. *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, 10 pp.

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

[Meland 2008] Meland, P. H., Spampinato, D. G., Hagen, E., Baadshaug, E. T., Krister, K. M., & Velle, K. S. (2008). SeaMonster: Providing tool support for security modeling. *Norsk Informasjonssikkerhets-konferanse, NISK*.

[Mitre-1] Common Vulnerabilities and Exposures. Online. See <https://cve.mitre.org/>.

[Mitre-2] Common Weakness Enumeration. Online. See <https://cwe.mitre.org/>.

[Mitre-3] Common Attack Pattern Enumeration and Classification. Online. <https://capec.mitre.org/>

- [Nessus] Online. <https://www.tenable.com/products/nessus-vulnerability-scanner> (accessed 2016-08-03).
- [NGMN 2015] NGMN Alliance, “5G White Paper”, Public Deliverable, NGMN 5G Initiative, Feb 2015.
- [NSA] NSA ANT Product catalogue. Online. <https://nsa.gov1.info/dni/nsa-ant-catalog/>
- [OWASP 2013] OWASP Top 10 (2013). https://www.owasp.org/index.php/Top_10_2013-Top_10.
- [Parasuraman 1997] Parasuraman, R., Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors*, 39(2), 230-253.
- [Schoorman 2007] Schoorman, F. D., Mayer, R. C. & Davis, J. H. 2007. An integrative model of organizational trust: Past, present, and future. *Academy of Management review*, 32, 344-354.
- [Seigneur 2004] Seigneur, Jean-Marc and Jensen, Christian Damsgaard, “Trading Privacy for Trust”, Trust Management: Second International Conference, iTrust 2004, Oxford, UK, March 29 - April 1, 2004.
- [Shaik 2016] A. Shaik, R. Borgaonkar, J. Seifert, N. Asokan, and V. Niemi, “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems”, In the proceedings of Annual Network and Distributed System Security Symposium, (NDSS 2016 USA)
- [Shirey 2007] Shirey, R. 2007. RFC 4949: Internet Security Glossary v2. Online. Last accessed April 2016. See [www: http://www.ietf.org/rfc/rfc4949.txt](http://www.ietf.org/rfc/rfc4949.txt).
- [Shostack 2014] Shostack, A. (2014). *Threat Modeling: Designing for Security*. John Wiley & Sons.
- [Sollner 2012] SÖLLNER, M., HOFFMANN, A., HOFFMANN, H., WACKER, A. & LEIMEISTER, J. M. 2012. Understanding the Formation of Trust in IT Artifacts. *International Conference on Information Systems*. Orlando Florida.
- [Stajano 1999] Stajano, Frank, and Ross Anderson. "The resurrecting duckling: Security issues in ad-hoc wireless networks. 1999." *Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science*, Springer-Verlag.
- [Stevens 2014] Ryan Stevens, Clint Gibler, Jon Crussell, Jeremy Erickson, Hao Chen, “Investigating User Privacy in Android Ad Libraries”, *Mobile Security Technologies (MOST) 2014*
- [Surridge 2013] Surridge, M., Nasser, B., Chen, X., Chakravarthy, A., & Melas, P. (2013, September). Run-Time Risk Management in Adaptive ICT Systems. In *Eighth International Conference on Availability, Reliability and Security (ARES)*, 2013, (pp. 102-110). IEEE.
- [Swiderski 2004] Swiderski, F. and Snyder, W. (2004) *Threat modelling*. Microsoft Press.
- [Taneja 2010] Sunil Taneja, Ashwani Kush, “A Survey of Routing Protocols in Mobile Adhoc Networks”, *International Journal of Innovation, Management and Technology*, Vol. 1, No. 3, August 2010.
- [ThreatModeller 2016] Online. <http://myappsecurity.com/> (accessed 2016-04-11).
- [USECA 2016] USECA: UMTS Security Architecture, Final Report, <http://www.isrc.rhul.ac.uk/useca/Reports/FinalReport.pdf> (accessed 2016-05-12).

[Wen 2010] Wen, L.I., Lingdi, P., Chunming, W. and Ming, J., 2010, April. Distributed Bayesian Network Trust Model in Virtual Network. In Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on (Vol. 2, pp. 71-74). IEEE.

[WS-Trust] Online. <https://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html> (accessed 2016-08-03).

[Xin 2012] Xin, L., Guang, R. & Thatcher, J. B. 2012. Does Technology Trust Substitute Interpersonal Trust? Examining Technology Trust's Influence on Individual Decisionmaking. *Journal of Organizational and End User Computing*, 24, 18-38.

[Xinming 2006] Xinming Ou, Wayne F. Boyer, and Miles A. McQueen. A scalable approach to attack graph generation. In 13th ACM Conference on Computer and Communications Security (CCS), 2006.

[Yu 2010] Yu, H., Shen, Z., Miao, C., Leung, C. and Niyato, D., 2010. A survey of trust and reputation management systems in wireless communications. *Proceedings of the IEEE*, 98(10), pp.1755-1772.