Deliverable D2.5
Trust model (final)

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	V2.0: 2017-11-15 This update V2.2: 2018-02-07	
Lead beneficiary	IT Innovation	Mike Surridge: ms@it-innovation.soton.ac.uk
Authors	IT Innovation: Mike Surridge, Toby Wilkinson, Peter Maynard, Stephen C. Phillips, Gianluca Correndo, Stefanie Wiegand Orange: José Manuel Sanchez Vilchez, Ghada Arfaoui Nixu: Seppo Heikkinen VTT: Marja Liinasuo, Pekka Ruuska, Suomalainen Jani EAB: Christian Schaefer, Mats Näslund, Christine Jost Oxford: Ravishankar Borgaonkar, Piers O'Hanlon TASE: Gorka Lendrino, Carla Salas TS: Edith Felix, Pascal Bisson TCS: Sébastien Keller, Frédéric Motte TIIT: Pier Luigi Zaccone, Luciana Costa, Baltatu Madalina	

Version	Date	Change(s)	Author(s)
D2.2 v0.1	11/04/2016	Skeleton document	Stephen C. Phillips
D2.2 v0.2	21/04/2016	Adds some more detail and assigns most sections	Stephen C. Phillips
D2.2 v0.3	06/05/2016	Adds terminology; cleans up styles	Stephen C. Phillips, Mike Surridge
D2.2 v0.4	10/05/2016	Sections 3, 6.1, 6.2	Jose Sanchez
D2.2 v0.5	24/05/2016	Human trust	Marja Liinasuo
D2.2 v0.6	25/05/2016	Merge of contributions	Gianluca Correndo
D2.2 v0.7	06/06/2016	Title, reference markings and some text added to section 4 (Human trust)	Marja Liinasuo
D2.2 v0.8	08/06/2016	Added again VTT originating text that was not included by mistake from the previous version (chapters 7.1.9 and 7.1.18)	Marja Liinasuo
D2.2 v0.9	14/07/2016	Added final partner contributions, plus the introduction, foreword and conclusions and the exec summary.	Stephen C. Phillips, Mike Surridge, with contributions from several other partners.
D2.2 v1.0	12/08/2016	Addressed partner peer review comments. To be submitted as Deliverable D2.2: Trust Model (draft) v1.0.	Stephen C. Phillips, Madalina Baltatu, Ghada Arfaoui
D2.2 v1.1	22/11/2016	Update addressing comments from 1st Review Meeting report. Resubmitted as Deliverable D2.2: Trust Model (draft) v1.1.	Stephen C. Phillips
D2.5 v0.9	02/05/2017	First draft of the interim version of Deliverable D2.5: Trust Model (final), designed to explain the methodology for finding trust dependences based on the UC analyses from T2.2 and T2.3, and illustrate this with a subset of UCs . Includes updates on the chapters 'Trust in 5G Networks', and 'Use Cases' based on analysis carried out by partners.	Pete Maynard, Mike Surridge, Toby Wilkinson using analysis inputs from partners across T2.2 and T2.3.
D2.5 v0.91	03/05/2017	Initial draft 'Common Annex' inserted, based on individual UC analysis forms from partners.	Pete Maynard
D2.5 v1.0	09/05/2017	Addressed partner peer review comments. To be submitted as Deliverable D2.5: Trust Model (interim) v1.0.	Pete Maynard
D2.5 v1.5	23/10/2017	Added placeholders for pending contributions. Reordered Section 6 and updated it to reflect the final methodology, inserted results from initial trust model analysis (as used in the Cyber Threat Summit presentation). Inserted missing UC analyses in the Common Annex (all except 2 now included).	Toby Wilkinson, Mike Surridge using analysis inputs from partners across T2.2 and T2.3.
D2.5 v1.7	30/10/2017	Inserted the User Attitudes Survey (Section 6.3 and Annex B). Renumbered the Common Annex containing UC analyses as Annex A, fixed numbering of figures in Annex A.	Marja Liinasuo, Mike Surridge, Toby Wilkinson
D2.5 v1.9	12/11/2017	Replaced the trust model in Section 6.4 with two models (3rd parties and virtualisation models) using the final threat library and the control set minimisation heuristic, and added remarks on the assumptions and results. Filled in the final changes in the Introduction (including summary of changes since the interim D2.5 v1.0), exec summary and conclusions sections.	Mike Surridge using input from Toby Wilkinson and Stefanie Wiegand
D2.5 v2.0	15/11/2017	Addressed partner peer review comments. To be submitted as Deliverable D2.5: Trust Model (final) v2.0.	Mike Surridge
D2.5 v2.1	21/11/2017	Update fixing some formatting issues prior to submission.	Timo Kyntäjä
D2.5 v2.2	29/01/2017	Update addressing comments from 2nd Review Meeting: removing placeholder text for UC analyses that are still incomplete, fixing broken cross-references.	Mike Surridge
D2.5 v2.2	07/02/2018	Added a version history page. The version published on the project website doesn't need this. No change in the content so the version number was not incremented.	Mike Surridge

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 (NFV) and software defined networking (SDN) 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 also 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 summarise the use cases from deliverable D2.1 and explain how their analysis fed into the trust model development.

Section 6 then describes the overall procedure used to identify and analyse trust dependencies, and provides additional input concerning privacy aspects and from a survey of user attitudes conducted by 5G-ENSURE partners working on human factors related to trust. This shows that users are willing to be quite pragmatic, and take some responsibility for their own security, but for the network to be trustworthy, they expect network operators to play a full role. The results from this survey (see Section 6.3 and Annex B) and the use case analyses (see Annex A, which covers risk and trust analysis) are then brought together in two trust models described in Section 6.4. The first captures the relationships between core network operators and third parties providing independent IDM for groups of users or devices, independent access network operators, and service providers for OTT and IoT services. The second covers the relationships between stakeholders involved in provisioning and running services over virtualised networks.

The main conclusions are that in the most general case, trust dependencies in 5G networks will be extensive. We speculate that vertical applications will seek to isolate themselves (using virtualisation) from many of the concerns identified here, so in practice most 5G networks can manage with a subset of our trust relationships.

Contents

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.

Trust is at its core, a response to the presence (or assumed presence) of risks. A stakeholder (trustor) who chooses to trust other stakeholders and/or technology components is making a decision to assume that those other stakeholders or technologies will protect them from risks. A trustor may contribute to mitigating the risk, but does not take sufficient steps to protect themselves unless the entities they trust do their part.

Due to the dependency between trust assumptions and risks and their relationship to the 5G-ENSURE security architecture, the project adopted the approach of working in two iterative cycles. Initial "drafts" of the three corresponding reports are produced up to the "half-time" point of the project. The initial draft version of the trust model was described in Deliverable D2.2 [d2.2], risk analysis was covered in D2.3 [d2.3] and the architecture in D2.4 [d2.4]. The original proposal for 5G-ENSURE was to update the trust model half way through the second year of the project, 6 months ahead of the final versions of the other two reports. The plan was changed when it became clear that the trust model could not be finalised independently of the analysis of risk mitigation strategies. At that point it was agreed that the two should be progressed in parallel, based on a shared analysis of use cases from Deliverable D2.1 [d2.1] which would be documented in a common annex to the trust model and risk analysis reports (this document and Deliverable D2.6 [d2.6]).

Because simply delaying the updated trust model would increase the risk in the project, it was also agreed to produce an interim version 6 months before the end of the project including a partial version of the common annex. This was delivered as Deliverable D2.5 v1.0 Trust Model (Interim Version) [d2.5a]. This final report is therefore D2.5 v2.0 Trust Model (Final), providing a further update of the interim version.

Since the initial draft document (D2.2), the early sections on Terminology (Section 2), the State of the Art in modelling human and machine trust (Section 3), and trust assumptions in 4G networks (Section 4) have not been changed in any significant ways.

In the interim version (D2.5 v1.0), Section 5 on trust in 5G networks was updated in two main respects:

- the discussion of 5G business models was updated to align with the terminology used (notably for different roles and stakeholders) in the analysis of the 5G-ENSURE security architecture as covered in D2.4 and D2.7;
- a section was added summarising the analysis of some of the use cases from D2.1, the details of which were provided in the common annex to be shared between D2.5 and D2.6 (Annex A).

Section 6 was also updated to provide some updates on the approach used for the analysis, along with some initial observations drawn from the use cases analysed up to M15.

In this final version of the trust model report, the following changes have been made:

- The rest of the use cases (with two exceptions) have been analysed, and all those analyses are now described in detail in the common annex with D2.6 (Annex A).
- An explanation of how the use case analysis results were used for the trust model analysis has been added at the start of Section 5.2.
- The rest of that section has been reduced to a simple summary of use cases analysed from each cluster, and the most significant findings for the trust model. The extended summary of material from Annex A included in D2.5 v1.0 [d2.5a] has been removed for the sake of brevity.
- The presentation of the trust model in Section 6 has been extensively revised:
    - Section 6.1 has been updated slightly to reflect some refinements in the analysis procedure used to synthesise the trust model based on the use case analyses;
    - Section 6.2 on privacy is unchanged, but was moved to before the main analysis sections;
    - Section 6.3 is a totally new section describing a trust survey conducted in the first half of 2017, which provided input to the trust model – notably that users may consider almost any threat to reflect on the trustworthiness of a 5G network;
    - Section 6.4 is also new, describing how the use case analyses were combined into two models, created using Trust Builder, and analysed using machine reasoning to identify threats and their likely impact on stakeholders (trustors) taking account of secondary effect cascades, and to determine which stakeholders (trustees) they should depend on to manage the corresponding risks.
    - Section 6.5 provides reflections on the results from this analysis, which indicate that in general purpose networks a high level of mutual dependency exists, so vertical applications will almost certainly need privacy, dedicated slices restricted to a few trusted actors. This section also provides some discussion of the relationship to the 5G-ENSURE architecture, including hints on how 5G-ENSURE enablers could be used to ensure trustworthiness.

The partial analysis from the initial and interim versions (D2.2 and D2.5 v1.0 respectively) have been removed as these are now replaced by sections 6.3, 6.4 and 6.5.

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. (In 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.

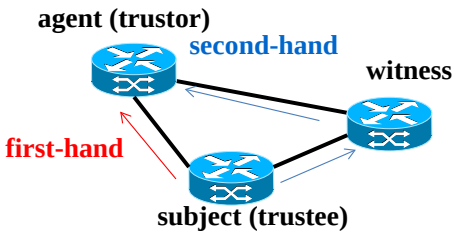

Figure 1. First-hand and second-hand evidence to evaluate trustworthiness

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 WSAN, 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.

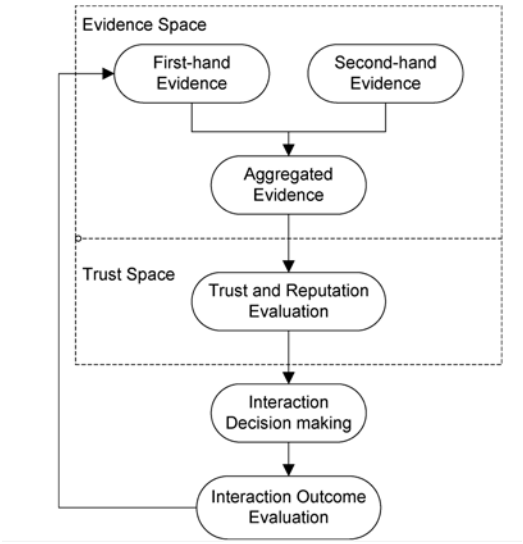

Figure 2. Interaction decision making process procedure in individual-level trust

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 <p,n>, where p means a positive outcome an 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.

$$Rep_{Agent} = \sum < p_i, n_i > \Big|_{Witness}$$

$$Rep'_{Agent} = Rep_{Witness} \sum < p_i, n_i > \Big|_{Witness}$$

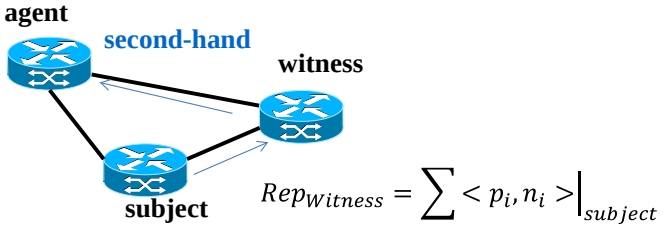

Figure 3. Inclusion of witness reputation in the reputation of subject node

Trust space: This phase is about mapping the aforementioned evidence space <p,n> 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 polices 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.

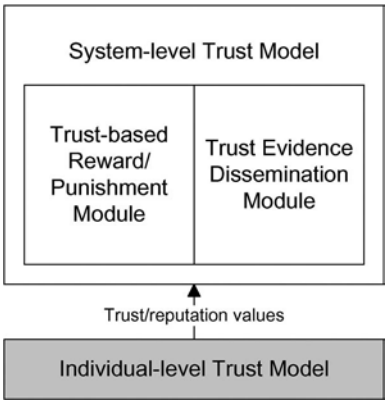

Figure 4. Components of a system-level trust and its relationship with individual-level trust

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.

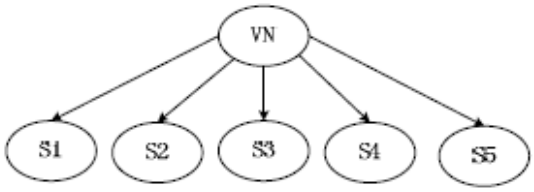

Figure 5. Bayesian Network of a given Virtual network supporting 5 services

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 aims 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 (Section 6.4), 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 (Section 6.5.2) 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 PulSAR (Proactive Security Assessment and Remediation) 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 Grundshutz 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.

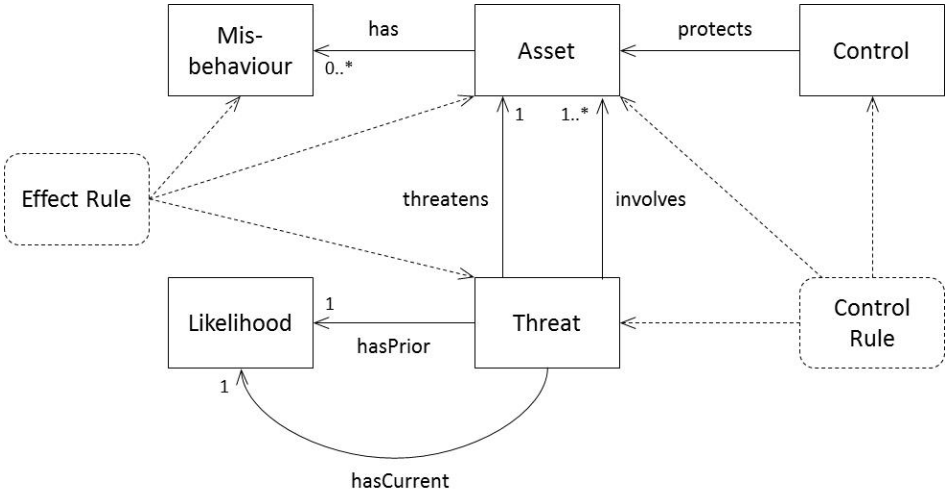

Figure 6. Security Classification Ontology

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.

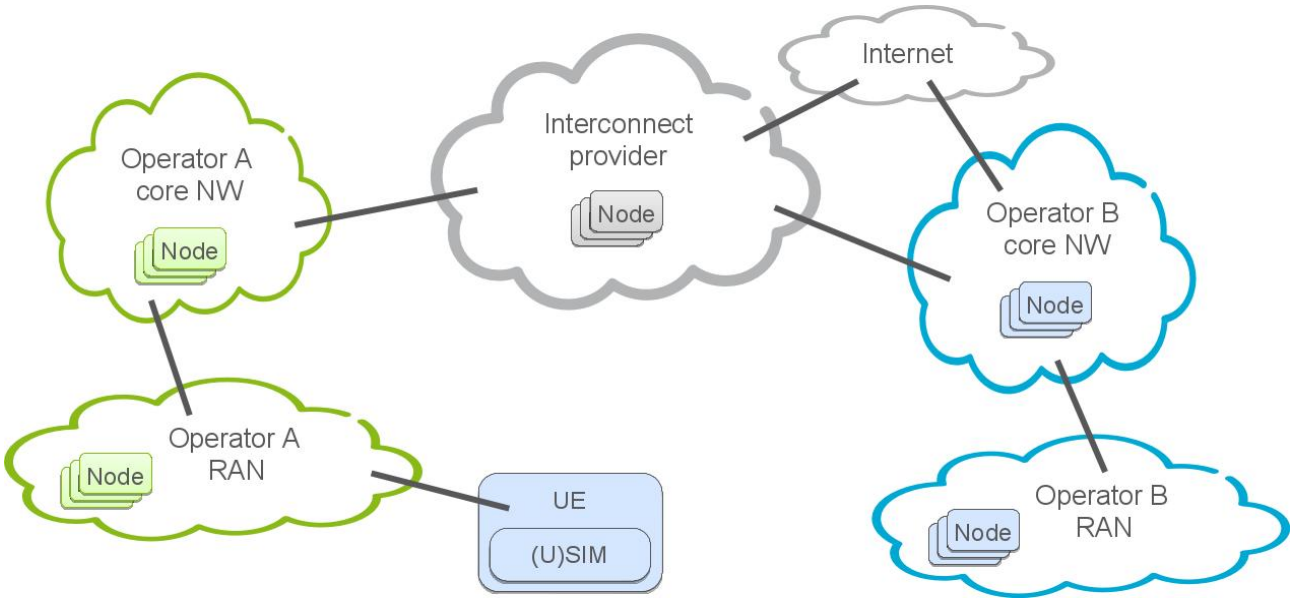

Figure 7: Main Actors in 4G

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.

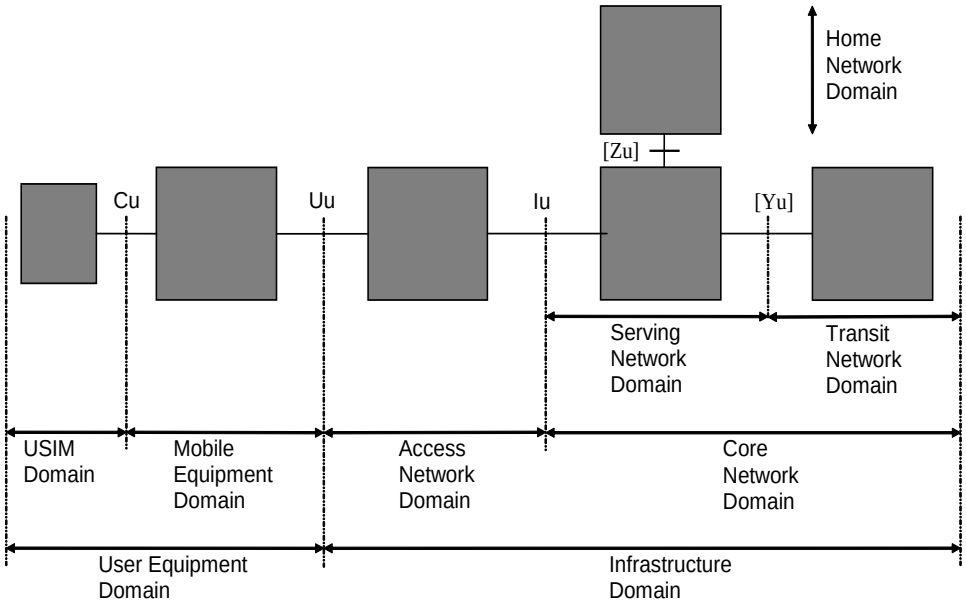

Figure 8. 3GPP TS 23.101 domain model.

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.

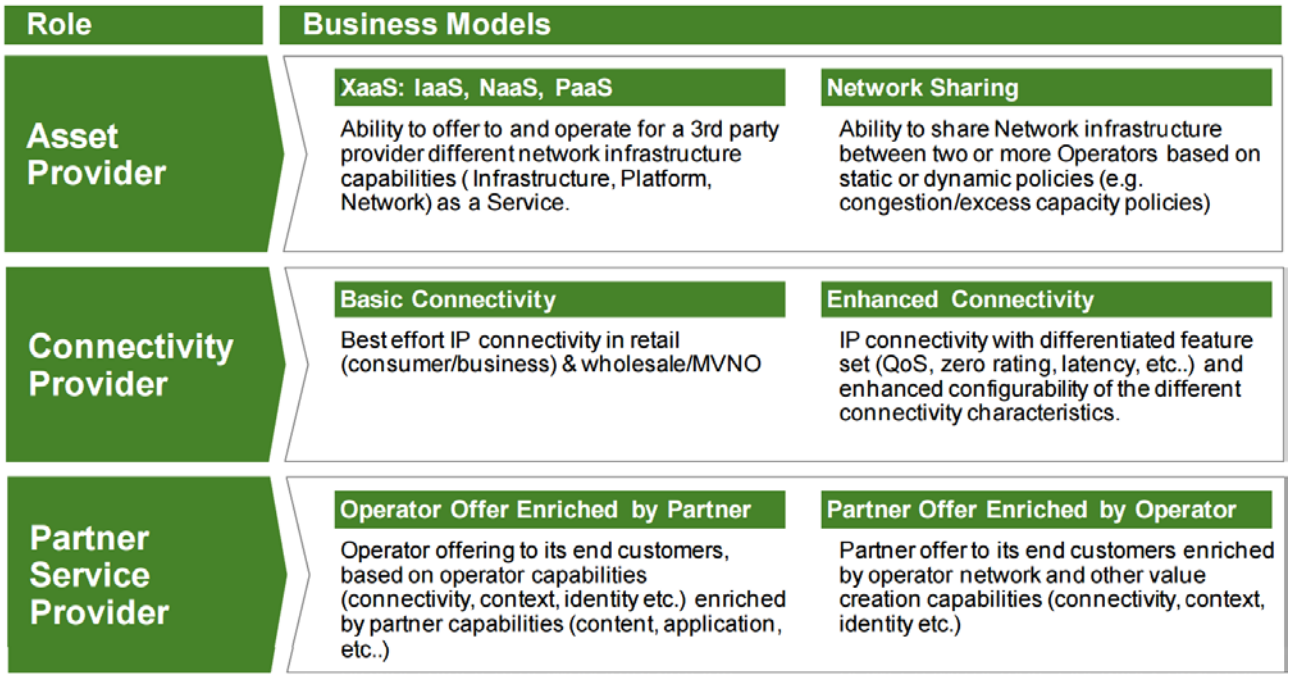

Figure 9. Network operator business models and roles defined by NGMN

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.

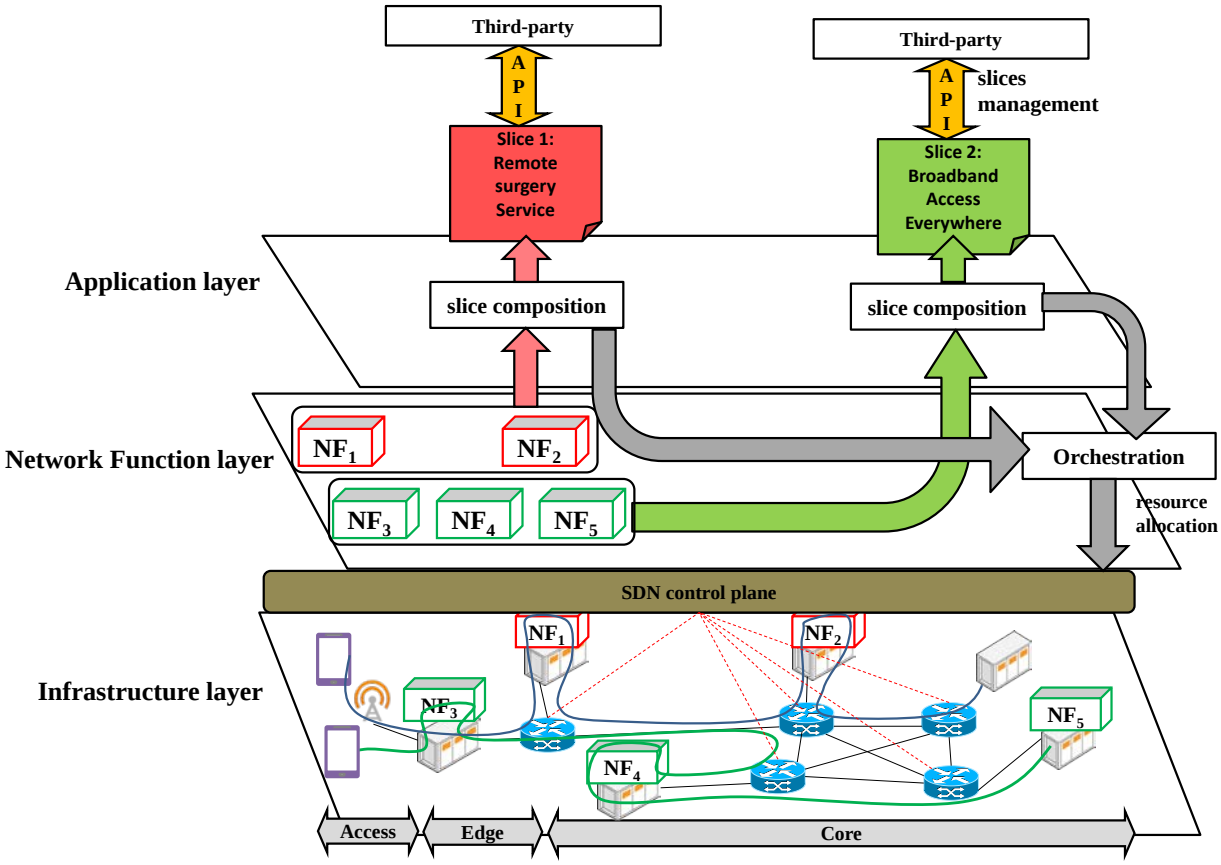

Figure 10. Preliminary 5G slicing architecture

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, or 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 kinds 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.

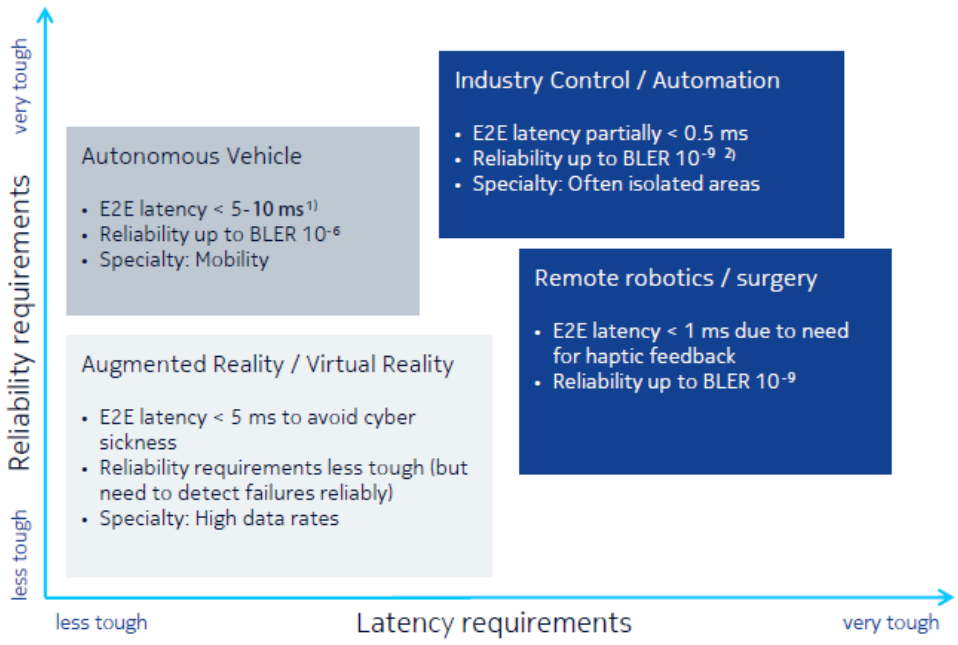

Figure 11. 5G Use cases requiring low latency and/or high reliability

5.1.1.1 Autonomous vehicles

Autonomous vehicles are 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 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 (M2M) 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

5G networks will enabled new 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.

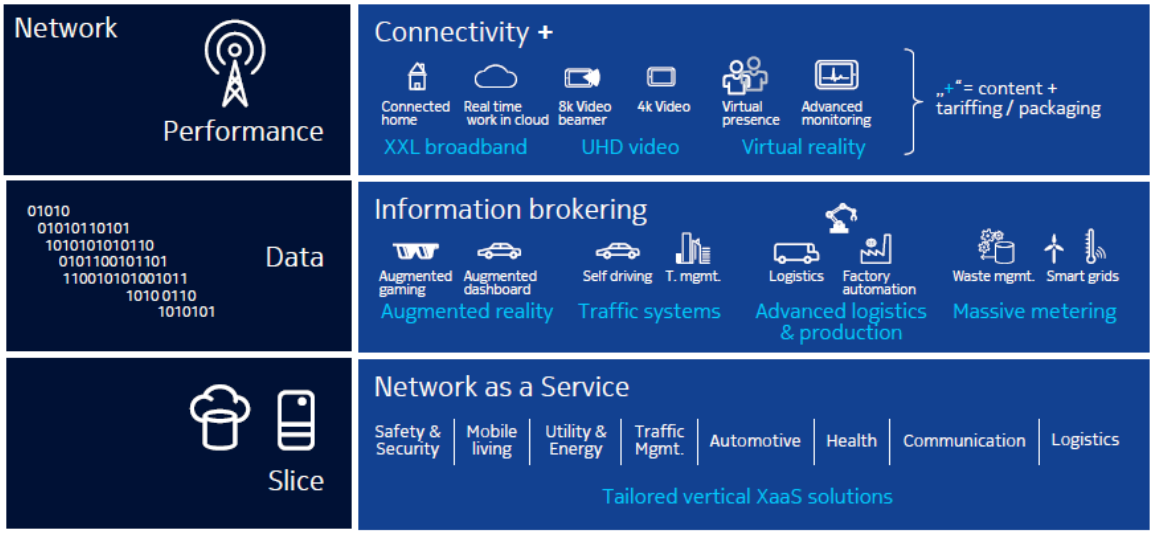

Figure 12. A variety of business models powered by network performance, data and slicing

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 or 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 (note: this list is not exhaustive, as the new business opportunities offered by 5G networks may generate additional actors). 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

5.2.1 Overview

The trust model for 5G networks is derived from an analysis of the use cases identified in deliverable D2.1, and recognized as representative of the needs of a 5G network. Each use case is analysed in detail in a Common Annex shared between deliverables D2.5 and D2.6 (see Annex A).

The common annex was created as a joint effort between Tasks 2.2 (on Trust) and 2.3 (on Risk Analysis). In practice the two tasks are strongly interdependent, since (as noted in Section 2) trust is a response to risk,

and risk mitigation choices are a manifestation of the trust each stakeholder has in the technology and other stakeholders.

Our intention was that the bulk of the analysis done by the two tasks would be documented in the use case analysis reports that make up the common annex. Then to produce the final deliverables including the final models for trust and risk mitigation, the leaders of each task would analyse the information provided by the analysts of each use case.

In practice, this could not be done in a straight forward manner in order to extract the trust model, for two reasons main reasons:

- The use cases as defined early in the project were not always consistent in their assumptions regarding the location of network functions and their orchestration.
- Each use case analysis focused on threats identified in that use case, but most threats can arise in several use cases so really each scenario is subject to a large number of possible threats that aren't considered in the detailed analysis.

Considerable efforts were made throughout the project to use uniform terminology and approaches. However, the use cases were analysed over a long period of time, so those done early in the project naturally align with different expectations than those done towards the end. It was not feasible to repeat the analysis for the early cases to realign with terminology used in later cases. One reason for this is the effort it would have required, but another is the need to remain consistent with work done in other tasks. Ultimately, it was considered more important to keep things consistent with Deliverable D2.1 (in which the UCs were first catalogued and described), Deliverable D2.4 (the first version of the 5G-ENSURE architecture, which was a reference point for the early UC analyses). In this report (but not in Annex A), we have sought to align as far as possible with the terminology from Deliverable D2.7 (the final 5G-ENSURE architecture specification) and documentation for the final (Release 2) 5G-ENSURE security enablers.

Once enough use case analyses were available, the approach to analysing them to determine the trust model was based on the use of Trust Builder. This 5G-ENSURE enabler was designed to allow end-to-end networks to be modelled, and threats identified including so-called secondary effect propagation. This plays a critical role in analysing trust, because it determines which of the effects likely to cause concern for stakeholders could be triggered by each of the identified threats. The UC analysis reports identified likely impacts on stakeholders, but in most cases this considered only the direct effects of the threat, and a few obvious propagation mechanisms to adjacent stakeholders. Trust Builder uses machine reasoning to analyse a model of system assets and interconnections, making it possible to pick up a lot of additional effects from secondary effect propagation mechanisms that were overlooked, or effects from simple (non 5G-specific) threats that were not the focus of any specific use case scenarios.

This section combines the analysis for the individual use cases in each use case cluster, and summarises the trust relationships identified. Any additional trust relationships identified during this synthesis are also discussed.

5.2.2 Cluster 1 – Identity Management

This cluster is centred around identify management within 5G networks. It contains the following use cases:

1. Factory Device Identity Management for 5G Access (UC 1.1)
2. Using Enterprise Identity Management for Bootstrapping 5G Access (UC 1.2)

3. Satellite Identity Management for 5G Access (UC 1.3)
4. MNO Identity Management Service (UC 1.4)

In the first two use cases the AAA service and credentials are stored within the enterprise's control. Any access to the 5G network is provided by the (V)MNO to devices owned and operated by the enterprise.

Clearly in these use cases it is essential that trust be established between the (V)MNO and the third party IDM provider, whether the identities being managed are those of individuals or devices. During the analysis it was also realised that these third party IDM and access management services may in some cases piggy back on the (V)MNO's existing business models and enforcement services. If they do, additional dependencies are created between different third party IDM providers, and also other stakeholders.

5.2.3 Cluster 2 - Enhanced Identity Protection and Authentication

This cluster addresses enhancements to identity protection and authentication in 5G compared to existing 3G and 4G networks. It contains the following use cases:

1. Device Identity Privacy (UC 2.1)
2. Subscriber Identity Privacy (UC 2.2)
3. Enhanced Communication Privacy (UC 2.3)

These use cases cover the related issues of protecting device identifiers or subscriber identifiers from an attacker who wishes to track users as well as the passive interception of communication data after successful authentication.

Trust must exist between the Home N/W, Serving N/W and the user's device, although in many cases it is the UICC rather than the user's device that must be trusted. During the course of the analysis some additional dependencies were discovered. For example, the UICC is technically a server that hosts the USIM, which in turn acts as a service that controls access to the IMSI. It may therefore be possible for an attacker in (say) the Serving or Access N/W to overload the UICC, with the consequence that the USIM becomes unavailable. If this happens the ME will be unable to attach to the network, and the end user will lose trust in the HMNO.

5.2.4 Cluster 3 - IoT Device Authentication and Key Management

This use case cluster focuses on IoT device authentication and key management. It is comprised of the following two use cases:

1. Authentication of IoT Devices in 5G (UC 3.1)
2. Network-Based Key Management for End-to-End Security (UC 3.2)

The use case covers a group of IoT devices which connect using a variation of network methods, such as 5G, WiFi, or an IoT gateway. There is an issue when using an IoT gateway that it makes it difficult to identify which device requested access via the gateway. This cluster describes three methods in which a sensor or group of sensors can authenticate with the 5G provider.

Trust relationships clearly must exist between the (V)MNOs and the user equipment including the IoT Gateway and IoT Sensors. If any of these are compromised, it would be easy to overload the core network by virtue of the number of devices that could be affected.

No matter which method of authentication is used, basic, group, or relayed. The trust ultimately resides with the sensors. If the sensors themselves are compromised then the data they are transmitting back to the cloud

storage cannot be trusted. There needs to be a method for the users to measure the amount of trust they have with the sensor. This could be, by restricting physical access to the device, or by segmenting network access of the device from others. It is also important to manage any firmware/software updates to the device by using a system to verify the update is correct, such as using a TPM device to verify the binary before it is applied. In the analysis (notably in the inter-stakeholder trust model described in Section 6.4.3) it became clear that the IoT sensor operator will be expected to contribute to the security of most other stakeholders.

5.2.5 Cluster 4 – Authorization of Device-to-Device Interactions

This cluster covers the following use cases:

1. Authorization in Resource-Constrained Devices Supported by 5G Network (UC 4.1)

This cluster covers two threats, both of which are designed to allow unauthorised access to sensors over a 5G network. The first involves forging an access token, possibly by capturing a token from a message stream and using it for a replay attack. The second involves amending an access control policy so the user can use a genuine token.

This cluster introduces some highly specialised threats within an IoT network. The trust model models threats at a higher level than this, but includes threat classes that do cover both these threats.

does take both these threats into account. takes these types of threats into account, but included IoT acess violations

not incorporated into either of the trust analyses described in Section 6.4.

5.2.6 Cluster 5 - Software-Defined Networks and Virtualization

5.2.6.1 Cluster overview

This section covers the following use cases:

1. Virtualized Core Networks and Network Slicing (UC 5.1)
2. Adding a 5G node to a virtualized core network (UC 5.2)
3. Reactive Traffic Routing in a Virtualized Core Network (UC 5.3)
4. Verification of the Virtualised Node and the Virtualisation Platform (UC 5.4)
5. Control and monitoring of slice by service provider (UC 5.5)
6. Integrated Satellite and Terrestrial Systems Monitor (UC 5.6)

In this cluster, the flexible nature of software defined networks meant that the usual stakeholder roles did not all appear, and there were some variations in the assignment of roles within the cluster. For this reason, the main trust model (described in Section 6.4.3) did not include software defined networks and virtualisation features. Instead, a much simpler second model was produced based on this cluster, with several simplifying assumptions allowing all the stakeholders to be mapped onto one of four classes: virtualised infrastructure providers, virtual mobile network operators, service providers, and equipment (including software) suppliers.

5.2.7 Cluster 6 – Radio Interface Protection

In this section we examine the following use cases:

1. Attach Request During Overload (UC 6.1)
2. Unprotected User Plane on Radio Interface (UC 6.2)

This cluster describes two use cases addressing availability and integrity of the radio interface. The first, considers overload and denial of service attacks of the radio interface and how devices with priority should be prioritized in order to be able to attach even during a high load situation. The second considers user plane data integrity protection.

The most likely and common threat to the availability of the radio interface is the loss of connectivity allowing users to communicate with the MNO and onwards. This can happen at many locations throughout the path of the user though the MNO. For example, if the eNodeB becomes overloaded it would not be possible for new or existing users to connect to the 5G network. The same could happen at the serving network or home network resulting in the same loss of trust.

The trust relationships identified by the use case analysts involved the end user, their device manufacturer and the (V)MNO. Of course, there are secondary effect propagation mechanisms at work, since roaming users will be affected leading to some disruption of normal functioning of (say) the Home N/W. However, since the attack affects only one RAN on the edge of the end-to-end 5G network, the impact should be small and this cluster was therefore not considered very important in the overall trust model development.

5.2.8 Cluster 7 - Mobility Management Protection

5.2.8.1 Cluster Overview

This cluster consists of a single use case:

1. Unprotected Mobility Management Exposes Network for Denial-of-Service (UC 7.1)

This use case describes possible methods that an adversary could use to perform a persistent denial of service on an UE. This type of attack is possible due to the lack of confidentiality or integrity protection in the current 3GPP standard, allowing an adversary to intercept, decode, and alter messages. Again, the trust relationships identified by the use case analyst referred to trust between the end user, the (V)MNO and their device manufacturers.

This scenario is between the UE and the eNodeB. It is feasible that the backhaul communication between the eNodeB and the backbone could be intercepted. It is common to encrypt the connections to the backhaul, but there may be cases where this does not happen, either due to a configuration problem or a technical fault. In these circumstances it may be possible to man-in-the-middle the backhaul communications, especially if this is done wirelessly. For example, it is possible for cell towers or 5G base stations to form a mesh to improve resilience. Attacking unencrypted traffic on such a mesh is easily accomplished using standard wireless technologies.

5.2.9 Cluster 8 - Ultra-Reliable and Standalone Operations

5.2.9.1 Cluster overview

This cluster includes two use cases relating to ultra-reliable and standalone operations. The first focuses on the Transport Network Architecture (TNA) which combines both satellite and terrestrial transport architectures, to allow for satellite to take over if traditional terrestrial methods are disrupted. The second is based on standalone EPC, where an eNodeB has the capability to provide an EPC services to the local commercial subscribers:

1. Satellite Network Monitoring (UC 8.1)
2. Standalone EPC (UC 8.2)

The use case analysts for this cluster identified threats to trust for the End User and the VMNO.

5.2.10 Cluster 9 - Trusted Core Network and Interconnect

5.2.10.1 Cluster overview

These use cases deal with the trusted core network and interconnection between different entities:

1. Alternative Roaming in 5G (UC 9.1)
2. Privacy in Context-Aware Services (UC 9.2)
3. Alternative Roaming in 5G (UC 9.1)Authentication of new network elements (UC 9.3)

The threats in this cluster relate to spoofed messages when roaming or using context-aware services. Also the 5G network should be able to ensure the interacting entities are authentic ones and spoofing of messages cannot take place. This should not be based on implicit security assumptions, but instead use explicit security solutions.

Trust relationships implied or impacted by these scenarios are between the end user and (V)MNO, the (V)MNO and the VIP, and the (V)MNO and their equipment manufacturers. We did not include the virtualised infrastructure aspects in the main trust model, but we did investigate whether secondary effects might lead to impacts in these scenarios affecting other stakeholders.

5.2.11 Cluster 10 - 5G Enhanced Security Services

5.2.11.1 Cluster overview

This cluster contains three use cases describing various enhanced security services that could be offered in 5G networks. This section covers the following use cases:

1. Botnet mitigation (UC 10.1)
2. Privacy Violation Mitigation (UC 10.2)
3. SIM-based and/or Device-based Anonymization (UC 10.3)

The first use case deals with malicious mobile applications that allow an attacker to take control of a UE, causing a direct monetary impact. The second use case addresses the issue of unauthorised access of sensor data, disregarding stakeholder's privacy policies. The issue addressed in the third use case is that an application a user may install on their mobile device may leak sensitive information to the application provider (perhaps through requesting permissions that the application does not actually need to provide its functionality). Such a leak may violate the privacy of the user.

These scenarios were not considered in formulating either of the trust models described in Section 6.4.

5.2.12 Cluster 11 - Lawful Interception

5.2.12.1 Cluster overview

This cluster contains two use cases relevant to lawful interception in 5G networks:

1. Lawful Interception in a Dynamic 5G Network (UC 11.1)
2. End to end encryption in a LI aware network (UC 11.2)

In order to ensure user privacy there is a move towards the use of end-to-end encryption of user communications. Law Enforcement Agencies (LEAs) also need to be able to intercept user communications –

whether encrypted or unencrypted - in order to detect crime and protect the public. The technical issue is how to protect user privacy whilst allowing LEAs to access user communications when they need to.

The use cases in this cluster imply that trust relationships must exist between the law enforcement agencies, the Home and Serving (V)MNOs, and their End Users. In practice, these relationships are forced by legislation so we did not consider them when creating the trust models described in Section 6.4.

6 Trust Model

6.1 Proposed Approach

6.1.1 Trust model requirements

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 wished 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, early work on trust models in D5.2 and the related work on risks in D2.3 informed 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.

6.1.2 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:

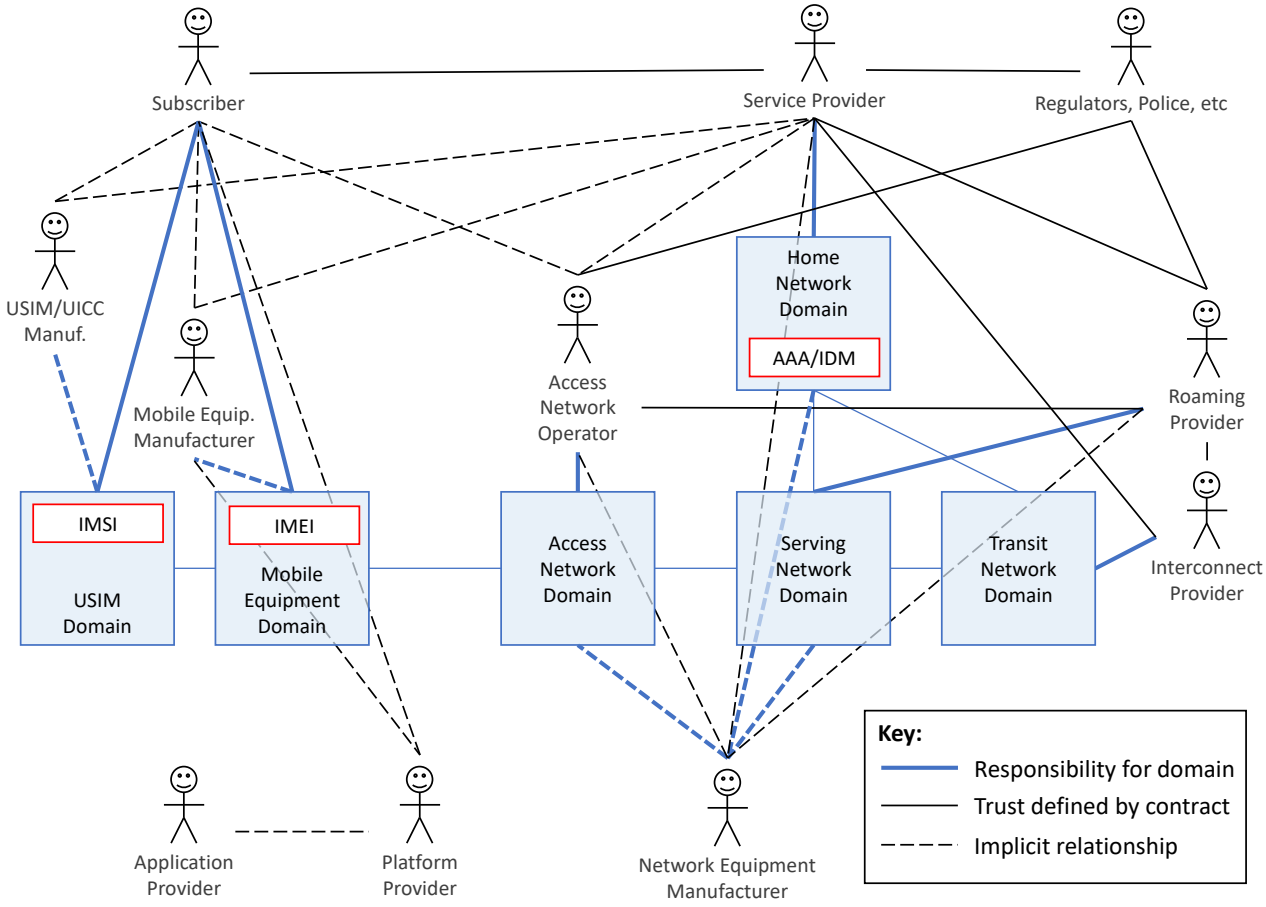

Figure 13. Explicit and Implicit Trust in 4G Networks

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.

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.

6.1.3 For what does a trustor trust?

6.1.3.1 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 believes[1] 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.

The 5G-ENSURE trust model was therefore developed by first producing a comprehensive model of risks in each applicable scenario. This was done using an approach developed in the FP7 OPTET project to capture security and trust requirements. It involves defining machine understandable models of both the system to be analysed, and expert knowledge on potential risks, 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.

The idea is to use the machine understandable model to identify threats in the system, ensuring that every known threat (i.e. every known way in which the network may be attacked or accidentally compromised) is taken into account at every point in the network. Using machine reasoning to generate the threat catalogue means we can be sure nothing was overlooked, assuming the system description in terms of assets is correct. We can then also model the ways in which each threat can be counteracted, providing a basis for deciding how to treat threats in the threat catalogue.

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.

[1] But see Section 6.1.5 below.

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.

6.1.3.2 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.

Stakeholders will expect 5G networks to provide good data transfer rates with relatively low latency on demand, so trust will be lost if the network suffers any significant loss of availability. They will also expect 5G networks to protect their privacy (see Section 6.3), so any loss of confidentiality in their communications will cause concern. This is true for network-related metadata (e.g. identifiers for users or devices, or related tracking data linked to their movements), as well as communications. Stakeholders will also be concerned

that this metadata is stored securely with no unauthorized access – this is mainly a concern for metadata as this is likely to be stored and used for network management or billing purposes, whereas communications content is not normally stored by the network over which they pass. The other main concern is likely to be misappropriation of service, in which a malicious party uses network services in such a way that they are billed to another user (defrauding that user), or to nobody (defrauding the service provider).

These are the main reasons why users would lose trust in a 5G network. However, they may arise for a wide range of reasons, many of which involve accidental or malicious compromise in the integrity of network functions. Thus to analyse trust dependencies between stakeholders, we will need to consider a full range of potential security threats against confidentiality, integrity and availability. We also needed to capture a range of secondary effect propagation mechanisms whereby the effect of a security breach propagate through the network and affect stakeholders other than the one responsible for assets affected by the initial breach. The use of secondary effect models to find out who is affected is one of the main reasons for using automated analysis methods to find trust dependencies.

6.1.3.3 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 5.2.12 (and Section 6.2, below), 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.

6.1.3.4 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.

6.1.4 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 $<p_1, n_1>$ and $<p_2, n_2>$ represent the number of positive and negative outcomes from previous first- and second-hand interactions, and $<p_0, n_0>$ 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 6.1.3. 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 6.1.3 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 $<p_0, n_0>$ 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 6.1.3.1 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. However, a statistical interpretation makes it relatively easy to combine contributions from multiple threats, and understand how the algorithms used reflect assumptions about the system. In D2.2 we proposed 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.

Neither of these assumptions is strictly correct. Some threats represent knock-on consequences from the misbehaviour of one asset on other assets with which it interacts, i.e. secondary threat mechanisms. Those are clearly not statistically independent of threats causing the initial misbehaviour. 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. 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.

In practice, both these effects are most relevant when analysing trust and trustworthiness in a given system. Correlations between primary threats are related to the types of attackers who wish to harm the system. The level of concern stakeholders will have about different types of network failings depend on why they need to use the network. In this report, we are mainly concerned with the trust implications of the 5G-ENSURE architecture when used in arbitrary applications. The goal is to identify dependencies between stakeholders and understand how they could distribute responsibility for counteracting security threats. It is therefore reasonable to assume that every potential trustor concern is equally important and should be considered in the analysis. In a specific application some types of disruption may be more or less likely, and more or less important to stakeholders, but we should not base our analysis on any specific application.

6.1.5 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.

6.2 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.

Privacy is an important driver of the approach taken to model the 5G-ENSURE architecture and extract the underlying trust model. Privacy, possibly more than any other security goal, involves trading risks between different types of threats – so making stakeholder concerns about these threats explicit makes it possible to use the resulting model to understand the implications for privacy. Privacy is also one of the security goals whose fulfilment (or otherwise) has a large effect on how stakeholders view a system.

6.3 User Attitudes Survey

6.3.1 Survey design and distribution

Before formulating a specific, concrete trust model aligned with the 5G-ENSURE architecture, a survey was conducted to check on user attitudes regarding potential network threats.

The survey was designed to check the composition of the population who responded (in terms of nationality, gender, age and so forth), their attitudes to Internet use and their inclination towards trusting behaviour, and their level of concern and likely responses to various types of network-related threats. The survey was make available online, and promoted within and via 5G-ENSURE partners and via SIGCHI Finland (Special Interest Group of Human-Computer Interaction).

A detailed description of the survey and the data obtained from it is given in Annex B.

6.3.2 Respondent group characteristics

There were 53 respondents to the survey, of which 56% were male, 39% female and the rest chose not to specify gender. Most were either Finnish or Swedish, and almost all the rest were European. Their ages ranged from 25 to 61 years old, and most had a technical education to degree or PhD level. Most considered themselves experienced Internet users – the average daily usage of the Internet was 5 hours.

Respondents to this survey were broadly less trusting than a typical population, possibly a result of their experience of Internet usage. In analysing his privacy surveys, Westin discerned three categories of responses from the general public [Kumaraguru and Cranor 2005]. Around 25% are fundamentalists (choosing privacy over consumer benefits), 57% are pragmatists (willing to trade privacy for benefits on a case-by-case basis), and 18% are unconcerned (happy to trade privacy in any circumstances where there is some benefit). The respondents in our survey broadly fit this characterisation, but with some variations as shown in Table 1:

Issue	Totally disagree	Somewhat disagree	Somewhat agree	Totally agree
It is OK for authorities to use personal data for counter-terrorism	27%	25%	33%	15%
It is OK for authorities to use personal data for unspecified reasons	58%	31%	9%	2%

Issue	Totally disagree	Somewhat disagree	Somewhat agree	Totally agree
It is OK for companies to use personal data for marketing purposes	20%	39%	33%	8%
Westin's Privacy Indexes	25% Fundamentalist	57% Pragmatist	18% Unconcerned	

Table 1. Trust in the use of personal data

The first of these responses is in line with Westin's observations, suggesting that while the survey respondents are unusually well educated, they are not significantly more or less trusting that the average. The second response indicates far less trust when there is no identifiable benefit, as one would expect. The last response is not quite consistent with Westin's averages: when data is used for commercial purposes the respondents are on average less trusting than the average, most notably in the small number of 'unconcerned' respondents. However, there are also fewer responses fitting the 'fundamentalist' category, and far more 'pragmatists' than one would expect. This may be because the respondents are mostly tech savvy, and more aware of both benefits and risks of using technology than the average person.

When it comes to applications of advanced networking technology, the pattern is as expected, as shown in the summary from Table 2:

Issue	Totally disagree	Somewhat disagree	Somewhat agree	Totally agree
It is OK for my heating system to be operated via the network	28%	31%	35%	6%
It is safe to use a car that navigates using information from the network	15%	33%	47%	5%
Trust telemonitoring of health of a patient living at home is safe	13%	29%	45%	13%
It is OK to use a fridge that orders food for me when they appear in the shops	35%	38%	25%	2%
I would consider fitting a lock with a network operated key to my home	40%	34%	24%	2%

Table 2. Trust in advanced network applications

In these questions, the level of acceptance is directly related to the level of risk and benefit. Health monitoring for patients living at home is clearly beneficial, and we get clear majority who favour the use of such an application. Autonomous navigation for a car is also favoured, though here the risks seem to carry more weight relative to the benefits. For the remaining applications, it seems there is more objection, probably because the benefits are less clear in relation to the potential risks.

6.3.3 Attitudes and responses to potential threats

Questions about possible risks produced a less clear pattern. The main lessons from the survey for the 5G trust model come from three aspects:

- Whether the respondent thinks the threat could be avoided
- Whether it would affect their behaviour (i.e. make them less inclined to use the network)
- Whether it is considered a reflection of the trustworthiness of the network itself

The survey turned up some interesting responses, the details of which can be found in Annex B. A broad summary is shown in Table 3:

Threat	Proportion of respondents who think this threat is		
	Avoidable/ Unavoidable[2]	Would affect their use of networks[3]	Reflects on network untrustworthiness
Voice calls disabled by attacks on the network	45%/22%	26%	79%
Phone conversations are wiretapped	43%/35%	55%	68%
Location of a mobile device is tracked by a burglar	62%/22%	45%	69%
Subscriber/device IDs are leaked	60%/16%	44%	70%
Ransomware attack on a mobile device	60%/13%	76%	59%
False hotel evaluations via online sources	64%/13%	41%	43%
Burglars interfering with a networked alarm system	46%/24%	57%	74%
Application running up a high networking bill	83%/2%	54%	50%
Network attack to drain a mobile device battery	57%/17%	35%	72%
Password stealing via a mobile network	65%/11%	68%	58%

Table 3. Attitudes to network-related threats

For the first of these threats, respondents were also asked if this threat would make them more willing to change their network service provider. Only 11% said it would not, but most of the rest said it would only make them a bit more willing to do so.

The above table contains three interesting facts that should be taken into consideration in creating the 5G-ENSURE trust model:

1. Users who have an opinion think most threats are avoidable, with only wiretapping and network interference being considered avoidable by less than half of respondents.
2. Most threats are considered to reflect a lack of trustworthiness in the network, with the exception of false data from services accessed over the network.
3. Most threats would affect how people use the network, but there is no clear correlation with the degree to which network trustworthiness is considered to be a factor.

On the first point, it seems that wiretapping is considered less avoidable because this was assumed to include lawful interception by the authorities (which network operators are not allowed to block). Interference attacks (by attackers on the network, or by burglars on a home alarm system) were also considered less avoidable, possibly because the attacker was assumed to have direct physical access to the devices under attack. Everything else can be avoided, but it isn't clear whether our tech savvy respondents were thinking of technical measures that could be used by network operators. It seems likely that in many cases they were, because some of these threats cannot be easily mitigated by any action that could be taken by a subscriber.

[2] Some respondents in each case said they didn't know if the threat could be avoided.
[3] Based on those who said the threat would highly or clearly affect their use of the network

This indicates a feeling that network operators should be responsible for addressing threats on behalf of (at least) subscribers.

The second point also suggests this. In most cases, a majority of respondents considered the threat to be related to the trustworthiness of the network. The exceptions are where the threat stems from the use of untrustworthy data or applications provided via the network, as one might expect.

The last point is in some ways the most interesting. The threat that was most widely considered to reflect on the trustworthiness of the network is DoS against voice calls, yet this is also the one that has least impact on user behaviour. The threat least considered to reflect on trustworthiness of the network is false information delivered by the network, yet this too would affect use of the network by only a minority of users. The threat that has most impact on user behaviour is ransomware attack but only 59% of users felt this is related to network trustworthiness – a majority but quite a narrow one compared with other threats that have less impact on user behaviour.

It seems that users will modify their behaviour if (a) they think doing so would reduce the potential harm caused by a threat, or (b) they think the level of harm caused is high compared to the benefits of accepting the risk. Thus users would change their behaviour to manage risks of ransomware or of password theft by someone impersonating a service provider, because the harm caused is high and they think changing behaviour would reduce the risk. They are less inclined to change behaviour to manage risks of DoS on voice calls or DoS to drain their battery because they don't think a change in behaviour would stop the attack, and doing without phone calls for a while is not very harmful.

The conclusion seems clear:

- More or less any threat arising in the network could be a cause for concern over the trustworthiness of the network: the trust model should try to consider all threats;
- Subscribers expect network operators to manage risks from these threats, using technical measures within the network – this is what they mean by a 'trustworthy' network;
- Users do expect they can help to manage risks, e.g. by changing their behaviour – although it should be noted that the survey respondents were especially 'tech savvy'; and
- Some threats may be acceptable to users, where substantial harm can be avoided – but this probably depends on the purpose of networked applications they are using.

These points were taken into account, alongside the analysis of use cases when devising models of networks and stakeholders to capture and analyse trust dependencies.

6.4 Trust Models

This section describes in detail the trust model derived from the use case analysis of Section 5.2.

We first address the issue of consistent stakeholder naming, by mapping names from use cases onto a set of names used in the analysis of the architecture (see Deliverables D2.4 and D2.7). This is followed by a discussion of scenarios, explaining how we decided on the two models used as a basis for the analysis.

Sections 6.4.3 and 6.4.4 contain descriptions of the two models examined, and the analysis used to identify trust relationships between stakeholders. In section 6.4.3 we also go into some details of the algorithms used to analyse the models and determine these trust relationships.

Section 6.5 then brings together the results from the two models, and provides an overall statement of the proposed trust model with reference to the 5G-ENSURE architecture. This concludes by specifying which stakeholder(s) should be considered responsible for implementing the security architecture (specifically its security control classes) in each architectural domain.

6.4.1 Mapping of Stakeholders

The use case analysis of Section 5.2 is derived from the material in the Common Annex (included in this document as Annex A), which also forms input to Deliverable D2.6 on risk mitigation. The Common Annex is the product of the work of many different analysts, and as a result there are discrepancies between the names used for stakeholders. Moreover, during the project the terminology has evolved as our understanding of how stakeholders interact has increased, and this has also contributed to the inconsistency in stakeholder naming.

To address this Table 4 presents standardised names for the stakeholders identified during the use case analysis, and a mapping to the alternative names found in Section 5.2 and the Common Annex (Section A). The list of stakeholder names in Table 4 extends those found in the table in Section 1.4 of D2.4.

Trust Relationship Names	**Analysis Names**
(V)MNO Customer	Bank Service Provider
(V)MNO Customer	Cloud Provider
3rd Party ID Provider	Enterprise Owner
3rd Party Factory Owner	Factory Owner
ME manufacturer	ME Manufacturer
Device Manufacturer SW Provider	User equipment SW provider
End-user	Device Owner
End-user	End-user
End-user	Subscriber
Home Network Operator	Home Network Operator
Infrastructure Provider (IP)	Infrastructure Provider
Interconnect network provider	Interconnect network provider
Law Enforcement Agency	Law Enforcement Agency
Mobile Network Operator (MNO)	Mobile Network Operator
Network access equipment manufacturer	Network equipment manufacturer
Network access provider	Network access provider
Regulator	Regulator
Robot manufacturer	Robot Manufacturer
Satellite Network Operator	Satellite Network Operator
Sensor Owner	Sensor Owner
3rd Party WiFi Operator	Service provider
OTT Service Provider	Service provider
Serving Network Operator (SNO or SNMNO)	Serving Network Operator
UICC Manufacturer	UICC Manufacturer
ME manufacturer	User equipment manufacturer
Vehicle Manufacturer	Vehicle Manufacturer
Virtualised Mobile Network Operator (VMNO)	Virtualised Mobile Network Operator
Virtualized Infrastructure Provider (VIP)	Virtualized Infrastructure Provider

Table 4 Stakeholder mapping from annex to trust model

6.4.2 Selection of scenarios

At the start of the project we envisaged that we would create one single model based on all the use cases, reflecting the architectural decisions made in the project. The plan was to create and analyse this model using Trust Builder (one of the 5G-ENSURE trust enablers), to extract risks and find how stakeholders would need to depend on each other to address those risks. Now as we approach the end of the project, it is clear that we cannot include everything in one network model as it would become too complex to analyse in a reasonable time. One option would be to model each use case separately, but this was rejected because (a) there are a lot of use cases and to model them all would also take a long time, and (b) most of the use cases contain a lot of common features, so it makes sense to combine sets of use cases into one model.

Based on the above observations, we have created two separate models containing features:

- a model of third party involvement in operating and using a 5G network; and
- a model of a 5G network in which core network components are provisioned using virtualisation.

In the first model we have not specified the provisioning approach, so network functions may or may not be virtualised. The focus is to capture who is responsible for each function and what dependencies that creates between stakeholders. This was the first model to be analysed using Trust Builder. This first model is based largely on use cases UC1.1, UC 1.2, UC1.3, UC2.1, UC3.1 and elements from UC2.2, UC6.1, UC6.2, UC7.1, UC8.1 and UC8.2 and other use cases.

In the second model we have no 'third party' domains in the network, but there is a separate infrastructure provider, whose infrastructure is shared by multiple network operators. Network functions are provisioned on this shared infrastructure using MANO-style VNF management. This is based mainly on UC5.1, 5.2, 5.3, 5.4 and 5.5.

From the trust survey summarised in Section 6.3 we surmised that it is important to include a lot of basic threats, e.g. infection by malware, that are not specific to 5G networks, but which are nevertheless seen by users as reflecting the trustworthiness of 5G networks.

6.4.3 Trust Model 1: New business actors

6.4.3.1 Model description

The focus for this first model is the effect of using 3rd party services in a 5G network. From the use cases, we identified several examples of this:

- In UC 1.1, a smart factory owner uses a 5G network to interconnect devices in their factory. To allow this, they provide their own AAA service which is used by the mobile network operator's IAC to authenticate the connections made by factory devices.
- In UC 1.2, an enterprise wishes to supply its employees with 5G devices (mobile phones, laptops, etc.). In agreement with the MNO, the enterprise's AAA service is able to provision the employee's 5G devices with 5G credentials (eSIM).
- In UC 1.3, we have dual access via terrestrial 5G or via satellite networks in regions of poor 5G coverage. Here 5G credentials are used by the satellite network operator to control access to the satellite network.

- In UC 2.1, we have a (potentially untrustworthy) WiFi access network. In this UC, the key point is that the access network is not provided by the serving or home network operators, creating opportunities for malicious spoofing to attack the end user's privacy.
- In UC 3.1, IoT sensors connect to a 5G network. The sensors are simple and do not have 5G radio access, they connect to the 5G network either via an IoT Gateway device, or via a subscriber's UE.

The model was created in Trust Builder, starting from these five use cases and adding elements from other UCs where these do not depend on virtualisation aspects. The overall model is shown in Figure 14:

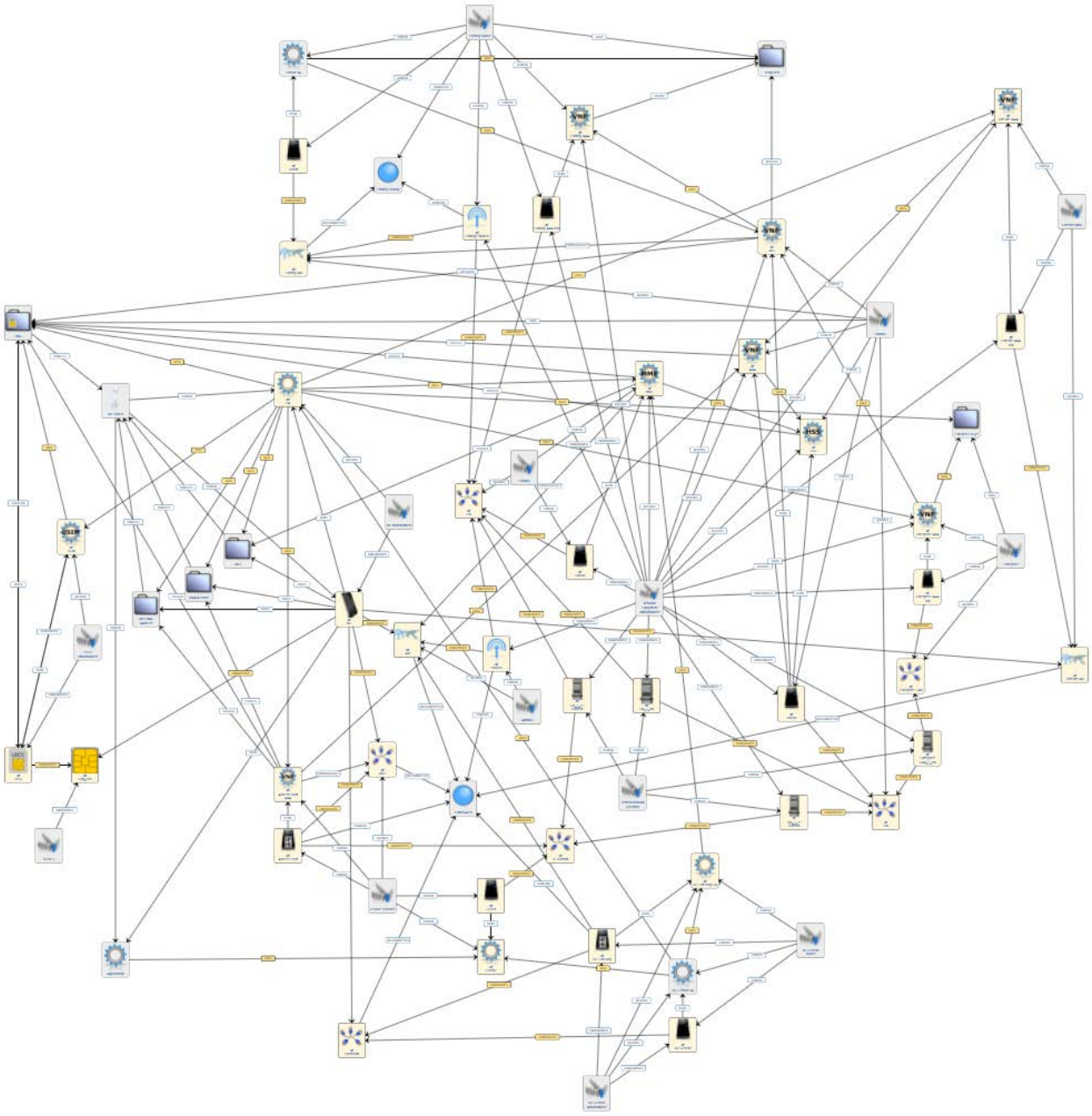

Figure 14. Model 1: New Business Actors: 3rd Party A/N and 3rd Party IDM for IoT devices

This screenshot was taken from Trust Builder, but the model is quite extensive and difficult to render in a report such as this. Figure 15 shows the same screenshot, but indicates the grouping of these elements into different 5G network domains to help orient the reader:

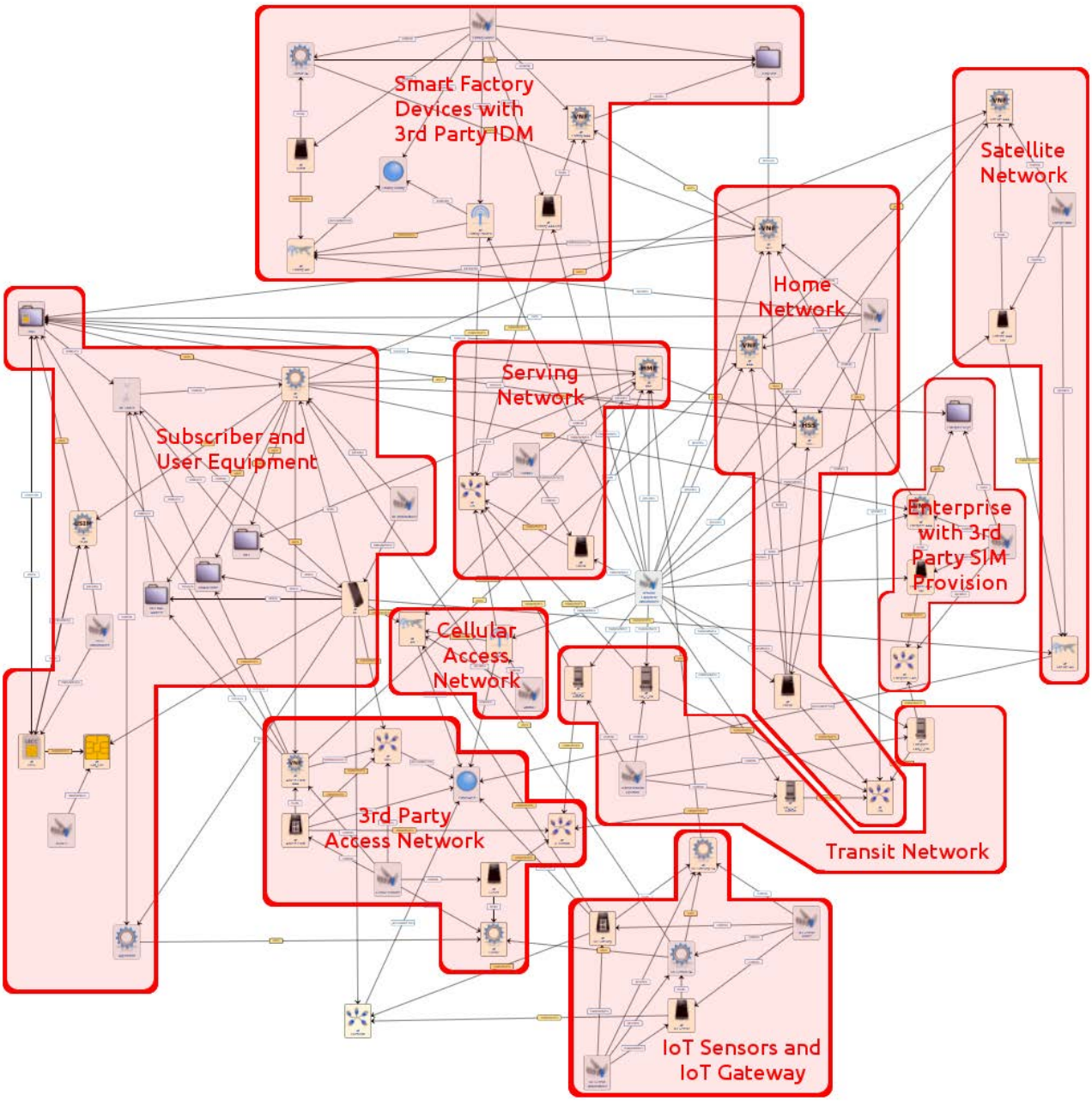

Figure 15. Model 1: New Business Actors: superimposed 5G domains

To keep things as simple as possible, only the control plane interactions are included in the model. This is because if the data plane is included, one may need to consider a wide range of possible user applications in order to capture different types of potential threats to end user experiences. The trust survey described in Section 6.3 indicates that users understand that errant behaviour in application services is usually not the fault of the network, and the majority do not regard such behaviour as a reflection of the trustworthiness of the mobile network itself. Over the top communication/content distribution services are included, but only the control plane (signalling between the user, the OTT service and the network) are captured.

6.4.3.2 Threats to stakeholder trust

Having defined the model in Trust Builder, the first step is to find all the threats in the model, which is done automatically using the Trust Builder's machine reasoning engine. This found a total of 8488 distinct threats in the end-to-end network. The majority of these threats are actually remote exploits against devices or the

services that run on them: they are always the most numerous because Trust Builder has to consider whether such attacks could be launched against each device/service from each of the subnets present in the network.

Of these threats, only 141 are direct threats to stakeholder trust. These are listed in the following table:

No	Trustor	Threat ID	Trustor Concern
1	Access N/W Operator	O.T.RNO.1_RNO_ANMNO_AN	Misappropriation (theft) of service from the Access Network
2	Access N/W Operator	St.A.StH.1_StH_eNodeB_ANMNO	Loss of availability in an eNodeB
3	Access N/W Operator	St.Ct.StH.1_StH_eNodeB_ANMNO	Loss of control over an eNodeB
4	Access N/W Operator	St.I.StH.1_StH_eNodeB_ANMNO	Loss of integrity in an eNodeB
5	Access N/W Operator	St.U.StH.1_StH_eNodeB_ANMNO	Unreliability in an eNodeB
6	3rd Party ID Provider	St.A.StD.1_StD_Enterprise Keys_Enterprise	Loss of availability in 3rd Party Credentials
7	3rd Party ID Provider	St.A.StH.1_StH_Enterprise AAA HW_Enterprise	Loss of availability in 3rd Party ID Equipment
8	3rd Party ID Provider	St.A.StP.1_StP_Enterprise AAA_Enterprise	Loss of availability in a 3rd Party AAA
9	3rd Party ID Provider	St.C.StD.1_StD_Enterprise Keys_Enterprise	Loss of availability for 3rd Party Credentials
10	3rd Party ID Provider	St.Ct.StH.1_StH_Enterprise AAA HW_Enterprise	Loss of control over 3rd Party ID Equipment
11	3rd Party ID Provider	St.Ct.StP.1_StP_Enterprise AAA_Enterprise	Loss of control over a 3rd Party AAA
12	3rd Party ID Provider	St.I.StD.1_StD_Enterprise Keys_Enterprise	Loss of integrity in 3rd Party Credentials
13	3rd Party ID Provider	St.I.StH.1_StH_Enterprise AAA HW_Enterprise	Loss of integrity in 3rd Party ID Equipment
14	3rd Party ID Provider	St.I.StP.1_StP_Enterprise AAA_Enterprise	Loss of integrity in a 3rd Party AAA
15	3rd Party ID Provider	St.U.StH.1_StH_Enterprise AAA HW_Enterprise	Unreliability in 3rd Party ID Equipment
16	3rd Party ID Provider	St.U.StP.1_StP_Enterprise AAA_Enterprise	Unreliability in a 3rd Party AAA
17	3rd Party Factory Owner	St.A.StD.1_StD_TempCred_Factory Owner	Loss of availability in a Factory Temporary Credential
18	3rd Party Factory Owner	St.A.StH.1_StH_Factory AAA HW_Factory Owner	Loss of availability in Factory N/W Equipment
19	3rd Party Factory Owner	St.A.StH.1_StH_Factory eNodeB_Factory Owner	Loss of availability in a Factory eNodeB
20	3rd Party Factory Owner	St.A.StH.1_StH_Robot_Factory Owner	Loss of availability in a Factory Robot
21	3rd Party Factory Owner	St.A.StP.1_StP_Factory AAA_Factory Owner	Loss of availability in a Factory AAA
22	3rd Party Factory Owner	St.A.StP.1_StP_Robot UA_Factory Owner	Loss of availability in a Factory Robot User Agent
23	3rd Party Factory Owner	St.C.StD.1_StD_TempCred_Factory Owner	Loss of availability for a Factory Temporary Credential
24	3rd Party Factory Owner	St.Ct.StH.1_StH_Factory AAA HW_Factory Owner	Loss of control over Factory N/W Equipment

No	Trustor	Threat ID	Trustor Concern
25	3rd Party Factory Owner	St.Ct.StH.1_StH_Factory eNodeB_Factory Owner	Loss of control over a Factory eNodeB
26	3rd Party Factory Owner	St.Ct.StH.1_StH_Robot_Factory Owner	Loss of control over a Factory Robot
27	3rd Party Factory Owner	St.Ct.StP.1_StP_Factory AAA_Factory Owner	Loss of control over a Factory AAA
28	3rd Party Factory Owner	St.Ct.StP.1_StP_Robot UA_Factory Owner	Loss of control over a Factory Robot User Agent
29	3rd Party Factory Owner	St.I.StD.1_StD_TempCred_Factory Owner	Loss of integrity in a Factory Temporary Credential
30	3rd Party Factory Owner	St.I.StH.1_StH_Factory AAA HW_Factory Owner	Loss of integrity in Factory N/W Equipment
31	3rd Party Factory Owner	St.I.StH.1_StH_Factory eNodeB_Factory Owner	Loss of integrity in a Factory eNodeB
32	3rd Party Factory Owner	St.I.StH.1_StH_Robot_Factory Owner	Loss of integrity in a Factory Robot
33	3rd Party Factory Owner	St.I.StP.1_StP_Factory AAA_Factory Owner	Loss of integrity in a Factory AAA
34	3rd Party Factory Owner	St.I.StP.1_StP_Robot UA_Factory Owner	Loss of integrity in a Factory Robot User Agent
35	3rd Party Factory Owner	St.U.StH.1_StH_Factory AAA HW_Factory Owner	Unreliability in Factory N/W Equipment
36	3rd Party Factory Owner	St.U.StH.1_StH_Factory eNodeB_Factory Owner	Unreliability in a Factory eNodeB
37	3rd Party Factory Owner	St.U.StH.1_StH_Robot_Factory Owner	Unreliability in a Factory Robot
38	3rd Party Factory Owner	St.U.StP.1_StP_Factory AAA_Factory Owner	Unreliability in a Factory AAA
39	3rd Party Factory Owner	St.U.StP.1_StP_Robot UA_Factory Owner	Unreliability in a Factory Robot User Agent
40	Home N/W Operator	O.T.RNO.1_RNO_HNMNO_Factory AN	Misappropriation (theft) of service from a Factory Access N/W
41	Home N/W Operator	St.A.StD.1_StD_IMSI_HNMNO	Loss of availability in an End User IMSI
42	Home N/W Operator	St.A.StH.1_StH_HNHW_HNMNO	Loss of availability in Home N/W Equipment
43	Home N/W Operator	St.A.StP.1_StP_AAA_HNMNO	Loss of availability in the Home N/W AAA
44	Home N/W Operator	St.A.StP.1_StP_HSS_HNMNO	Loss of availability in the Home N/W HSS
45	Home N/W Operator	St.A.StP.1_StP_IAC_HNMNO	Loss of availability in the Home N/W IAC
46	Home N/W Operator	St.C.StD.1_StD_IMSI_HNMNO	Loss of availability for an End User IMSI
47	Home N/W Operator	St.Ct.StH.1_StH_HNHW_HNMNO	Loss of control over Home N/W Equipment
48	Home N/W Operator	St.Ct.StP.1_StP_AAA_HNMNO	Loss of control over the Home N/W AAA
49	Home N/W Operator	St.Ct.StP.1_StP_HSS_HNMNO	Loss of control over the Home N/W HSS
50	Home N/W Operator	St.Ct.StP.1_StP_IAC_HNMNO	Loss of control over the Home N/W IAC
51	Home N/W Operator	St.I.StD.1_StD_IMSI_HNMNO	Loss of integrity in an End User IMSI

No	Trustor	Threat ID	Trustor Concern
52	Home N/W Operator	St.I.StH.1_StH_HNHW_HNMNO	Loss of integrity in Home N/W Equipment
53	Home N/W Operator	St.I.StP.1_StP_AAA_HNMNO	Loss of integrity in the Home N/W AAA
54	Home N/W Operator	St.I.StP.1_StP_HSS_HNMNO	Loss of integrity in the Home N/W HSS
55	Home N/W Operator	St.I.StP.1_StP_IAC_HNMNO	Loss of integrity in the Home N/W IAC
56	Home N/W Operator	St.U.StH.1_StH_HNHW_HNMNO	Unreliability in Home N/W Equipment
57	Home N/W Operator	St.U.StP.1_StP_AAA_HNMNO	Unreliability in the Home N/W AAA
58	Home N/W Operator	St.U.StP.1_StP_HSS_HNMNO	Unreliability in the Home N/W HSS
59	Home N/W Operator	St.U.StP.1_StP_IAC_HNMNO	Unreliability in the Home N/W IAC
60	IoT Sensor Operator	St.A.StH.1_StH_IoT Gateway_IoT Sensor Owner	Loss of availability in an IoT Gateway User Agent
61	IoT Sensor Operator	St.A.StH.1_StH_IoT Sensor_IoT Sensor Owner	Loss of availability in an IoT Sensor
62	IoT Sensor Operator	St.A.StP.1_StP_IoT Gateway UA_IoT Sensor Owner	Loss of availability in an IoT Gateway User Agent
63	IoT Sensor Operator	St.A.StP.1_StP_IoT Sensor UA_IoT Sensor Owner	Loss of availability in an IoT Sensor User Agent
64	IoT Sensor Operator	St.Ct.StH.1_StH_IoT Gateway_IoT Sensor Owner	Loss of control over an IoT Gateway User Agent
65	IoT Sensor Operator	St.Ct.StH.1_StH_IoT Sensor_IoT Sensor Owner	Loss of control over an IoT Sensor
66	IoT Sensor Operator	St.Ct.StP.1_StP_IoT Gateway UA_IoT Sensor Owner	Loss of control over an IoT Gateway User Agent
67	IoT Sensor Operator	St.Ct.StP.1_StP_IoT Sensor UA_IoT Sensor Owner	Loss of control over an IoT Sensor User Agent
68	IoT Sensor Operator	St.I.StH.1_StH_IoT Gateway_IoT Sensor Owner	Loss of integrity in an IoT Gateway User Agent
69	IoT Sensor Operator	St.I.StH.1_StH_IoT Sensor_IoT Sensor Owner	Loss of integrity in an IoT Sensor
70	IoT Sensor Operator	St.I.StP.1_StP_IoT Gateway UA_IoT Sensor Owner	Loss of integrity in an IoT Gateway User Agent
71	IoT Sensor Operator	St.I.StP.1_StP_IoT Sensor UA_IoT Sensor Owner	Loss of integrity in an IoT Sensor User Agent
72	IoT Sensor Operator	St.U.StH.1_StH_IoT Gateway_IoT Sensor Owner	Unreliability in an IoT Gateway User Agent
73	IoT Sensor Operator	St.U.StH.1_StH_IoT Sensor_IoT Sensor Owner	Unreliability in an IoT Sensor
74	IoT Sensor Operator	St.U.StP.1_StP_IoT Gateway UA_IoT Sensor Owner	Unreliability in an IoT Gateway User Agent
75	IoT Sensor Operator	St.U.StP.1_StP_IoT Sensor UA_IoT Sensor Owner	Unreliability in an IoT Sensor User Agent
76	End user	St.A.StH.1_StH_ME_ME Owner	Loss of availability in End User Mobile Equipment
77	End user	St.A.StP.1_StP_Application_ME Owner	Loss of availability in an End User App
78	End user	St.A.StP.1_StP_UA_ME Owner	Loss of availability in a User Agent
79	End user	St.C.PDH.1_PDH_DNAv4 Cache_ME Owner	Loss of availability for the End User DNAv4 Cache

No	Trustor	Threat ID	Trustor Concern
80	End user	St.C.PDH.1_PDH_IMEI_ME Owner	Loss of availability for an End User IMEI
81	End user	St.C.PDH.1_PDH_IMSI_ME Owner	Loss of availability for an End User IMSI
82	End user	St.C.PDH.1_PDH_WiFi MAC Address_ME Owner	Loss of availability for an End User WiFi MAC Address
83	End user	St.Ct.StH.1_StH_ME_ME Owner	Loss of control over End User Mobile Equipment
84	End user	St.Ct.StP.1_StP_Application_ME Owner	Loss of control over an End User App
85	End user	St.Ct.StP.1_StP_UA_ME Owner	Loss of control over a User Agent
86	End user	St.I.StH.1_StH_ME_ME Owner	Loss of integrity in End User Mobile Equipment
87	End user	St.I.StP.1_StP_Application_ME Owner	Loss of integrity in an End User App
88	End user	St.I.StP.1_StP_UA_ME Owner	Loss of integrity in a User Agent
89	End user	St.U.StH.1_StH_ME_ME Owner	Unreliability in End User Mobile Equipment
90	End user	St.U.StP.1_StP_Application_ME Owner	Unreliability in an End User App
91	End user	St.U.StP.1_StP_UA_ME Owner	Unreliability in a User Agent
92	OTT Service Provider	St.A.StH.1_StH_Server_Service Provider	Loss of availability in an OTT Service Host
93	OTT Service Provider	St.A.StP.1_StP_Service_Service Provider	Loss of availability in an OTT Service
94	OTT Service Provider	St.Ct.StH.1_StH_Server_Service Provider	Loss of control over an OTT Service Host
95	OTT Service Provider	St.Ct.StP.1_StP_Service_Service Provider	Loss of control over an OTT Service
96	OTT Service Provider	St.I.StH.1_StH_Server_Service Provider	Loss of integrity in an OTT Service Host
97	OTT Service Provider	St.I.StP.1_StP_Service_Service Provider	Loss of integrity in an OTT Service
98	OTT Service Provider	St.U.StH.1_StH_Server_Service Provider	Unreliability in an OTT Service Host
99	OTT Service Provider	St.U.StP.1_StP_Service_Service Provider	Unreliability in an OTT Service
100	Satellite N/W Operator	O.T.RNO.1_RNO_Satellite MNO_Satellite AN	Misappropriation (theft) of service from the Satellite Access N/W
101	Satellite N/W Operator	St.A.StH.1_StH_Satellite AAA HW_Satellite MNO	Loss of availability in the Satellite AAA Server
102	Satellite N/W Operator	St.A.StP.1_StP_Satellite AAA_Satellite MNO	Loss of availability in the Satellite Operator's AAA
103	Satellite N/W Operator	St.Ct.StH.1_StH_Satellite AAA HW_Satellite MNO	Loss of control over the Satellite AAA Server
104	Satellite N/W Operator	St.Ct.StP.1_StP_Satellite AAA_Satellite MNO	Loss of control over the Satellite Operator's AAA
105	Satellite N/W Operator	St.I.StH.1_StH_Satellite AAA HW_Satellite MNO	Loss of integrity in the Satellite AAA Server
106	Satellite N/W Operator	St.I.StP.1_StP_Satellite AAA_Satellite MNO	Loss of integrity in the Satellite Operator's AAA
107	Satellite N/W Operator	St.U.StH.1_StH_Satellite AAA HW_Satellite MNO	Unreliability in the Satellite AAA Server
108	Satellite N/W Operator	St.U.StP.1_StP_Satellite AAA_Satellite MNO	Unreliability in the Satellite Operator's AAA
109	3rd Party Access Provider	O.T.RNO.1_RNO_Service Provider_WiFi	Misappropriation (theft) of service from a 3rd Party WiFi Access N/W

No	Trustor	Threat ID	Trustor Concern
110	3rd Party Access Provider	St.A.StH.1_StH_Access Point_Service Provider	Loss of availability in a 3rd Party Access Point
111	3rd Party Access Provider	St.A.StP.1_StP_Access Point AAA_Service Provider	Loss of availability in a 3rd Party Access Provider AAA
112	3rd Party Access Provider	St.Ct.StH.1_StH_Access Point_Service Provider	Loss of control over a 3rd Party Access Point
113	3rd Party Access Provider	St.Ct.StP.1_StP_Access Point AAA_Service Provider	Loss of control over a 3rd Party Access Provider AAA
114	3rd Party Access Provider	St.I.StH.1_StH_Access Point_Service Provider	Loss of integrity in a 3rd Party Access Point
115	3rd Party Access Provider	St.I.StP.1_StP_Access Point AAA_Service Provider	Loss of integrity in a 3rd Party Access Provider AAA
116	3rd Party Access Provider	St.U.StH.1_StH_Access Point_Service Provider	Unreliability in a 3rd Party Access Point
117	3rd Party Access Provider	St.U.StP.1_StP_Access Point AAA_Service Provider	Unreliability in a 3rd Party Access Provider AAA
118	Serving N/W Operator	St.A.StH.1_StH_SNHW_SNMNO	Loss of availability in Serving N/W Equipment
119	Serving N/W Operator	St.A.StP.1_StP_MME_SNMNO	Loss of availability in an MME
120	Serving N/W Operator	St.Ct.StH.1_StH_SNHW_SNMNO	Loss of control over Serving N/W Equipment
121	Serving N/W Operator	St.Ct.StP.1_StP_MME_SNMNO	Loss of control over an MME
122	Serving N/W Operator	St.I.StH.1_StH_SNHW_SNMNO	Loss of integrity in Serving N/W Equipment
123	Serving N/W Operator	St.I.StP.1_StP_MME_SNMNO	Loss of integrity in an MME
124	Serving N/W Operator	St.U.StH.1_StH_SNHW_SNMNO	Unreliability in Serving N/W Equipment
125	Serving N/W Operator	St.U.StP.1_StP_MME_SNMNO	Unreliability in an MME
126	Transit N/W Operator	St.A.StH.1_StH_Enterprise LAN_2_HN_Transit Network Operator	Loss of availability in a 3rd Party ID Provider Gateway
127	Transit N/W Operator	St.A.StH.1_StH_HN_2_3P Domain_Transit Network Operator	Loss of availability in an OTT Service Provider Home N/W Gateway
128	Transit N/W Operator	St.A.StH.1_StH_SN_2_3P Domain_Transit Network Operator	Loss of availability in an OTT Service Provider Serving N/W Gateway
129	Transit N/W Operator	St.A.StH.1_StH_SN_2_HN_Transit Network Operator	Loss of availability in the Serving N/W Gateway
130	Transit N/W Operator	St.Ct.StH.1_StH_Enterprise LAN_2_HN_Transit Network Operator	Loss of control over a 3rd Party ID Provider Gateway
131	Transit N/W Operator	St.Ct.StH.1_StH_HN_2_3P Domain_Transit Network Operator	Loss of control over an OTT Service Provider Home N/W Gateway
132	Transit N/W Operator	St.Ct.StH.1_StH_SN_2_3P Domain_Transit Network Operator	Loss of control over an OTT Service Provider Serving N/W Gateway
133	Transit N/W Operator	St.Ct.StH.1_StH_SN_2_HN_Transit Network Operator	Loss of control over the Serving N/W Gateway
134	Transit N/W Operator	St.I.StH.1_StH_Enterprise LAN_2_HN_Transit Network Operator	Loss of integrity in a 3rd Party ID Provider Gateway
135	Transit N/W Operator	St.I.StH.1_StH_HN_2_3P Domain_Transit Network Operator	Loss of integrity in an OTT Service Provider Home N/W Gateway

No	Trustor	Threat ID	Trustor Concern
136	Transit N/W Operator	St.I.StH.1_StH_SN_2_3P Domain_Transit Network Operator	Loss of integrity in an OTT Service Provider Serving N/W Gateway
137	Transit N/W Operator	St.I.StH.1_StH_SN_2_HN_Transit Network Operator	Loss of integrity in the Serving N/W Gateway
138	Transit N/W Operator	St.U.StH.1_StH_Enterprise LAN_2_HN_Transit Network Operator	Unreliability in a 3rd Party ID Provider Gateway
139	Transit N/W Operator	St.U.StH.1_StH_HN_2_3P Domain_Transit Network Operator	Unreliability in an OTT Service Provider Home N/W Gateway
140	Transit N/W Operator	St.U.StH.1_StH_SN_2_3P Domain_Transit Network Operator	Unreliability in an OTT Service Provider Serving N/W Gateway
141	Transit N/W Operator	St.U.StH.1_StH_SN_2_HN_Transit Network Operator	Unreliability in the Serving N/W Gateway

Table 5. Threats to Stakeholder Trust

The algorithm used by Trust Builder to generate threat names is not based on the labelling scheme from Deliverable D2.1 (Use Cases) and the Common Annex (Annex A). It has to accommodate a range of generic as well as 5G-specific threats, and was designed to help one identify the nature of each threat:

- The first 1-2 characters is an abbreviated reference to the type of asset affected by the threat: in the above table they are all Stakeholders, in a few of cases restricted to Organisations.
- After the first dot comes an abbreviated reference to the nature of the compromise, which is usually C, I or A (referring to a loss of confidentiality, integrity or availability), or a potential cause or effect of secondary effects such as O (for overload) or U (for unreliability). All the threats in the above lead to a loss of trust, and for such threats we use the same abbreviation but referring to the type of compromise that leads to the loss of trust. So in this table 'T' refers to misappropriation of resources (i.e. theft), not 'trust' (they are all threats to trust).
- After the second dot comes a string which refers to the pattern of related assets involved in the threat. In every trust threat this pattern includes the affected stakeholder, plus other assets they are using and whose failings cause the loss of trust. Thus StH refers to a stakeholder using a host or device, RNO refers to an organisation operating a radio network, StD is a stakeholder and a data asset they own, and PDH is a stakeholder and a data asset that describes them (i.e. a piece of personal data and its subject).

After the third dot comes an enumerator string to distinguish different threat mechanisms that may require different mitigation strategies but happen to involve the same assets and produce the same type of compromise. After that comes a set of auto-generated identifiers that distinguish where in the system the threat arises: including the system-specific (rather than generic) pattern of involved assets, which has embedded in it the identifiers for system specific assets.

6.4.3.3 Secondary effect analysis: finding root causes

Every threat to trust is in fact a secondary threat, representing the effect some disruption in the system has on a stakeholder's feeling of confidence in the system. Threats to trust are based on stakeholder concerns, linked to some other asset(s) whose behaviour the trustor can sense (at the time or later). In most cases, the behaviour of those assets is disrupted due to some other threat in the system. To understand which stakeholder(s) are in a position to address each trustor concern, we must determine the root causes of the trust threat representing that concern. This capability is built into the Trust Builder enabler: one can select a misbehaviour in the system model (in this case LossOfTrust in a relevant Stakeholder), and get a list of the primary threats that contribute to causing that misbehaviour.

The algorithm used to do this is quite simple, but of course the number of dependencies is large so it would be very error prone if done manually. The algorithm used is as follows:

```
// Initialise lists: Effects are misbehaviours, Causes are threats
Initialise NewEffects = {Selected Misbehaviour}
Initialise Effects = {}
Initialise Causes = {}

Do While (NewEffects is not empty)
        // Select the next new effect and transfer it to the list of effects analysed
        Effect = Car(NewEffects)
        NewEffect = Cdr(NewEffects)
        Effects = Cons(Effect, Effects)

        // Find threats that cause this effect
        Threats = FindCauses(Effect)
        For Each Threat in Threats
                If Not (Threat in Causes)
                        // If the threat is new, add it to the list of causes
                        Causes = Cons(Threat, Causes)

                        // Then analyse its causes to see if they are new
                        NewCauses = FindCauses(Threat)
                        For Each Cause in Consequences
                                If Not ((Cause in Effects) Or (Cause in NewEffects))
                                        NewEffect = Cons(Cause, NewEffects)
                                End If
                        Next Cause
                End If
        Next Threat
End Do
```

Figure 16. Algorithm for finding causes of Loss of Trust

The function FindCauses(Effect) looks for threats that cause the misbehaviour Effect. Note that an effect is a misbehaviour in a specific asset, so threats can only cause an effect if they involve that asset and cause the relevant misbehaviour in it. The function FindCauses(Threat) looks for misbehaviours in assets that cause the threat. This function will return an empty list for a primary threat, but not for secondary threats.

At the end of the procedure described in Figure 16, the list Causes contains all threats that contribute to the secondary effect cascades that end in the misbehaviour originally selected. The primary threats in this list are the root causes leading to that misbehaviour. Applying this procedure for each of the Loss of Trust cases from Table 5, we find that the 141 threats to trust listed above may be caused by a total of 2850 primary threats. It turns out that most of the primary threats can cause multiple threats to trust, and there were 10,467 distinct chains of secondary threats linking the primary threats to the threats to trust. These chains represent paths by which the direct effects of a primary threat propagate through the system until they become evident to (and cause concern in) a stakeholder.

At this point we could list the root causes of each threat to trust, but a table with 10,467 rows would not provide much insight. It is more helpful to summarise by grouping the primary threats into broad classes and counting how many of each type can lead to each loss of trust. The classes chosen represent internal software bugs, remote attacks on connected hardware devices or services, network denial of service attacks, message spoofing (impersonation) or snooping (interception) attacks against communications, unauthorised or unaccountable access, or (in a few cases) physical intrusion and unauthorised local access to devices. The number of root causes of each type is shown in Table 6:

Trustor	No	Concern (Threat to Trust)	Message Interception	Message Spoofing	Network DoS Attack	Remote Exploit on Devices	Remote Exploit on Services	Software Bug	Unaccountable Network Access	Unauthorised Local Access
Access N/W Operator	1	Misappropriation (theft) of service from the Access Network				2	2			
	2	Loss of availability in an eNodeB				2		2		
	3	Loss of control over an eNodeB				2				
	4	Loss of integrity in an eNodeB				2				
	5	Unreliability in an eNodeB						2		
3rd Party ID Provider	6	Loss of availability in a 3rd Party AAA		2	30	5	12	3		
	7	Loss of control over a 3rd Party AAA				2	2			
	8	Loss of integrity in a 3rd Party AAA				2	2			
	9	Unreliability in a 3rd Party AAA		8	31	10	15	9		
	10	Loss of availability in 3rd Party ID Equipment		2	30	2	4	2		
	11	Loss of control over 3rd Party ID Equipment				2	2			
	12	Loss of integrity in 3rd Party ID Equipment				2	2			
	13	Unreliability in 3rd Party ID Equipment						2		
	14	Loss of availability in 3rd Party Credentials					4			
	15	Loss of availability for 3rd Party Credentials	4	2			2			
	16	Loss of integrity in 3rd Party Credentials		2			2			
3rd Party Factory Owner	17	Loss of availability in a Factory AAA		2	30	4	8	2		
	18	Loss of control over a Factory AAA				2	2			
	19	Loss of integrity in a Factory AAA				2	2			
	20	Unreliability in a Factory AAA						2		
	21	Loss of availability in Factory N/W Equipment		2	30	2	4	2		
	22	Loss of control over Factory N/W Equipment				2	2			
	23	Loss of integrity in Factory N/W Equipment				2	2			
	24	Unreliability in Factory N/W Equipment						2		

Trustor	No	Concern (Threat to Trust)	Message Interception	Message Spoofing	Network DoS Attack	Remote Exploit on Devices	Remote Exploit on Services	Software Bug	Unaccountable Network Access	Unauthorised Local Access
	25	Loss of availability in a Factory eNodeB				2		2		4
	26	Loss of control over a Factory eNodeB				2				5
	27	Loss of integrity in a Factory eNodeB				2				6
	28	Unreliability in a Factory eNodeB						2		
	29	Loss of availability in a Factory Robot				1		1		
	30	Loss of control over a Factory Robot				1				
	31	Loss of integrity in a Factory Robot				1				
	32	Unreliability in a Factory Robot						1		
	33	Loss of availability in a Factory Robot User Agent				4		3		4
	34	Loss of control over a Factory Robot User Agent				1				
	35	Loss of integrity in a Factory Robot User Agent				1				
	36	Unreliability in a Factory Robot User Agent		8	31	10	15	8		
	38	Loss of availability for a Factory Temporary Credential	4	2						
	39	Loss of integrity in a Factory Temporary Credential		2						
Home N/W Operator	40	Loss of availability in the Home N/W AAA		7	30	4	8	2		
	41	Loss of control over the Home N/W AAA				2	2			
	42	Loss of integrity in the Home N/W AAA				2	2			
	43	Unreliability in the Home N/W AAA		7	30	6	10	4		
	44	Misappropriation (theft) of service from a Factory Access N/W		2		3	3		1	
	45	Loss of availability in Home N/W Equipment		7	30	2	4	2		
	46	Loss of control over Home N/W Equipment				2	2			
	47	Loss of integrity in Home N/W Equipment				2	2			
	48	Unreliability in Home N/W Equipment						2		
	49	Loss of availability in the Home N/W HSS		7	30	4	8	2		
	50	Loss of control over the Home N/W HSS				2	2			
	51	Loss of integrity in the Home N/W HSS				2	2			
	52	Unreliability in the Home N/W HSS						2		
	53	Loss of availability in the Home N/W IAC		7	30	5	8	3		
	54	Loss of control over the Home N/W IAC		2		2	2			

Trustor	No	Concern (Threat to Trust)	Message Interception	Message Spoofing	Network DoS Attack	Remote Exploit on Devices	Remote Exploit on Services	Software Bug	Unaccountable Network Access	Unauthorised Local Access
	55	Loss of integrity in the Home N/W IAC				2	2			
	56	Unreliability in the Home N/W IAC		2	30	6	10	6		
	57	Loss of availability in an End User IMSI		2	30	2	10	1		
	58	Loss of availability for an End User IMSI	10	7		2	3			
	59	Loss of integrity in an End User IMSI		5		2	3			
IoT Sensor Operator	60	Loss of availability in an IoT Gateway User Agent		3	30	2	4	2		
	61	Loss of control over an IoT Gateway User Agent				2	2			
	62	Loss of integrity in an IoT Gateway User Agent				2	2			
	63	Unreliability in an IoT Gateway User Agent						2		
	64	Loss of availability in an IoT Gateway User Agent		4	31	8	12	6		
	65	Loss of control over an IoT Gateway User Agent				2	2			
	66	Loss of integrity in an IoT Gateway User Agent				2	2			
	67	Unreliability in an IoT Gateway User Agent		14	33	10	15	13		
	68	Loss of availability in an IoT Sensor				2		2		
	69	Loss of control over an IoT Sensor				2				
	70	Loss of integrity in an IoT Sensor				2				
	71	Unreliability in an IoT Sensor						2		
	72	Loss of availability in an IoT Sensor User Agent		4	31	7	6	5		
	73	Loss of control over an IoT Sensor User Agent				2				
	74	Loss of integrity in an IoT Sensor User Agent				2				
	75	Unreliability in an IoT Sensor User Agent		20	39	44	77	30		
End user	76	Loss of availability in an End User App		4	31	8	6	6		
	77	Loss of control over an End User App				2				
	78	Loss of integrity in an End User App				2				
	79	Unreliability in an End User App		5	32	3	5	8		
	80	Loss of availability for the End User DNAv4 Cache	4	2		2	2			
	81	Loss of availability for an End User IMEI	4	2		2	2			
	82	Loss of availability for an End User IMSI	10	7		2	3			
	83	Loss of availability in End User Mobile Equipment		2	30	2	4	2		

Trustor	No	Concern (Threat to Trust)	Message Interception	Message Spoofing	Network DoS Attack	Remote Exploit on Devices	Remote Exploit on Services	Software Bug	Unaccountable Network Access	Unauthorised Local Access
	84	Loss of control over End User Mobile Equipment				2	2			
	85	Loss of integrity in End User Mobile Equipment				2	2			
	86	Unreliability in End User Mobile Equipment						2		
	87	Loss of availability in a User Agent		7	33	14	28	9		
	88	Loss of control over a User Agent				2	2			
	89	Loss of integrity in a User Agent				2	2			
	90	Unreliability in a User Agent		19	38	29	52	26		
	91	Loss of availability for an End User WiFi MAC Address	4	2		2	2			
OTT Service Provider	92	Loss of availability in an OTT Service Host		3	30	1	2	1		
	93	Loss of control over an OTT Service Host				1	1			
	94	Loss of integrity in an OTT Service Host				1	1			
	95	Unreliability in an OTT Service Host						1		
	96	Loss of availability in an OTT Service		3	30	2	4	1		
	97	Loss of control over an OTT Service				1	1			
	98	Loss of integrity in an OTT Service				1	1			
	99	Unreliability in an OTT Service						1		
Satellite N/W Operator	101	Loss of control over the Satellite Operator's AAA				2	2			
	102	Loss of integrity in the Satellite Operator's AAA				2	2			
	103	Unreliability in the Satellite Operator's AAA		11	32	6	10	10		
	104	Loss of availability in the Satellite AAA Server		2	30	2	4	2		
	105	Loss of control over the Satellite AAA Server				2	2			
	106	Loss of integrity in the Satellite AAA Server				2	2			
	107	Unreliability in the Satellite AAA Server						2		
	100	Loss of availability in the Satellite Operator's AAA		5	32	9	14	7		
3rd Party Access Provider	109	Loss of availability in a 3rd Party Access Point		2	30	1	2	1		
	110	Loss of control over a 3rd Party Access Point				1	1			
	111	Loss of integrity in a 3rd Party Access Point				1	1			
	112	Unreliability in a 3rd Party Access Point						1		

Trustor	No	Concern (Threat to Trust)	Message Interception	Message Spoofing	Network DoS Attack	Remote Exploit on Devices	Remote Exploit on Services	Software Bug	Unaccountable Network Access	Unauthorised Local Access
	113	Loss of availability in a 3rd Party Access Provider AAA		2	30	4	4	3		
	114	Loss of control over a 3rd Party Access Provider AAA				1	1			
	115	Loss of integrity in a 3rd Party Access Provider AAA				1	1			
	116	Unreliability in a 3rd Party Access Provider AAA		9	31	6	10	6		
	117	Misappropriation (theft) of service from a 3rd Party WiFi Access N/W				3	3		1	
Serving N/W Operator	118	Loss of availability in an MME		4	30	5	8	3		
	119	Loss of control over an MME				2	2			
	120	Loss of integrity in an MME				2	2			
	121	Unreliability in an MME		7	30	6	10	6		
	122	Loss of availability in Serving N/W Equipment		4	30	2	4	2		
	123	Loss of control over Serving N/W Equipment				2	2			
	124	Loss of integrity in Serving N/W Equipment				2	2			
	125	Unreliability in Serving N/W Equipment						2		
Transit N/W Operator	126	Loss of availability in a 3rd Party ID Provider Gateway				2		2		
	127	Loss of control over a 3rd Party ID Provider Gateway				2				
	128	Loss of integrity in a 3rd Party ID Provider Gateway				2				
	129	Unreliability in a 3rd Party ID Provider Gateway						2		
	130	Loss of availability in an OTT Service Provider Home N/W Gateway				2		2		
	131	Loss of control over an OTT Service Provider Home N/W Gateway				2				
	132	Loss of integrity in an OTT Service Provider Home N/W Gateway				2				
	133	Unreliability in an OTT Service Provider Home N/W Gateway						2		
	134	Loss of availability in an OTT Service Provider Serving N/W Gateway				2		2		
	135	Loss of control over an OTT Service Provider Serving N/W Gateway				2				
	136	Loss of integrity in an OTT Service Provider Serving N/W Gateway				2				
	137	Unreliability in an OTT Service Provider Serving N/W Gateway						2		
	138	Loss of availability in the Serving N/W Gateway				2		2		

Trustor	No	Concern (Threat to Trust)	Message Interception	Message Spoofing	Network DoS Attack	Remote Exploit on Devices	Remote Exploit on Services	Software Bug	Unaccountable Network Access	Unauthorised Local Access
	139	Loss of control over the Serving N/W Gateway				2				
	140	Loss of integrity in the Serving N/W Gateway				2				
	141	Unreliability in the Serving N/W Gateway						2		

Table 6. Model 1: Root causes of loss of trust

6.4.3.4 Choosing control strategies and security controls: blocking sets

Because the threats to trust are at the end of chains of secondary threats, one doesn't necessarily need to address all 2850 of the threats found in order to prevent the situations arising that could undermine Stakeholder trust. We just need to block enough threats to cut the 10,467 cause-and-effect paths between the root causes and the disruption seen by stakeholders. To find such a 'blocking set', we use a recursive function:

```
Function getBlockingSets(ThreatTree)
        // Initialise result
        BlockingSets = Null

        // Find the Children of the root of the ThreatTree
        Children = ThreatTree.getChildren()
        If (Children.isEmpty)
                BlockingSets = {{}}
        Else
                For Each Child in Children
                        If (BlockingSets = Null)
                                BlockingSets = getBlockingSets(child)
                        Else
                                NewBlockingSets = {{}}
                                For Each Set in BlockingSets
                                        For Each ChildSet in getBlockingSets(child)
                                                Union = {}
                                                Union.addAll(Set)
                                                Union.addAll(ChildSet)
                                                NewBlockingSets.add(Union)
                                        Next ChildSet
                                Next Set
                                BlockingSets = NewBlockingSets
                        End If
                Next Child
        End IF
        ThisThreat = {{}}
        ThisThreat.add(ThreatTree.getData())
        BlockingSets.add(ThisThreat)
        Return BlockingSets
End

// Main programme where we use this recursive function
Initialise TrustThreat = Selected Threat to Trust
Initialise ThreatTree = Tree of Threats leading to TrustThreat
BlockingSet = getBlockingSet(ThreatTree)
```

Figure 17. Algorithm for finding a blocking set of threats

For each blocking set of threats (a set of threats which if addressed would address a loss of trust threat), there are frequently several possible choices of control strategy. A naïve application of the above algorithm quickly leads to difficulties as the number of available options becomes huge. It is not uncommon for a given loss of trust threat to have over 100 possible root causes, and if each of these has 2 possible control strategies, the number of possible combinations exceeds 2^{100}. Enumerating all of these combinations is clearly infeasible.

In practice the situation is not so intractable. Our model encodes each way to address a threat using a control strategy, which represents a set of security controls, each deployed to protect one of the assets involved in the threat. For example, to counter a snooping attack on messages exchanged between two processes, both

must implement encrypted communications. If either does not support encryption the threat is not addressed. It turns out that many of the possible control strategies for individual root cause threats involve the same security controls applied at the same assets. The number of distinct control strategies therefore collapses down quite dramatically, but care must be taken during the processing of the trust model to ensure that the data structures in memory remain manageable in size at every step of the analysis. Our strategy was therefore based on the above algorithm, but we did not store the blocking sets as shown in Figure 17. Instead we generated SPARQL queries to extract the security controls needed for each control strategy, storing only the controls needed to prevent each loss of trust, without ever storing the sets of control strategies and threats addressed.

Using this approach allowed us to find a minimal set of security controls (and hence a minimal set of dependencies) to address each threat to trust. The model covers all the usual mitigation approaches, e.g. using security patching or certified devices to minimise opportunities for remote exploits, packet filtering rules and access control policies to limit unauthorised access to networks, services and devices, mutual authentication against spoofing attacks and message encryption against snooping, security monitoring and traffic restrictions to detect and suppress malicious connected devices, and a control we referred to as 'load dependent charging' which represents a risk transfer approach ensuring that excessive network loads are billed to the stakeholder(s) who are in a position to manage the load imposed on the network.

6.4.3.5 Finding Trustees

For each security control specified in the control strategies, we can then ask which stakeholder(s) would need to implement the control within the network. For example, a control representing software patching of a host device operating system against remote exploits would typically require action from the operator of that device, or (for some types of devices) the supplier or manufacturer of the device. On looking through the table of threats that cause loss of trust, and the associated control strategies, we find that in many cases there is no ambiguity about which stakeholder needs to take action. The results are summarised in Table 7, which shows the number of root causes for threats whose control strategy involves each trustee:

Trustor	**Dependencies per Trustee**														
	Access N/W Operator	**3rd Party ID Provider**	**3rd Party Factory Owner**	**Home N/W Operator**	**IoT Sensor Manufacturer**	**IoT Sensor Operator**	**End User**	**ME Manufacturer**	**N/W Equip Manufacturer**	**OTT Service Provider**	**Satellite N/W Operator**	**3rd Party WiFi Operator**	**Serving N/W Operator**	**Transit N/W Operator**	**UICC Manufacturer**
Access N/W Operator	(5)								7				2		
3rd Party ID Provider	9	(39)	16	22		3	24	6	30	9	10	10	10	8	3
3rd Party Factory Owner	9	10	(79)	28		3	12		38	9	10	10	10	8	3
Home N/W Operator	21	26	28	(101)		7	42	4	65	21	26	30	30	10	24
IoT Sensor Operator	21	29	19	43	47	(59)	55	24	22	27	29	35	41	11	20
End user	23	28	18	33	8	19	(97)	47	15	27	28	52	34	13	35
OTT Service Provider	6	6	2	6		4	10			(31)	6	6	6	2	2
Satellite N/W Operator	12	10	4	22		5	24	5	30	9	(35)	19	10	6	3
3rd Party WiFi Operator	9	10	4	24		3	15		14	9	10	(40)	10	6	3
Serving N/W Operator	9	10	4	22	2	5	14		30	9	10	10	(35)	6	3

Trustor	Dependencies per Trustee														
	Access N/W Operator	3rd Party ID Provider	3rd Party Factory Owner	Home N/W Operator	IoT Sensor Manufacturer	IoT Sensor Operator	End User	ME Manufacturer	N/W Equip Manufacturer	OTT Service Provider	Satellite N/W Operator	3rd Party WiFi Operator	Serving N/W Operator	Transit N/W Operator	UICC Manufacturer
Transit N/W Operator									20					(20)	

Table 7. Model 1: Stakeholder Trust Dependencies

The pattern revealed by these tables is not unexpected:

1) Most stakeholders depend on most others for their security.
2) The manufacturers don't depend on anyone else: this is due to the fact that (a) we did not try to model supply chains so each device is considered to have only one manufacturer, and (b) we did not include threats to reputation which certainly would concern most manufacturers.
3) Security begins at home: in almost every case the trustor has to play a role in more control strategies than any of the other stakeholders (see figures in parentheses in Table 7).

The Access N/W Operator and Transit N/W Operator have fewest dependencies. This is because their role is simply to provide connectivity – they are not directly involved in providing management services. They do depend on their device manufacturers, and the Access N/W Operator does depend on the Serving N/W Operator to transmit subscriber checks and so prevent 'theft of service'. There are also few dependencies on the ME Manufacturer and IoT Sensor Manufacturer. This is because in our model, only the End User directly uses IoT services, and most threats originating in the ME domain are actually handled by depending on the tamper proof UICC, the exception being stakeholders running AAA services that use other forms of subscriber authentication.

The remaining stakeholders have a more or less 'all-to-all' dependency, because everyone can be affected in some ways by disruption originating almost anywhere in the end to end network. However, if we break down the dependencies in Table 7 and look at which trustor concerns (i.e. threats to trust) are involved, the pattern is more nuanced. If we consider the dependencies of the Access N/W Operator (below), we see that the only dependency on the Serving N/W Operator is to prevent theft of service from the Access Network:

Trustor: Access N/W Operator		Trustee													
No	**Concern**	Access N/W Operator	3rd Party ID Provider	3rd Party Factory Owner	Home N/W Operator	IoT Sensor Manufacturer	IoT Sensor Operator	End User	ME Manufacturer	N/W Equip Manufacturer	OTT Service Provider	Satellite N/W Operator	3rd Party WiFi Operator	Serving N/W Operator	Transit N/W Operator	UICC Manufacturer
1	Misappropriation (theft) of service from the Access Network									2				2		
2	Loss of availability in an eNodeB	2								2						

3	Loss of control over an eNodeB	1								1						
4	Loss of integrity in an eNodeB	1								1						
5	Unreliability in an eNodeB	1								1						

For the 3rd Party ID Provider, there are also near-singular dependencies:

Trustor: 3rd Party ID Provider		**Trustee**														
No	**Concern**	**Access N/W Operator**	**3rd Party ID Provider**	**3rd Party Factory Owner**	**Home N/W Operator**	**IoT Sensor Manufacturer**	**IoT Sensor Operator**	**End User**	**ME Manufacturer**	**N/W Equip Manufacturer**	**OTT Service Provider**	**Satellite N/W Operator**	**3rd Party WiFi Operator**	**Serving N/W Operator**	**Transit N/W Operator**	**UICC Manufacturer**
6	Loss of availability in a 3rd Party AAA	3	12	1	3		1	7	2	7	3	3	3	3	3	1
7	Loss of control over a 3rd Party AAA		2							2						
8	Loss of integrity in a 3rd Party AAA		2							2						
9	Unreliability in a 3rd Party AAA	3	5	14	16		1	4		10	3	4	4	4	4	1
10	Loss of availability in 3rd Party ID Equipment	3	9	1	3		1	5		4	3	3	3	3	1	1
11	Loss of control over 3rd Party ID Equipment		2							2						
12	Loss of integrity in 3rd Party ID Equipment		2							2						
13	Unreliability in 3rd Party ID Equipment		1							1						
14	Loss of availability in 3rd Party Credentials							2	2							
15	Loss of availability for 3rd Party Credentials		3					4	1							
16	Loss of integrity in 3rd Party Credentials		1					2	1							

This stakeholder depends on most of the others, but actually most of these dependencies come from three specific threats to trust. Closer inspection of the model reveals that the two stakeholders providing IDM services (the 3rd Party ID Provider and the Factory Owner) both depend on an IAC service (UC1.1 and UC1.2). In our model the IAC is provided by the Home Network, which of course interacts with a lot of other domains. Thus we see significant dependencies with the Factory Owner through which the IAC may be attacked directly, and availability problems from disruption of the Home Network which could originate anywhere.

Considering each trustor in turn, this finding is repeated for most operators. Everyone depends on their equipment manufacturers, of course. Availability or reliability can be compromised by root causes throughout the end-to-end network, through cause-and-effect cascades via the Home N/W HSS or IAC services, which in turn can affect AAA services or the function of MMEs. The root causes involved are Network DoS and remote exploits to compromise services or devices.

6.4.3.6 Stakeholder responsibilities

Finally, one can look at the types of security measures that each trustee would need to take in order to manage the trust concerns of their trustors. These are shown in Table 8:

Trustee	Type of Security Measure										
	Access Control	Authentication	Data Encryption	Identification	Load Based Charging	Message Encryption	Secure Configuration	Security Monitoring	Service Authentication	System Integrity	Traffic Suppression
Access N/W Operator								34		22	68
3rd Party ID Provider		4		15		2		38		41	68
3rd Party Factory Owner	4	11		22		2	4	41	2	88	
Home N/W Operator	9	13	3	18	1	2		47	2	138	68
IoT Sensor Manufacturer		6		5						46	
IoT Sensor Operator		6		16				40		46	
End user		11		22		16		11	11	86	136
ME Manufacturer										86	
Network Equip. Manufacturer										271	
OTT Service Provider		4						38		41	68
Satellite N/W Operator		4		13				38		41	68
3rd Party WiFi Operator		11		18	1	8		45		61	68
Serving N/W Operator		5		17		6		39		53	68
Transit N/W Operator								34		56	
UICC Manufacturer		6		3		4		38		45	

Table 8. Model 1: Security responsibilities of trustees

The categories used in our models of control strategies are:

- Access Control: restricting access to authorised users of networks, devices or services. In our model this is handled mainly by the Home N/W operator.
- Authentication: verifying the identity (or access rights) of remote or local users. Most stakeholders will need to implement this at enforcement points for their own services to prevent abuse.
- Data Encryption: storing data (typically keys or passwords) only in encrypted form. In our model these are stored and verified in the Home N/W, so only its operator needs this type of control.
- Identification: having a means of remote or local identification that can be authenticated. This is needed almost everywhere, the exception being the OTT service provider for the reason that our model assumes users would verify the identity of OTT services in the data plane.
- Load Based Charging: assigning liability for network loads to the stakeholder who has control, i.e. not using deals based on the number of devices gaining access, or simple monthly charges. In our model this is done by the Home N/W, and by 3rd party access providers to prevent theft of service.
- Message Encryption: transferring data only in encrypted form. Needed wherever services transfer sensitive information, including hiding IMSI/IMEI or other trackable IDs to ensure user privacy.

- Secure Configuration: configuring devices correctly, i.e. disabling default passwords, etc. In our model this was only an issue for the Factory Owner to prevent attacks within the factory. Most other devices were not considered to be accessible enough for such weaknesses to be exploited.
- Security Monitoring: monitoring of networks or targeted devices or services to detect malicious traffic and identify its source. It turns out this is the second most important security measure in terms of the number of threats to trust it helps to counter.
- Service Authentication: checking the authenticity of a service before communicating with it. This is mostly needed by End Users to avoid spoofing attacks notably spoofing functions of the Access or Serving N/W.
- System Integrity: measures (e.g. software patching or software certification) to remove or minimise exploitable software vulnerabilities or other bugs that could lead to a device acting maliciously. This is the most important measure in our model, and the one that involves manufacturers the most.
- Traffic Suppression: restricting access by devices that are identified (by security monitoring) to be the source of malicious traffic. This is also important in any domain that is likely to be a source of malicious traffic, i.e. any domain that is exposed to external attackers.

Our model does not specify how these measures should be implemented. In some cases, off-the-shelf security technologies can be used. However, these control measures have to be implemented in the control plane of the 5G network, using or extending standardised protocols, and in ways that don't introduce further risks, especially when operating over very large numbers of devices.

The 5G-ENSURE security enablers provide solutions for many of these challenges. For example, the 5G-ENSURE AAA enablers provide authentication, access control and accountability, in such a way that they can be used with large numbers of devices including IoT sensors without causing an overload on key AAA services. As we have seen, compromising these services is one of the main ways secondary effects can propagate through a network and affect large numbers of stakeholders. The 5G-ENSURE privacy enablers provide ways to authenticate to the Home N/W without revealing trackable identifiers within the Access and Serving N/W. 5G-ENSURE security monitoring enablers help to identify vulnerable or compromised devices and provide ways to trigger network management actions to contain them.

6.4.4 Trust Model 2: Virtualisation

6.4.4.1 Model description

The focus for the second model is the effect of using virtualisation technology, which introduces additional parties providing infrastructure on which network operators can obtain a slice in which to create and operate their networks.

The model as constructed in Trust Builder can be seen in Figure 18. Model 2: VirtualisationFigure 18.

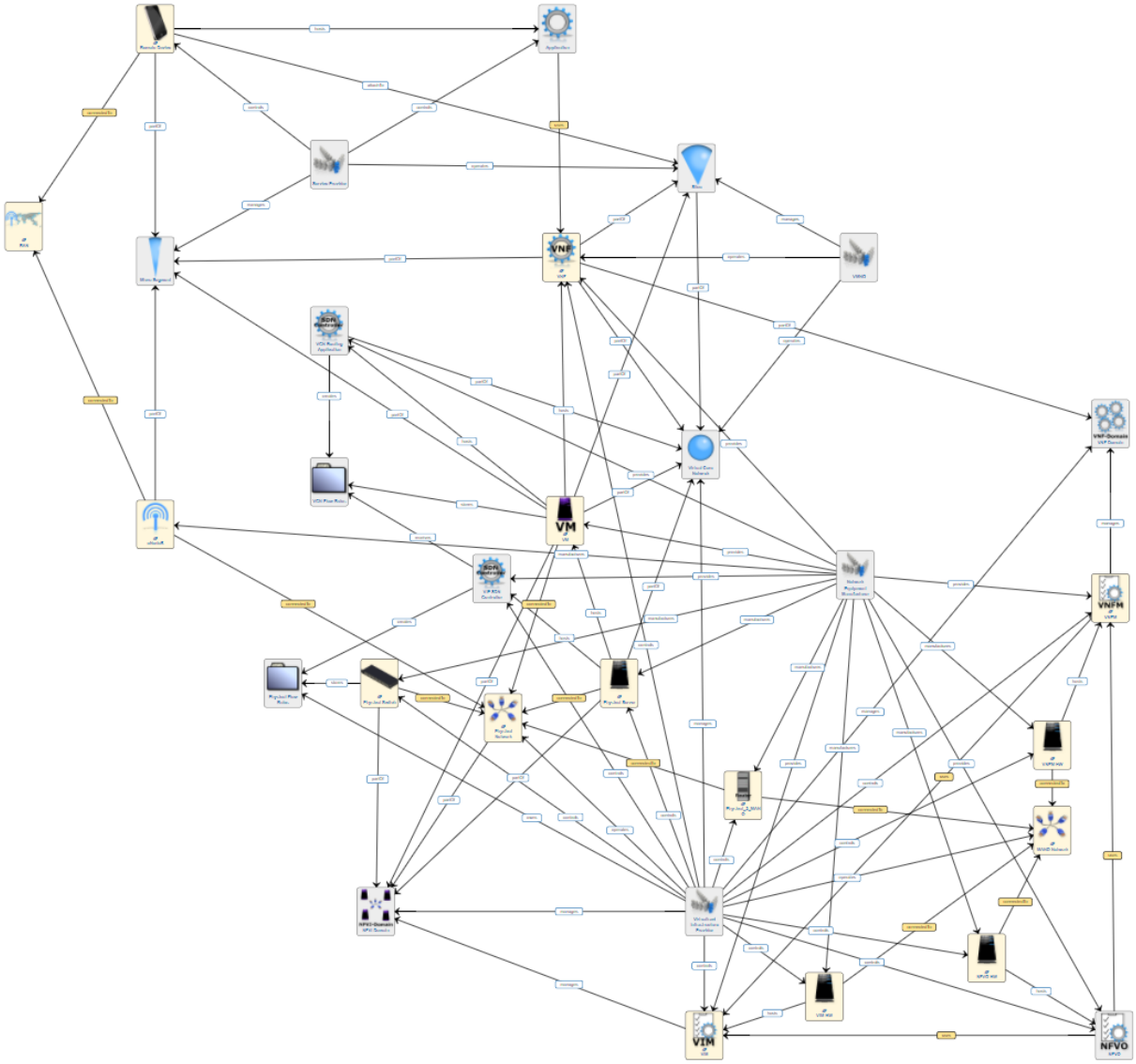

Figure 18. Model 2: Virtualisation

The model combines aspects of use cases UC 5.1, UC 5.2, UC 5.3, UC 5.4, and UC5.5 with an abstraction of the ETSI MANO management and orchestration architecture. More specifically, the model has:

- A Virtualised Infrastructure Provider (VIP) that operates the physical infrastructure (servers, switches, etc.). The VIP manages a Virtual Core Network (VCN) on this physical infrastructure using a combination of Network Function Virtualisation Orchestrators (NFVOs), Virtualised Infrastructure Managers (VIMs), and Virtualised Network Function Managers (VNFMs).
- A Virtualised Mobile Network Operator (VMNO) that operates the VCN. The VMNO partitions the VCN into slices, but relies upon the VIP to implement the partitioning.
- A Service Provider that operates a Slice provided by the VMNO. The Service Provider operates an application or service on the Slice, for example a massively multiplayer online game (MMOG), and further partitions the slice into micro segments according to the security requirements of their service.

These can be seen highlighted in the Trust Builder model in Figure 19.

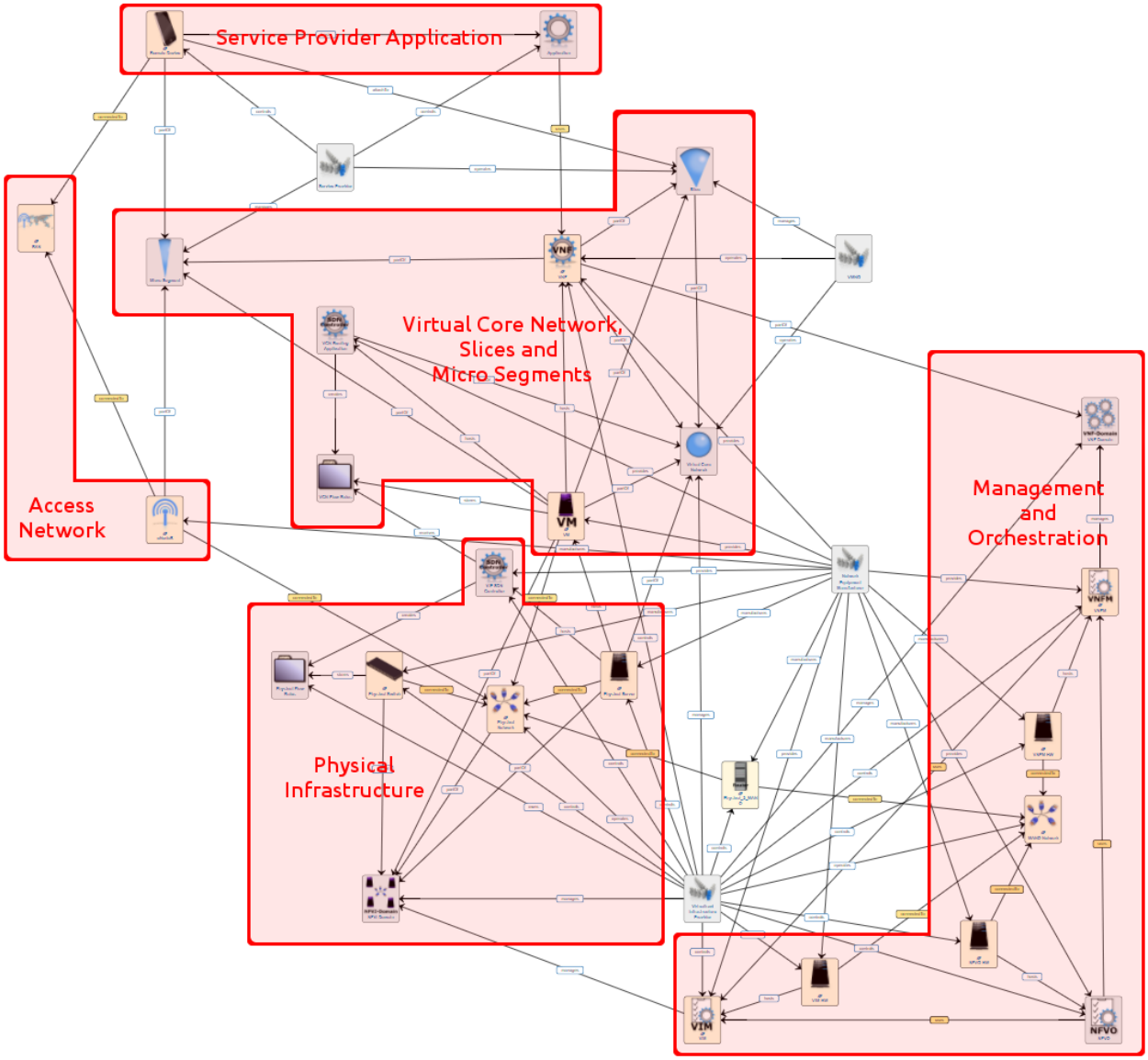

Figure 19. Model 2: Virtualisation: architectural and functional domains superimposed

This model is considerably smaller than the previous one, involving far fewer assets and stakeholders. However, the connections between assets are also much denser, as the entire (virtualised) network, with the exception of the radio access network, consists of a set of slices running on a common infrastructure.

Note that one reason this model is so much smaller is that the service provider is assumed to manage all end-user relationships within their application. Thus there is no Home N/W operator selling connectivity to end users and providing services to manage their identities and access rights. This simplification is based on our analysis of use cases, although clearly it is possible for the 'application' to consist of the usual functions from one or more 5G domains, in which case one would need to stack Model 1 on top of this Model 2.

6.4.4.2 Threats to trust

Processing the Trust Builder model as before allows a list of threats to trust (i.e. trustor concerns) to be extracted. This time there are 87 direct threats to trust for the 3 stakeholders, listed in Table 9:

Trustor	No	Threat To Trust	Trustor Concern
Service Provider	**1**	St.A.ManMicroSeg.1_ManMicroSeg_Micro Segment_Service Provider	Loss of availability in a micro segment
	2	St.A.OpSlice.1_OpSlice_Service Provider_Slice	Loss of availability in a slice
	3	St.A.StH.1_StH_Remote Device_Service Provider	Loss of availability in a remote device
	4	St.A.StP.1_StP_Application_Service Provider	Loss of availability in an End User App
	5	St.Ct.StH.1_StH_Remote Device_Service Provider	Loss of control over a remote device
	6	St.Ct.StP.1_StP_Application_Service Provider	Loss of control over an End User App
	7	St.I.ManMicroSeg.1_ManMicroSeg_Micro Segment_Service Provider	Loss of integrity in a micro segment
	8	St.I.OpSlice.1_OpSlice_Service Provider_Slice	Loss of integrity in a slice
	9	St.I.StH.1_StH_Remote Device_Service Provider	Loss of integrity in a remote device
	10	St.I.StP.1_StP_Application_Service Provider	Loss of integrity in an End User App
	11	St.O.ManMicroSeg.1_ManMicroSeg_Micro Segment_Service Provider	Misappropriation (theft) of service from a micro segment
	12	St.O.OpSlice.1_OpSlice_Service Provider_Slice	Misappropriation (theft) of service from a slice
	13	St.U.ManMicroSeg.1_ManMicroSeg_Micro Segment_Service Provider	Unreliability in a micro segment
	14	St.U.OpSlice.1_OpSlice_Service Provider_Slice	Unreliability in a slice
	15	St.U.StH.1_StH_Remote Device_Service Provider	Unreliability in a remote device
	16	St.U.StP.1_StP_Application_Service Provider	Unreliability in an End User App
Virtualised Infrastructure Provider	**17**	St.A.ManNFVIDomain.1_ManNFVIDomain_NFVI Domain_Virtualised Infrastructure Provider	Loss of availability in an NFVI domain
	18	St.A.ManVCN.1_ManVCN_Virtualised Infrastructure Provider_VCN	Loss of availability in a VCN
	19	St.A.ManVNFDomain.1_ManVNFDomain_Virtualised Infrastructure Provider_VNF Domain	Loss of availability in a VNF domain
	20	St.A.StD.1_StD_Physical Flow Rules_Virtualised Infrastructure Provider	Loss of availability in physical flow rules
	21	St.A.StH.1_StH_NFVO HW_Virtualised Infrastructure Provider	Loss of availability in the NFV orchestrator server
	22	St.A.StH.1_StH_Physical Server_Virtualised Infrastructure Provider	Loss of availability in a physical server
	23	St.A.StH.1_StH_Physical Switch_Virtualised Infrastructure Provider	Loss of availability in a physical switch
	24	St.A.StH.1_StH_Physical_2_MANO_Virtualised Infrastructure Provider	Loss of availability in the physical to MANO network gateway
	25	St.A.StH.1_StH_VIM HW_Virtualised Infrastructure Provider	Loss of availability in the virtual infrstructure manager server
	26	St.A.StH.1_StH_VNFM HW_Virtualised Infrastructure Provider	Loss of availability in the VNF manager server
	27	St.A.StP.1_StP_NFVO_Virtualised Infrastructure Provider	Loss of availability in the NFV orchestrator
	28	St.A.StP.1_StP_VIM_Virtualised Infrastructure Provider	Loss of availability in the virtual infrstructure manager

Trustor	No	Threat To Trust	Trustor Concern
	29	St.A.StP.1_StP_VIP SDN Controller_Virtualised Infrastructure Provider	Loss of availability in the VIP SDN controller
	30	St.A.StP.1_StP_VNF_Virtualised Infrastructure Provider	Loss of availability in a VNF
	31	St.A.StP.1_StP_VNFM_Virtualised Infrastructure Provider	Loss of availability in the VNF manager
	32	St.C.StD.1_StD_Physical Flow Rules_Virtualised Infrastructure Provider	Loss of availability for physical flow rules
	33	St.Ct.StH.1_StH_NFVO HW_Virtualised Infrastructure Provider	Loss of control over the NFV orchestrator server
	34	St.Ct.StH.1_StH_Physical Server_Virtualised Infrastructure Provider	Loss of control over a physical server
	35	St.Ct.StH.1_StH_Physical Switch_Virtualised Infrastructure Provider	Loss of control over a physical switch
	36	St.Ct.StH.1_StH_Physical_2_MANO_Virtualised Infrastructure Provider	Loss of control over the physical to MANO network gateway
	37	St.Ct.StH.1_StH_VIM HW_Virtualised Infrastructure Provider	Loss of control over the virtual infrstructure manager server
	38	St.Ct.StH.1_StH_VNFM HW_Virtualised Infrastructure Provider	Loss of control over the VNF manager server
	39	St.Ct.StP.1_StP_NFVO_Virtualised Infrastructure Provider	Loss of control over the NFV orchestrator
	40	St.Ct.StP.1_StP_VIM_Virtualised Infrastructure Provider	Loss of control over the virtual infrstructure manager
	41	St.Ct.StP.1_StP_VIP SDN Controller_Virtualised Infrastructure Provider	Loss of control over the VIP SDN controller
	42	St.Ct.StP.1_StP_VNF_Virtualised Infrastructure Provider	Loss of control over a VNF
	43	St.Ct.StP.1_StP_VNFM_Virtualised Infrastructure Provider	Loss of control over the VNF manager
	44	St.I.ManNFVIDomain.1_ManNFVIDomain_NFVI Domain_Virtualised Infrastructure Provider	Loss of integrity in an NFVI domain
	45	St.I.ManVCN.1_ManVCN_Virtualised Infrastructure Provider_VCN	Loss of integrity in a VCN
	46	St.I.ManVNFDomain.1_ManVNFDomain_Virtualised Infrastructure Provider_VNF Domain	Loss of integrity in a VNF domain
	47	St.I.StD.1_StD_Physical Flow Rules_Virtualised Infrastructure Provider	Loss of integrity in physical flow rules
	48	St.I.StH.1_StH_NFVO HW_Virtualised Infrastructure Provider	Loss of integrity in the NFV orchestrator server
	49	St.I.StH.1_StH_Physical Server_Virtualised Infrastructure Provider	Loss of integrity in a physical server
	50	St.I.StH.1_StH_Physical Switch_Virtualised Infrastructure Provider	Loss of integrity in a physical switch
	51	St.I.StH.1_StH_Physical_2_MANO_Virtualised Infrastructure Provider	Loss of integrity in the physical to MANO network gateway
	52	St.I.StH.1_StH_VIM HW_Virtualised Infrastructure Provider	Loss of integrity in the virtual infrstructure manager server
	53	St.I.StH.1_StH_VNFM HW_Virtualised Infrastructure Provider	Loss of integrity in the VNF manager server
	54	St.I.StP.1_StP_NFVO_Virtualised Infrastructure Provider	Loss of integrity in the NFV orchestrator
	55	St.I.StP.1_StP_VIM_Virtualised Infrastructure Provider	Loss of integrity in the virtual infrstructure manager
	56	St.I.StP.1_StP_VIP SDN Controller_Virtualised Infrastructure Provider	Loss of integrity in the VIP SDN controller

Trustor	No	Threat To Trust	Trustor Concern
	57	St.I.StP.1_StP_VNF_Virtualised Infrastructure Provider	Loss of integrity in a VNF
	58	St.I.StP.1_StP_VNFM_Virtualised Infrastructure Provider	Loss of integrity in the VNF manager
	59	St.O.ManNFVIDomain.1_ManNFVIDomain_NFVI Domain_Virtualised Infrastructure Provider	Misappropriation (theft) of service from an NFVI domain
	60	St.O.ManVCN.1_ManVCN_Virtualised Infrastructure Provider_VCN	Misappropriation (theft) of service from a VCN
	61	St.O.ManVNFDomain.1_ManVNFDomain_Virtualised Infrastructure Provider_VNF Domain	Misappropriation (theft) of service from a VNF domain
	62	St.U.ManNFVIDomain.1_ManNFVIDomain_NFVI Domain_Virtualised Infrastructure Provider	Unreliability in an NFVI domain
	63	St.U.ManVCN.1_ManVCN_Virtualised Infrastructure Provider_VCN	Unreliability in a VCN
	64	St.U.ManVNFDomain.1_ManVNFDomain_Virtualised Infrastructure Provider_VNF Domain	Unreliability in a VNF domain
	65	St.U.StH.1_StH_NFVO HW_Virtualised Infrastructure Provider	Unreliability in the NFV orchestrator server
	66	St.U.StH.1_StH_Physical Server_Virtualised Infrastructure Provider	Unreliability in a physical server
	67	St.U.StH.1_StH_Physical Switch_Virtualised Infrastructure Provider	Unreliability in a physical switch
	68	St.U.StH.1_StH_Physical_2_MANO_Virtualised Infrastructure Provider	Unreliability in the physical to MANO network gateway
	69	St.U.StH.1_StH_VIM HW_Virtualised Infrastructure Provider	Unreliability in the virtual infrstructure manager server
	70	St.U.StH.1_StH_VNFM HW_Virtualised Infrastructure Provider	Unreliability in the VNF manager server
	71	St.U.StP.1_StP_NFVO_Virtualised Infrastructure Provider	Unreliability in the NFV orchestrator
	72	St.U.StP.1_StP_VIM_Virtualised Infrastructure Provider	Unreliability in the virtual infrstructure manager
	73	St.U.StP.1_StP_VIP SDN Controller_Virtualised Infrastructure Provider	Unreliability in the VIP SDN controller
	74	St.U.StP.1_StP_VNF_Virtualised Infrastructure Provider	Unreliability in a VNF
	75	St.U.StP.1_StP_VNFM_Virtualised Infrastructure Provider	Unreliability in the VNF manager
Virtualised Network Operator	**76**	St.A.ManSlice.1_ManSlice_VMNO_Slice	Loss of availability in a slice
	77	St.A.OpVCN.1_OpVCN_VMNO_VCN	Loss of availability in a VCN
	78	St.A.OpVNF.1_OpVNF_VMNO_VNF	Loss of availability in a VNF
	79	St.Ct.OpVNF.1_OpVNF_VMNO_VNF	Loss of control over a VNF
	80	St.I.ManSlice.1_ManSlice_VMNO_Slice	Loss of integrity in a slice
	81	St.I.OpVCN.1_OpVCN_VMNO_VCN	Loss of integrity in a VCN
	82	St.I.OpVNF.1_OpVNF_VMNO_VNF	Loss of integrity in a VNF
	83	St.O.ManSlice.1_ManSlice_VMNO_Slice	Misappropriation (theft) of service from a slice
	84	St.O.OpVCN.1_OpVCN_VMNO_VCN	Misappropriation (theft) of service from a VCN
	85	St.U.ManSlice.1_ManSlice_VMNO_Slice	Unreliability in a slice
	86	St.U.OpVCN.1_OpVCN_VMNO_VCN	Unreliability in a VCN
	87	St.U.OpVNF.1_OpVNF_VMNO_VNF	Unreliability in a VNF

Table 9. Model 2: Threats to trust

These 87 threats can be triggered by a total of 264 primary threats, there being 2518 distinct paths of secondary effect propagation links from the primary threats to stakeholder concerns. The longest of these paths is only 5 steps long (i.e. the fifth secondary effect propagation mechanism is the one leading to the stakeholder's loss of trust).

6.4.4.3 Trustees

Proceeding as above, we then find control strategies capable of preventing the causes of these threats to trust, and the stakeholders (trustees) who are in a position to implement those controls. These are the trustees on whom the trustors in Table 9 depend. As before, we can get a measure of the degree of trust that is needed from the number of root cause threats each trustor assumes each trustee will help to prevent:

Trustor	**Dependencies per Trustee**			
	Network Equip. Manufacturer	**Service Provider**	**Virtualised Infrastructure Provider**	**Virtualised Network Operator**
Service Provider	23	30	127	108
Virtualised Infrastructure Provider	135	9	334	108
Virtualised Network Operator	10	5	88	70

Table 10. Model 2: Stakeholder trust dependencies

It is fair to say that between virtualised infrastructure providers, virtualised network operators using their infrastructure, and service providers operating on those networks there must be a great deal of mutual trust. Moreover they all depend on the manufacturers of the equipment (and software) used.

6.4.4.4 Stakeholder responsibilities

Finally, we can consider the types of security measures the trustors expect each trustee to implement. These are also found from the control strategies needed to prevent threats to trust, but (as in Section 6.4.3) one considers what types of controls are needed from each responsible party.

The results of this analysis are summarised in table Table 11:

Trustee		**Type of Security Measuer**										
	Access Control	**Authentication**	**Data Encryption**	**FCAPS Management**	**Identification**	**Security Monitoring**	**Slice isolation**	**System Integrity**	**Traffic Suppression**	**VM Migration**	**VNF Certification**	**VNF Scaling**
Network Equip. Manufacturer								162			6	
Service Provider					21			23				
Virtualised Infrastructure Provider		8	2	6	8	62	132	154	121	55		1
Virtualised Network Operator		21				21		244				

Table 11. Model 2: Security responsibilities of trustees

The categories are the same as before, but here we see some of the old categories are not required. This is largely due to the fact that in Model 2 we assumed that identity management and access control would be handled within the Service Provider's application.

However, to counteract threats within the virtualised 5G ecosystem, we also need some new types of security controls associated with fault management and virtual resources. The key additions are:

- VNF certification: the VNO is only allowed to run certified VNFs, i.e. VNFs that have been extensively security tested and certified by a trusted party to a known (and high) evaluation level. In our model we assumed this certification is handled by the equipment (in this case software) manufacturer.
- VNF migration and scaling: implemented by the VIP to handle excessive loads on virtualised devices by adding resources to cope with demand or (if the demand is malicious) to migrate virtualised devices to different VNF domains where they will be safer from attackers.
- Slice isolation: also implemented by the VIP to ensure that tenants in one slice cannot through their actions harm tenants in other slices.

Again, the trust model does not specify how these security measures should be implemented. However, all of the above requirements have been investigated by 5G-ENSURE, and security enablers from WP3 may be used to assist in their implementation.

6.5 Remarks

6.5.1 Variations in trust

The detailed analysis of interdependencies described in this section was only possible through the use of automated analysis of network models created using the Trust Builder enabler. The manual analysis of use cases conducted during the project formed the most important input for the creation of models. However, the manual analysis could not possibly uncover all the trust dependences for the following reasons.

1. Firstly, the number of interdependencies is huge (over ten thousand in the first of our two models), and it is simply not possible to trace these manually. The 5G-ENSURE use case analysts working within Tasks 2.2 and 2.3 very sensibly chose not to attempt this.
2. As a result, each use case analysis focused on specific threatening scenarios related to 5G technology, and ignored the potential for other threats (some also 5G-related identified in other use cases) might arise in the same use case.
3. These threats combine together to create the means by which adverse effects can be triggered or propagated through the 5G network, leading (in some cases) to very deep chains of secondary effects impacting users on the far side of the network.

The final analysis sought to overcome these problems by combining the features of different use cases into one model, and using machine reasoning in Trust Builder to extract a more comprehensive set of threats and interdependencies. However, it must be stressed that in doing this, we had to make assumptions about how different use cases could be combined, and which features could be modified in each use case to map them onto a single end-to-end network model.

A good example of this is the dependency on the Home N/W to provide identity management and subscriber access control services in Model 1. In some use case scenarios, the IAC service (or its equivalent) was located

in other domains. When integrating these use cases, we moved the IAC service to align the use case with those already integrated.

Another example was found in while modelling Mobile user interception and information interception (T_UC2.2_2). Trust Builder identified that the UICC is in actual fact a server (it hosts the USIM service), and thus is potentially vulnerable to the standard threats that affect any server: overload leading to unavailability for example. This was unexpected, as it had not been highlighted by any use case analysts, and was not taken into account as a mechanism for propagation of overload effects caused by threats elsewhere.

In that sense, each of our models represents one possible configuration. In choosing how to integrate use cases in Model 1, we sought to maintain a reasonably good (though by no means unique) picture of how a traditional set of network operators might interact with 3rd parties providing access, identity management or over the top services. The assumption was that these 3rd parties would build on existing capabilities and even business models (e.g. for managing end user subscriptions and billing).

We also assumed that stakeholders may regard any threat to trust as important, so the model assumed that every threat to trust must be addressed. Again, this is a reasonable assumption in a traditional network where the network aims to support a wide range of different users, so almost any threat is likely to be important to at least some of them.

These assumptions lead to two important outcomes from the analysis:

- Since every threat is considered important to a trustor, control strategies are needed for them all, and the number of stakeholders involved (trustees) is very high. In some sense, our models extracted the maximum amount of dependency possible in the network.
- Since some key services were in effect centralised in Model 1, the number of stakeholder dependencies was further increased, since a breach in almost any stakeholder's domain may lead to problems with these key services, which then affects almost all stakeholders.

Under the circumstances, it is not surprising that (e.g. in Table 7) almost every stakeholder depends to some extent on almost every other.

In practice, in a given scenario some of these dependencies are likely to become weak enough to ignore, where either (a) some threats to trust are considered acceptable by the affected stakeholders, or (b) design choices when provisioning the network lead to fewer dependencies than we see in Model 1. It makes sense to ask where the dependencies are greatest and so least likely to become negligible in practice. One way to do this is to count how many control strategies each trustee contributes to in Model 1. The results are shown in Figure 20. This shows only the top three dependencies for each trustor, plus additional dependencies which in the opinion of the authors are unlikely to be broken in practice. This includes a large number between the Home N/W Operator.

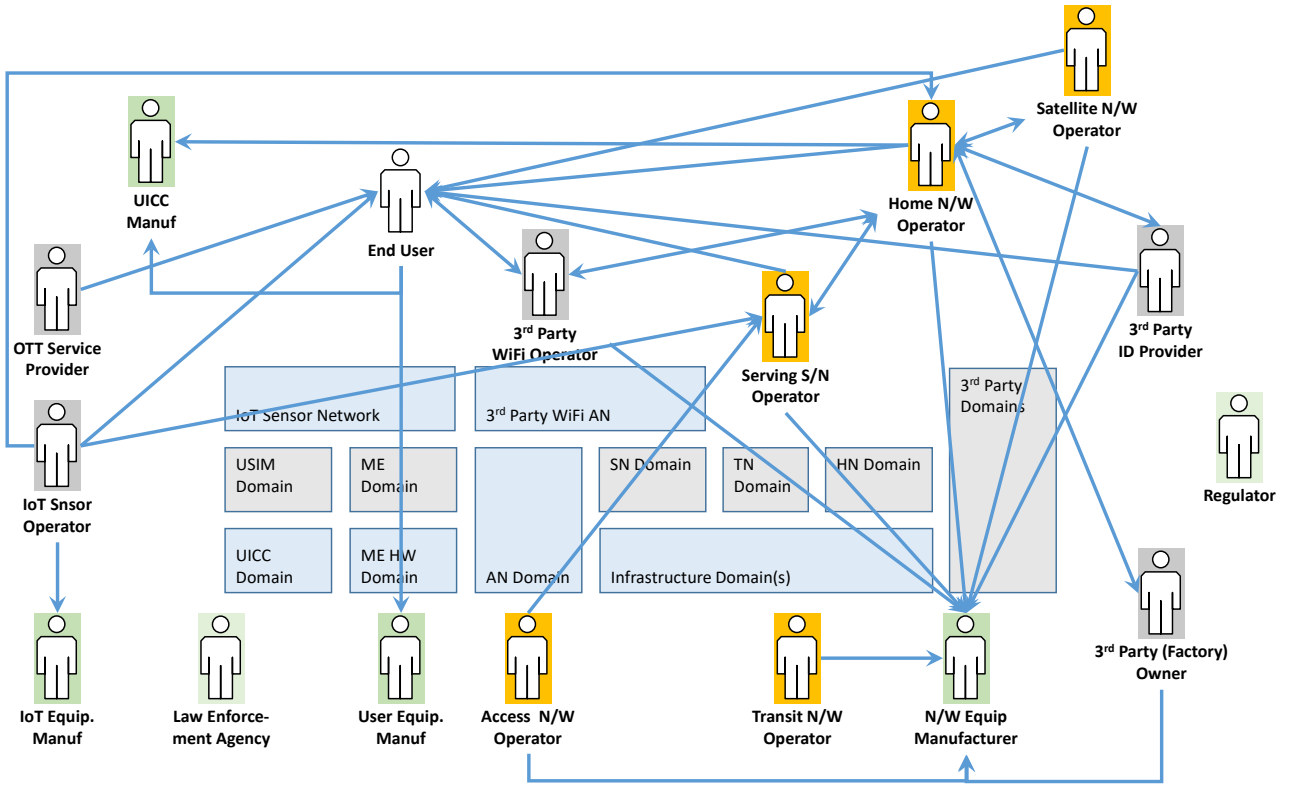

Figure 20. Model 1: main trust interdependencies

In some sense, Model 2 is the complete opposite. Focusing only on the use cases that considered threats from or addressed by the use of virtualisation, this model has very few stakeholders. Again, the network of trust dependencies is very dense with almost every stakeholder depending on the rest. However, in Model 2 this arises because we left out stakeholders who aren't as deeply coupled to the VIP, VMNO and Service Provider.

In practice, any of the stakeholders in Model 1 (except the manufacturers, satellite network operator and probably the end user) could operate over a virtualised network. If they did so, they would simultaneously be acting as the service provider or in some cases the VMNO in Model 2. We believe that some 5G networks probably will operate in this way, where end users need services to be integrated with their existing mobile connectivity. For example, an enterprise wishing to pay for connectivity for employees on their own devices would need to integrate somewhat with their existing mobile service providers.

However, in many vertical applications, we now believe service providers will not attempt to act like any of the stakeholders from Model 1. They will commission network capacity from a VMNO or (if there is one spanning the required physical region) directly from a VIP. The network will then be used directly to support a vertical application: an ecosystem of services with their own identity management, access control and data protection measures. This allows the service provider to integrate their offering with user expectations in these vertical sectors, and in many cases there will be little or no interference with existing user devices. For example, a network could be commissioned by an automotive manufacturer to support connected vehicles through their own embedded mobile equipment. Drivers and passengers would be able to interface their own devices with the vehicle and benefit from its mobile connectivity (e.g. to access entertainment or navigation services). However, their own personal communication devices would not connect directly with the vehicle manufacturer's virtualised network.

Obviously, much depends on the specifics of each application, but we expect each network will in practice need to consider a subset of the dependencies found in one or other of our models. Trust builder was designed to support identification and analysis of potential trust dependencies by the relevant stakeholders, helping them to decide which need to be specified explicitly via service level agreements, and which can be left implicit or ignored altogether.

6.5.2 Relationship to the 5G-ENSURE architecture

The trust model is intimately related to the 5G-ENSURE security architecture, as documented in Deliverable D2.4 [d2.4] and updated (though after much of the analysis reported here) in D2.7 [d2.7]. Section 2.2 in Deliverable D2.7 explains how we expect the trust model will be used by anyone wishing to adopt the 5G-ENSURE architecture.

Firstly, implementers should use the Trust Builder enabler from 5G-ENSURE Task 3.3 (see Deliverable D3.6 [d3.6]) to analyse their specific trust and security requirements. As noted above, in most cases we expect the trust relationships will be a subset of those found and described in Sections 6.4.3 and 6.4.4.

As a result of this analysis, each stakeholder can find out what security control classes they must contribute to in order that the end-to-end network will be sufficiently secure to satisfy trustor expectations. The archetypical examples are shown in Table 8 and Table 11, although in a specific scenario it is likely that some control classes (especially from Table 8) may not be needed. Note that Table 8 and Table 11 list security mechanisms that should be deployed to protect assets controlled by each trustee. These work together to support security control classes defined in Section 4.5 of Deliverable D2.7, with each security mechanism potentially contributing to more than one of the security control classes. For example, traffic restrictions contribute directly to Integrity and Availability, and may help with other security control classes by preventing remote exploits designed to undermine Confidentiality or Privacy.

The trust model does not specify how security mechanisms should be implemented. However, in many cases one must use a specialised form of the underlying mechanism so it can be integrated with the regular 5G network architecture as defined by 3GPP. This is where 5G-ENSURE enablers come in. It is beyond the scope of this report to describe how these enablers can be used to implement threat mitigation strategies. In summary:

- authentication and access control mechanisms can benefit from the 5G-ENSURE AAA enablers from Task 3.1, especially if scalability and integration with 5G authentication mechanisms is needed;
- the Privacy enablers from Task 3.2 provide ways to implement encrypted communications for trackable user and device identifiers even during 5G network sign-on or transfer between cells;
- the Trust enablers from Task 3.3 include Trust Builder itself for analysing trust dependencies, but also provide mechanisms VNF certification and for attestation of microsegment trustworthiness;
- security monitoring is one of the most frequently required security measures to counteract remote attacks, especially DoS attacks, and this is well supported by enablers from Task 3.4;
- the virtualisation and management enablers from Task 3.5 can also be used to detect and mitigate the effect of malicious attacks, including containing them within a single slice using virtualisation management and isolation measures.

These finding will be reported to the 3GPP GSMA standardisation working group dealing with trust in 5G networks after the end of the project, at a meeting in early December 2017.

7 Conclusions and Next Steps

This document revises and builds upon D2.2 “Trust model (draft)” and therefore shares much content. The main changes since D2.2 are as follows:

- Section 5.2 has been added explaining how the use cases from D2.1 were analysed. The interim version of this report summarised the results from the analysis done up to that point, but in this final version the summary description has been replaced by an explanation of how the analysis results were used to create a set of 5G trust models. The details are now confined to Annex A, which contains many more use case analyses than the interim version of this report.
- Section 6.3 is totally new, and covers the trust survey conducted and analysed in the first half of 2017. This survey was filled in mainly by ‘tech savvy’ users some of whom clearly had a good level of knowledge of IT networks, though not necessarily 5G networks. Nevertheless, comparison with previous studies showed their attitudes (if not their level of knowledge) formed a typical spread. Their concerns were also quite typical, though weighted towards pragmatism. The main output of the survey was that practically any threat may be considered to reflect on 5G trustworthiness, and while users expect to play a part, they also expect network operators to protect them.
- Section 6.4 is also totally new, and describes how the results of the use case analysis and survey were used to determine security dependencies and trust assumptions (i.e. trustee responsibilities). Two models were used to capture the important features, one covering the dependencies arising from the involvement of third party stakeholders, and the other addressing dependencies arising from the use of virtualisation. These models were used not only to extract information about the dependencies and corresponding trust assumptions, but also to identify the security control classes that each trustee should implement to fulfil the potential trust assumptions of trustors.
- Section 6.5 provides a summary of findings from the previous two sections. The main conclusion is that in a very general purpose 5G network the number and strength of trust dependencies will be very high, and it seems likely that if virtual networks can be isolated, they will be used to separate out different (especially high security) applications, within which the network construction may be tailored to reduce interdependencies.

Section 6.5 concludes with some discussion of the relationship between the trust model analysis results and the 5G-ENSURE architecture. This shows how trust considerations can be embedded ‘by design’ into the proposed architecture, using a methodology based on the 5G-ENSURE Trust Builder enabler leading to actionable requirements that can be addressed through the use of other 5G-ENSURE enablers. This section also provides hints on which 5G-ENSURE security enablers may be used to address each type of risk, although the details of risk mitigation are not discussed as these lie beyond the scope of this report on trust.

We believe that Phase 2 Projects active on Security and Trust (e.g. NRG5) would take these results on trust and its relationship to risk mitigation fully into account, especially when formulating vertical applications. This is something we would suggest should be promoted through the 5G-PPP SEC WG. The results may also have a bearing on other dimensions, such as business models (which are often also based on or constrained by trust relationships).

The details of the use case analysis are appended in Annex A, and the raw data from the trust survey forms Annex B. Note that Annex A is a common annex with Deliverable D2.6, which covers how one should mitigate risks identified in the use cases.

Due to the strong relationship between trust and risk mitigation, and the unexpectedly rich and complex nature of trust dependencies, it was not possible to produce anything like a complete trust model until the very end of the project. The next step is to socialise the approach to analysing trust and the main findings. Fortunately we have been able to present an interim version of our first trust model at the Cyber Threat Summit in Dublin in October 2017, and IT Innovation has been invited to present the final results to the GSMA FSAG Working Group on Trust in December 2017 – a date we plan to keep despite it falling after the project.

Last but not least the Trust model(s) together with the methodology and enablers accompanying have been advertised in the context of the 5G-PPP Security Working Group now moved to 5G Industry Association where they would continue to advertised/promoted for any project (would it be Phase 2 or Phase 3) interested to consider and possibly make use of them.

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

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

[Kumaraguru and Cranor 2005] Privacy indexes: a survey of Westin's studies. (2005).

[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.

[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.

A Common Annex for D2.5 and D2.6: Use Case Analysis

This section forms a Common Annex for Deliverables D2.5 and D2.6. It contains detailed analysis of the use cases from D2.1 and the corresponding threats identified in D2.3. The Common Annex provides the common starting point for the analysis of trust relationships in D2.5 and the analysis of risk mitigation measures in D2.6.

For each use case an overview is presented mapping the use case to the Security Architecture defined in D2.4. This is the “sunny day” scenario. Then each of the corresponding threats identified in D2.3 is analyzed in turn. These are the “rainy day” scenarios.

A.1 Factory Device Identity Management for 5G Access (UC 1.1)

A.1.1 Use case description with architectural components

In this use case, we consider factory robots accessing a factory network over 5G connectivity but using credentials and AAA managed by a Factory Owner. The factory owner installs 5G base stations in the factory but will rely on an MNO to perform services such as IP connectivity and mobility.

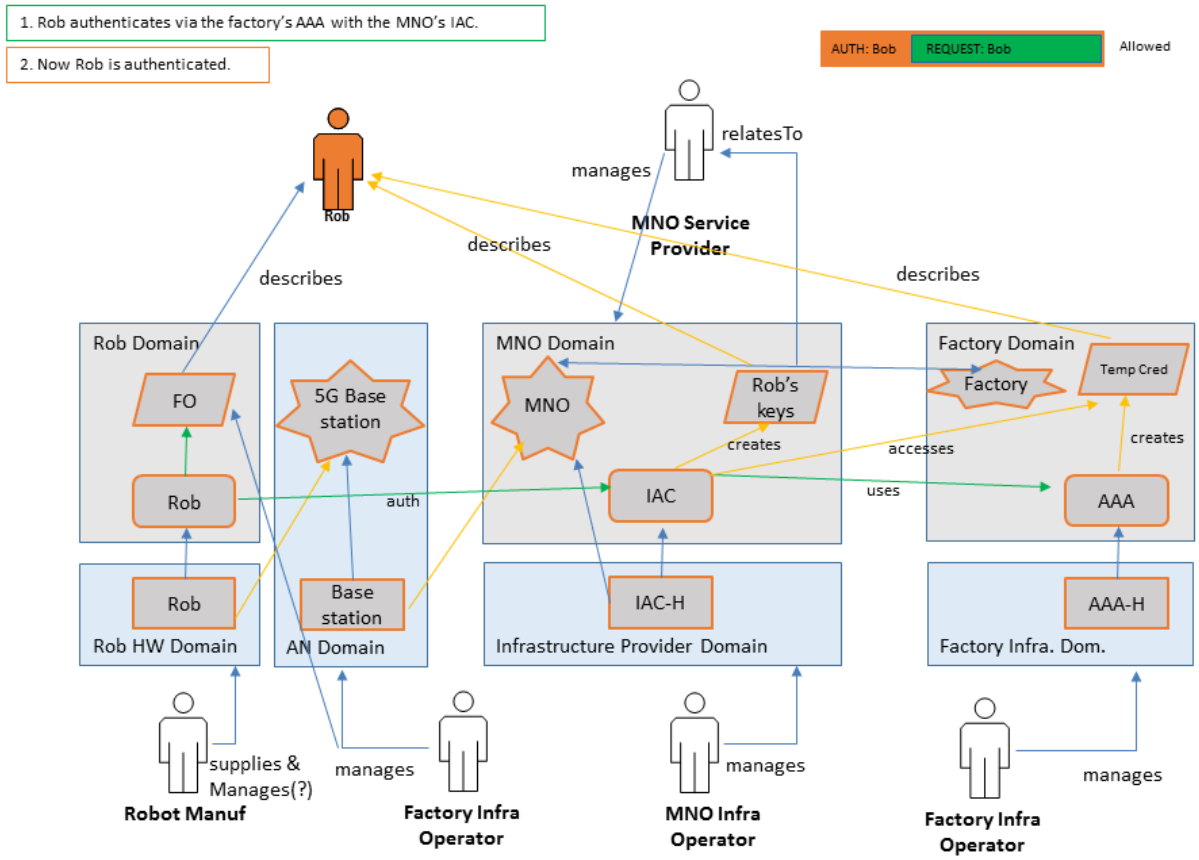

Figure A.21. Factory Device Identity Management for 5G Access (UC 1.1): sunny day scenario

Figure A.21 describes the use case in relation to the architecture, in the absence of any threat (sunny day scenario). When the robot establishes a connection to the base station the base station will ask the IAC for authentication. The IAC forwards the robot's identity in the factory owner identity space to the AAA of the factory owner. After the AAA of the factory owner and the robot have successfully authenticated each other (or IAC and the robot have successfully authenticated each other with support of the factory owner AAA), the MNO starts to provide connectivity services to the robot.

A.1.2 Identified threats

A.1.2.1 Attacker tries to freeride devices authenticated by factory owner (T_UC1.1_1)

The attacker's motive is to freeride devices. When the robot establishes a connection to the base station the base station will ask the IAC for authentication. The attacker could be the factory owner manipulating the AAA for its own advantage, by bringing own devices on network which should not (according to contract), or offering a connection service to third parties. The attacker could also be a third party which has hacked the factory owner's AAA to get own devices onto the network for free.

In Figure A.22, the threat is explained in relation to the architecture. Alice authenticates via the factory's AAA with the MNO's IAC. The attacker Mallory has manipulated the factory owner's AAA server to issue temporary credentials, although service for Alice is not included in the service agreement between MNO and the Factory owner.

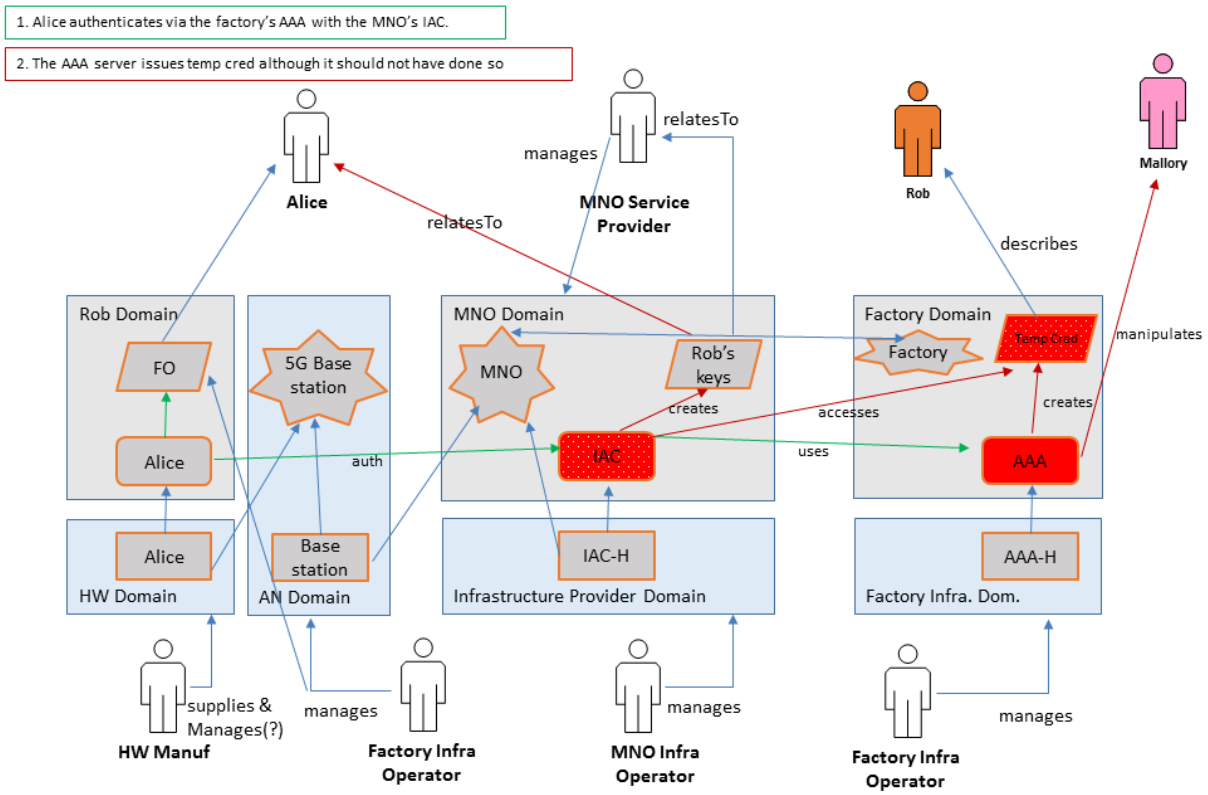

Figure A.22. Attacker tries to freeride devices authenticated by factory owner (T_UC1.1_1) – 'rainy day'

This threat affects particularly the relation between MNO and factory owner. If the factory owner either purposely freerides devices or has not secured its AAA server properly to prevent attackers from doing so, the MNO may be fooled to provide service to the factory owner or external attacker without being paid for the service. Furthermore, general network quality may be affected if a large number of devices freeride the MNO service. In consequence, network quality for legitimate users of the MNO services (the factory owner itself or possibly other users) may be degraded.

Trust implications

This threat affects primarily the MNO:

- The MNO may lose income due to freeriding devices that use the MNO's service without payment.

- The MNO may also lose trust from legitimate users if the network quality degrades due to a large number of illegitimate devices using the MNO's network.

However, the threat also affects legitimate customers of the MNO. The legitimate customers could be the factory owner, but also other customers of the MNO:

- Network quality could degrade due to a large number of illegitimate devices using the MNO's network.

The factory owner may also be affected specifically:

- If the attack was performed by an external attacker to a legitimate factory owner and the attack is finally discovered, the factory owner may lose trust from the MNO.

Threat mitigation strategy

The threat should be addressed both at the MNO domain and the factory domain.

At the MNO domain, the MNO should deploy charging and network management solutions that are designed to ensure both payment for provided services and adequate network quality. In detail:

- The charging solution towards the factory owner should be load-dependent. In this way, the factory owner will not be able to freeride devices without paying for them. Such a charging solution will also give incentive to the factory owner to secure its AAA server properly against external attacks.
- The network management solution should make it possible to isolate the factory owner's network resources, so that other users of the network are not influenced by possible attacks in the factory owner domain. Technically, this could be solved by QoS or slicing, or simply by providing a separate network infrastructure to the factor owner that is not shared with other customers.

At the factory domain, the factory owner should secure its AAA server against external attacks.

A.2 Using Enterprise Identity Management for Bootstrapping 5G Access (UC 1.2)

A.2.1 Use case description with architectural components

This use case describes a situation where an enterprise wants to provide its employees with devices that are 5G enabled. It is wishes to use its existing collection of credentials to authenticate with the MNO operator, however the enterprise does not wish to operate its own HSS. So the MNO operator is willing to allow provisioning of 5G credentials to the enterprise.

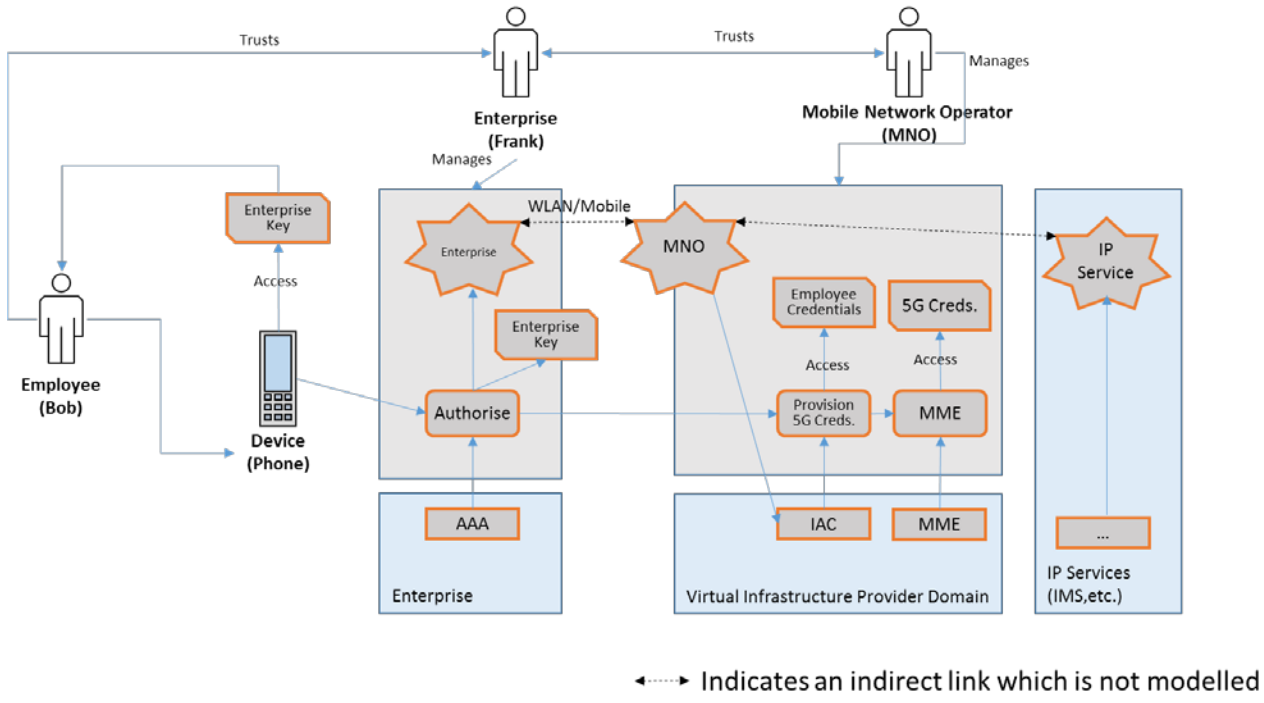

Figure A.23. Using Enterprise Identity Management for bootstrapping 5G Access (UC 1.2): sunny day scenario

Starting from left to right of Figure A.**23**, we have the enterprise's device, which is used by the employee. The device will use the enterprise key, which is maintained by the enterprise's AAA server, to request access to the MNO's 5G service. The MNO will authenticate the device based on the employee's credentials, and provision access to the 5G network to the device. The MNO trusts the enterprise to maintain control over who has access to the devices and credentials. The enterprise trusts that the MNO does provide its devices with adequate service and does so in a secure fashion.

A.1.1 Identified threats

A.2.1.1 Leaked AAA credentials (T_UC1.2_1)

The root cause is the leaking of AAA credentials from the employee network, allowing unauthorised actors to authenticate with the MNO. The MNO may provide them with access to 5G connectivity, at the expense of the enterprise. The credential data leak could be from a malicious insider, or phishing attack on the enterprise, or even on the employee.

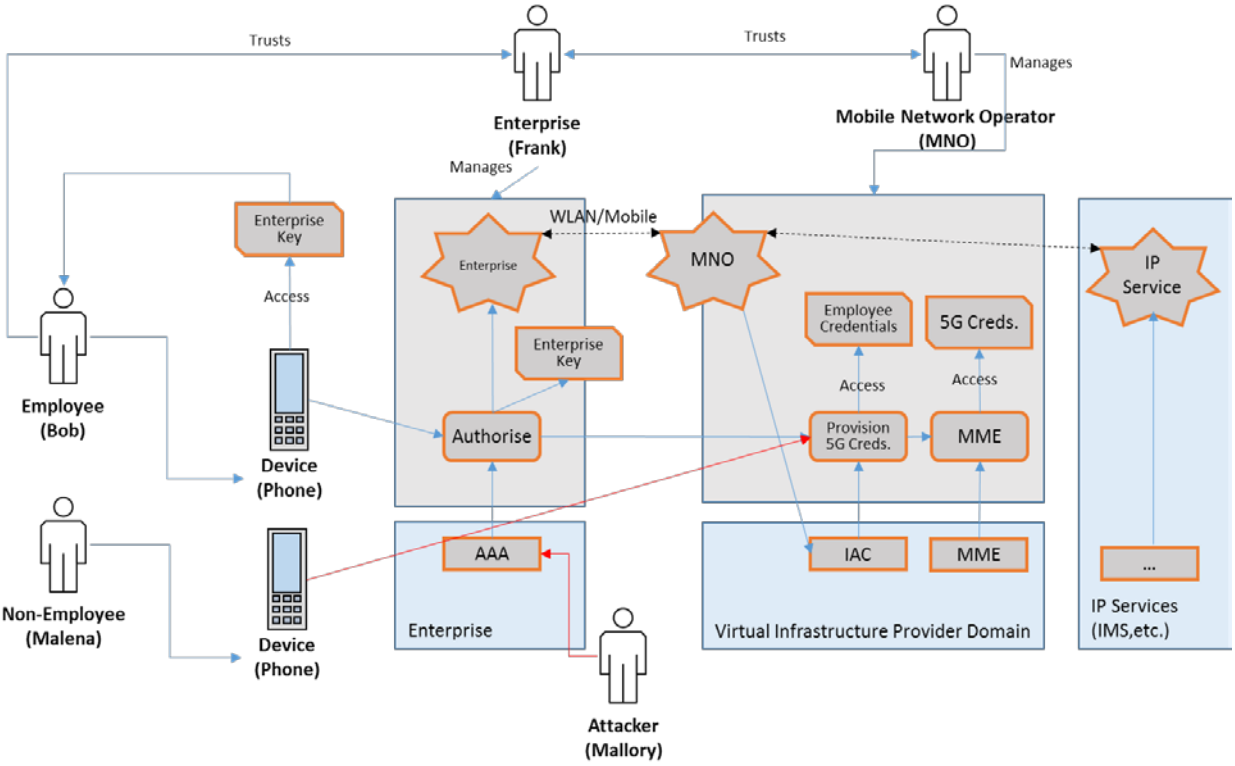

Figure A.24 Leaked AAA credentials T_UC1.2_1 – 'rainy day'

Once credentials are leaked from the AAA server, as shown by the attacker 'Mallory', it would then be possible for malicious users to connect to the MNO using the enterprise details. As showing by Malena. Once an unauthorised user is able to connect to the MNO as an employee they will have access rights which match the compromised credentials. This could allow for further lateral movement with the enterprise. It also means that what usage costs occur will be charged to the enterprise, Frank.

Secondary effects of this could be the loss of access for employee's who have had their details compromised. It could also result in a loss of availability between the enterprise and the MNO if a large quantity of the malicious users were to access the MNO at once.

Trust implications

The MNO trusts that the enterprise will secure their AAA server and employee devices enough to prevent such data leakage and abuse of the system. The enterprise also trusts that the MNO would alert the enterprise to any anomalous access to their network, which could be the result of unauthorised activity from. One other such trust issue to consider here is that the employee might use the enterprise credentials for personal use of the MNO's network. This again might be something the enterprise would want the MNO to prevent, such as only provisioning access to 5G networks from certain locations.

Threat mitigation strategy

Once such mitigation strategy would be to limit credentials to device and user, this would mean that even if an attacker is able to compromise the AAA server and steal the certificates/hashes. They can only be used on a specific device. This mitigation would be completed by the enterprise who manage the credentials. Another mitigation method would be to enable EAP based authentication to the AAA server. Again, this would have to be completed by the enterprise, but would provide a more secure authentication method.

A.3 Satellite Identity Management for 5G Access (UC 1.3)

A.3.1 Use case description

This use case is focus on represent the scenario where a Service Provider needs to warranty the authenticity of the satellite network devices across the network to avoid the appearance of unauthorized or fake satellite devices that can be enable the access to the network resources to end users with not trustable goals. The next figure represents the start scenario and the elements involved, in this case the satellite network domain will have a special focus.

The SNO systems is collecting information about all the Satellite eNodeB and GW Satellite across the system offering real time information to the operator about the devices status.

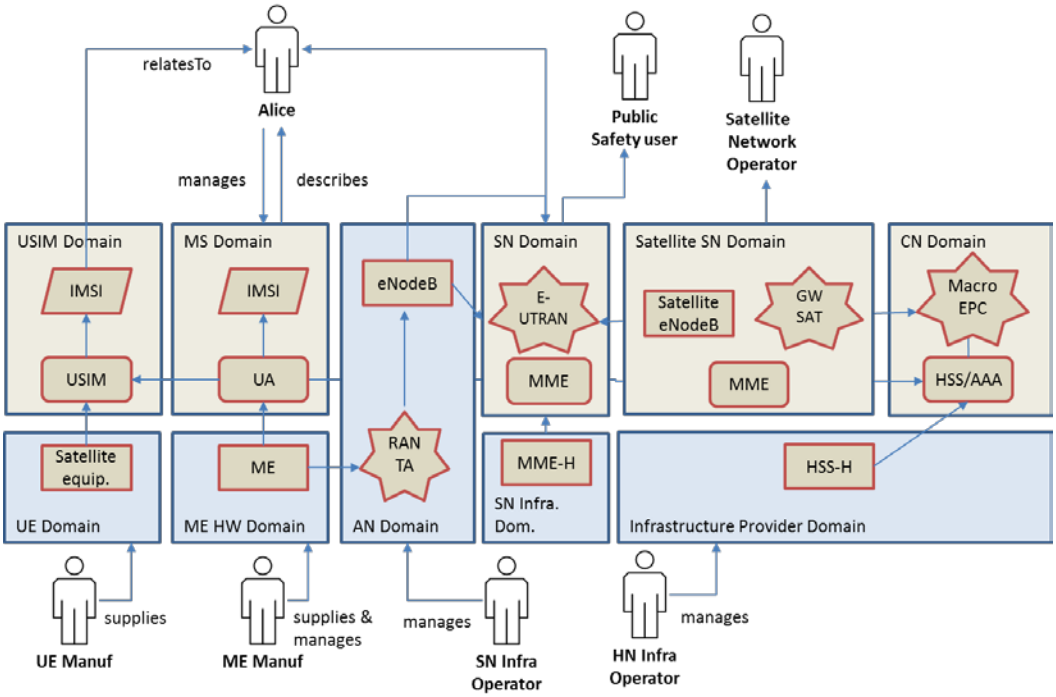

Figure A.25. Satellite Identity Management (UC 1.3): sunny day scenario

A.3.2 Identified threats

A.3.2.1 Unauthorised activities related to satellite devices or (satellite) network resources (T_UC1.3_1)

A Service Provider (i.e. a telecommunications company) has a contract with the Satellite Network Operator (SatNO) to supply a suitable satellite system capacity to be assigned to the customer in a dynamic way. However this capacity use is limited and should be strictly controlled/monitored to warranty the correct use and avoid extra-charges for satellite capacity extra consumption or generate possible interference or unreal work load over the network that can limit the resources assignation across the users.

This threat can impact on a wide amount of services present over the network.

In this case, Alice detect a decrease in the network performance accessing to different applications, in parallel the SNO detects an increase in the satellite capacity resources uses from one or multiple Satellite eNodeB, the SNO after analyse the traffic consumption statistics from previous days can determine that an unauthorized application is requesting a huge amount of satellite resources, regarding to warranty the resources for the rest of the users, the application is blocked at Satellite eNodeB level to avoid service

degradation. As a result the threat have been neutralized and the service impact for the users have been minimized.

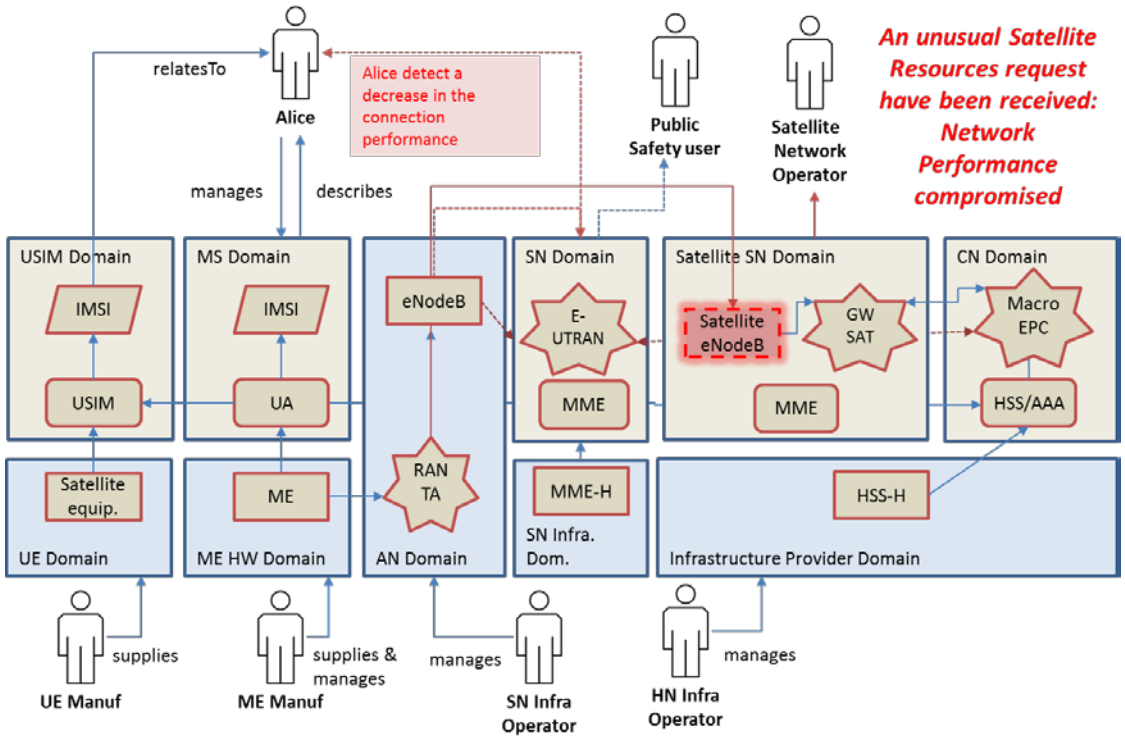

Figure A.26. Unauthorised activities related to satellite devices or (satellite) network resources (T_UC1.3_1) – 'rainy day'

Main domains involved in this actions are shown in Figure A.26, AN Domain cover the Radio Access network capabilities where traditional eNodeB are located, SN domain offers the connection between the Satellite SN Domain compose by Satellite eNodeB and GW Satellite shows the necessary components to provide satellite resources allocation into the network.

Without the mechanisms present, reliability of the system is in risk, presenting a potential point of failure in the network.

Trust implications

Potential Trust Implications:

- Customers can perceive a lack of trust based on the network performance and the capabilities for the VMNO to guarantee their service level agreements.
- The VMNO needs to demonstrate a trustable recovery actions regarding to guarantee the control over the VNO, offering detailed action plans that cover typical operations issues in sensible highly exposed locations.
- In this use case, the threat is specially focus in an insider attack that can be try to access to collapse the network affecting a huge amount of customers.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Real time data gathering about network status and trends analysis can supply the foundations to accurate network performance and generate patterns consumptions at Satellite eNodeB level.
- Establish clear action plans identifying critical elements and contentions actions as suggested in the rainy scenario can be key to mitigate the risks.
- Generate pre-emptive configuration policies across the Satellite eNodeB can decrease the reaction time and automatize the network recovery process, decreasing the SNO / VMNO actions and dependencies.

A.3.2.2 Fake roaming from terrestrial network into satellite network (and vice versa) (T_UC1.3_2)

A Service Provider (i.e. telecommunications company) has a contract with the Satellite Network Operator (SatNO) to supply a suitable system capacity associate to an specific number of Satellite eNodeB, this satellite eNodeB are responsible to provide services access to the end users in a determinate coverage area, the Satellite Network Operator needs to warranty the end users connectivity across the satellite eNodeB resources for the scenarios identified, any attend of access to these resources can generate extra charges for capacity use, decrease the network performance or generate potential security breaches.

This threat can be impact in the performance of several services when service lost scenarios or service recovery appears and satellite resources are incorrectly allocated or the satellite capacity cost is increased in a non-justifiable way.

In this case a natural disaster occurs and connection between Alice and eNodeB is lost, the network manager detects the failure event and proceed to performs topology calculation to guarantee ultra-reliable services. The new topology is configuration is populate across the network elements and the satellite-capable eNB activates the alternative route to Macro EPC via the satellite link. As a result the service lost is minimized and service restore is achieved, the issue appears when the network connection across the eNodeB is recovered and connection needs to be re-established using the old path, during all the time that the calls have been routed using the Satellite eNodeB a Fake Roaming scenarios is on-going, network operator needs to minimize the time and the traffic involved.

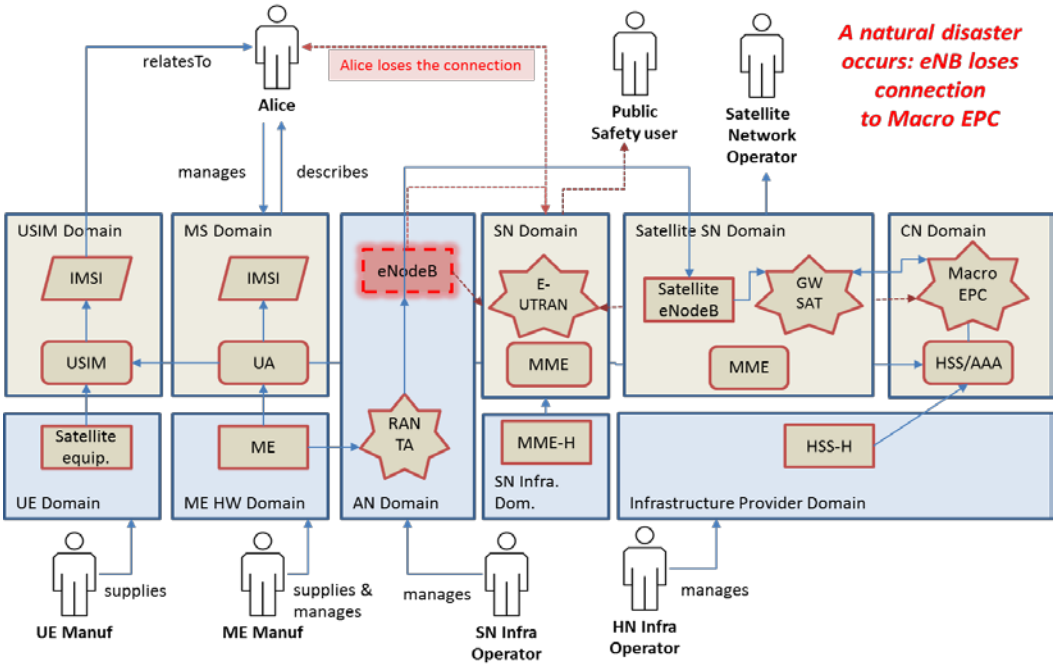

Figure A.27. Fake roaming from terrestrial network into satellite network (and vice versa) (T_UC1.3_2) – 'rainy day'

Main domains involved in this actions are shown in Figure A.27, AN Domain cover the Radio Access network capabilities where traditional eNodeB are located, SN domain offers the connection between the Satellite SN Domain compose by Satellite eNodeB and GW Satellite shows the necessary components to provide satellite connections capabilities to the network increasing the recovery time and decreasing the service lost, but adding the possibilities to generate fake roaming scenarios for the calls involved between both systems under different scenarios.

Without the mechanisms present, service lost time will be increasing, reliability of the system is decrease and mitigations actions are limited, presenting a potential point of failure in the network.

Trust implications

Potential Trust Implications:

- Customers can perceive a decrease of the network performance due to use satellite resources while terrestrial network resources are still available. Additionally in the opposite way customer can perceived that network is unavailable when they are incorrect assign to resources over the terrestrial network when this is not fully available.
- In this use case, the threat the issue specially focus in the service recovery and service lost operation scenarios, where availability in the eNodeB or satellite eNodeB can be the root case, and service level agreement can be compromised.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Establish monitoring Probes focus in not just verify the status of the access at lowest layers and check the service status in the highest layers before balance the traffic between satellite and terrestrial networks.
- Establish clear action plans identifying critical elements and contentions actions as suggested in the rainy scenario can be key to mitigate the risks.
- Generate ad-hoc mechanism to control the switch over process to identify the elements involved and the traffic flows across them.

A.4 MNO Identity Management Service (UC 1.4)

A.4.1 Use case description

This use case describes an MNO which provides an advanced management service to a 3rd party service provider on behalf of a user. When the user Bob, connects to the MNO with his device the MNO assigns a 'Network ID' to him. This network ID allows the service provider to gain detailed information about Bob which is provided by the MNO. Note that the MNO can share the user data only if the user has already agreed on that. The service provider may use this information to determine the level authentication methods needed to access the service.

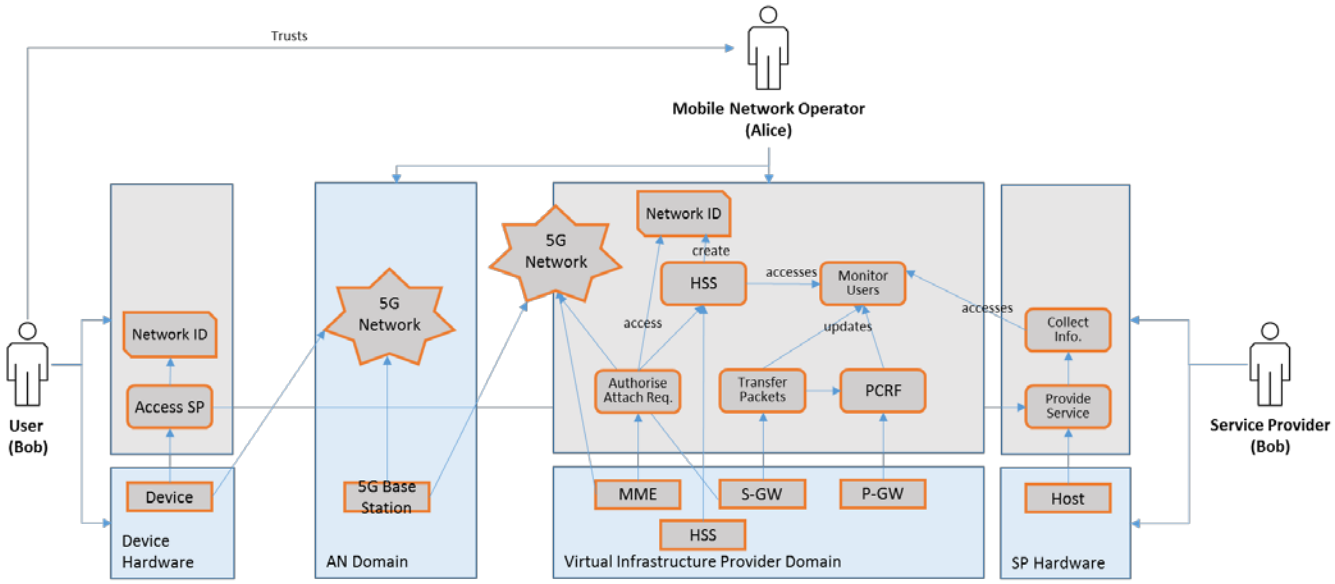

Figure A.28. MNO Identity Management Service (UC 1.4): sunny day scenario

The key stakeholders in this instance are the MNO and Service Provider. The MNO agrees to provide the service provider with details on the user's device, such as the location it is in, software and hardware version and so on. This allows for the service provider to determine what types of authentication to challenge the user. This allows the service provider to better secure their infrastructure from attacks. This means that the user will have to trust both the MNO and SP with more personally identifiable information.

A.4.2 Identified threats

A.4.2.1 Compromised data (T_UC1.4_1)

The root cause of this attack is an attacker compromising a network component, in this case the device. Then forcing the device to use a weaker protocol which is susceptible to decryption attacks. This will allow the

attacker to effect the integrity and confidentiality of the data which is collected by the MNO then sent to the SP. Resulting in a secondary effect of the service provider being feed misinformation. In certain cases this may prevent the user from accessing the service.

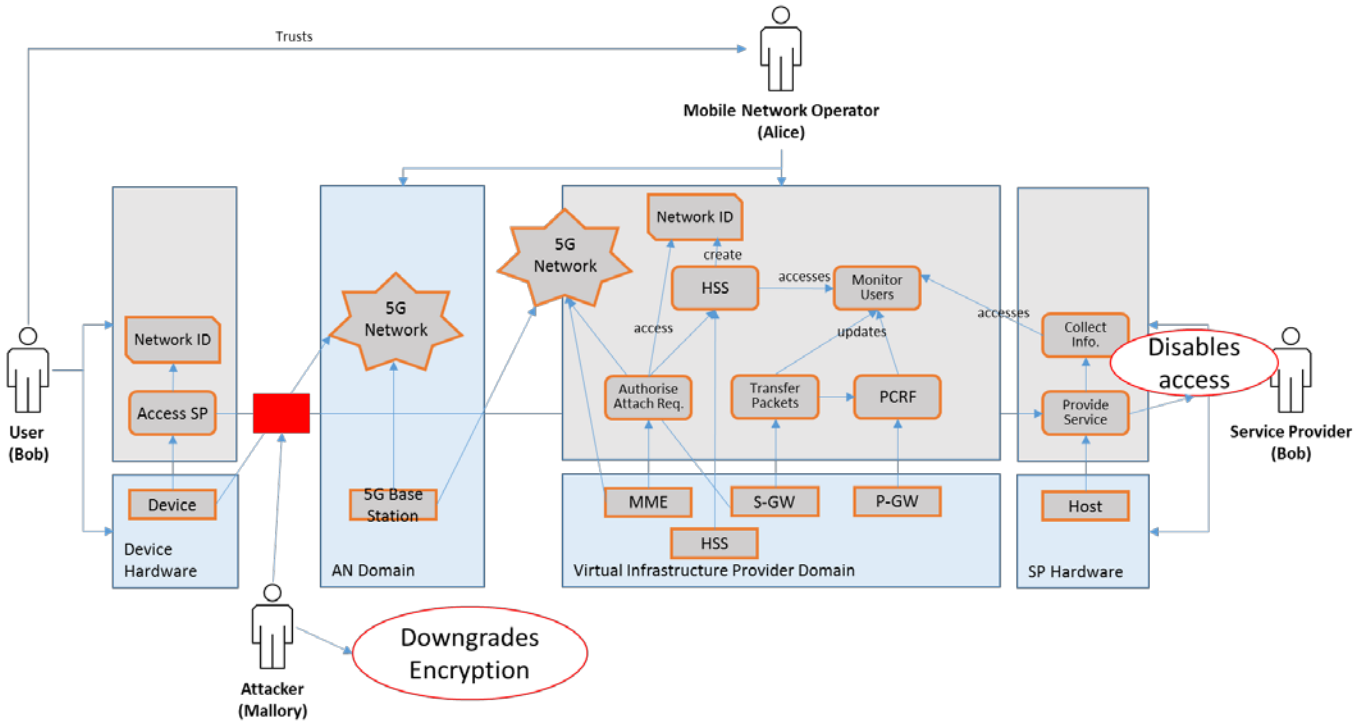

Figure A.29. Compromised data (T_UC1.4_1)

The key components for this threat are the user's device and the service provider which relies on the metrics provided by the MNO. This threat exploits the fact that the device is unable to prevent the downgrade attack, and that the MNO accepts the invalid data fed to it by the attacker, Mallory.

Secondary effects arising from this threat would be other attacks which Mallory is capable of accomplishing other than the bypassing the service providers extra authentication. Such as manipulating data from the user to the MNO and vice versa. This could have a catastrophic effect on the network if Mallory is able to perform a DoS to one or more of the MNO services.

Trust implications

The service provider trusts the data received from the MNO is accurate. Indeed, the MNO should apply mechanisms to verify that the reported network information is not compromised. If this data is incorrect or falsified then the actions which the service provider takes do not match the real world scenario and result in a loss of trust between the MNO and the service provider. The MNO may try to transfer this trust over to the user or device manufacturer which allows for the downgrade attack to succeed.

Threat mitigation strategy

In order to protect against this threat, the MNO needs to perform validity checks on the collected data. This might include remote attestation protocols such as Direct Anonymous Attestation (DAA), which enables remote authentication of a trusted computer whilst preserving privacy of the platforms user. This would be placed in the MNO network when data is collected about the device. This would be expected to be completed

by the MNO since they are the stakeholders which will be collecting the data. It would be performed each time the user's device connects to the network. Another mitigation, again expected to be completed by the MNO, would be to roll out new encryption protocols which prevent encryption downgrade attacks. This would be placed on either the device or the access network.

A.4.2.2 User's privacy attack (T_UC1.4_2)

In this threat, we can distinguish two types of attackers: an external attacker and an internal attacker. In the first case, an external attacker can try to intercept exchanges between the MNO and the service provider to get the metrics about the user. In the second case, the service provider is considered as malicious. The service provider may try to get information about the user more than what is really needed to enhance the security of the service. The goal of the service provider can be to construct profiles of user and use it to other purposes than the security of the service such as oriented publicity. Normally, the MNO collects data about user (after user's agreement), performs cryptographic computations on the collected data to obtain metrics. These metrics are going to be shared with the service provider (Step (d) in Figure 5 of the deliverable D2.1). If the computed metrics do not properly anonymize user's data, this can break the user's privacy. These are the main sources of the threat.

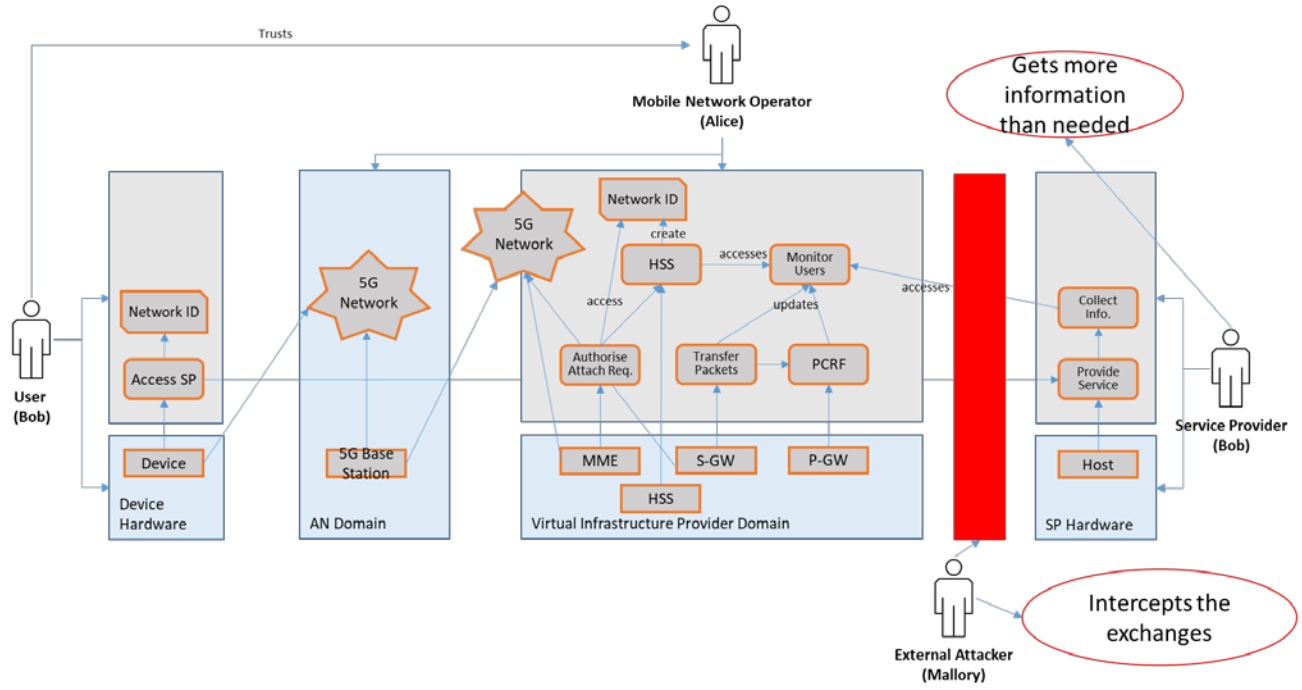

Figure A.30. User privacy attack (T_UC1.4_2)

Trust implication

In the first case, the user trusts the MNO and service provider that the exchanges are secured.

In the second case, the user trusts the MNO that he collects only data agreed on previously when adhering to this service. The user also trusts the MNO that he properly anonymizes the collected data and share only metric with the service provider.

Threat Mitigation strategy

In order to protect against this threat, the MNO and the service provider need to use approved security protocols to secure their exchanges, such as IPsec. The MNO should also use securely approved algorithms to anonymize the collected data such as k-anonymity algorithm. The MNO can also provide the user the ability to check and modify the shared metrics and the level of anonymization.

A.5 Device Identity Privacy (UC 2.1)

A.5.1 Use case description with architectural components

The use case relates to a user attaching to a 5G network. The description of this procedure and its related function blocks are illustrated in Figure A.31, which illustrates the scenario with respect to the architecture, in the absence of any threat (the sunny day scenario).

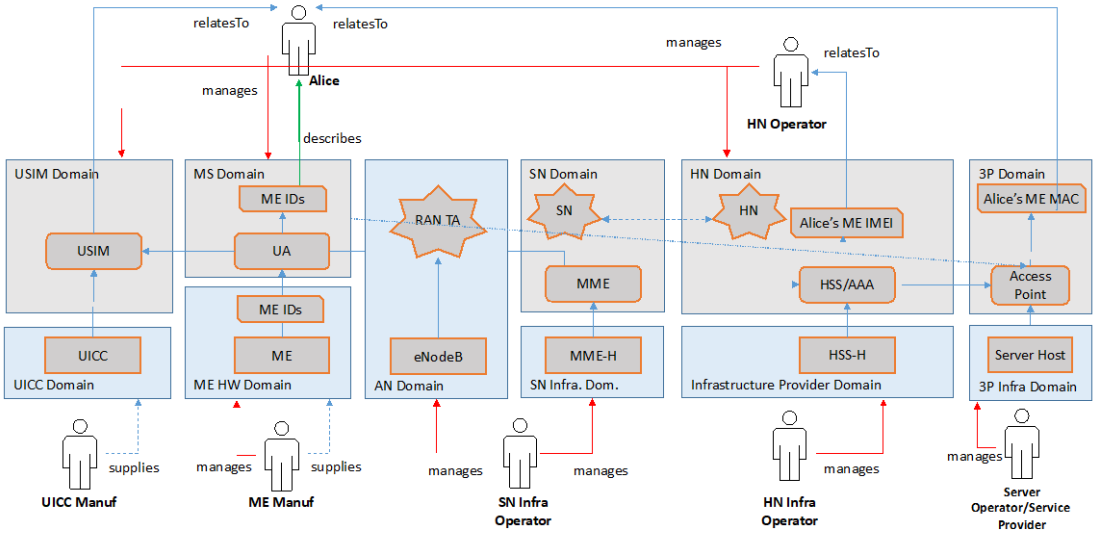

Figure A.31 Device Identity Privacy (UC 2.1): sunny day scenario

Alice has a subscription with a Mobile Network Operator (MNO) and she has been provisioned with USIM credentials in her UE which has certain fixed identifiers (ME IDs) associated with her Mobile Equipment (ME) device such as her International Mobile Equipment Identifier (IMEI) and WiFi MAC address.

When Alice's UE is switched on, the ME connects to the mobile serving network (SN) using the NAS-level Security Mode Command procedure which attempts to establish a security context. Provided Allice's ME has supplied an authorized identity to the SN a security context will be instantiated, after which Alice's ME will respond to request for its International Mobile Equipment Identifier (IMEI).

Alice's UE may also establish a non-3GPP connection via a 3P domain which may be authenticated through the use of Alice's USIM credentials. In the case where Alice's UE utilizes 'WLAN direct IP access' (3GPP TS33.234) to attach to an MNO controlled Access Point (AP) in a 3P domain, or any other AP, it will expose it's WiFi MAC address to the AP and if using the DNA protocol (IETF RFC4436) it can also leak MAC addresses of previously visited APs and the order in which they were visited.

A.5.2 Identified threats

A.5.2.1 Mobile user interception and information interception (T_UC2.1_1)

The attacker, Mallory, wants to gather the ME device identifiers (e.g. IMEIs) of users which are active in a geographic area.

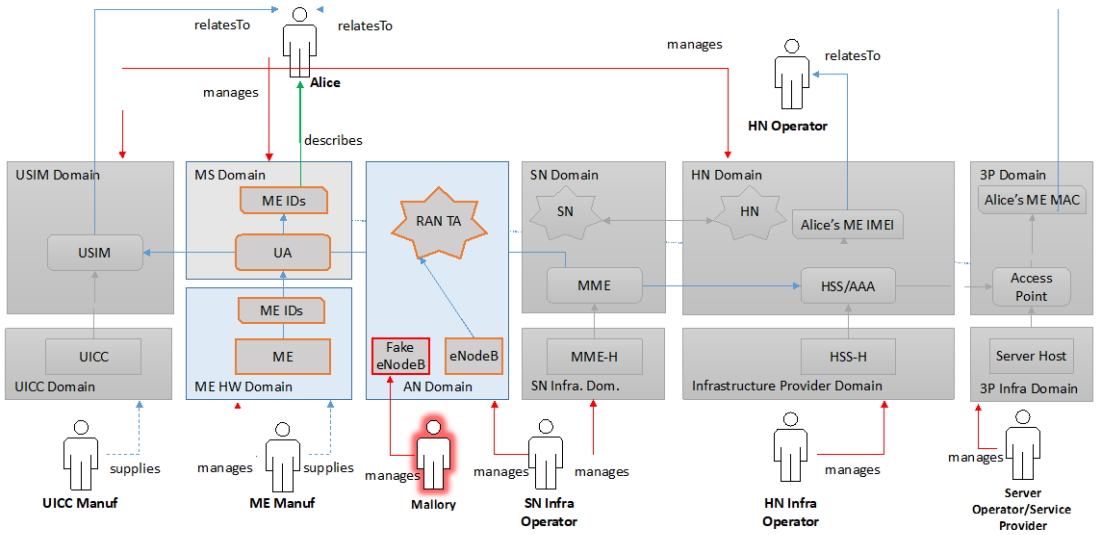

Figure A.32. Mobile user interception and information interception (UC 2.1) – 'rainy day'.

In Figure A.32, Mallory can achieve this by setting up a fake eNodeB which can passively monitor the radio spectrum in the AN domain to obtain IMEIs from emergency calls.

The consequence of this attack is that the private device identity can be obtained by an unauthorised party. When the IMEI is obtained then the attacker also knows the device's Type Allocation Code (TAC) is the initial eight-digit portion of the IMEI, which uniquely identifies the device and indicates the GSMA-approved organization that registered the device.

Trust implications

The use case involves several actors: the user and the MNO (HN) to which the user has a subscription, the SN and the AN provider. The current trust model is based on the following relationships.

- The ME trusts its HMNO as part of the direct service agreement.
- The HMNO trusts the SMNO as part of the roaming agreement contract. The IMEI is exchanged to ensure it is not on a blacklist of devices.

The implication related to the trust model are:

- The user/ME has no way to detect the trustworthiness of the AN
- The user/ME connects to an AN and it is unaware that it is a compromised third party since the user/ME trusts it unconditionally.
- Since the IMEI is not encrypted when initiating an emergency call the fake eNodeB can capture the IMEI.

Threat mitigation strategy

Mitigation of this threat may be achieved through protection of the device identifier during transport. Such an approach might protect the transfer of the IMEI between the UE and AN using transport layer encryption. Another approach might be to use a mobile Operator supplied key to just encrypt the IMEI in transit. These solutions should ensure that the user's IMEI is not sent in clear text during network attachment. Whilst these approaches would make passive interception significantly harder, these solutions may not prevent the UE from attaching to a rogue eNodeB, but they would raise the bar in making it more difficult for an attacker to obtain the IMEI.

A.5.2.2 Tracking of device's (user's) location (T_UC2.1_2)

The attacker, Mallory, wants to track the UE, based upon its ME device identifiers, in this case WiFi MAC address and associated protocols. Mallory can achieve this by setting up a WiFi monitor near the AP(s) in the location of interest and observing the protocol interactions.

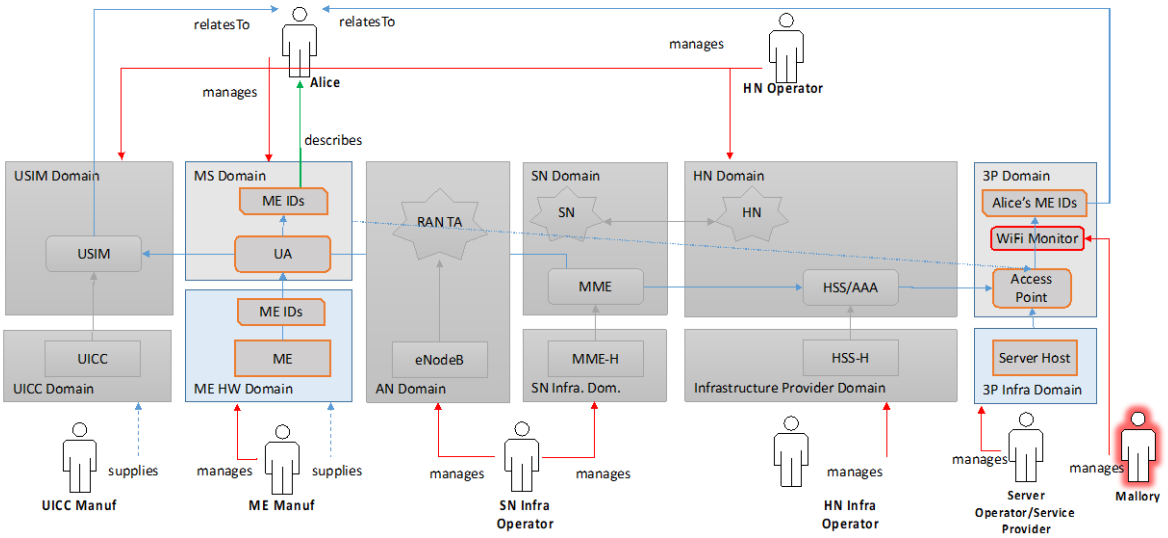

Figure A.33. Mobile user interception and information interception (UC 2.1) – 'rainy day'.

Based on Figure A.33, Mallory sets up a rogue WiFi monitor near the Access Point(s) of interest so can passively observe the MAC address of the device. Also, provided the device uses RFC4436, Mallory can also potentially monitor the MAC addresses of previously visited APs and the order in which they were visited.

The consequence of this attack is that the presence of the device in that location may be revealed and also potentially the previous points of attachment and the order of their visitation. Once Mallory knows the MAC addresses, due to their format he also knows the manufacturer of the user's device and potentially those to which the user has previously attached. The subscriber's previous location may also be linked to the user's previously visited MAC addresses using Geolocation lookup APIs such as those offered by Google and others.

Trust implications

The use case involves several actors: the user and the MNO (HN) to which the user has a subscription, and the 3P domain. The current trust model is based on the following relationships:

- The ME trusts its HMNO as part of the direct service agreement
- The HMNO trusts the 3P domain to host their Access Points (AP)
- Both HMNO and 3P domain trust their interconnection provider

The implications related to the trust model are:

- The user/ME has no way to detect the trustworthiness of the AP.
- The user/ME connects to an AP and it is unaware that it may be monitored by a third party since the user/ME trusts it unconditionally.

Threat mitigation strategy

The threats may be mitigated in this case through the deployment of privacy enhanced functionality into the UE. One approach to limit tracking is to provide for randomisation of the device's MAC addresses. Whilst a number of mobile Operating Systems do now provide for randomisation of the device's MAC addresses these are typically limited in their privacy protection as the randomisation only occurs in a limited set of protocol interactions.

Other solutions can ensure that MAC addresses associated with sensitive locations may be not be reused and that noise may be added to the information an attacker may obtain through randomisation of the ordering of emitted MAC addresses and by dummy MAC address injection. The 'Device Identity Privacy' enabler provides such features to enhance the location privacy afforded to the UE.

A.6 Subscriber Identity Privacy (UC 2.2)

A.6.1 Use case description with architectural components

The use case relates to a user attaching to a 5G network for the first time (e.g. in a roaming situation or after the user's ME is switched on). The description of this procedure and its related function blocks is illustrated in Figure A.34.

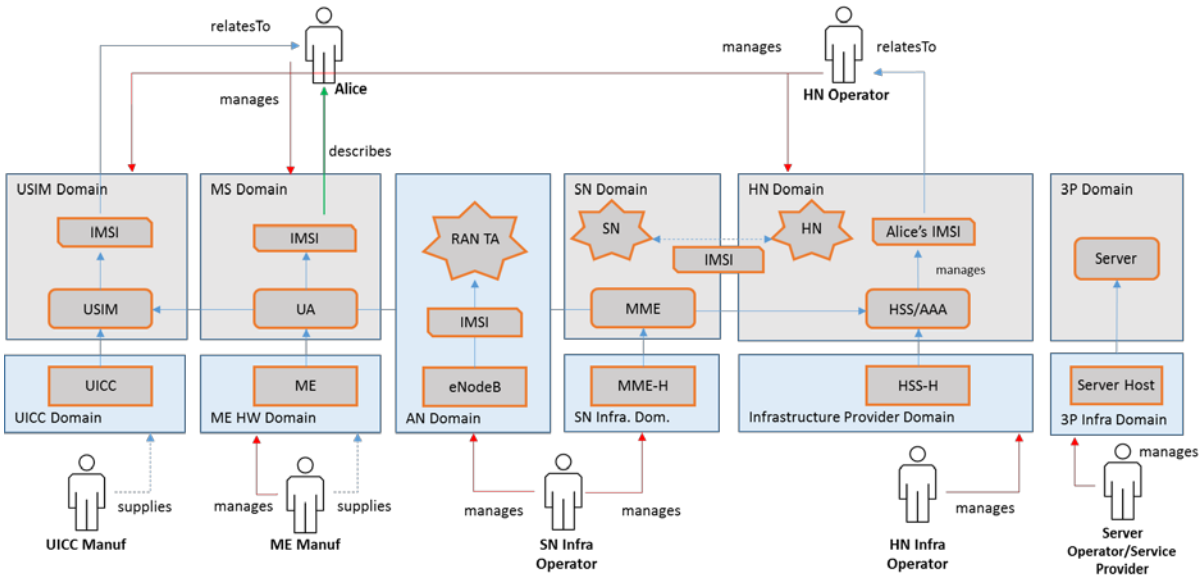

Figure A.34 Subscriber Identity Privacy (UC 2.2): sunny day scenario

Figure A.34 shows the scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

Alice has a subscription with a Mobile Network Operator (MNO) and she has been provisioned with credentials (the IMSI and the secret key Ki). The secret key Ki has been stored on the UICC domain. When Alice's ME is switched on, the ME attempts to attach to the mobile serving network (SN) by sending an **Attach**

Request message. Alice's ME does not have a short or temporary subscriber identifier (i.e. the GUTI in LTE) because this is the first attach to the network. Alice's ME sends the permanent or long-term subscription identifiers (i.e. IMSI) over the access network (AN) domain towards the serving network (SN) domain. Alice's IMSI is sent in clear text because no cryptographic material has yet been negotiated between the ME and the AN/SN. The SN uses Alice's IMSI to route the request towards the HN domain. The HN uses the IMSI to identify Alice's subscription and to start the authentication procedure by providing the SN with an authentication vector. After Alice's successful authenticate, the ME and the SN have negotiated a security context used to protect Alice's traffic over the AN domain.

A.6.2 Identified threats

A.6.2.1 Tracking of device's (user's) location (T_UC2.2_1)

Mallory wants to track a target user Alice in Figure A.35.

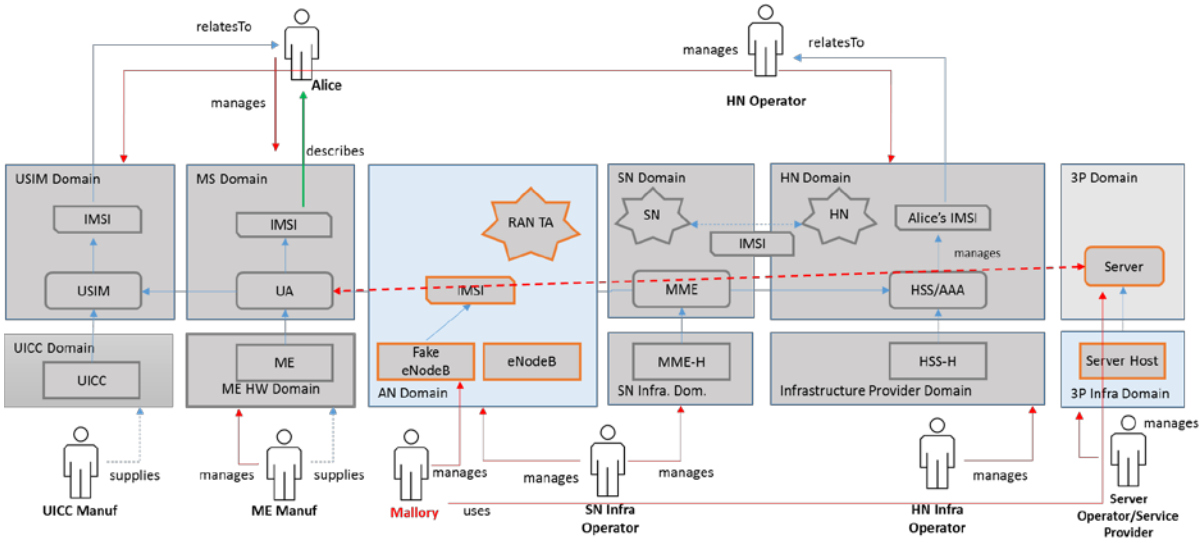

Figure A.35 Tracking of device's (user's) location (UC 2.2) – 'rainy day'.

In a first phase Mallory operates in passive mode. Mallory's objective is to collect a set of users' identities, permanent (IMSIs) and temporary (GUTIs), which can be used for two purposes. One is to link subscriber's presence to a certain area, and other is to reveal his past and future movements in that area. To achieve this, Mallory sniffs over the AN (Figure A.35) and decode broadcast paging channels to extract IMSIs and GUTIs.

Mallory then needs to map IMSI or GUTI associated with a particular subscriber (e.g. Alice) to reveal his/her presence in that area. The mapping between GUTI and IMSI is possible using semi-passive attacks.

The objective of the semi-passive attack is to determine the presence of a subscriber in a Tracking Area (TA) and further, to find the cell in which the subscriber is physically located in. In particular, Mallory tracks Alice's current location by triggering the mobile network into initiating the generation of paging messages to Alice's ME (e.g. by using social media application hosted on a 3P server to initiate unobtrusive communications)

Mallory observes the paging messages sent and can potentially correlate the contained GUTI with Alice's social network identity.

Trust implications

The use case involves several actors: the user and the MNO (HN) to which the user has a subscription, the SN and the AN provider. The current trust model is based on the following relationships.

- the ME 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 implication related to the trust model are:

- The user/ME has no way to detect the trustworthy of the AN
- The user/ME connects to an AN and it is unaware that it is a compromised third party since the user/ME trusts it unconditionally.
- The user/ME answers to the rogue AN/SN request asking the transmission of the user's permanent identity (IMSI).

Threat mitigation strategy

Subscriber identities are transmitted unprotected over the AN enabling tracking of MEs.

To protect IMSI transmission over AN during the first network attach solutions based on the use of a public key encryption can be used like the *Encryption of Long Term Identifiers* feature and the *Home Network-centric IMSI protection* feature. Those features also limit the possibility for Mallory to locate a user.

A second mitigation strategy is to ensure temporary subscriber identities are reallocated often enough to avoid tracking. Today the reallocation of temporary user's identity depends entirely on the operator network's configuration with the risk that they tend to remain the same even if a ME is moving. Hence temporary identities are not really temporary. This allows an attacker to perform passive attacks. In addition the generation mechanism for the temporary identities is vendor dependent and not defined. Often the newly assigned temporary identity differed from the old one by only one hexadecimal digit. This implies that temporary identities were not chosen randomly.

The *"Privacy Enhanced Identity Protection"* enabler provides the *IMSI pseudonymization feature* to mitigate the user's location tracking. The feature provides:

- A generation function for temporary or short term identifier having the following properties:
    - it ensures that the temporary subscriber identifier are univocal random numbers (Random Temporary Mobile Subscriber Identity - RTMSI) over the entire Tracking Area
    - it ensures that the probability of collisions between the RTMSI allocated to different MEs over the entire Tracking Area is sufficiently small.
- A mechanism for triggering the RTMSI refreshing and it's periodically update to avoid dependence on the operator's network configuration. The new RMTSI is triggered after each usage (one-time).

The solution impacts the SN that needs to support the *IMSI pseudonymization feature.* The SN can trigger the use of a new one-time pseudonym (after each usage) according to the "push model".

The solution can impact also the user's ME in the case where a "synchronized" model is adopted. In this case also MEs have to implement the *IMSI pseudonymization feature* to generate and update the new RTMSI in a synchronized way, after each usage.

A.6.2.2 Mobile user interception and information interception (T_UC2.2_2)

The attacker, Mallory, wants to gather the IMSIs of all users which are active in a geographic area.

Mallory can achieve this in two different ways: passive and active. Mallory opts for the more effective active attack allowing at any time to retrieve users IMSIs, instead of waiting for users MEs to send out their IMSIs as in the passive attack.

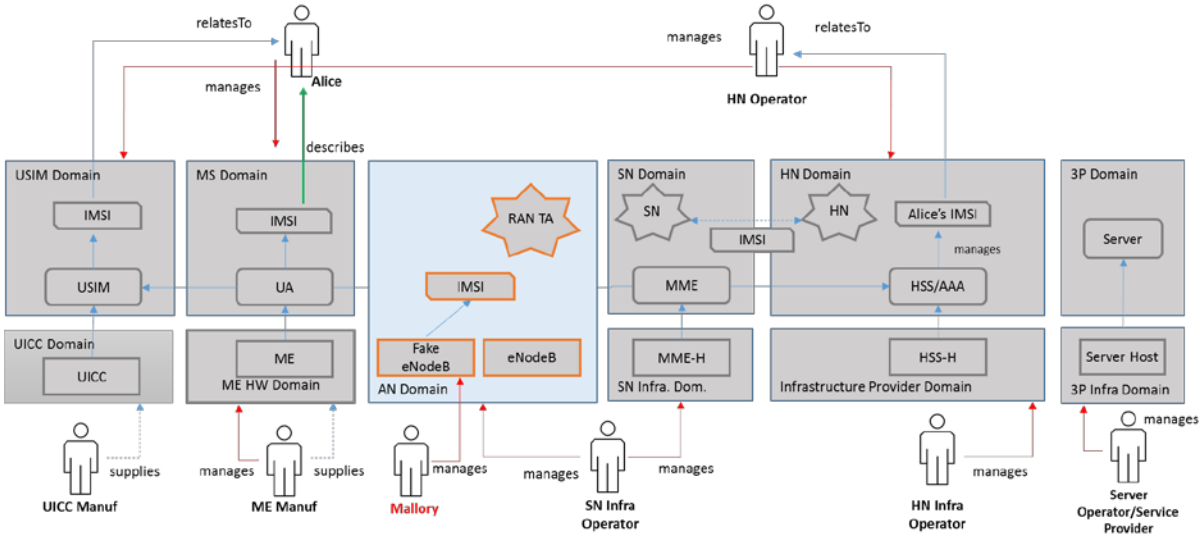

Figure A.36. Mobile user interception and information interception (UC 2.2) – 'rainy day'.

Based on Figure A.36, Mallory sets up a rogue 5G Base Station (known as an IMSI catcher), operating with higher power than the legitimate one, to which MEs in the neighbourhood will attempt to connect. Mallory's IMSI catcher acts between the target ME and the SN's real towers. As such it is considered a Man-in-The-Middle (MiTM) attack and usually is undetectable for the users MEs.

Alice's ME, as part of its scanning activity for 5G Base Station with the best signal power around it, camps on the rogue 5G Base Station (Mallory). The fake base station then simply commands Alice's ME to identify itself. Alice's ME returns in response Alice's IMSI. Mallory is able to retrieve Alice's user identity since it is transmitted in clear text over the AN.

The consequence effects of users' identifiers exposure over-the-air signalling messages mostly relate to the issue that the subscription identifier is disclosed or made inferable to an unauthorized party. Once the Mallory knows the IMSI, due to its format she also knows the home country where subscriber resides and the home mobile network operator. Also the subscriber's location might be linked to the user's identifier as the transmission of the IMSI reveals the user approximate location.

The information gained exploiting the lack of IMSI protection during the initial attach opens the door to other attacks like the sending of fake signalling messages (e.g. SS7) towards the HN having impact on the HSS (e.g. fake Authentication Request to retrieve user's authentication vector or fake Location Update Request to redirect the target user in another location under Mallory's control or to create a user's DoS).

Trust implications

The use case involves several actors: the user and the MNO (HN) to which the user has a subscription, the SN and the AN provider. The current trust model is based on the following relationships.

- The ME 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 implication related to the trust model are:

- The user/ME has no way to detect the trustworthy of the AN
- The user/ME connects to an AN and it is unaware that it is a compromised third party since the user/ME trusts it unconditionally.
- The user/ME answers to the rogue AN/SN request asking the transmission of the user's permanent identity (IMSI).

Threat mitigation strategy

The types of trust required in this use case can be ensured/guaranteed through technical solutions in addition to agreements between partners. These solutions should ensure that the user's IMSI is not sent in clear text during the first attack to the network (Attach Request) or in case of explicitly Identity Request. From the technical point of view this can be achieved, for example, by 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 keys are yet negotiated between the ME and the network.

These solution do not prevent to a ME to attach to a rogue AN, but they significantly make ineffective the attack since Mallory can't be able to retrieve the user's IMSI.

The "Privacy Enhanced Identity Protection" enabler provides two alternative features to counteract this threat based on different approaches.

The *Home Network-centric IMSI protection* feature demands to the user's HN the responsibility for performing the decryption of user's IMSI and the sharing afterwards of the clear-text IMSI to the rest of the network elements on the system that may need it (i.e. the SN for LI purpose). The feature needs to be implemented on the ME and on the HN. The ME uses the HN's public-key to encrypt only part of the user's IMSI. The Mobile Country Code (MCC) and the Mobile Network Code (MNC) of the IMSI are left in clear-text, to allow the SN to route the encrypted IMSI to the user's HN.

The *Encryption of Long Term Identifiers* feature demands to the SN the responsibility for performing the decryption of user's IMSI. In this case the entire IMSI is encrypted by the ME using a global public key generated according to the KP-ABE scheme combined with an attribute that identifies the SN to which the user's ME is connected to. This means that the same public key is used also when the user is in roaming. Only the attribute changes since it is the one that identify the current trusted SN.

A.7 Enhanced Communication Privacy (UC 2.3)

A.7.1 Use case description

This use case details the user Bob communicating securely via a device over the eNodeB and into the MNO network. Bob wants his communications to be resistant to passive interception. The use case discusses ways which this might be by passed, and Bob's communications are compromised via a passive attacker.

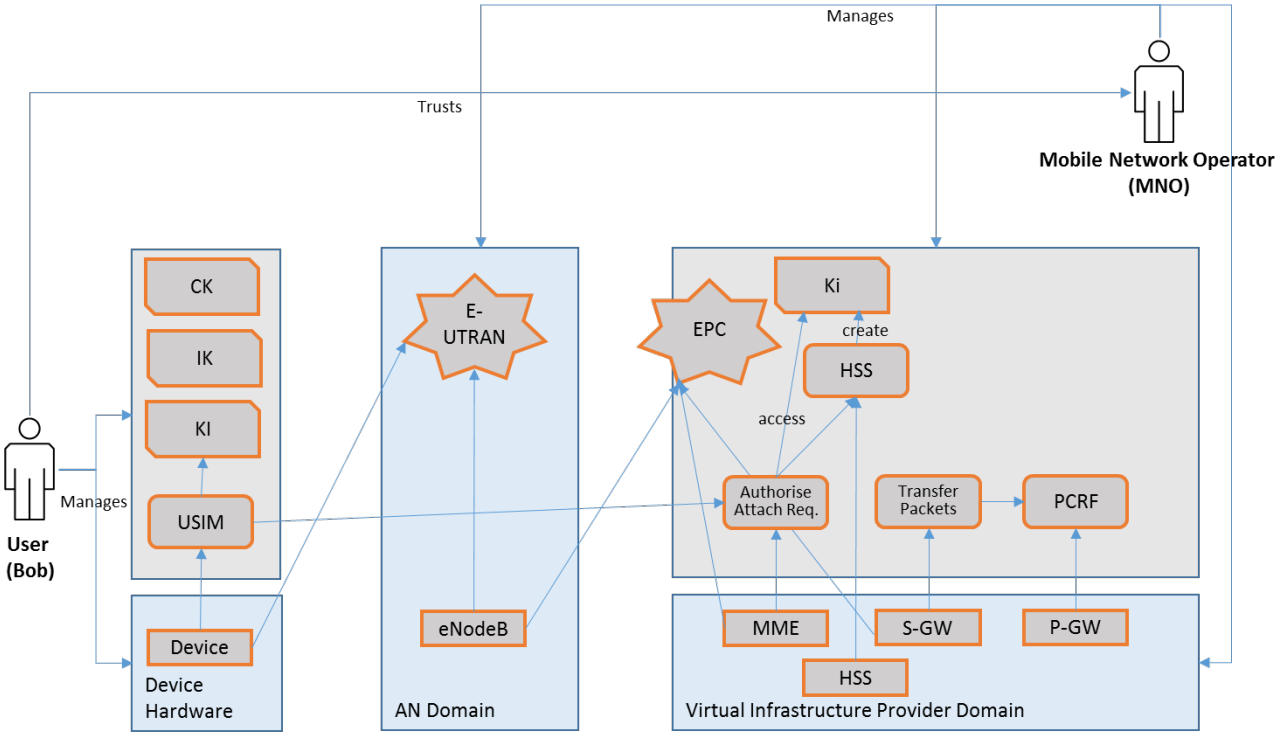

Figure A.37. Enhanced Communication Privacy (UC 2.3): sunny day

User Bob manages a device which connects to the MNO's network via the access network. The AN and MNO network is both managed by the mobile network operator, the hard for the MNO network can be managed by the MNO, for this scenario there is no difference. Bob, the user, trusts the network is correctly managed by the MNO. And when his device authenticates with the USIM with the network it will be accepted and his communications are to be secured from any and all adversaries.

A.7.2 Identified threats

A.7.2.1 Passive communication interception (T_UC2.3_1)

The attacker has compromised bob's user-specific Ki, 'Ki'. This gives Malory to ability to decrypt data which Bob transfers to the MNO, which is authenticated using the Ki. Malory is able to perform this attack without any activing influence on the either the user or operator, because of this there is no way which either can detect the attack.

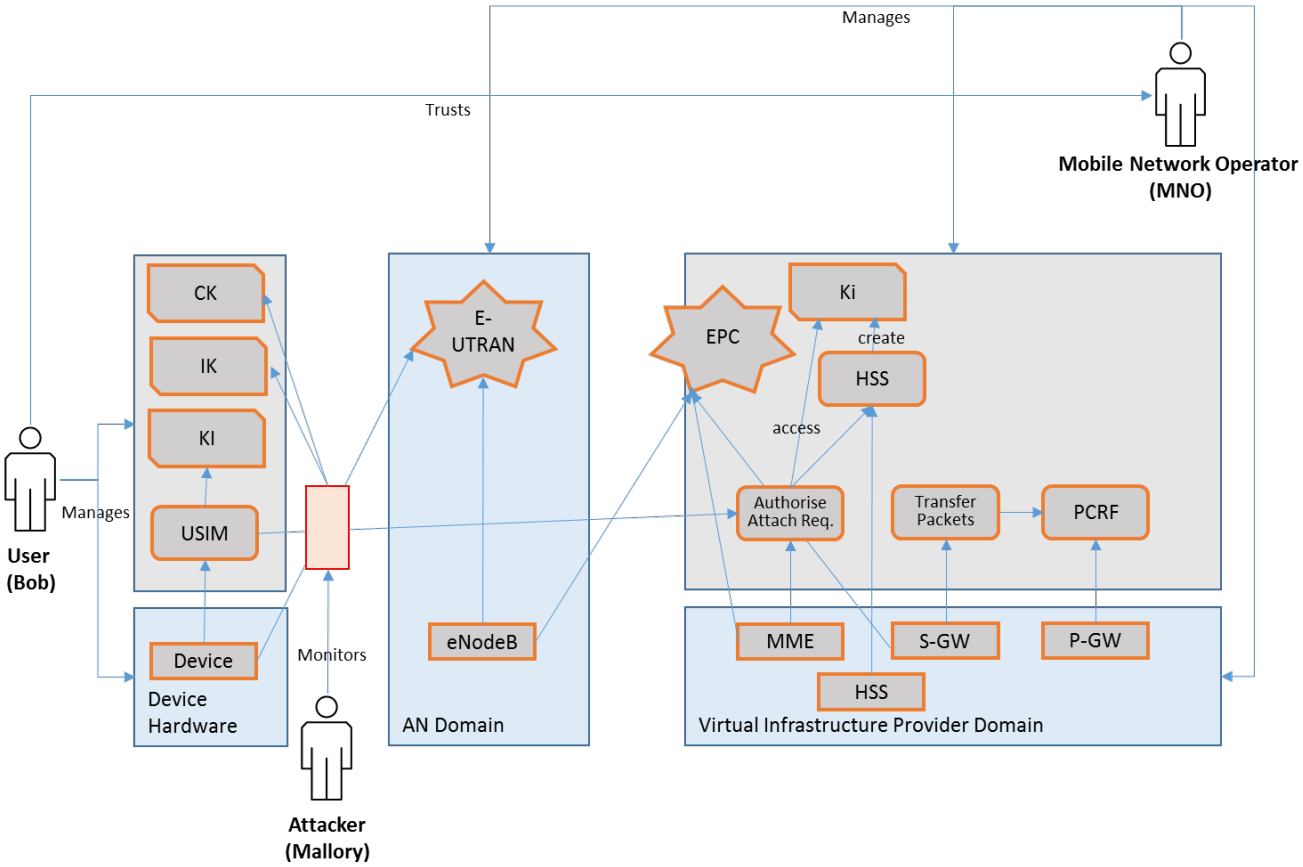

Figure A.38. Passive communication interception (T_UC2.3_1) – 'rainy day'

When Mallory performs this attack any and all communication between the users can be intercepted. Because this is a passive attack Mallory is limited in what he can do. This can cause leaking of secure information from users of the network. Since a user has more trust in the phone network than they would a traditional computer network. They might feel they can talk more freely over the telephone network resulting in a larger personal or commercial impact when private information is leaked from this attack. If the device compromised is used to administer other devices on the 5G network then they could also become compromised as well as Bob's device.

Trust implications

Bob who manages the device connecting to the network, trusts the MNO will not allow passive attacks like this to happen. The MNO may transfer responsibility of trust from them to the receiver of the communications i.e. whomever bob is talking to. Because the MNO is not required to encrypt user plane data, and this is the responsibility of the user. Bob may choose to use end to end encryption to protect his communication. To a certain degree the MNO has to take responsibility, this depends on the severity of data being compromised on their network otherwise their customers will lose faith in their abilities.

Threat mitigation strategy

Aside from what was discussed with end to end encryption for the users. A better solution for the 5G network would be to force data plane encryption which support perfect forward secrecy. This would force the attack from passive to an active attack, which would increase the complexity of the attack required. This mitigation technique would be implemented on the user's device and within the MNO's network. Stakeholders who

would be expected to enforce and implement this would be the MNO and maybe the device/USIM manufacturer.

A.8 Authentication of IoT Devices in 5G (UC 3.1)

A.8.1 Use case description with architectural components

The use case relates to IoT authentication following different ways depending on their capabilities. The figure below describes the different possible scenarios for using 5G resources.

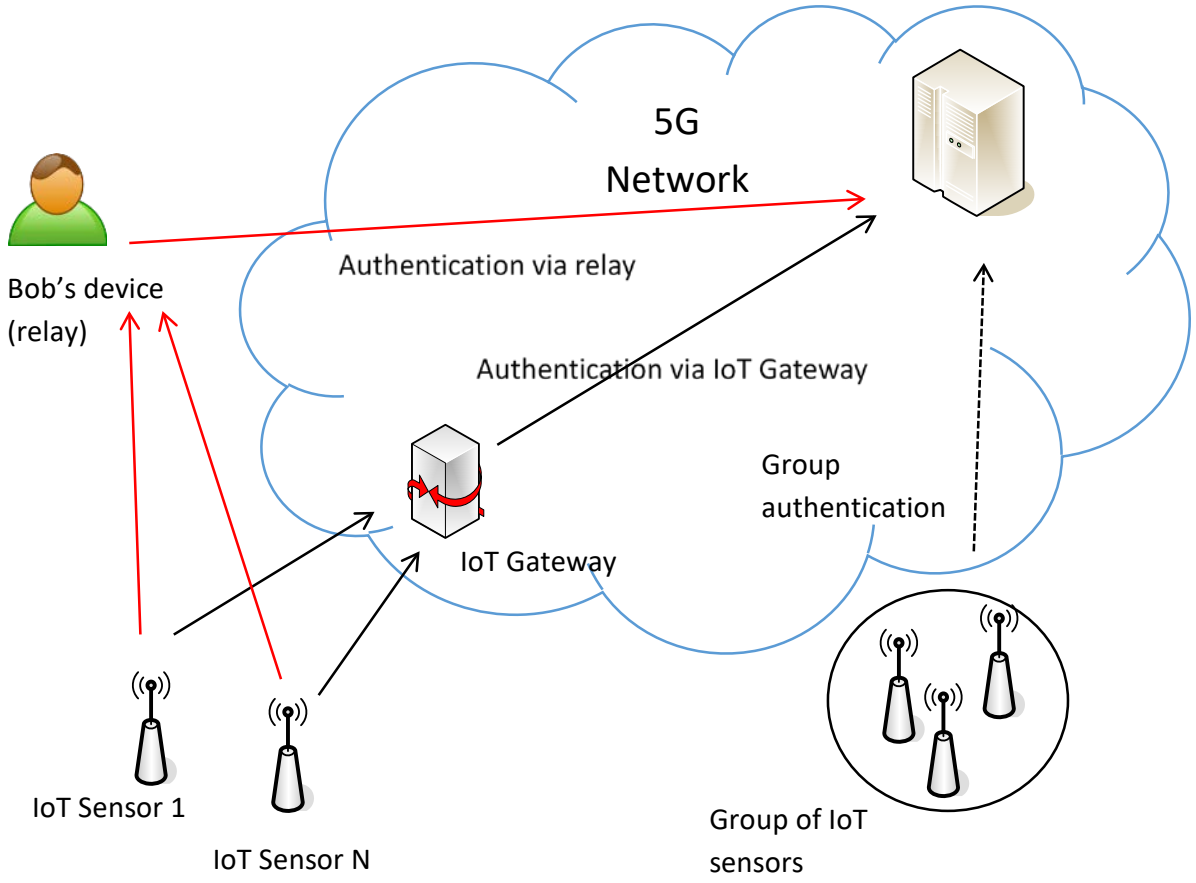

Figure A.39: Authentication of IoT Devices in 5G (UC 3.1)

The description of different scenarios and their related function blocks are illustrated in the next three figures, which illustrates the different scenarios with respect to the architecture, in the absence of any threat (the sunny day scenario). On the different architecture diagram, the scenario is the storage of a sensor data in a cloud infrastructure offered by a cloud provider.

A.8.1.1 Basic IoT Authentication by 5G UE

The more simple way to allow a sensor to call services hosted by a cloud provider is to re-use an existing authorized access, which can be offered by a user's UE or a specific IoT gateway. For the architectural description, we simplify by using only a user's ME (Bob's ME) because the IoT gateway could be seen as a specific user's UE. For this basic IoT authentication, all operations are performed at the user's UE without impact on the rest of the architecture. The sunny day described in Figure A.40 is very simple.

For the targeted scenario:

1. Bob defines all authorized equipment for using his UE.
2. The sensor is authenticated to Bob's UE (or IoT gateway)
3. The sensor call a storage service hosted by the cloud provider and use Bob's account to store its data.

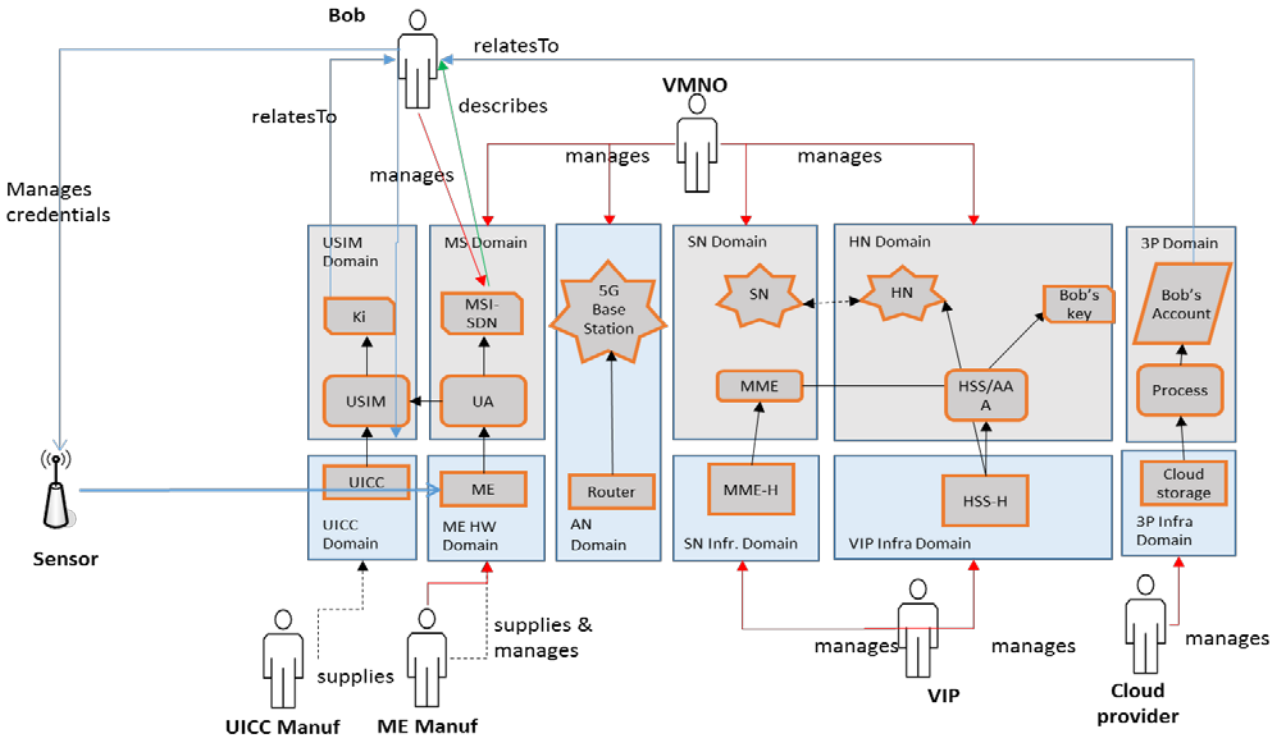

Figure A.40: Authentication of IoT Devices in 5G (UC 3.1): sunny day scenario for basic IoT authentication by 5G ME

A.8.1.2 IoT Authentication relayed by 5G ME

Another way for a device to call services hosted by a cloud provider is to have its own credential but by using the ME to communicate with the HSS/AAA. This case is relevant when the device is not using the standard 5G interfaces. In this specific case, the ME has to implement the specific interface before being able to relay the authentication information. In our scenario, the sensor owner is associated with Bob for using the cloud storage service. The following Figure A.41 describes this scenario.

For the targeted scenario:

1. The sensor owner has registered his sensors and their credential in the HSS.
2. Bob's ME (or IoT gateway) is configured to relay specific sensors authentication.
3. The sensor call a storage service hosted by the cloud provider and use Bob's ME to perform its authentication and then, to store its data.

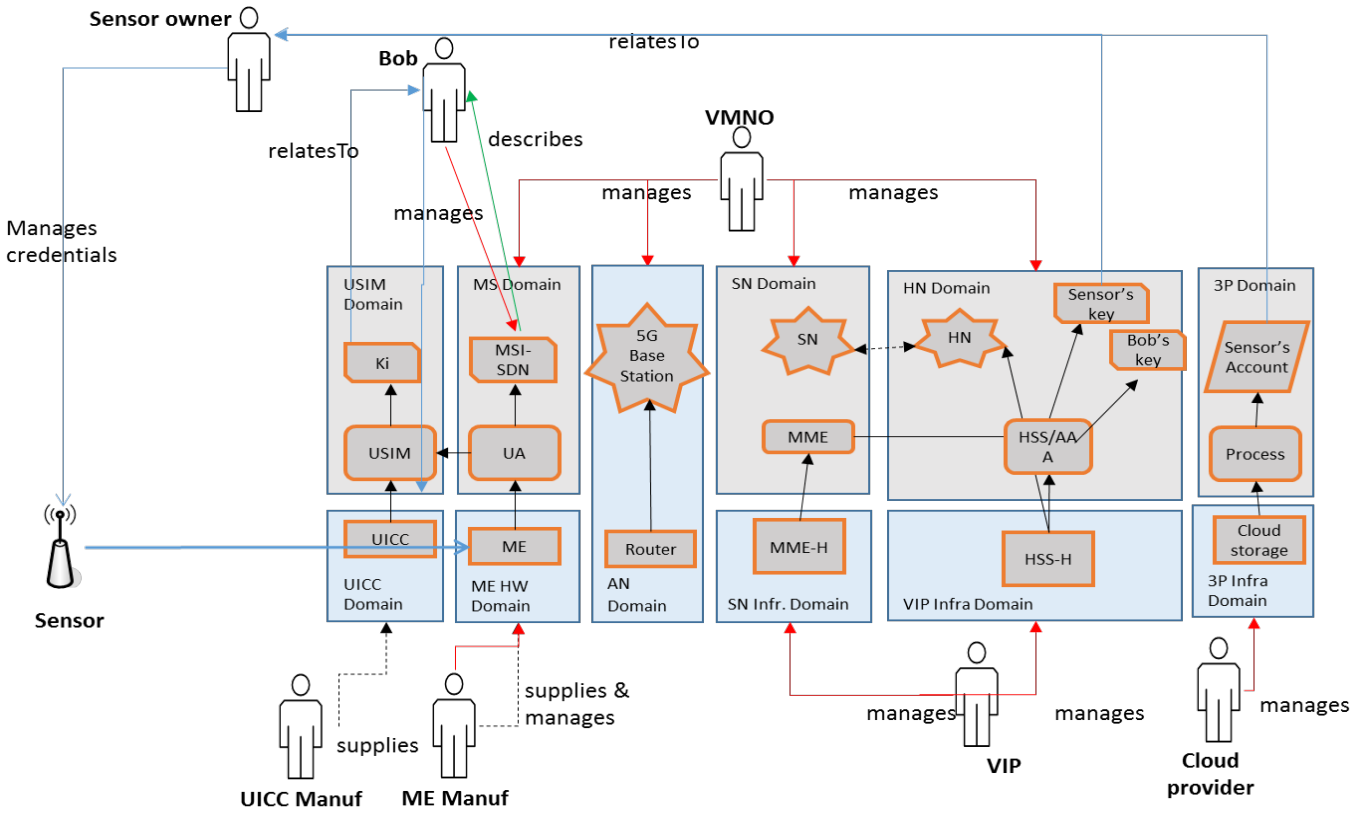

Figure A.41: Authentication of IoT Devices in 5G (UC 3.1): sunny day scenario for IoT Authentication relayed by 5G ME

A.8.1.3 IoT Group based authentication

For this kind of authentication, we use the open specifications of "Internet-of-things" enabler described in D3.6. With this enabler, the authentication is performed, for the first MTC, with the HSS but, for the other MTC (Machine-Type Communication) belonging to the same group, the authentication is performed by the MME. The Group-based authentication involves MTC(s), MME and HSS configuration.

For the targeted scenario:

1. The MTC(s) owner (group of sensors) has registered his group and their credential in the HSS. Each MTC USIM stores the group ID.
2. The MME is configured to perform group-based authentication
3. One of the MTC call a storage service hosted by the cloud provider and use its own credentials to perform its authentication and then, to store its data.

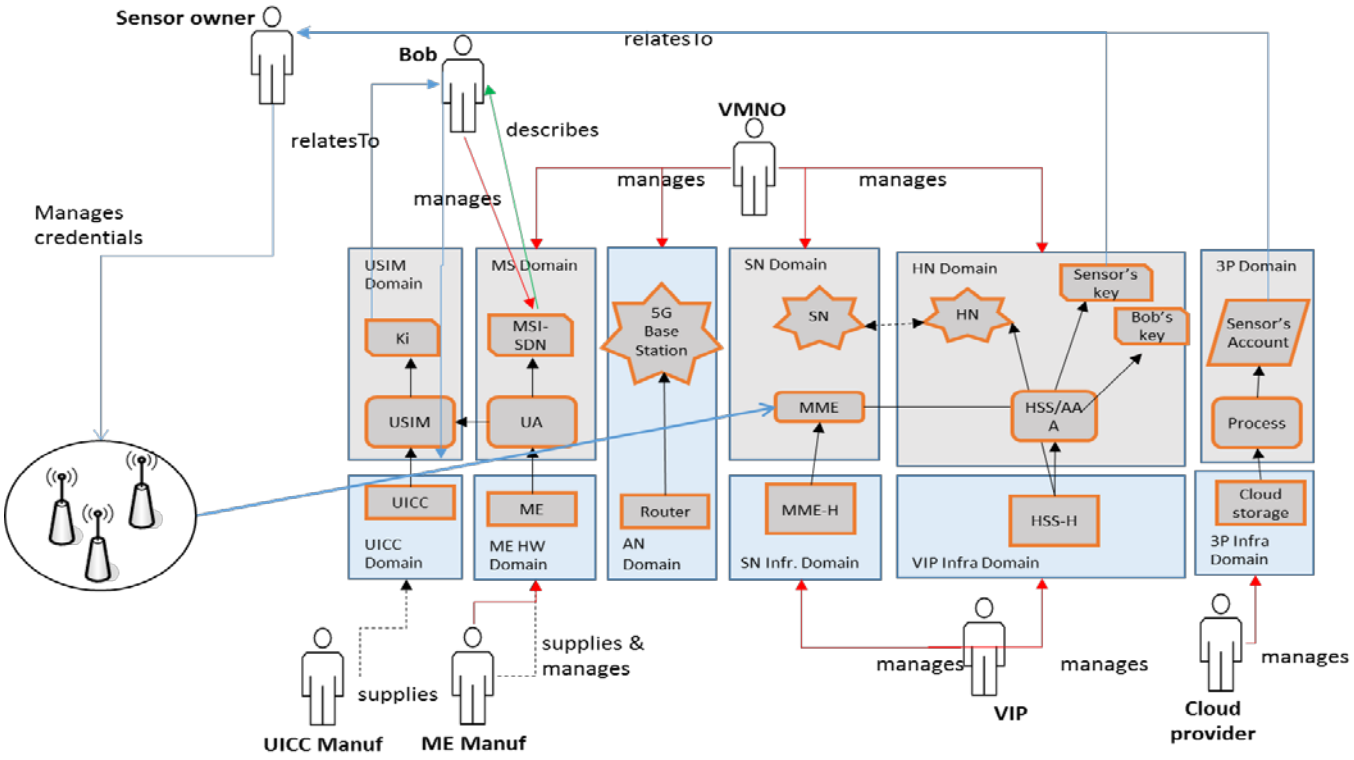

Figure A.42: Authentication of IoT Devices in 5G (UC 3.1): sunny day scenario for IoT Group based authentication

A.8.2 Identified threats

A.8.2.1 Authentication traffic spikes (T_UC3.1_1)

The attacker, Mallory, wants to perform a denial-of-service attack. For that, she initiates traffic spikes or emphasize the effects of natural traffic spikes with IoT aiming to be connected. As a consequence, the network will experience more signaling and authentication functions needs to perform more processing. Potentially, the authentication of authorized devices may fail and these devices may lose connectivity.

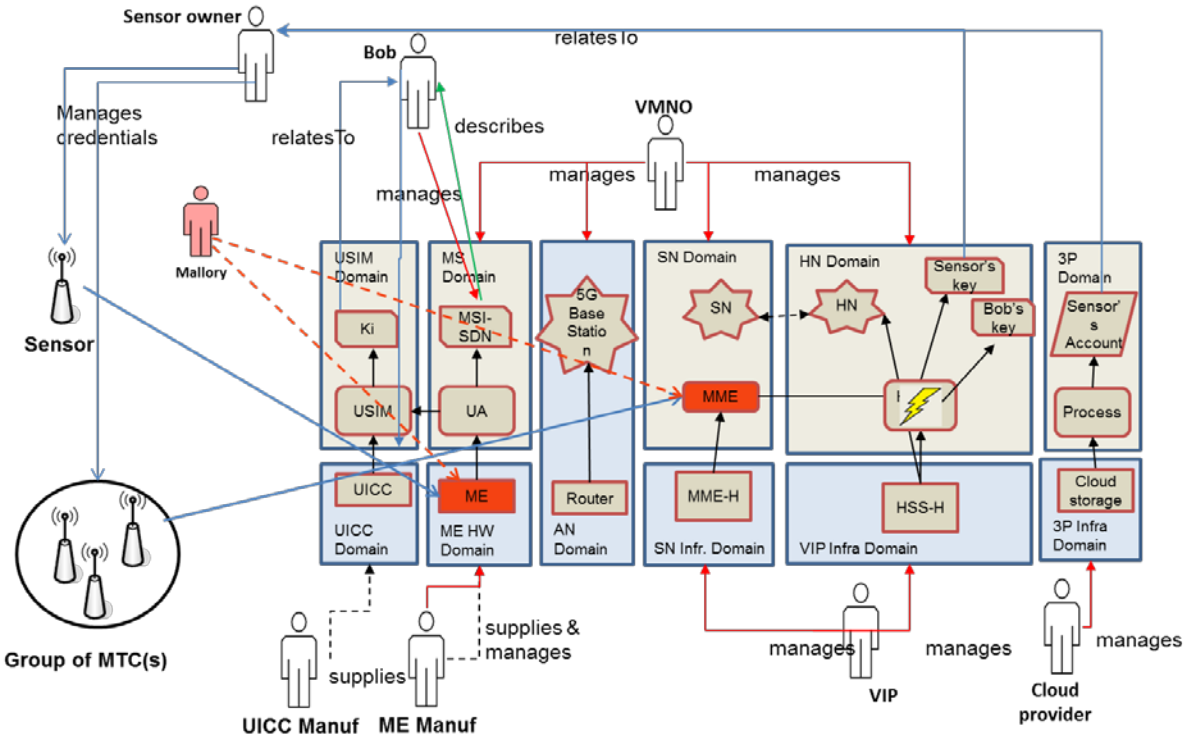

Figure A.43: Authentication traffic spikes (T_UC3.1_1) – 'rainy day'

Based on Figure A.43, Mallory has two options for that. She can increase the number of connections at the MME level (3rd scenario) or she can increase the number of connections at the UE level (2nd scenario). This threat didn't affect the first scenario because the authentication lacks are more the problem than the number of connections (all connections will be performed by the same user or IoT Gateway owner). For the 2 last scenarios, each time a connected device is attached to the network, an authentication is performed between the device and the MME but also between the MME and the HSS. If the HSS is overload, other connection of legitimate devices could be rejected.

Trust implications

This use case involves several actors: the sensors, the relay (Bob's UE or IoT gateway), the sensors owner, the relay owner and the VMNO (HN) to which the user has a subscription, and the 3P domain. The current trust model is based on the following relationships.

- The VMNO is secured and its HSS is protected against identity theft (specifically for the 2nd and 3rd scenarios).
- The sensor owner never discloses the sensors information (and especially their identity)
- The VMNO trusts the User equipment software developer/provider delivering the specific application on ME (specifically for the last 2 scenarios) and on the HSS.

The implications related to the trust model are:

- The MME are not able to detect that unauthorized device try to be connected.

Threat mitigation strategy

The threats may be mitigated in this case at the MME level to avoid traffic spikes regarding the signalisation (authentication mechanisms). For example the Group-based authentication mechanism is a good way to limit the number of complete authentications involving MTC, MME and HSS.

A.8.2.2 Compromised authentication gateway (T_UC3.1_2)

The attacker, Mallory, wants to intercept data exchange between sensors and the services provided by the cloud provider (a storage service for example). For that, she compromises specifically an IoT gateway or a mobile phone. In this case, she could act as a man-in-the-middle. As a result, data collected from IoT devices may leak from to wrong parties and IoT devices may receive commands from malicious party. The group-based authentication is not impacted due to the usage only of signalization mechanisms without gateways.

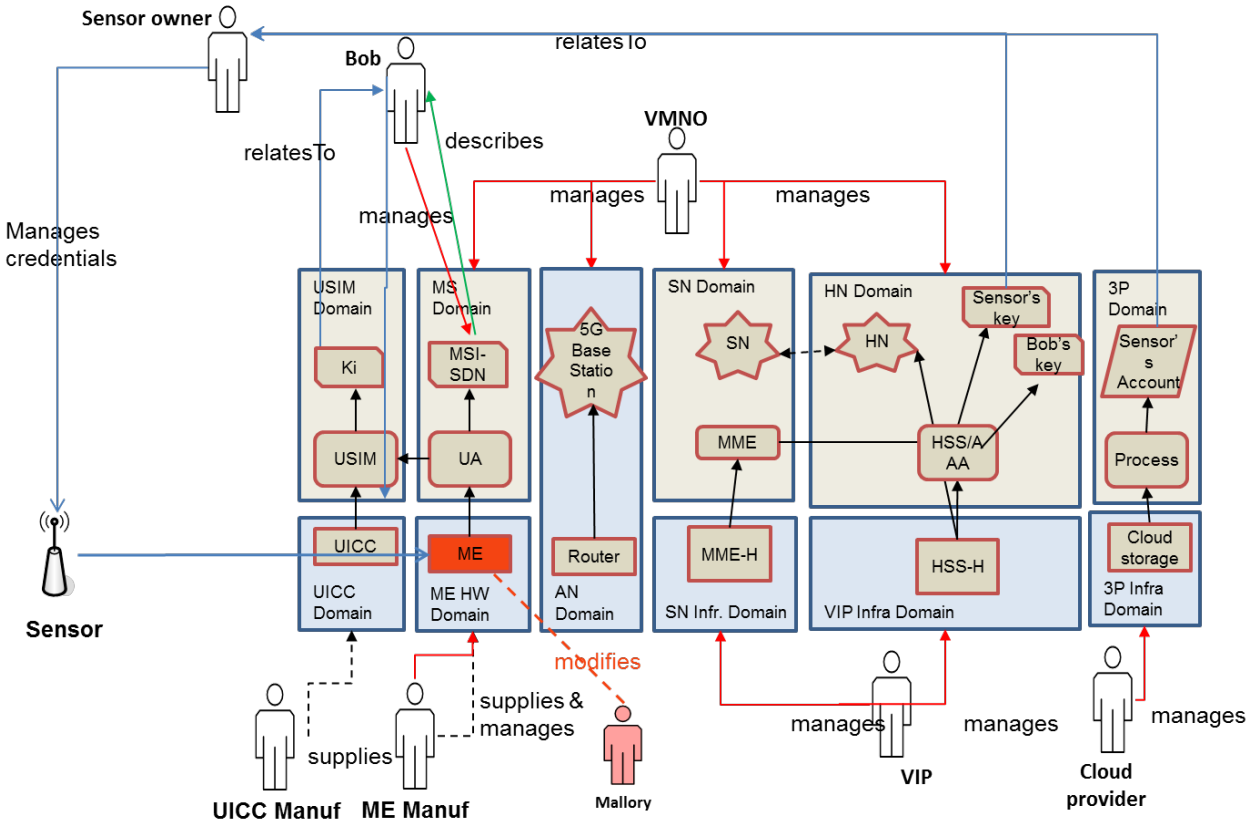

Figure A.44: Compromised authentication gateway (T_UC3.1_2) – 'rainy day'.

In Figure A.44, Mallory can achieve this by modifying the user's ME or the IoT gateway. In this case, Mallory is able to have all the traffic exchanged between the sensors and the services provider. Another way to perform this attack would be to have an exact copy of the ME (including UICC card).

Trust implications

The use case involves several actors: the sensors, the relay (Bob's UE or IoT gateway), the sensors owner, the relay owner and the VMNO (HN) to which the user has a subscription, and the 3P domain. The current trust model is based on the following relationships:

- The sensor owner never discloses the sensors information (and especially their identity)
- The VMNO trusts the User equipment software developer/provider delivering the specific application on ME (specifically for the 2 first scenarios).
- The relay owner (user's mobile phone or the IoT gateway owner) trust the User equipment software developer/provider.

The implication related to the trust model are:

- The sensor owner has no way to detect an abnormal behaviour of the relay (user's mobile phone or the IoT gateway owner)

Threat mitigation strategy

Mitigation of this threat may be achieved by using certified software and/or certified hardware. Another way is to guarantee the confidentiality between the sensor and the service using these data by cipher mechanisms. In this last case, all man in the middle attacks won't be able to interpret the data.

A.9 Network-Based Key Management for End-to-End Security (UC 3.2)

A.9.1 Use case description with architectural components

An IoT device is connected to a 5G network and authenticated to use the network. The communication should be end-to-end secured (encrypted and authenticated) but the endpoints have no means to connect each other securely (e.g., they do not share secret keys). The IoT device needs to communicate with an IoT backend service (operated by Alice) which utilizes 5G systems' network-enabled key management service. The key management service provides keys and the connected IoT device achieves secure end-to-end communication to the IoT backend service located, e.g., in the cloud. Figure A.45 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

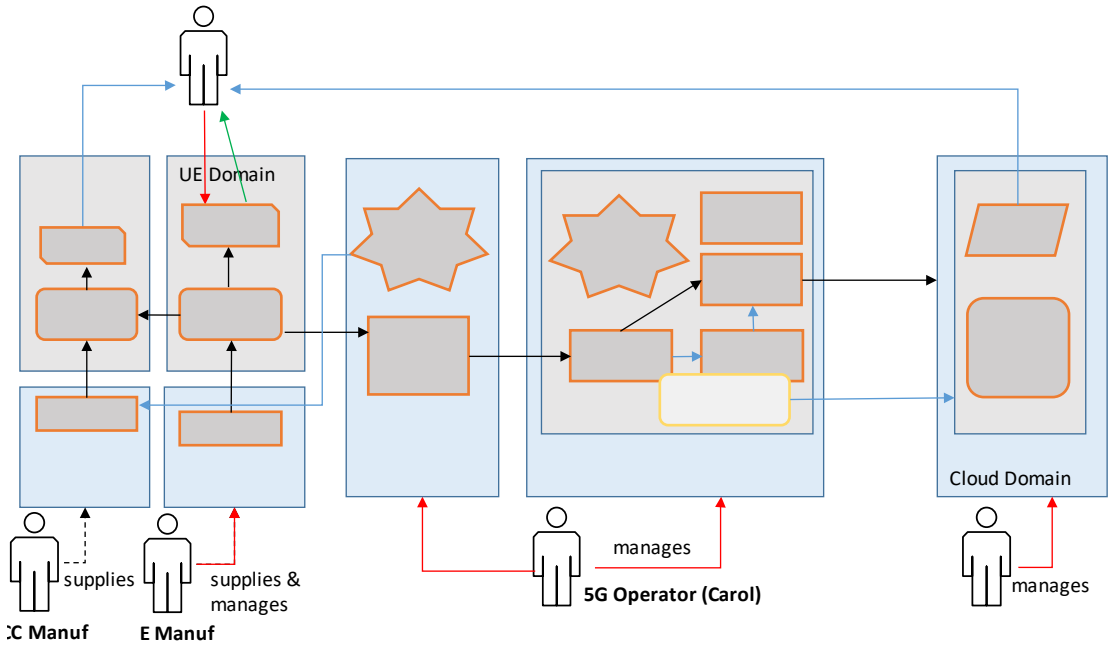

Figure A.45. Network-Based Key Management for End-to-End Security (UC 3.2): sunny day scenario

A.9.2 Identified threats

A.9.2.1 Leaking keys (T_UC3.2_1)

End-to-end keys may be stolen or leak from the centralized key servers. The key server may also become tampered. As a consequence, the end-to-end secured communication is vulnerable for different attacks and adversaries can gain an access to the end-points. They may e.g. provide false information to application services or send malicious commands to IoT devices. The VNFs which may get involved are indicated in Figure A.46.

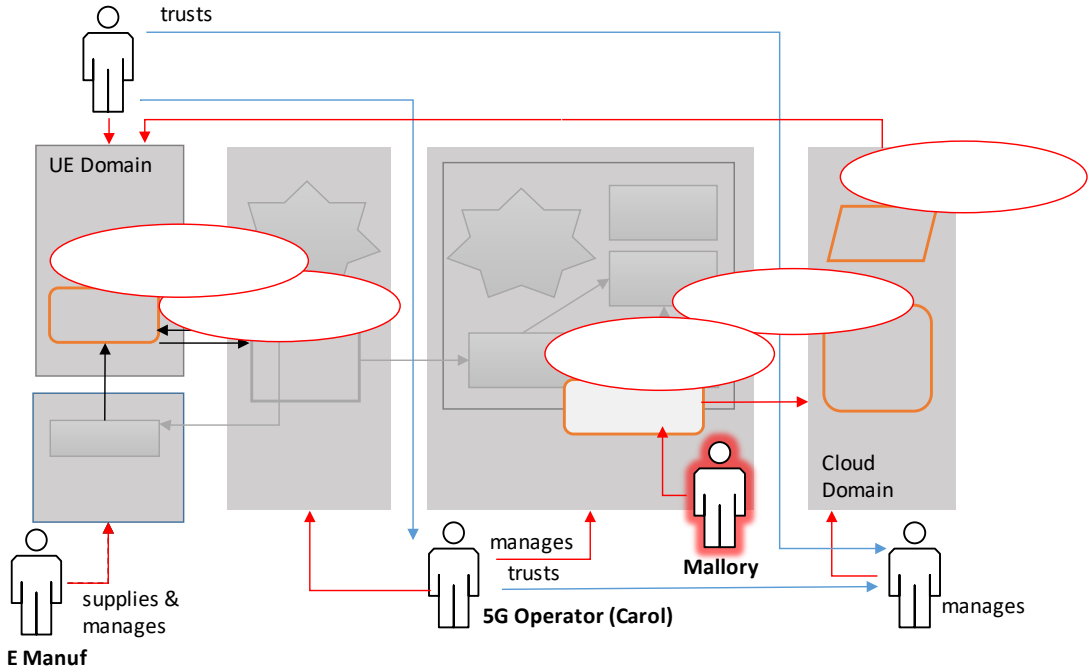

Figure A.46. Leaking keys (T_UC3.2_1) – 'rainy day'

Trust implications

Potential trust implications are the following:

- Bob loses trust to both the 5G system operator (Carol) and the IoT Backend Service Operator (Alice) since his system does not work properly or its data leaks to outsiders
- Alice probably loses trust to Carol although the adversary may actually tamper only the IoT Backend System which should be under Alice's own control.
- Carol, the MNO may lose trust to Alice as it is possible that the real adversary never gets identified. It is also possible that Bob's system look malicious and Carol loses trust to Bob.

Threat mitigation strategy

Potential ways to mitigate this risk:

- If lawful interception is not required (it is always required in some countries) implementing a key management server to a 5G system is not quite necessary
- Service and device discovery can be controlled to limit utilization of leaked keys. IoT service can be configured without providing any address of remote IoT service. In that case the 5G mobile

operator may fully control the IoT devices and Alice may not need the device addresses, while all communication is encrypted.

A.10 Authorization in Resource-Constrained Devices Supported by 5G Network (UC 4.1)

A.10.1 Use case description with architectural components

The use case relates to authorization management performed at the sensor level. As the sensor could be considered as a resource-constrained device, the authorization should be delegated to an AAA server. The following figure describes the different actors involved in the use case.

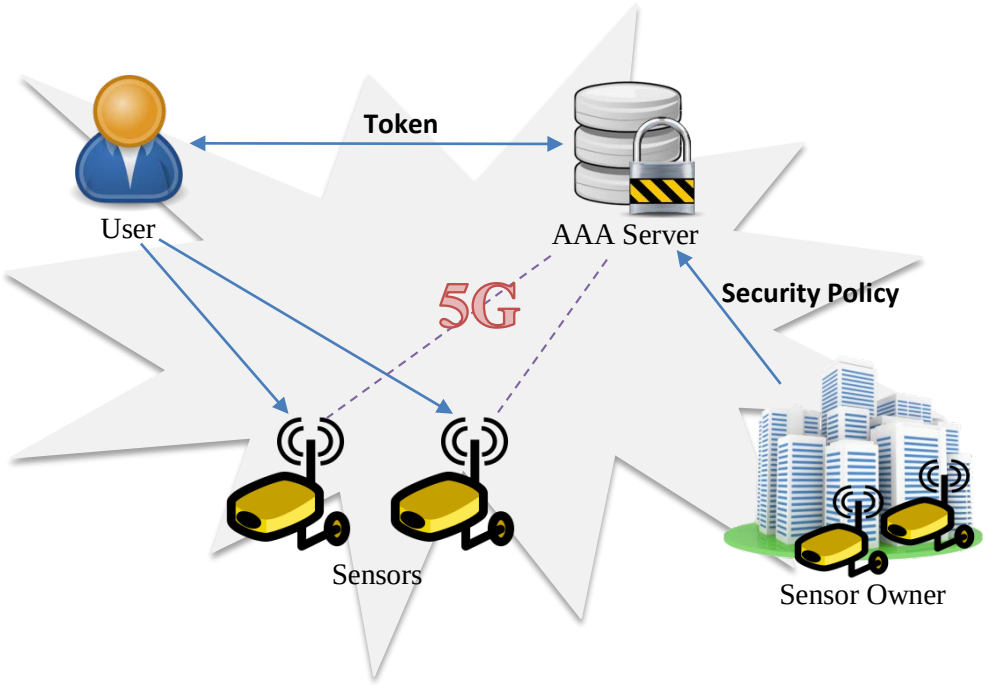

Figure A.47: Setting for Authorization in Resource-Constrained Devices

The main components of the architecture involved are specifically the HSS (the AAA server) and the different components used in standard authentication of a ME.

A.10.2 Sunny day scenario

For this scenario, the different actors are:

- Alice: she wants to use one sensor
- Sensor's owner: he manages the sensors and has defined the access control rights for using them.

The prerequisites are:

- The sensors and Alice use their 5G credentials to be authenticated in 5G context.
- The AAA server was modified to accept to check an authorization token for a specific token.
- The HSS was modified to manage security policy for sensors and especially to use token access control for specific sensors. The security policies are provided by the sensor's owner.
- 5G operator trusts the sensor's owner and allows him to define the security policies at AAA server level

The standard scenario is the following:

- The sensors' owner issues security policies to the AAA Server concerning access to its sensors to the AAA Server.
- The sensors have used their 5G credential to be connected.
- Alice uses her 5G credential to be connected.
- Alice authenticates to the AAA Server and requires access to the sensors.
- The AAA Server issues an authorization token based on 5G credentials of Alice according to the security policies.
- Alice uses this token for accessing the sensors
- The sensors contact the AAA server to check the token
- If the token is valid and authorizes Alice, she has access to the sensor(s)

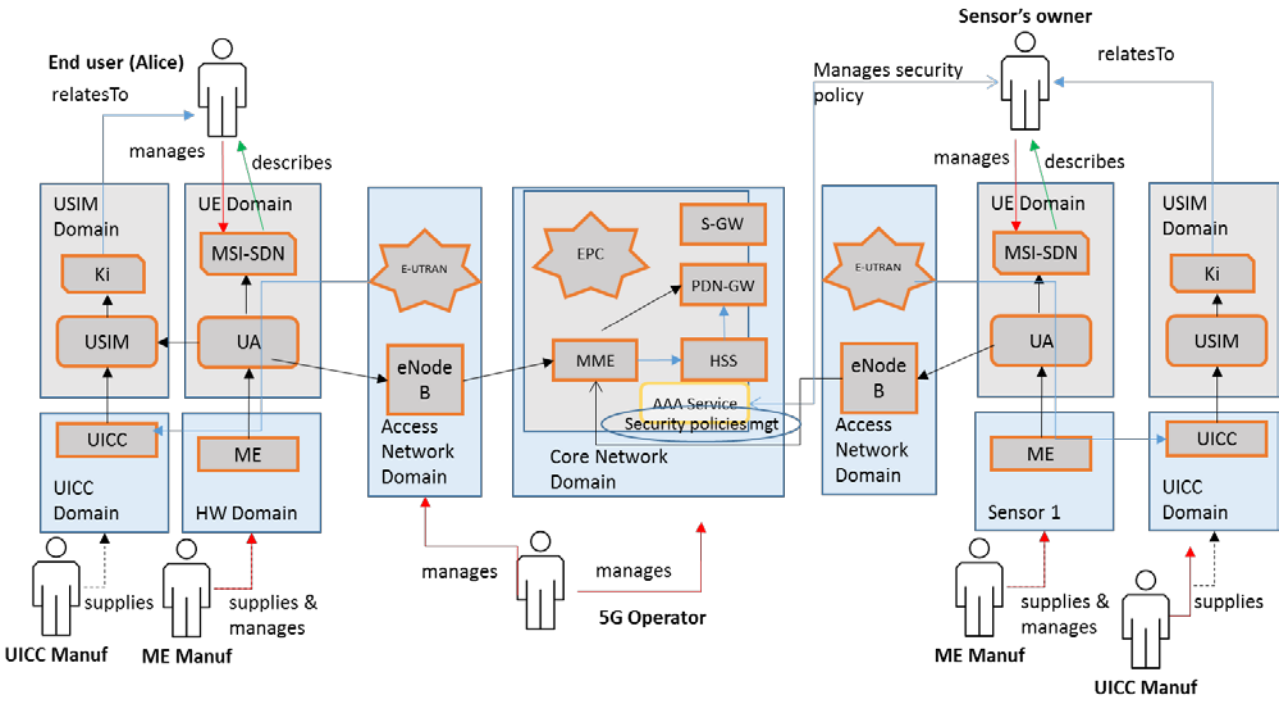

Figure A.48: Authorization in Resource-Constrained Devices Supported by 5G Network (UC 4.1): sunny day scenario

A.10.3 Identified threats

The way to obtain tokens, to validate tokens or to generate tokens are not standardized for now and so this analyse doesn't take into account the threats of this detailed interfaces.

A.10.3.1 Unauthorized data access (T_UC4.1_1)

The attacker, Mallory, wants to access the sensors' data without authorization. She can exploit the two main vulnerabilities by trying to generate a fake token or by trying to modify the security policy to get access to the sensors. The new vulnerabilities, due to the AAA server modifications are not in the scope of this use case.

Generation of a fake token or replay of an existing token: Two specific attacks could be performed by Mallory regarding the token. The first one is to build a new token giving all the right to use sensor data. The second one is to capture an existing token and to replay it in another context. To avoid this vulnerability, a specific attention should be given to the design of the token. The token will be injected at UA level (see Figure A.49).

Modification of security policies: The token generation and the associated security policy are not standardized for now and so, different modifications should be performed. The main one is to develop an interface with AAA server to configure the security policy. This interface must guarantee that only the sensor's owner can modify the security policy and only for his sensors (see Figure A.49).

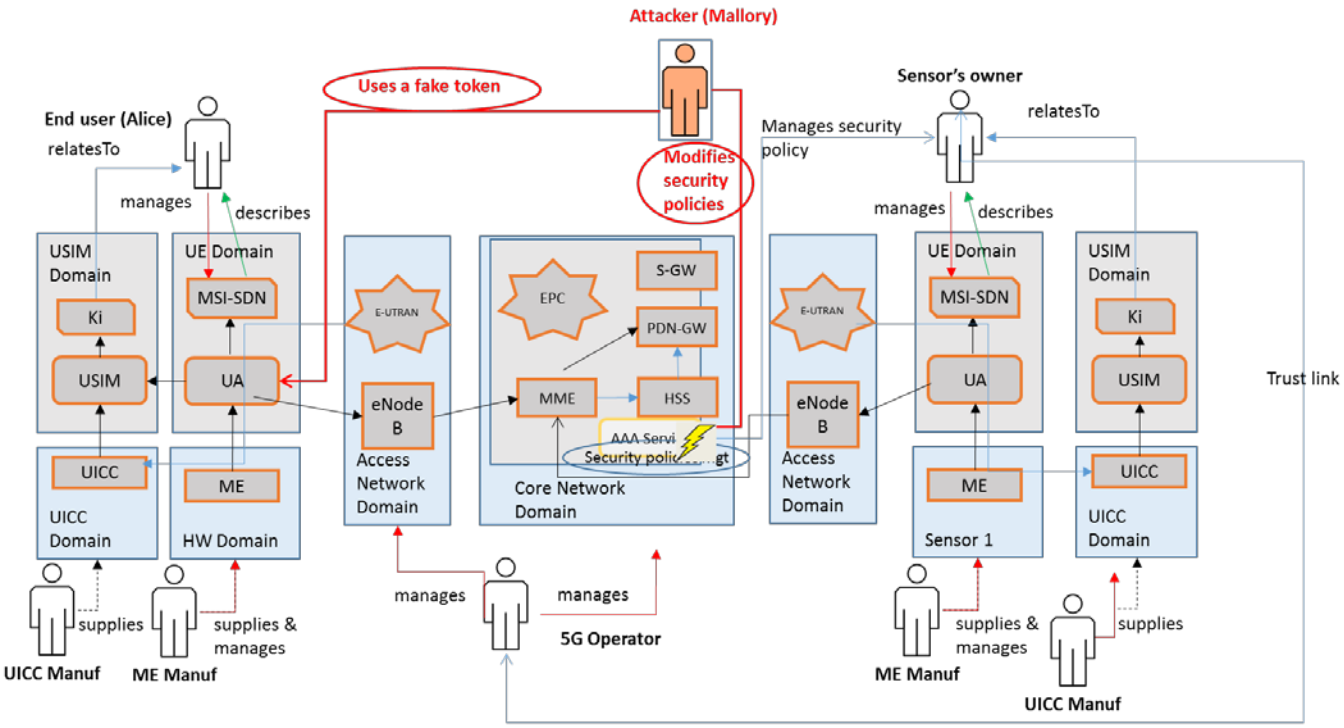

Figure A.49: Unauthorized data access (T_UC4.1_1) – 'rainy day'

The different parts of the architecture involved in the attacks are displayed in Figure A.49. The two main components involved are the user's UA and the AAA server (especially the modifications).

Trust implications

This use case involves several actors: the sensors, Alice's UE, the sensors owner, the 5G Operator to which the user and the sensor's owner have a subscription. The current trust model is based on the following relationships.

- The agreement between the 5G Operator (VMNO) and the sensor's owner. If this agreement is not clear and if the liability of the two parties is not well established, the sensor's owner could, for example, gives to anyone the credentials to modify a security policy. This weakness could be used by Mallory.
- The sensor's owner trust Alice

Threat mitigation strategy

The main action to mitigate the threats is at the token level. A specific attention should be given to the design of the token with, for example, a timestamp to avoid the token replay and crypto mechanisms (signature) to limit the possibility to build a new fake token.

A.11 Virtualized Core Networks and Network Slicing (UC 5.1)

A.11.1 Use case description with architectural components

This use case concerns micro-segmentation as a good way to ensure isolation of end-users' specific needs to manage their own sensors through the 5G infrastructure. Network slicing (and further sub-slicing) could be used to create portions of the underlying network which can be further used to provide network services with particular properties. Micro-segmentation could provide a more fine-grained approach than traditional network slicing and with micro-segmentation it may be possible to create secure segments where more granular access controls and stricter security policies can be enforced.

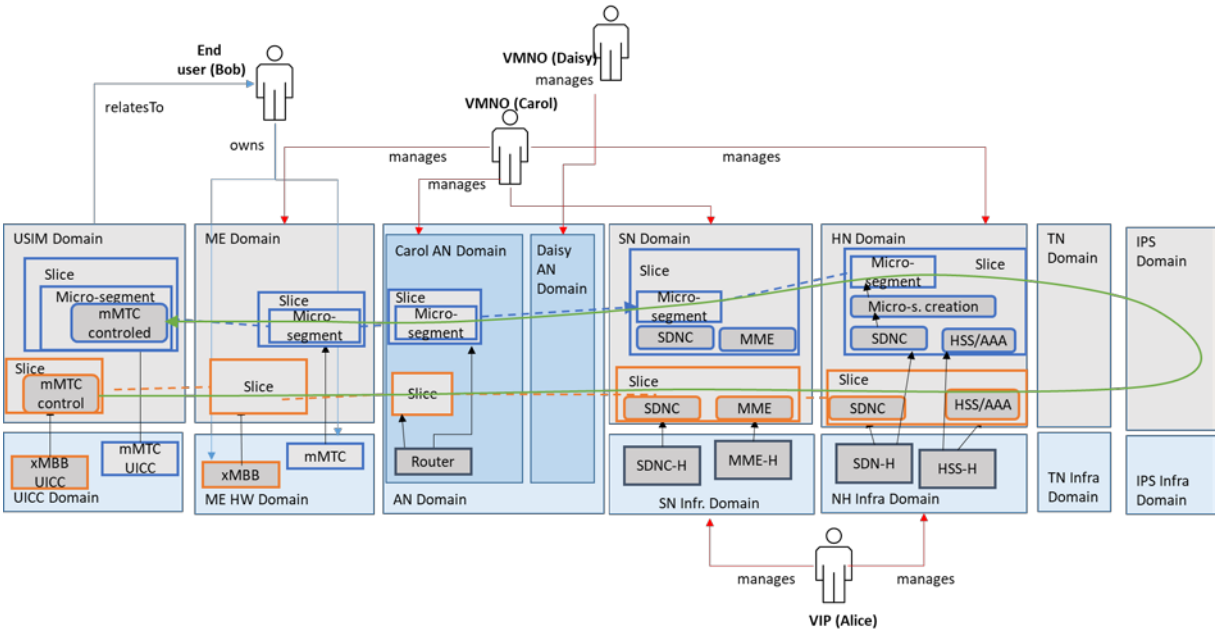

Figure A.50. Virtualized Core Networks and Network Slicing (UC 5.1): sunny day scenario

Figure A.50 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario). The subscriber (Bob) has two different devices and has a subscription to the virtualised network provided by the VMNO (Carol) for both devices, a 5G xMBB device and also a sensor that is a 5G mMTC device. VMNO (Carol) is providing an Internet accessible API for 5G mMTC device subscribers to control the behaviour of the mMTC devices.

Bob turns on the power in his 5G xMBB device and 5G mMTC sensor, and the attach requests are routed via the 5G radio network (AN). The base station (AN) contacts the MMEs in the VMNO network slices for xMBB and mMTC. The devices are authenticated towards the HSS/AAA of their slice after attachment. The VMNO decides to create a micro-segment for Bob's mMTC communications. This micro-segment is extended to include this 5G base station if not already included. The micro-segments are allocated for the devices that are authorized for it. The micro-segment has a security mechanism of its own.

The Network Slices are configured in such way that one slice does not accept commands from another slice. Nevertheless, through VMNO's Internet accessible API for 5G mMTC device subscribers, Bob can command his mMTC sensor by means of his xMBB device (Green flow).

A.11.2 Identified threats

A.11.2.1 Misbehaving control plane (T_UC5.1_1)

Malicious or compromised control plane may jeopardize the network and the data plane.

For instance, a compromised SDN controller or virtualization orchestrator may prevent data flows or direct them to a man-in-the-middle switch for eavesdropping or tampering. Centralized network controllers are an alluring targets for attacks as adversaries are not required to compromise switches or network functions it is enough that they steer data flows to their own malicious components.

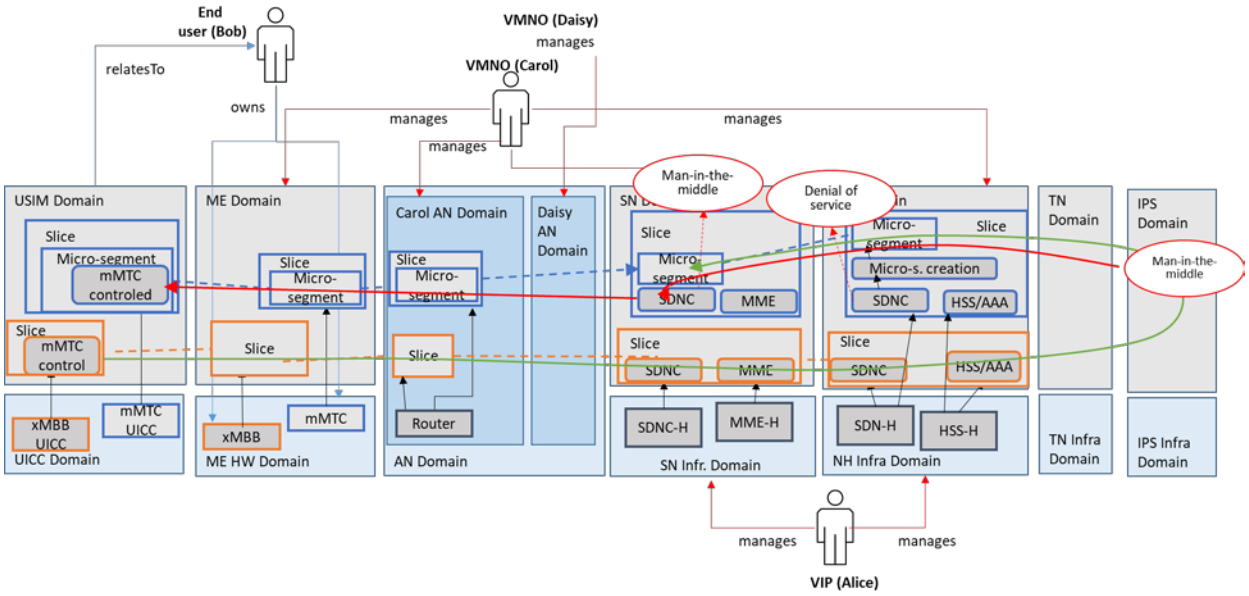

Figure A.51. Misbehaving control plane (T_UC5.1_1) – 'rainy day'

Figure A.51 shows the primary threat by which this attack is carried out, and the architectural components involved in the attack.

Since SN Domain micro-segment serving the mMTC sensor is accessible from the Internet through the an Internet accessible API for 5G mMTC, and if the micro-segment controller has a vulnerability, this could be a way for attackers to send fake commands to the mMTC device, or to compromise the SN SDN controller of the related mMTC slice in order to reach the mMTC device with fake commands (the red flows).

Also if compromised the SN SDN controller could deny the service to command the mMTC device.

Trust implications

The trust implications of this are as follows:

- The Subscriber (Bob) cannot manage his own mMTC sensor if his VMNO is compromised. Therefore, Bob has to trust his VMNO.
- The VMNO (Carol) suffers because her network is degraded and her customers (like Bob) will lose confidence in her services. The VMNO has a responsibility to manage the risk from this threat on behalf of her customers. Transferring any liability to the customers via service agreements is possible, but will not prevent their loss of trust.

Threat mitigation strategy

To mitigate this risk, the following option is possible:

- Micro-segmentation should split network slices into smaller parts with more restricted and controlled security policies dedicated for specific application services or users. By combining micro-segments similar guaranteed security levels can be provided even over multiple network domains and multiple network operators.

A.12 Adding a 5G node to a virtualized core network (UC 5.2)

A.12.1 Use case description with architectural components

In this use case, we assume that each UE is associated with a network slice before they have been authenticated. A new network slice requires configuring a new virtual MME which is done with software provided by a 5G Node Provider (5GNP). The control plane of SDN should not and cannot modify the physical network resources reserved to another Virtualized Core Network. Figure A.52 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

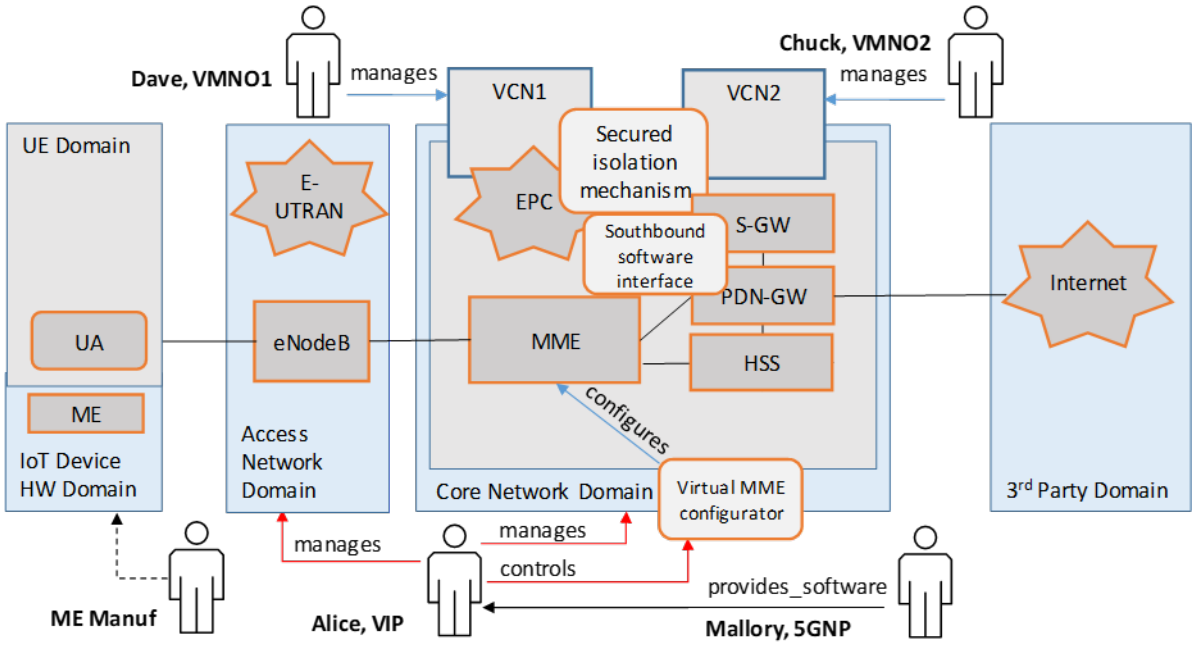

Figure A.52. Adding a 5G node to a virtualized core network (UC 5.2): sunny day scenario

A.12.2 Identified threats

A.12.2.1 Add malicious nodes into core network (T_UC5.2_1)

Software tools which are used to create a new MME or a new network slice can be corrupted, if they were obtained from a precarious vendor (Mallory). In such case, a new network node, which Alice carefully installs, may eavesdrop, tamper or even prevent data flows. Confidentiality, integrity and availability of communication gets severely compromised. Meanwhile, Alice can be completely unaware of this. Figure A.53 depicts the VNFs involved in the occurrence.

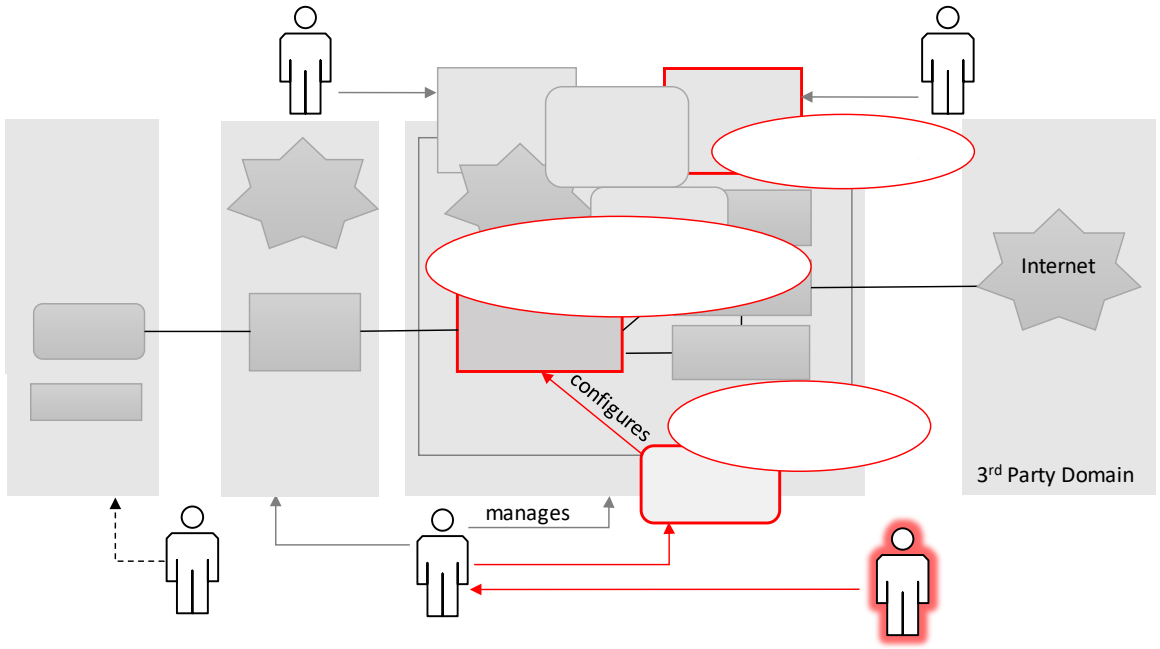

Figure A.53. Add malicious nodes into core network (T_UC5.2_1) – 'rainy day'

Trust implications

Potential trust implications are the following:

- Both VMNOs, Dave and Chuck, lose their trust to Alice since they may not be aware of Mallory's real role in the occurrence.
- Dave's and Chuck's customers, which are the end users of 5G network services, may lose their trust to their operators (Dave or Chuck) and even their trust in that 5G systems in general can offer any reliable service.
- Alice may lose her trust to Mallory for a reason, but also to some other software vendors although they have not done anything undesirable or malicious on purpose.
- Alice may think that either Chuck or Dave have ignored some important security measures either on purpose or accidentally

Threat mitigation strategy

Potential ways to mitigate this risk:

- All stakeholders, Alice, Chuck and Dave should apply advanced security verification procedures, both technical and organisational, to all software which they acquire
- Only authenticated and authorized entities should be allowed to add nodes to SDN
- Specific verification procedures should be utilized to assure that all added nodes are trustworthy
- Strict security monitoring of behaviour of added nodes as well as to communication over the network.

A.12.2.2 Forwarding logic leakage (T_UC5.2_2)

A network application (serving VCN2) at the southbound interface may be able to see the forwarding logic installed in the physical switches which are supporting another virtual network operator's domain (VCN1). Such information leak can be malicious and it can enable intercepting messages, gathering statistic

information and analysing installed forwarding rules of another competing VCN. Even confidential application data could be captured. Among potential effects is serious loss of confidentiality, outsiders may get to know positioning of virtual network components or critical service elements. This information can be used to infer end users or to disrupt reliability of a VMNO's system.

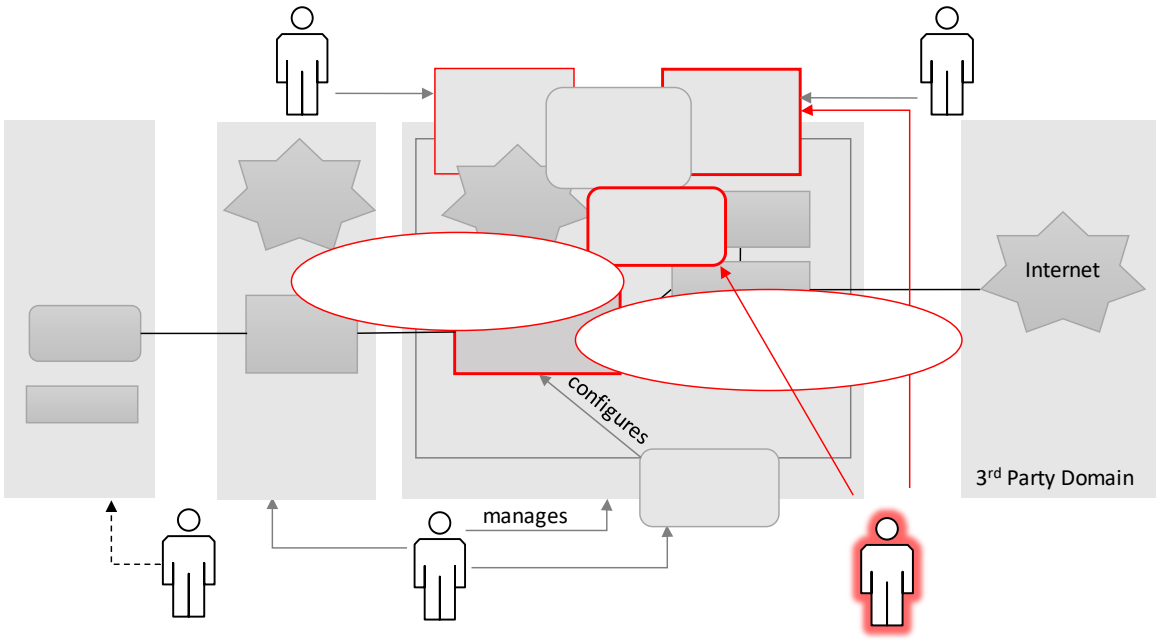

Figure A.54. Forwarding logic leakage (T_UC5.2_2) - 'another rainy day'

Trust implications

Potential trust implications are the following:

- Dave may lose trust to Alice, although Chuck or Mallory can be the real threat
- Chuck may not be aware of Mallory's malicious actions and his trust may not change at all
- If Chuck utilizes the leakage, he will lose some trust to Alice, if Alice does not notice the leak or if she cannot stop it
- Chuck can hardly trust Mallory, even if Mallory lets him use the leaked information
- Alice may lose trust to Chuck, even when Mallory is the only guilty stakeholder
- The end users of 5G network services may lose their trust to their operators (Dave or Chuck) and even their trust in that 5G systems in general can offer any reliable service.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Inserting a reference monitor at the southbound interface

A.12.2.3 Manipulation of forwarding logic (T_UC5.2_3)

The basic setting is the same as in T_UC5.2_2 except that in this case the intruder acts more aggressively. In addition to collecting confidential information of the competitor, malicious actions that change data flows are executed. Potential effects are: overflow of switch tables which causes slower and degraded performance, manipulating forwarding rules to trigger denial of service, modifying the rules to redirect traffic to allow intercepting every message and modifying system to tamper user's data.

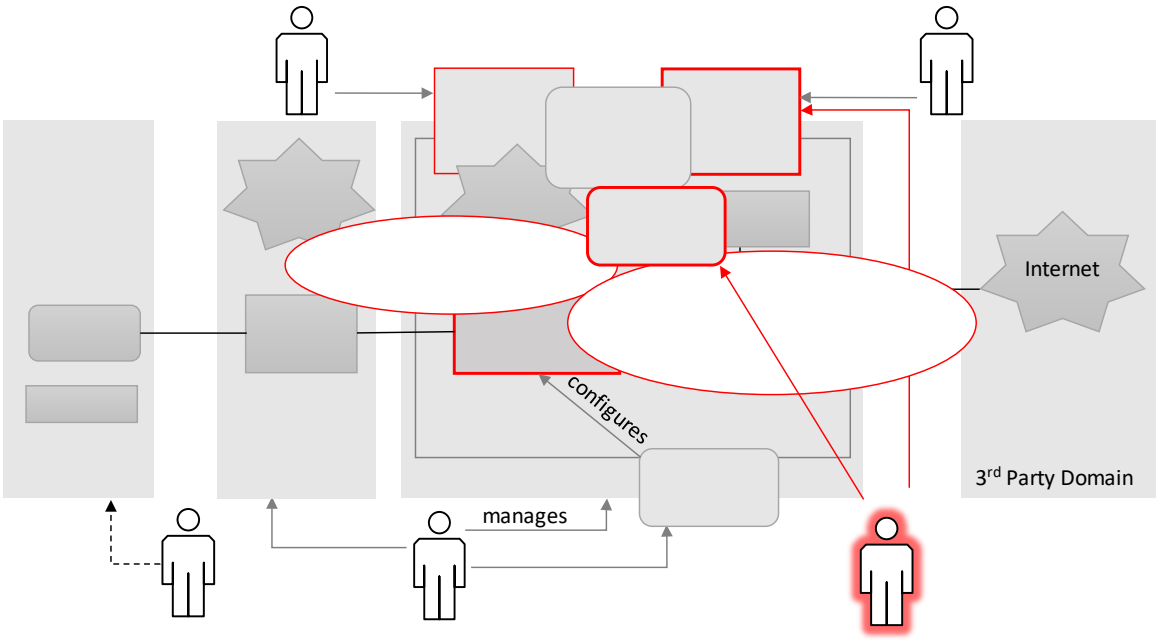

Figure A.55. Manipulation of forwarding logic (T_UC5.2_3) - 'yet another rainy day'

Trust implications

Potential trust implications are the same as with T_UC5.2_2 or the following:

- Dave may lose trust to Alice, although Chuck or Mallory can be the real threat
- Chuck may not be aware of Mallory's malicious actions and his trust may not change at all
- If Chuck utilizes the leakage, he will lose some trust to Alice, if Alice does not notice the leak or if she cannot stop it
- Chuck can hardly trust Mallory, even if Mallory lets him use the leaked information
- Alice may lose trust to Chuck, even when Mallory is the only guilty stakeholder
- The end users of 5G network services may lose their trust to their operators (Dave or Chuck) and even their trust in that 5G systems in general can offer any reliable service.

Threat mitigation strategy

Potential way to mitigate this risk is the same as with T_UC5.2_2:

- Inserting a reference monitor at the southbound interface

A.13 Reactive Traffic Routing in a Virtualized Core Network (UC 5.3)

A.13.1 Use case description with architectural components

This use case concerns reactive forwarding of network traffic in a Virtual Mobile Network Operator's core network. Subscribers connect via third party access networks, acting as roaming subscribers with respect to the VMNO's network. 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. A (virtualised) SDN controller then reconfigure the flow tables of the switches to provide the required connectivity.

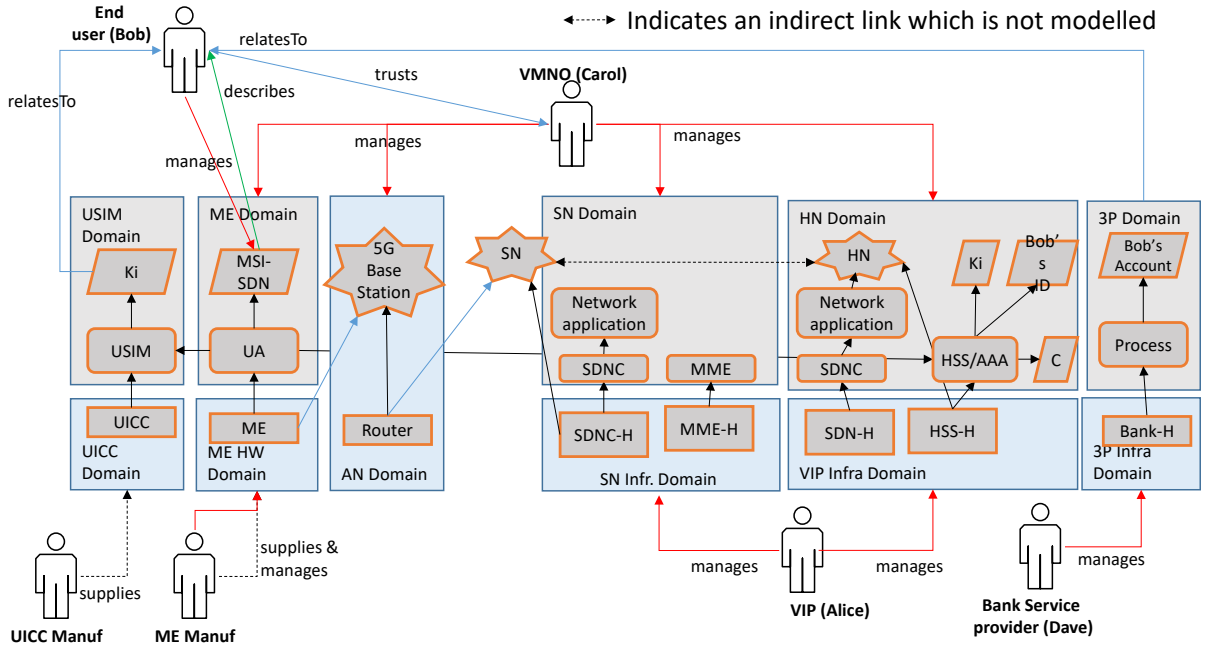

Figure A.56. Reactive traffic routing in a virtualised core network (UC5.3): sunny day scenario

Figure A.56 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario). The subscriber (Bob) connects to the virtualised network provided by the VMNO (Carol), and uses it to access services such as a Bank Service from a service provider (Dave). This service provider may have an agreement with the VMNO to provide related services, such as enhanced authentication of subscribers, although this is not essential to the scenario. The VMNO provisions their core network as a slice obtained from a Virtualised Infrastructure Provider (Alice). The VMNO's core network is therefore implemented using VNFs running on the physical infrastructure, including a Software Defined Network Controller (SDNC) providing connectivity for the Home Domain. In Figure A.56 we assume the VMNO has a similar arrangement to provide Serving Network domains connected to third party Access Network infrastructure, although this too is not essential to the scenario.

A.13.2 Identified threats

A.13.2.1 Fingerprinting attack on a virtualised network (T_UC5.3_1)

The threat in this case is a denial of service (DoS) attack against the VMNO's core network, caused by an attacker overloading the Home Domain SDNC. To do this, the attacker first carries out a fingerprint attack, measuring the response time of the network and determining how to trigger reconfiguration of the routing

tables at the SDNC. Having done this, the attacker provokes this reconfiguration by sending packets that force frequent updates and a massive increase in flow rules until the SDNC is overloaded and becomes unavailable.

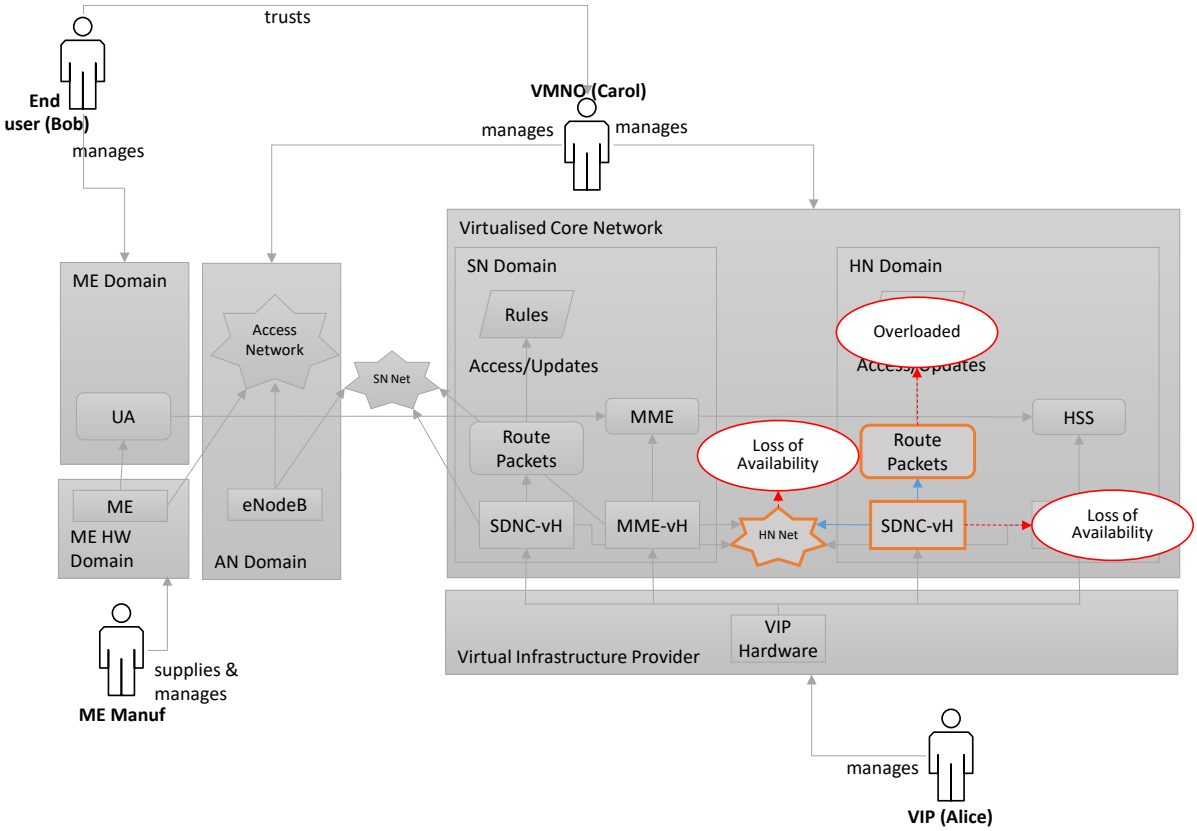

Figure A.57. Fingerprinting attack on a virtualised network (T_UC5.3_1) – 'rainy day'

Figure A.57 shows the primary threat by which this attack is carried out, and the architectural components involved in the attack. Essentially the routing function running on the (virtualised) SDNC in the HN domain is overloaded, the virtualised SDNC becomes unavailable, and the core network within the HN domain becomes unavailable.

Secondary effects caused by this attack include loss of access from the SN domain to control plane services in the HN domain such as the HSS, which prevents authentication of subscribers cutting them off from the Serving Network and in most cases also the Access Network. Another possible secondary effect is the overloading of the VIP Hardware (the physical SDNC and switches providing the virtualised HN domain core network), which may lead to a loss of availability in other slices supported by the physical infrastructure.

Trust implications

The trust implications of this are as follows:

- The Subscriber (Bob) cannot access the VMNO's network, which may also mean he cannot access specific services (like the Bank) if authentication depends on using that network. Bob cannot reasonably manage this risk, and depends on the VMNO to do that.
- In that case, the Bank becomes unavailable to customers they authenticate via that network. The Bank also cannot manage this risk, although any liability (towards Bob) might be transferrable to the VMNO via their service agreement covering authentication.

- The VMNO (Carol) suffers because her network is degraded and her customers (like Bob and possibly Bob's Bank) will lose confidence in her services. The VMNO has a responsibility to manage the risk from this threat on behalf of her customers. Transferring any liability to the customers via service agreements is possible, but will not prevent their loss of trust.
- The VIP provider (Alice) may also suffer degradation of her physical infrastructure. The VIP provider could take responsibility for managing the risk from this threat, or transfer the risk to their VMNO customers through their service agreement.

Threat mitigation strategy

The VIP provider could monitor loads from each slice, and constrain the physical network capacity made available to each slice. This does not prevent the primary threat, but would help to contain secondary effects that may damage the VIP provider.

A.14 Verification of the Virtualised Node and the Virtualisation Platform (UC 5.4)

A.14.1 Use case description with architectural components

This use case describes a situation where a virtualized network function (VNF) provider is running its VNF on top of a virtualized infrastructure and later wants to verify various security requirements through monitoring. In this use case we consider that the VNF is running on top of an ETSI network function virtualization (NFV) compliant architecture.

Figure A.58 shows this scenario in relation to the ETSI NFV architecture for management and orchestration, in the absence of any threat (the sunny day scenario). In this case the management & orchestration (MANO) administrator performs its duties as agreed with the OSS/BSS provider i.e. storing the correct versions of the software images of the VNFs in the repositories. Before launching the VNF instance, the VNF manager (VNFM) checks the signature of the software images and verifies the integrity and authenticity. As a result, a legitimate instance of the VNF gets launched on the network function virtualization infrastructure (NFVI).

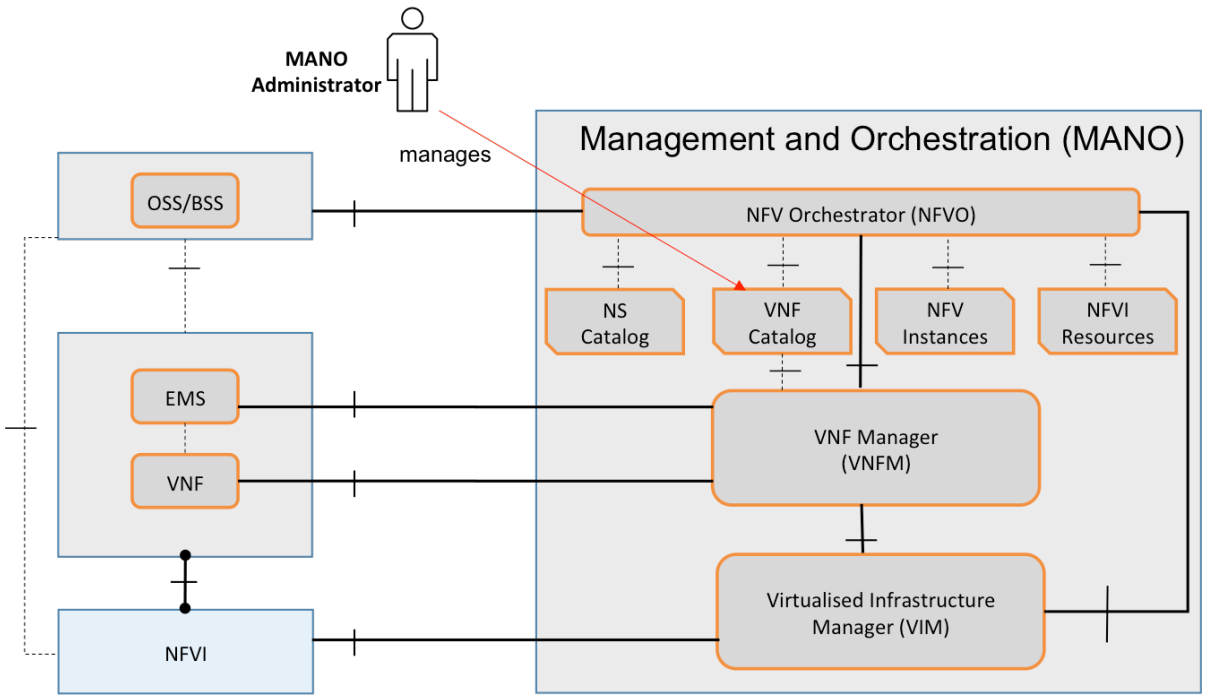

Figure A.58. VNF instance running on NFVI in a sunny day scenario

A.14.2 Identified threats

A.14.2.1 Generic Location hacking (T_UC5.4_1)

We document four alternative threats that are related to falsified geographical data fed into the system. The actual ingress point of the falsified data depends on the implementation. The data may be fed from the hardware or from software layer, depending on the actors.

The main risk is that if the system cannot guarantee real geographical location information, any monitoring policies, notifications or alarms are effectively useless.

Alternative 1: Generic service disruption: If attackers manage to infiltrate the geographical data system and feed misinformation e.g. that the physical platform is located in another country, the automated counter-measure systems may cause cascading failures throughout the system.

First the virtualized node (VN) or any other party that monitors VNs will notice that the VN is in foreign country. The VN (or the manager) will request migration back to origin country immediately. This may overload the rest Virtual Platforms.

Alternative 2: Behaviour altering: Behaviour of the VN may change based on the geographical location. For example, the encryption requirements may be more relaxed in neighbouring countries, or legal interception warrant may be valid only in one country. By modifying the location data, the attackers may cause the legal interception functionality to stop working.

Alternative 3: Malicious operator: This threat arises from the fact that the operator may have temporary difficulties in containing all required VNFs within the data center in France. Since the operator is operating in multiple countries, they temporarily move the VNF into Germany, still within their own data centers. However, not to reveal the breach of contract, they feed wrong location information to the Virtualization Platform's location "sensors" (i.e. GPS jamming/IP routing tricks).

Alternative 4: Physical hardware relocation: In this threat, the actual physical platform is moved to another geographical location, either by mistake or intentionally. If an operator has data centers in more than one country (or other important geographical boundaries), a mistake may happen in shuffling hardware between the sites. The risk is elevated if one of the sites is used as a global assembly/configuration point for all physical machines, and then shipped to the final data centers.

The risk comes from the fact that any hardware secure modules likely contains an imprinted geotag set by the operator. If the hardware is moved to another country, but the geotag is not updated, any monitoring services querying for location information will receive invalid information.

Trust implications

If the attackers manage to feed false location data into the system, any location based systems and services are going to be compromised.

Threat mitigation strategy

For all alternatives, the key issue is detecting foul play.

For alternative 1 and 2, the physical hardware could be imprinted with the current location when it enters the data center. This minimizes the software footprint and the attack surface. It does not, however, help against a malicious operator.

For alternative 3, no real mitigation strategy. Depends also on how much effort the operator is spending in order to cover up the contractual breach. If the platform and the VNs support TPM/HSM binding, they could use that to detect the change. Otherwise, the VNs can try to perform statistical analysis on packet delays and other network characteristics to determine that they are further than they should be. This is costly and very hard to prove conclusively.

For alternative 4, no real mitigation strategy. This should be easier case than alternative 3 as the incident is likely unintentional. Network traces may provide an important clue. The TPM/HSM binding will not work, as the whole physical machine is relocated.

A.14.2.2 Manipulation of data stored in repository (T_UC5.4_2)

This is an attack against the integrity verification of the virtualised network functions (VNFs). The most likely attack scenario is that the attacker is an insider administrator of the repository of VNF images or has access to this image repository. With sufficient privilege the attacker is able to alter existing software image in image repository. In this attack scenario, we assume that the attacker is able to replace the legitimate image with an older vulnerable version of the same image. We assume that the infrastructure provider verifies the image integrity and authenticity during launch time by verifying the image signature. However, to bypass this verification process, the attacker uploads an authentic older image version with a known vulnerability that the attacker can exploit. Now, the verification still passes since this image is still signed by the VNF vendor and was not modified by the attacker anyway.

Figure A.59 depicts the scenario of a rainy day where the MANO administrator is an attacker. In this case the MANO admin has access to the repositories of the software images and he/she replaces one or more software images with the older version of the same software images. Now, the verification of signature by the VNFM still gets passed since the replaced old image is still signed by the same vendor. Also, it is the lack of checking that the version is not verified during these phase will allow the attack to take place. After this verification, the vulnerable VNF instance is launched on the NFVI. Now the attacker can take advantage of exploiting the vulnerable VNF instance.

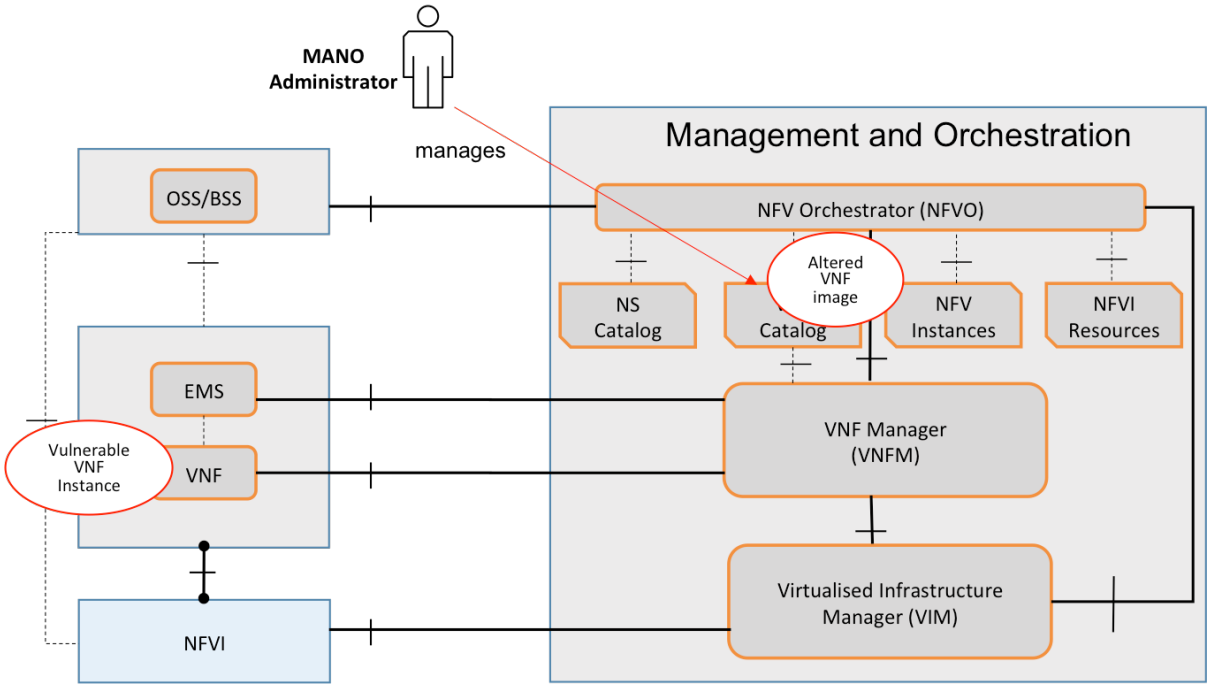

Figure A.59. Vulnerable VNF instance running on NFVI in a rainy day scenario

Trust implications

The trust implications of this are as follows:

- The VMNO is not able to run the right version of the VNF. This makes a big risk for the VMNO from both security and cost perspective. In this scenario the VMNO is running a vulnerable version while it is still paying for the legitimate software to be run in the system.
- The attacker has the opportunity to exploit vulnerability. This may imply that the attacker is able to still data from the VMNO application.

Threat mitigation strategy

To mitigate this risk, first of all we need to ensure that the software version (or image version in this case) is verified before a launch of a VNF. So, basically three things need to be checked before a launch:

- During loading the virtualised infrastructure shall only load software image if the authenticity is verified.
- During loading the virtualised infrastructure shall only load software image if the integrity is verified.
- Verification shall include software image versions in the above two cases and the virtualised infrastructure should know which version to run.

Another alternative to the above three steps is that the VMNO verifies all the software images once it is launched. However, this alternative still gives a window of opportunity to the attacker to exploit the vulnerability after the VNF gets launched in the NFVI and before it gets verified by the VMNO.

A.14.2.3 Compromised software signing key (T_UC5.4_3)

Secret keys used by the software vendor to integrity protect the software are compromised, and the incident goes undetected. Such a case may arise e.g. when a malicious administrator/employee copies the keys. The attacker now can create a malicious binary, sign it, and distribute it to the clients.

Trust implications

The VMNOs will be executing untrusted and potentially malicious binaries, which may compromise the whole network.

Threat mitigation strategy

The software vendor must have strong security policies set for software release. Signing the software is not enough. Also a strong checksum of the content must be published in a separate place (e.g. a web page). That information must be signed with another (and physically disconnected) set of secrets.

A.14.2.4 Integrity of the testing machine is compromised (T_UC5.4_4)

According to the use case description, Carol runs a test on the Virtualization Platform to attest the security and privacy characteristics. The attackers have, however, compromised the test program (or the test machine), and give false results.

Trust implications

Carol is left with the impression that everything is fine in the system, when in reality not all is good.

Threat mitigation strategy

There should be a system where all concerned parties are able to extract kind of audit trail of the system, and then compare the result for any anomaly. While the attackers may fool parts of the system, it is unlikely they can do that for each different actor.

A.15 Control and monitoring of slice by service provider (UC 5.5)

A.15.1 Use case description with architectural components

A 3rd Party Service Provider requires a secure network with some QoS guarantees to be used by their customers (game players). The Service Provider has a contract with the VMNO for the VMNO to supply a suitable sub-slice of the VCN for the Service Provider's customers to use. The Service Provider is allowed to monitor the sub-slice and also to control the parameters of the sub-slice within some predefined bounds.

The term "sub-slice" is here being used to mean a portion of a network slice. This use case maintains most of its features, if the Service Provider is a direct customer of a MNO and the MNO provisions a "slice" of the core network for the SP.

Figure A.60 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario). Dave, an employee of the SP monitors the QoS provided to the game players (Bob and others) and notices that the capacity provisioned for the players may soon degrade to unacceptable level. Dave requests more capacity to meet the demand. The VMNO (Carol) first checks that Virtual Mobile Network can support the increased capacity and then accepts the request.

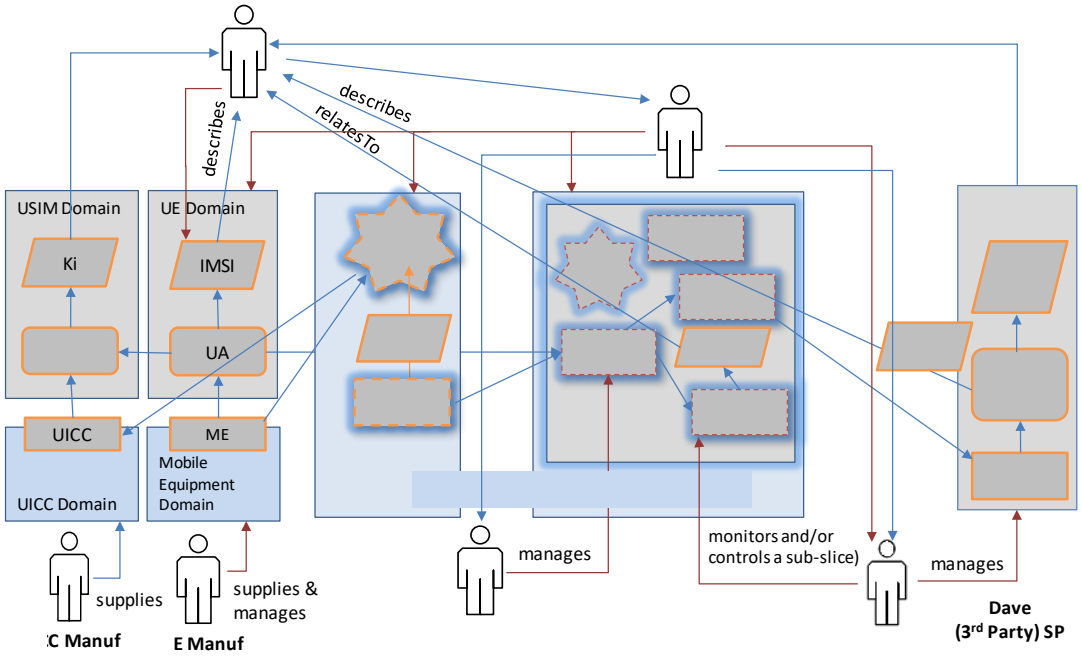

Figure A.60. Control and monitoring of slice by service provider (UC 5.5): sunny day scenario

A.15.2 Identified threats

A.15.2.1 Misuse of open control and monitoring interfaces (T_UC5.5_1)

The SP (Dave) may misuse the access to control interfaces and cause service disruptions to other customers or an external party may exploit or attack SP's systems. Monitoring information and data flow may get captured to profile end-users.

When a sub-slice or slice exceeds its capacity limits, QoS offered to other users suffers, or service becomes unavailable, and core or access network may get overloaded. Figure A.61 shows the VNFs involved in the occurrence.

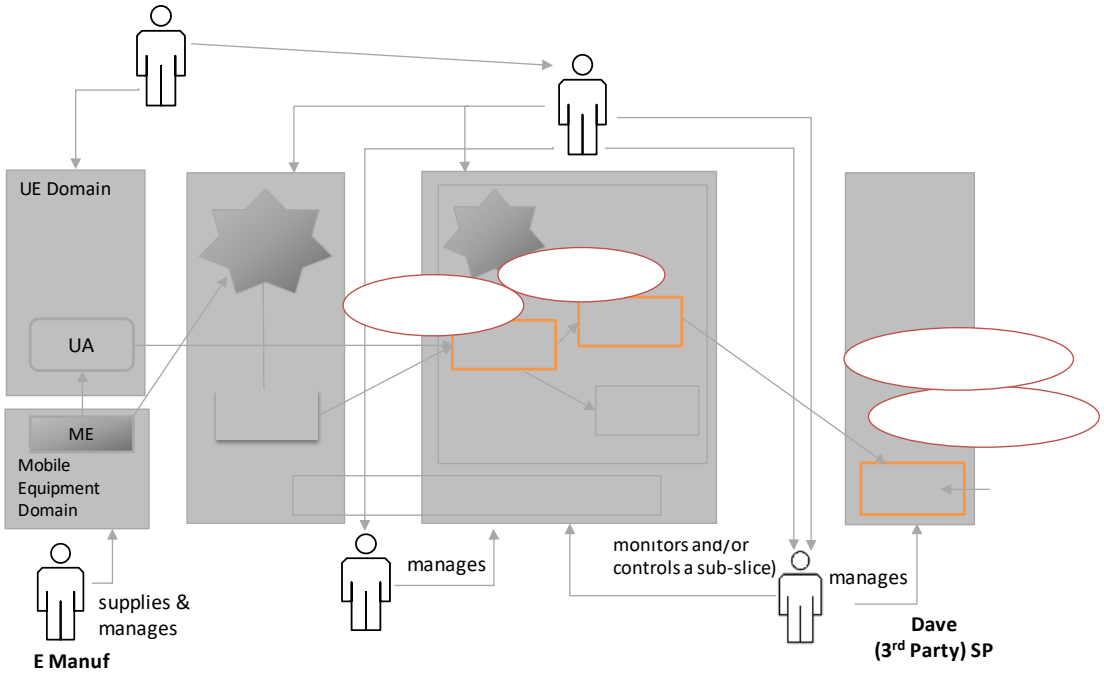

Figure A.61. Misuse of open control and monitoring interfaces (T_UC5.5_1) – 'rainy day'

Consequence effects include potential loss of communication security and privacy in a VMN. An overloaded or congested PDN-GW may disturb adjacent systems as well and these may also get congested or unavailable. This use case indicates that when critical interfaces are opened for several service providers they may also become available for other adversaries.

Potential secondary effects include preventing authentication of subscribers through the HSS which denies access from them. Furthermore, if the identity of the end users leaks to outsiders, this information could be used in criminal actions against them.

Trust implications

Potential trust implications are the following:

- SP's customers (Bob) may get better service than they expected, if SP (Dave) intentionally gives them more resources and better QoS than VMNO (Carol) allowed. Bob's trust to Dave may only improve from these actions. Still, if Bob uses other services through the same VMNO, he may suffer from limited resources and lose his trust to VMNO (Carol). Service level agreement between SP and VMNO should cover these cases.
- If the customer's (Bob) identification or other personal data leaks to outsiders, the customers may lose their trust completely, both to SP (Dave) and to VMNO (Carol).
- The VMNO (Carol) is responsible of that SP's (Dave) cannot control network outside their own slice or that they cannot exceed their allowed resources without a permission. And yet, the service level agreement between VMNO and SP should prohibit SPs from doing any unapproved actions and financial sanctions should follow, when this occurs.
- When VMNO (Carol) cannot control the VMN she loses trust of some or all customers. VMNO cannot transfer responsibility of her own customers to other stakeholders.

- VMNO should be able to trust that SP does not try to take control of other slices or the whole network and that SP's systems are not vulnerable. If the service provider (Dave) can prevent intrusion to his system, the service level agreement with VMNO (Carol) should cover liability of all consequences, to which SP's systems can be responsible.
- The VIP provider (Alice) may also suffer degradation of her physical infrastructure. The VIP provider could take responsibility for managing the risk from this threat, or transfer the risk to their VMNO customers through their service agreement.

Threat mitigation strategy

Potential ways to mitigate this risk:

- The VIP provider and VMNO should monitor and constrain the physical network capacity made available to each slice. As EPC especially is vulnerable to this threat, EPC monitoring and control systems should take care of counteracts.
- SPs should control their systems properly and also strictly monitor their customers since they may abruptly turn to hostile exploiters.
- SLAs should clearly specify each stakeholder's responsibilities and oblige to severe financial consequences from all potential violations.

VMNO may use the Micro-Segmentation Enabler, which is developed in 5G-ENSURE, to deploy sub-slices to SPs. This enabler can control and defend micro-segments in various ways. Furthermore, another 5G-ENSURE's enabler, the Security Monitor for Micro-Segments enables accurate security incident detection and also adaptation of micro-segment's defences against this type of threat.

A.15.2.2 Unauthorized access to a network slice (T_UC5.5_2)

If VMNO (Carol) misconfigures SP (Dave), she may authenticate and authorize SP to access or control resources that belong to the VMNO or other SPs. Such error may jeopardize availability and security of VMNO's and other SP's resources. Figure A.62 shows the VNFs involved in the occurrence.

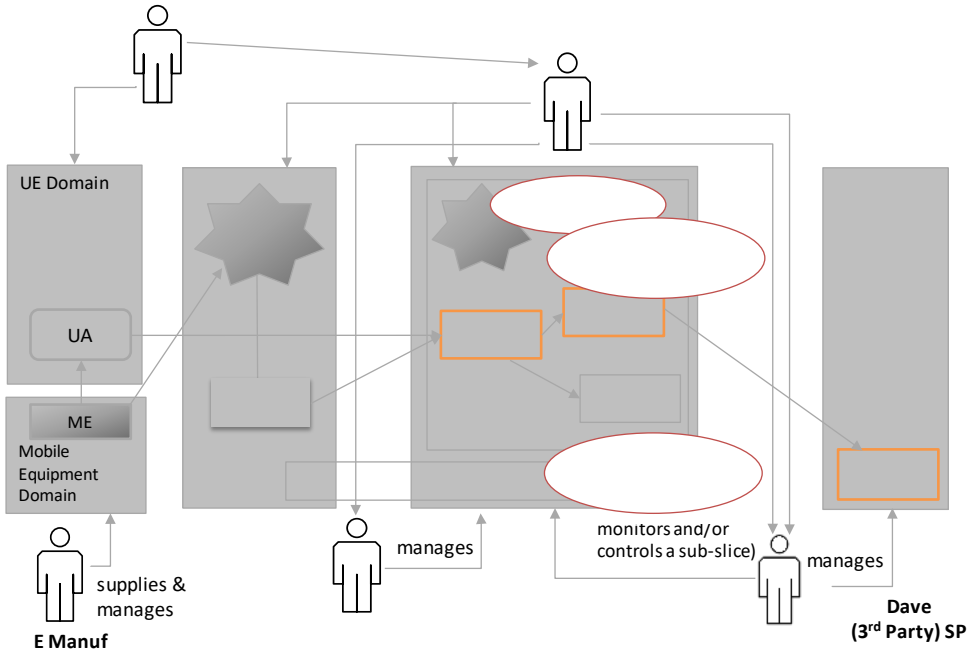

Figure A.62. Unauthorized access to a network slice (T_UC5.5_2) - 'another rainy day'

Although this threat arises though a different procedure, its basic consequences are about the same as those mentioned with T_UC5.5_1. The effects include potential loss of communication security and privacy in a VMN.

Potential secondary effects include preventing authentication of subscribers through the HSS which denies access from them. Furthermore, if the identity of the end users leaks to outsiders, this information could be used in criminal actions against them. SP could also utilize or sell information from VMNO's and other SP's customers.

Trust implications

Potential trust implications are the following:

- SP's customers (Bob) may get better service than they expected, if SP (Dave) intentionally gives them more resources and better QoS than VMNO (Carol) allowed. Bob's trust to Dave may only improve from these actions. Still, if Bob uses other services through the same VMNO, he may suffer from limited resources and lose his trust to VMNO (Carol). Service level agreement between SP and VMNO should cover these cases.

Threat mitigation strategy

Potential ways to mitigate this risk:

The VIP provider and VMNO should monitor and constrain the physical network capacity made available to each slice. As EPC especially is vulnerable to this threat, EPC monitoring and control systems should take care of counteracts.

A.15.2.3 Bogus monitoring data (T_UC5.5_3)

Tampered monitoring data or measurement procedures may cause control plane to perform wrong control actions. For instance, adversary may impair the availability of the system by getting nodes (which will appear malicious) to be dropped from the topology. The adversary may also change forwarding policies in order to affect availability or to direct data flows into nodes that are e.g. under the control of the adversary and may thus perform eavesdropping or tampering. Figure A.63 shows the VNFs involved in the occurrence.

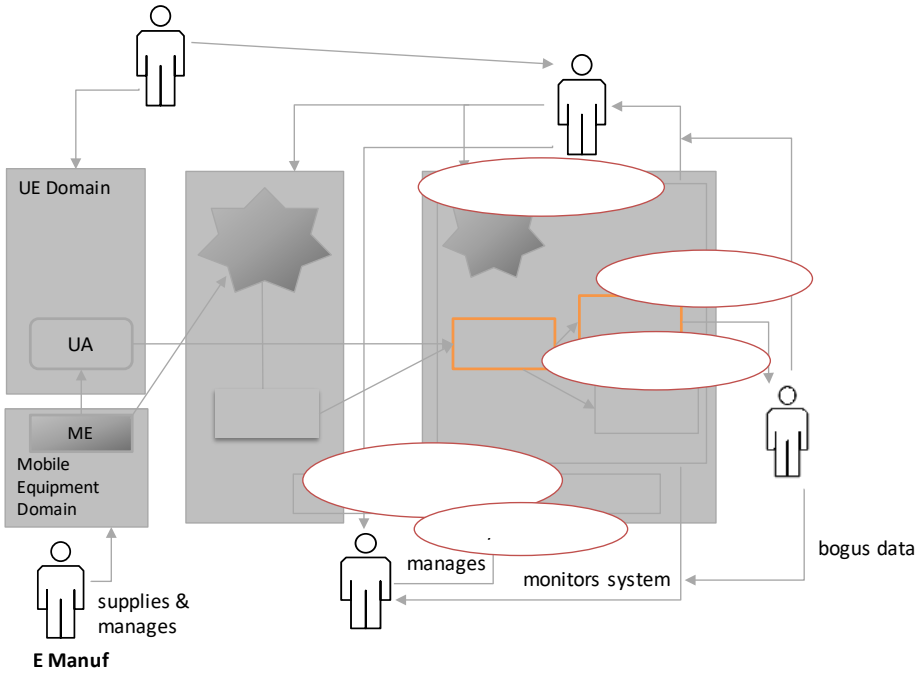

Figure A.63. Bogus monitoring data (T_UC5.5_3) - 'another rainy day'

The adversary (Mallory) may utilize unauthorized measurement points or monitoring systems. The adversary may finally take full control of the system as some or all security measures can be cancelled. This may open a slice or the whole system for any type of malicious activities. The attacker may redirect traffic flows or block users, or take all resources for one user. The system may even lose some or all of its authentication, authorization and accounting functions.

Potential secondary effects include severe financial losses for the VMNO which may include reclaims from the end users (Bob).

Trust implications

Potential trust implications are the following:

- The Subscriber (Bob) cannot access the VMNO's network, which may also mean he cannot access any of the services that he typically uses. Bob cannot reasonably manage this risk, and depends on the VMNO to do that.
- The SPs cannot provide their services to their customers, which will cause them financial losses. The SPs cannot manage this risk, although any liability (towards Bob) might be transferrable to the VMNO via their service agreement covering authentication.
- The VMNO (Carol) suffers because her network is degraded and her customers will lose confidence in her services. The VMNO has a responsibility to manage the risk from this threat on behalf of her

customers. Transferring any liability to the customers via service agreements is possible, but will not prevent their loss of trust.

- The VIP provider (Alice) may also suffer degradation of her physical infrastructure. The VIP provider may have to take responsibility for managing the risk from this threat, or transfer the risk to their VMNO customers through their service agreement.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Sources of monitoring data should be authenticated and the source identity information should be available for the information user.
- In cases where monitored data is processed, or aggregated, and then made available for other parties, the original sources of data could be available to enable information users to make sufficient estimates on the reliability of the data.

The sources of bogus measurements may be detected by monitoring the measurements streams and analysing the data against correlated data sources.

A.15.2.4 No control of cyber-attacks by the Service Providers (T_UC5.5_4)

The use case features a Service Provider (SP) offering an online game service to gamers. The SP buys network service from a VMNO which itself relies on an Infrastructure Provider (VIP). The VMNO supplies a sub-slice to the SP with the required QoS.

The SP's system can be subject to cyber-attacks. SP signs a contract with a third party Security Service Operator (SSO) to monitor and remediate cyber-security attacks. Thanks to the terms of the contract between the SP and the VMNO, the SSO can benefit from network topology information and routing tables from the slice controller. Nevertheless, since SSO gets no information about the configuration of the VNF and their vulnerabilities, SSO cannot build a classical attack graph to monitor the cyber-attacks against the VIP.

SPs systems may seem protected while VNFs (MME, HSS, PDN-GW) can be under attack. Figure A.64 shows the VNFs involved in the occurrence.

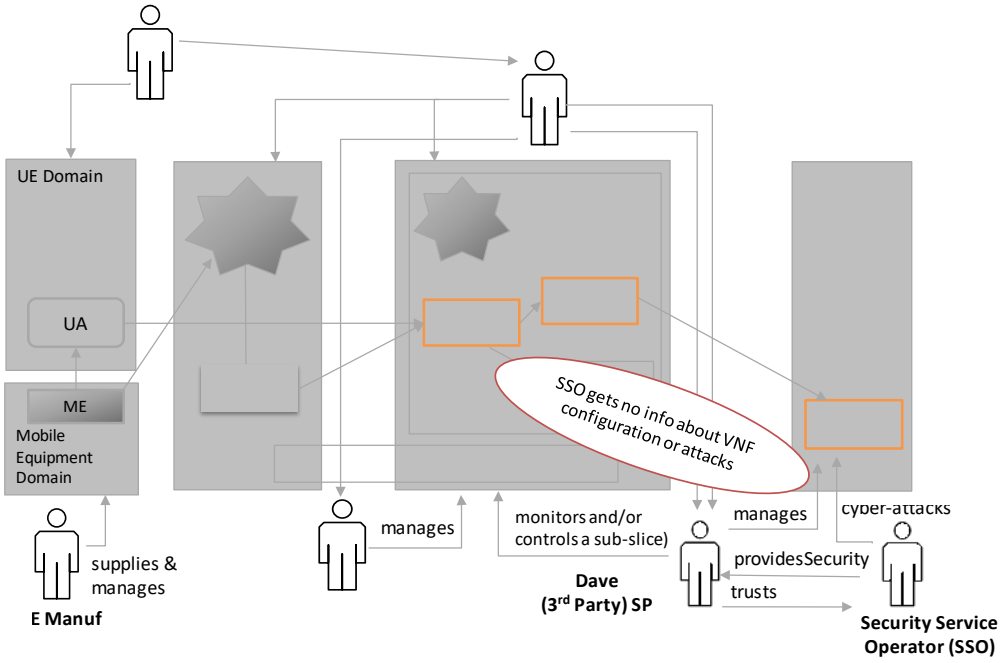

Figure A.64. No control of cyber-attacks by the Service Providers (T_UC5.5_4) - 'rainy day'

Core network may get congested and SP (Dave) cannot provide the game service to end users (Bob) although SP expects SSO to resolve such cases. End users may lose communication or their communication privacy directly or as a consequence of secondary effects from these threats.

Trust implications

Potential trust implications are the following:

- Bob may suffer from limited resources and lose his trust to VMNO (Carol). Service level agreement between SP and VMNO should cover these cases.
- If the customer's (Bob) identification or other personal data leaks to outsiders, the customers may lose their trust completely, both to SP (Dave) and to VMNO (Carol).
- When VMNO (Carol) or VIP (Alice) cannot control the VMN or VI she loses trust of some or all customers. VMNO or VIP cannot transfer responsibility of her own customers to other stakeholders.
- SP should be able to trust that VMNO's systems are not vulnerable. The service level agreement with VMNO (Carol) should cover liability of all consequences, to which VMNO's systems can be responsible.
- SP should trust that SSO can control all threats against SP's systems. When SSO cannot control VIP's system, there should be an agreement that limits SSO's responsibilities in these cases.
- The VIP provider (Alice) may also suffer degradation of her physical infrastructure. The VIP provider could take responsibility for managing the risk from this threat, or transfer the risk to their VMNO customers through their service agreement.

Threat mitigation strategy

Potential ways to mitigate this risk:

- A possible solution is to enable the SSO to get access to the information from the infrastructure domain, especially the type of software used to implement NFV in order to determine its vulnerabilities.

Another way to this threat is to separate the responsibilities by contract between the infrastructure domain and the VMNO. Then the SP may rely on the VMNO interface and will only control its cyber-threats at application level

A.16 Integrated Satellite and Terrestrial Systems Monitor (UC 5.6)

A.16.1 Use case description

This use case integrates the security methods used in satellite systems and terrestrial systems. Using this way, the SNO focuses on the monitoring of both system using a simple way where both security systems are accessible from the same server, using a centralized server for this task. The monitoring is done managing the alarms and events coming to the system in order to analyse the network involved. With the help of this method for monitoring combined in both systems, the issues detected in terms of security as threats can raise in a shorter period of time.

The system collects different data from events, indicators and alarms and the patterns of security threats from satellite and terrestrial systems to make a semi-automatic method of monitoring based on machine learning and the experience of past events.

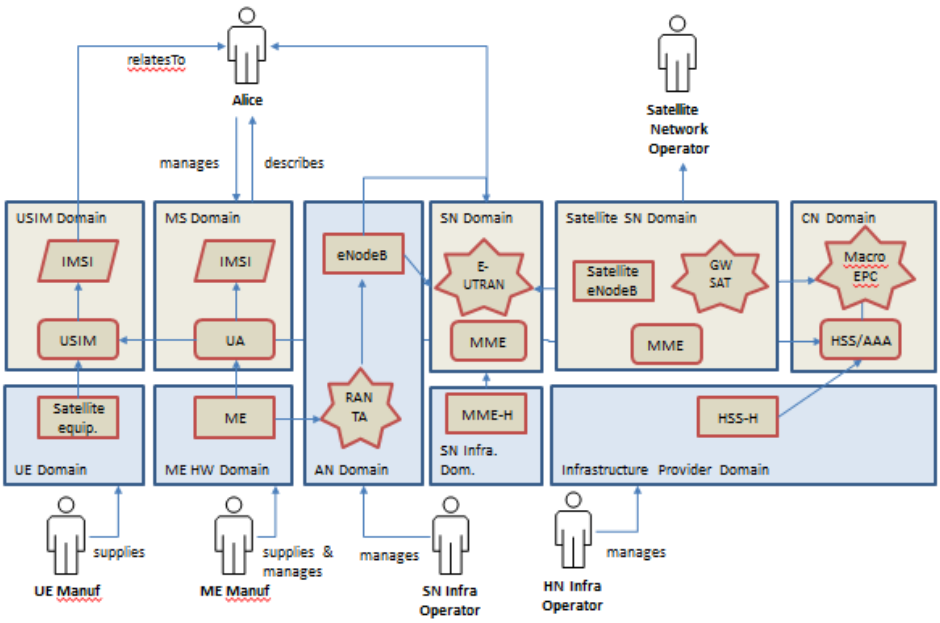

Figure A.65. Integrated Satellite and Terrestrial Systems Security Monitor (UC 5.6): sunny day scenario

A.16.1.1 Security threats in a satellite network (T_UC5.6_1)

A Service Provider (i.e. telecommunications company) has a contract with the Satellite Network Operator (SatNO) to supply a suitable system capacity with some QoS guarantees to be used by its customers. The service provider uses the behaviour known (in case of being a terrestrial operator) or rent this information to a terrestrial one to incorporate this knowledge and help the monitoring of satellite network under threats not known.

In this case an event never known (or not planned), i.e a threat in the satellite network occurs in the management system. A natural disaster occurs and the link communication between the satellite transmission system and the receptor antenna is cut due an obstacle placed between them. The operator cannot manage the satellite and it is vulnerable to attacks and different threats affecting to the satellite. Using a known system used in terrestrial networks as the reconfiguration of the topologies, the satellite system can learn of this and reconfigure the haze to focus in another point in order to re-establish the communication again.

Due the natural disaster nature, the public organizations and users (Alice) will re-establish the communications after some time, when the satellite's haze has been reallocated.

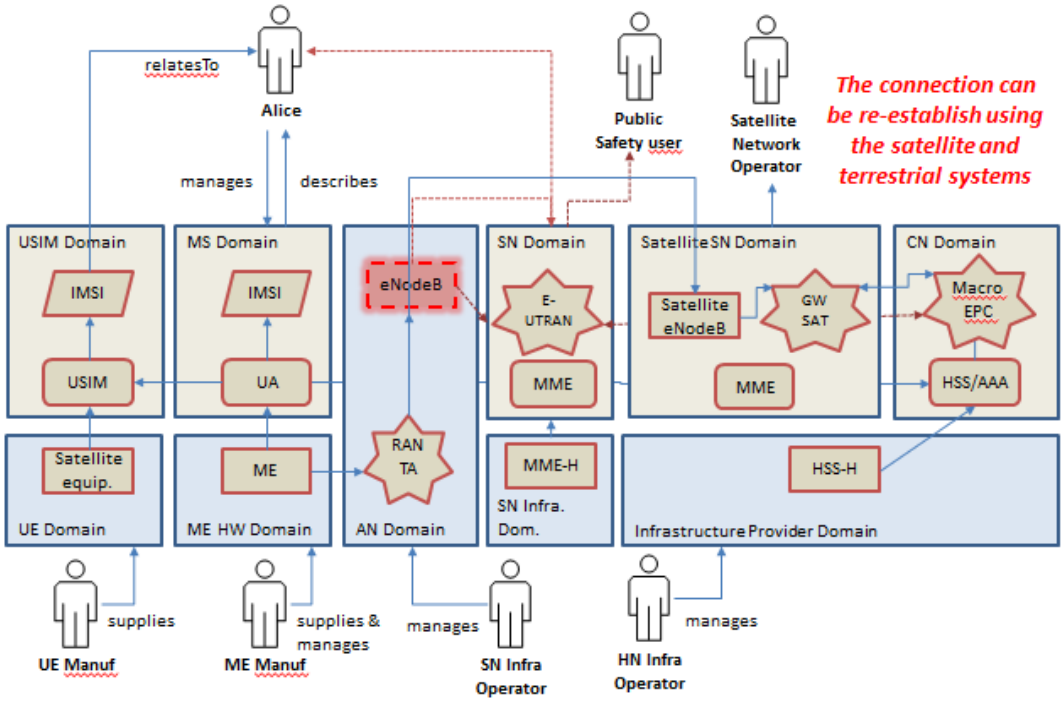

Figure A.66. Re-establishing the communication, Security threats in a satellite network (T_UC5.6_1)

With the events and alarms received regarding the failure of communication, the system learns of the terrestrial monitoring system and focuses its haze to another antenna received not blocked with direct communication to the base station affected without direct contact to the satellite.

After the distribution of the signal, the affected base station receives the signal again just using a reconfiguration in the haze of the satellite to avoid the blocks due the natural disaster and the satellite operator can manage the satellite again.

Without the integrated system security monitor present, the recovery time of the service will be much higher and the human will be necessary in order to reallocate the service. Also during the time when there is no connectivity the security will leak, presenting a potential trouble in terms of security and loss of service.

Trust implications

Potential Trust Implications:

- Customer trust in the service provider or operator based on the lack of availability and the managing of facing issues under pressure.
- The service provider or operator seems not to have a plan for disasters or a system to recover the control as faster as possible based on recurrent events.
- The SLA, which can be associated to different contractual offers or contracts cannot be accomplished with the difficulties and the delay in the re-structuration of the topology network based on the threats.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Events and alarms management of real time data to control the network through network statuses and analysis.
- Establish clear action plans identifying critical elements, contentions actions and terrestrial networks as suggested in the rainy scenario can be key to mitigate the risks.
- Integrating Satellite and Terrestrial systems can be used the knowledge acquired in one or other system to mitigate threats in satellite networks. An example of this is a reallocation of the topology based on terrestrial networks.

A.17 Attach Request During Overload (UC 6.1)

A.17.1 Use case description with architectural components

This use case details a device attaching to an overloaded MNO network. This could be use to an emergency situation or simply access to the MNO network is overcapacity. Ideally all devices should be able to connect to the network without any issue, which is not always the case. The alternative is to apply quality of service (QoS) to certain device which will higher priority to connect first.

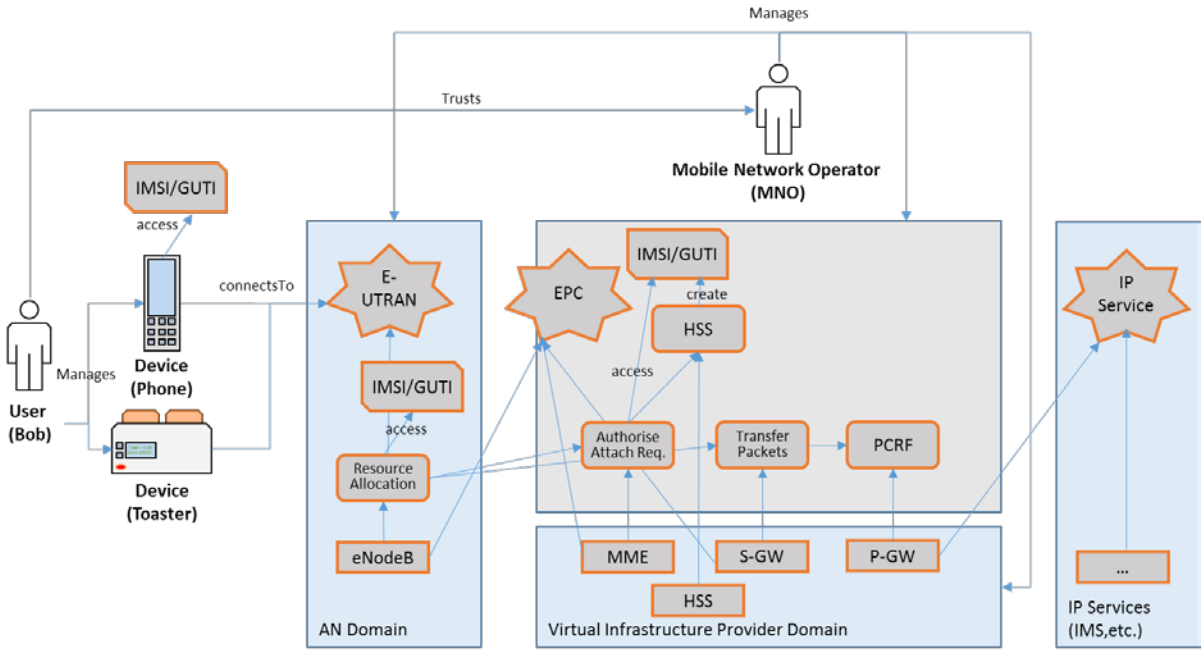

Figure A.67. Attach Request during overload (UC 6.1): sunny day scenario

Figure A.67 details the sunny day scenario. From left to right we see the entire sequence of how a user's device connects to the access network, and onwards to the MNO's service and out onto the wider internet. This use case is focused on the method which a device attaches to the MNO's network. When the user's device attaches it first connects to the eNodeB which will allocate resource and communicate back to the NMO's network so it can authorise the request. If all is well the user's device is authorised onto the 5G network. The MNO is in control of the eNodeB and the EPC. The end user, or subscriber, trusts that they can connect their devices to the 5G network without delay or issue.

A.17.2 Identified threats

A.17.2.1 Unable to attach when Overloaded (T_UC6.1_1)

The primary cause is a service in the path of a subscriber's device is overloaded resulting in the device being unable to connect to the MNO network. It may not involve a malicious attacker, but simply be down to high demand or inefficient design. This can threat can happen in more than one location, as shown in the figure below.

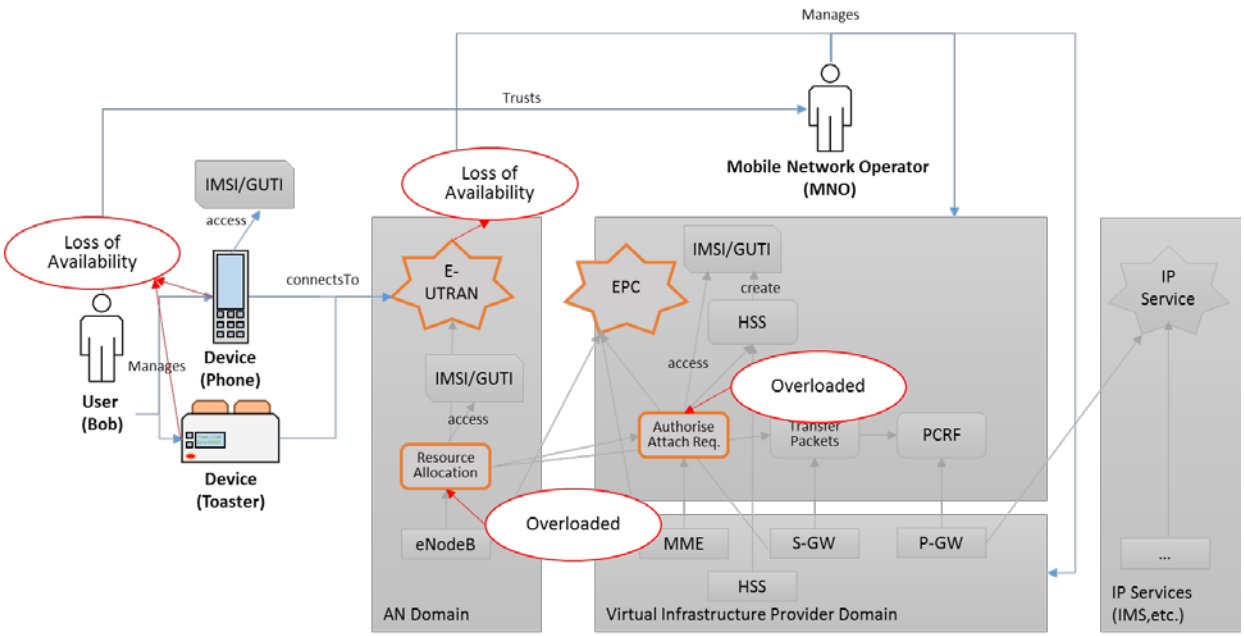

Figure A.68. Unable to attach when overloaded (T_UC6.1_1) – 'rainy day'

As mentioned above it is possible that this attack could occur in multiple locations. The first being in the eNodeB, access network. If the eNodeB consumes too much resources it will be unable to accept new or existing refresh connections, due to being overloaded. The second location this risk could arise could be within the MNO network. If the MNO is unable to authorise a new device connecting to the network via the eNodeB then again the user's device will be unable to attach.

If there are multiple eNodeB's in a mesh styled formation, then when one becomes overloaded it will cause extra demand to on the others resulting in that device to become overloaded as well. Also, once the eNodeB becomes available again, it may cause devices which were attempting to attach one at a time to simultaneously attach. Resulting in an increased load on the MNO services, which could cause it to become overloaded.

Trust implications

The first implication is clearly between the user, Bob, and the MNO. Bob has expectations that the service he is paying for will reliably be available. If he is unable to attach to the network then he will lose trust in the service. If the eNodeB is provided by a MNO, and is used by a virtual MNO and the eNodeB becomes unavailable then the VMNO will lose trust in the MNO.

Threat mitigation strategy

A possible mitigation strategy is could be to enforce quality of service (QoS) and limiting access to the MNO or the eNodeB it would be possible to prevent overloading of the systems. It would be performed by the owner of the access network, which might be the VIP or MNO and in some cased the VMNO. Alternative mitigation methods would be to save resources by rejecting illegitimate or non-prioritised requests at an earlier stage that is done now. Another method would be to give priority to reconnecting devices to prevent them from becoming out of sync and allowing the attack to succeed. Again this are will be performed and located in the access network.

A.18 Unprotected User Plane on Radio Interface (UC 6.2)

A.18.1 Use case description with architectural components

This use case details issues which may arise from having insignificant protection of the user data plane. The signalling data between the UR and the network is protected via integrity validation. Though in in order to conserve battery power on the device, by minimising the signalling, it introduces a vulnerability in that the data plane lacks protection from both encryption and integrity.

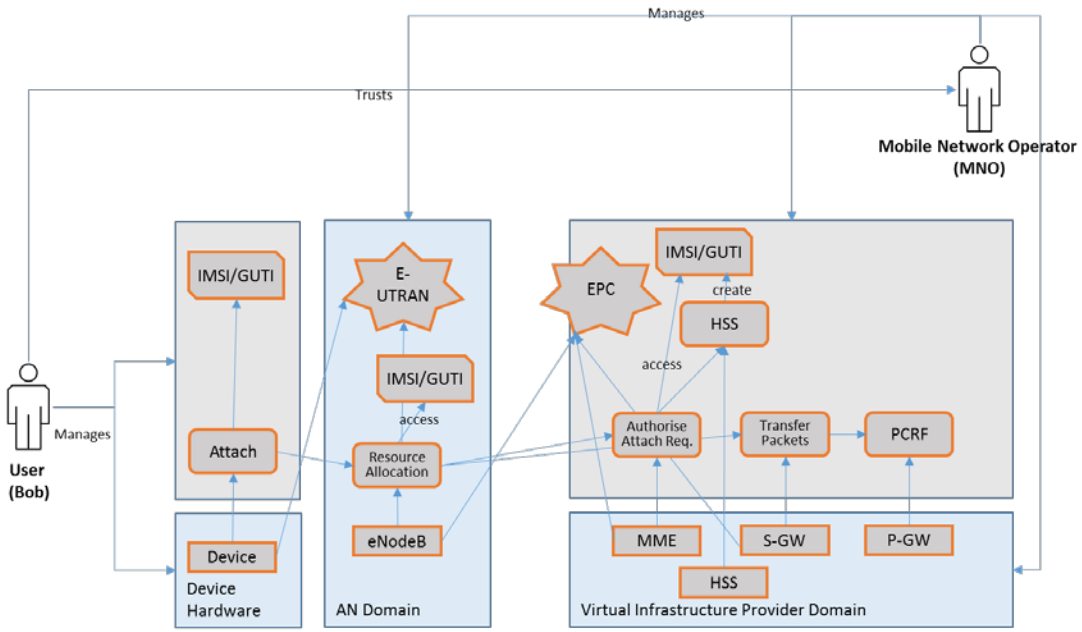

Figure A.69. Unprotected User Plane on Radio Interface (UC 6.2): sunny day scenario

The sunny day scenario shows a user, Bob, attaching his device to the mobile network operator's network via the access network. The device communicates with the eNodeB, where it negotiates what resources are to be allocated to it. This is done via the signalling protocols which in this scenario are integrity protected. Which means there is no way for an attacker to interfere with negotiations between the device and the eNodeB. Once the resources have been allocated by the eNodeB, the drive can complete the attach request with the operator. Again, this communication between eNodeB and MNO are integrity protected. From this

we can infer that the device owner trusts the network operator to enforce integrity of the signalling channel to maintain a secure connection.

A.18.2 Identified threats

A.18.2.1 Unprotected User Plane on Radio Interface (T_UC6.2_1)

Due to an attempt to conserve battery power of the device connecting to the network, the amount of signalling traffic is reduced. Which leaves an authenticated channel open to attackers. This results in the network being unable to verify the authenticity of data from the user plane. This is where Malory is able to intercept user data passing between the Device and the eNodeB. Providing they have the equipment, such as a software defined radio and are in a suitable physical location to target the user's device. They are able to exploit the fact that neither the device nor the eNodeB verify the data it receives.

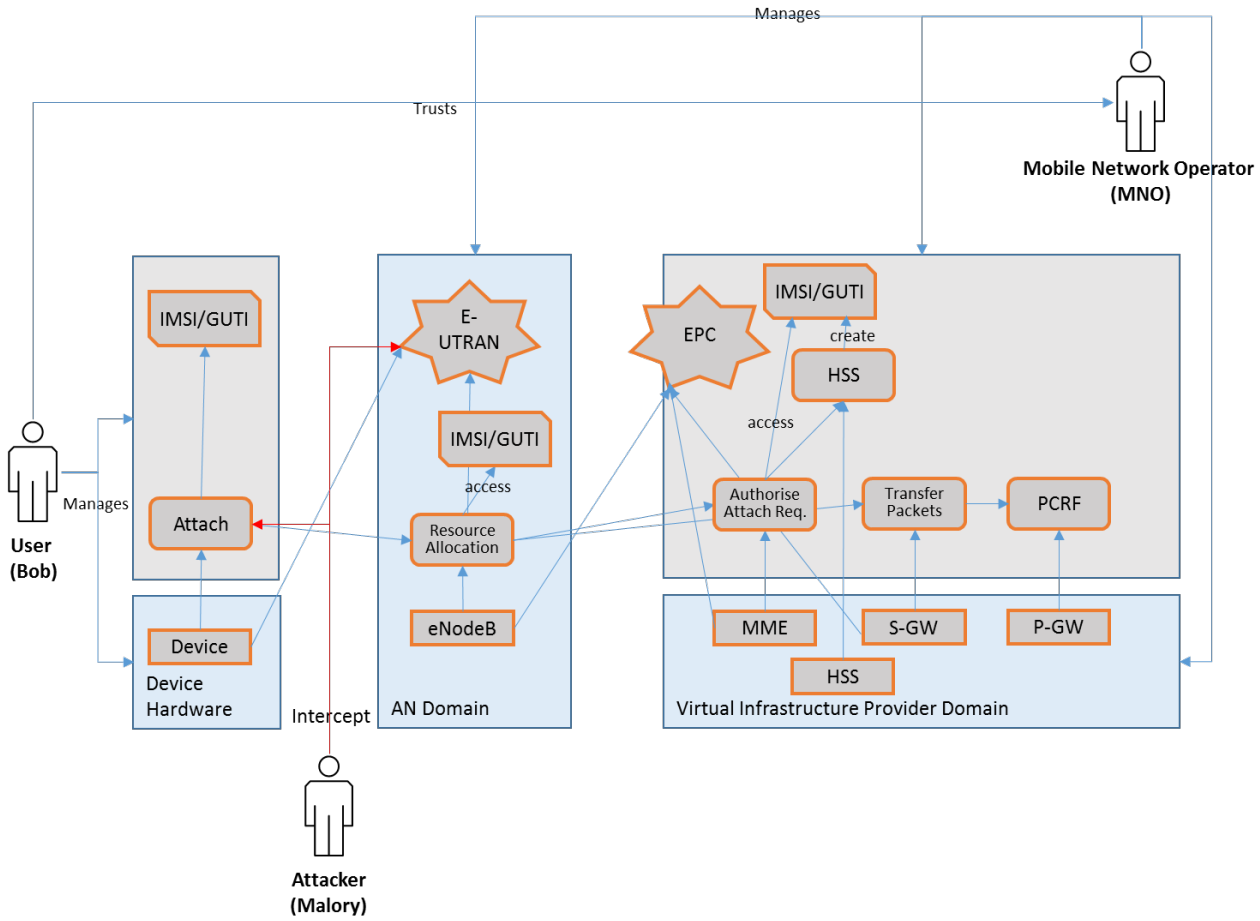

Figure A.70. Unprotected User Plane on Radio Interface (T_UC6.2_1) – 'rainy day'

Secondary effects of this threat is any data passing through the network can be intercepted, modified, and replayed. If traffic is intercepted then the threat is the privacy of the content is affected. This could result in espionage or divulging of classified information. If traffic is modified this would undermine the trust a user has with the network. It would also allow an attacker to control any system which may use the network. Replaying traffic which has been previously captured could allow an attacker access to parts of the network allowed for specific users, such as administrators or restricted accounts.

Trust implications

The User of the device trusts the MNO to operate a network which is not vulnerable to this kind of threat. If this is not possible then the user should attempt to use end to end encryption, which would place the trust on the sender and receiver of the communications. The user data plane is not encrypted because of regulations see TS33.401. The network operators may transfer responsibility of this risk over to the regulators under which they are bound by law to obey.

Threat mitigation strategy

To mitigate the threat in its entirety, the network operators will should implement similar protections for the traffic as they do for the signalling plane. This is, to force integrity checking on packets to insure that they originate from the user's device and not the attacker imposing as the user. This control would be placed on the eNodeB, at the access network. If that is not possible due to resource, then it could be placed on the edge of the EPC network provided by the MNO.

To mitigate data between two users being compromised from this threat, it is possible to use end to end encryption. This force all communication between the users to be encrypted in transport and only decrypted at the destination. This would be suitable for certain types of users, it would allow for the network operators to still obey the regulations they are restricted by.

A.19 Unprotected Mobility Management Exposes Network for Denial-of-Service (UC 7.1)

A.19.1 Use case description with architectural components

This use case describes a subscriber's device, phone or sensor, attaching to the 5G network. I details the method which a device connects and how it can be subverted by an attacker, and the device will fail to attach as expected.

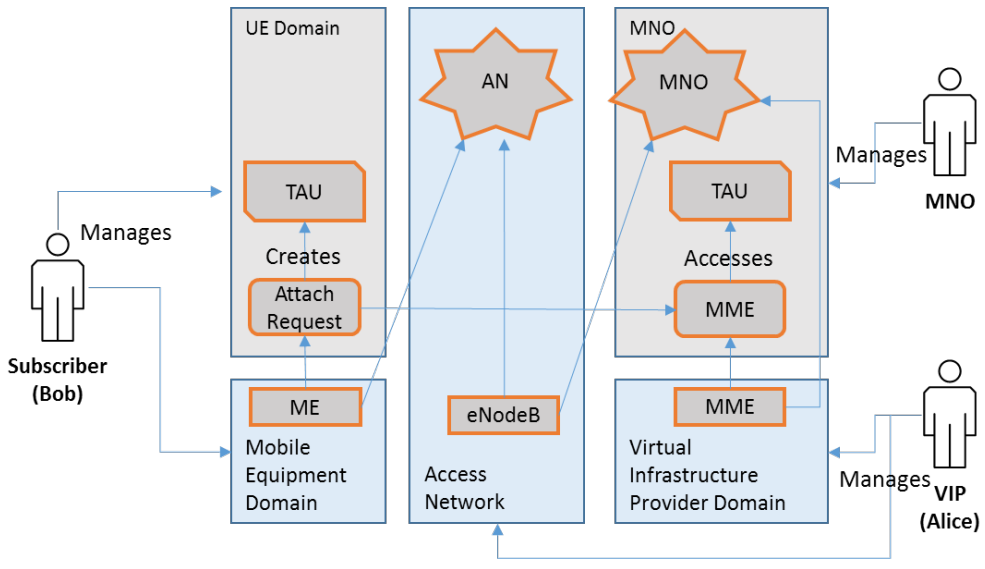

Figure A.71. Unprotected Mobility Management Exposes Network for Denial-of-Service (UC 7.1): sunny day scenario

From right to left, we have the mobile network operator (MNO) and virtual infrastructure provider (VIP). The VIP manages the access network and the infrastructure for the MNO. The MNO manages their internal network and provisions access to it for the subscriber, Bob. When the subscriber wishes to attach to the MNO, their device (UE) will send an attach request. Once connected the UE will send periodic tacking area

updates (TAU) to the MME, via the eNodeB. The subscriber is required to trust that the VIP will deliver their requests unaltered and without a reasonable amount of delay. Likewise, the MNO trusts the VIP is also relaying their communications to subscriber. The subscriber may not be aware of the existence of the VIP, but only the MNO, as that is who they have come to an agreement with. The MNO must trust the VIP will provide them with secure and robust infrastructure. The security implications of this configuration are the eNodeB and subscriber. Since by their nature have a large exposure to public access, and are both designed to work under emergency conditions. These conditions might require foregoing security measures to maintain resilience and availability. For example, if there was a failure of the encryption module in the eNodeB, unless it falls back to unencrypted methods, subscribers might not be able to communicate in an emergency.

A.19.2 Identified threats

A.19.2.1 Denial of service due to Unprotected Mobility Management Exposes Network (T_UC7.1_1)

The threat is from a malicious attacker, in Figure A.72 they are shown as Mallory. The root cause is due to the eNodeB being over powered with a stronger signal and the subscriber connecting to the Mallory service instead. Mallory intercepts the tracking area updates being sent from Bob to the MNO's MME. The intercepted TAU is modified before being relayed onto its original destination, the MME. The attacker can modify it so as to make the subscriber's device believe that the MME does not support certain services, and will downgrade to a service which Mallory wants.

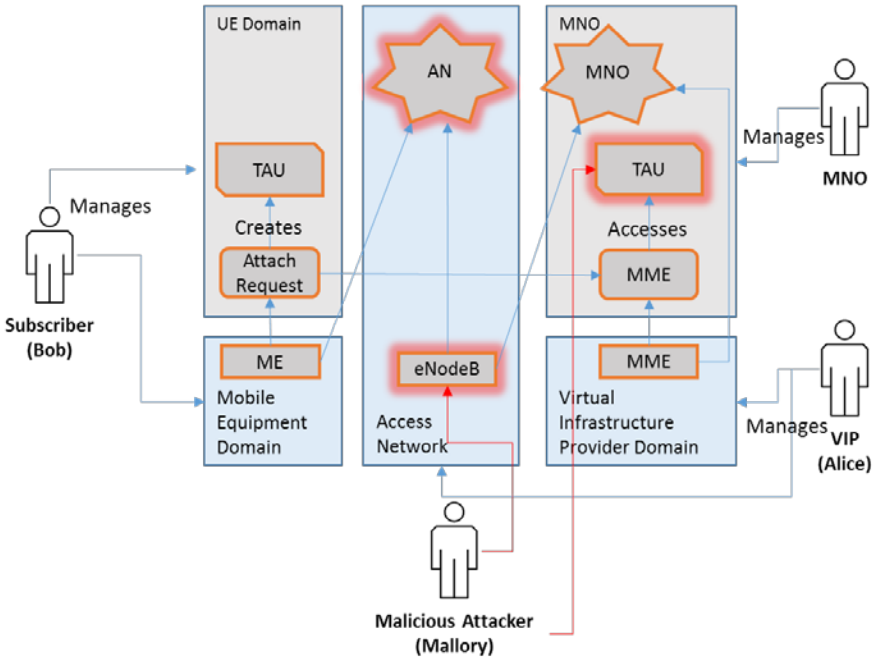

Figure A.72. Denial of service due to Unprotected Mobility Management Exposes Network (T_UC7.1_1) – 'rainy day'

The eNodeB is directly involved, as the attacker is able to convince the subscriber to connect by impersonating the eNodeB. This allows for Mallory to compromise communication between them and the MNO. Mallory would be able to perform not only a DoS for the subscriber but also intercept communications between them. By forcing Bob to communicate over an insecure method, using the same method as the DoS, Mallory would be able to eavesdrop on Bob's communication with the MNO.

Trust implications

- The MNO trusts that the VIP will secure their equipment and detect any anomalous changes which might happen, such as the rouge eNodeB attack.
- The Subscriber trusts that the MNO will not allow and will actively prevent his communications from being intercepted. If this loss of trust occurs then it could result in a complete loss of trust with the MNO.

A.20 Satellite Network Monitoring (UC 8.1)

A.20.1 Use case description with architectural components

The SNO mainly focus on tasks related to network monitoring and issues detection, are visualizing the satellite terminals status and throughput associated to network and spectrum resource utilization. Other network operators responsible are making the same work in different slices and sub-slices as Figure A.73 represents.

The SNO systems collecting different data indicator as network patterns use, authentication exchange schemes, to detect and mitigate the possible threats blocking the traffic or access at application layer for an Authentication Server with sensible information content.

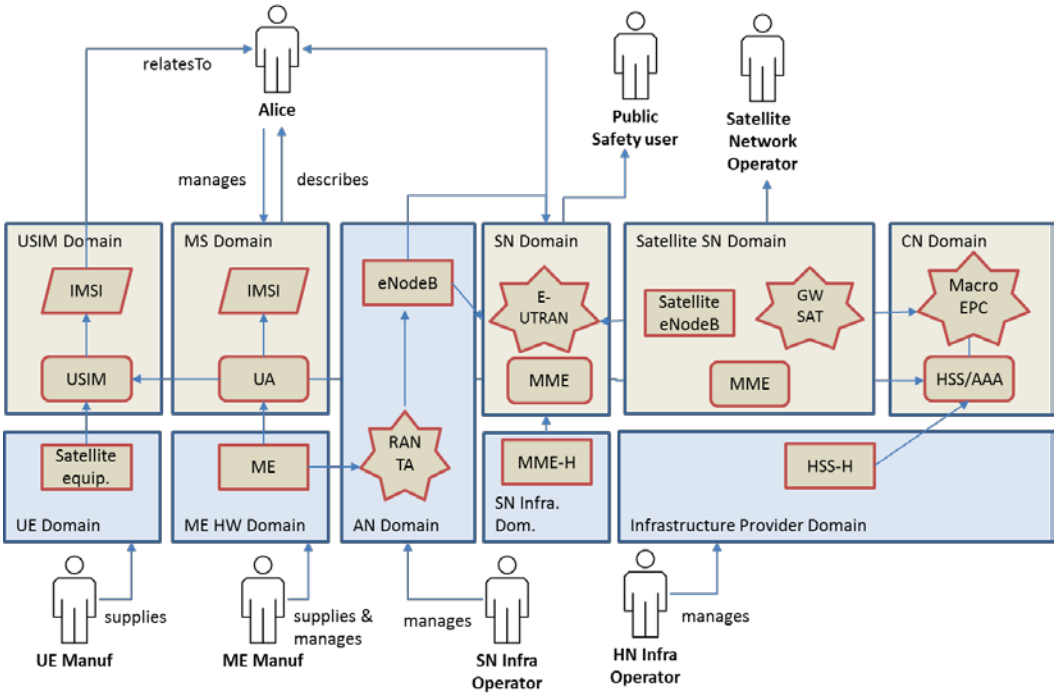

Figure A.73. Use case title (UC 8.1): sunny day scenario

A.20.2 Identified threats

A.20.2.1 Service failure over satellite capable eNB (T_UC8.1_1)

A Service Provider (i.e. telecommunications company) has a contract with the Satellite Network Operator (SatNO) to supply a suitable system capacity with some QoS guarantees to be used by its customers. Therefore, the Service Provider has to ensure that the SatNO is providing what is required by the contract (SLA).

This threat is particularly acute in ultra-reliable services (i.e. e-health, lifeline communications, and military scenarios).

In this case a natural disaster occurs and connection between Alice and eNodeB is lost, the network manager detects the failure event and proceed to performs topology calculation to guarantee ultra-reliable services. The new topology is configuration is populate across the network elements and the satellite-capable eNB activates the alternative route to Macro EPC via the satellite link. As a result the service lost is minimized and service restore is achieved.

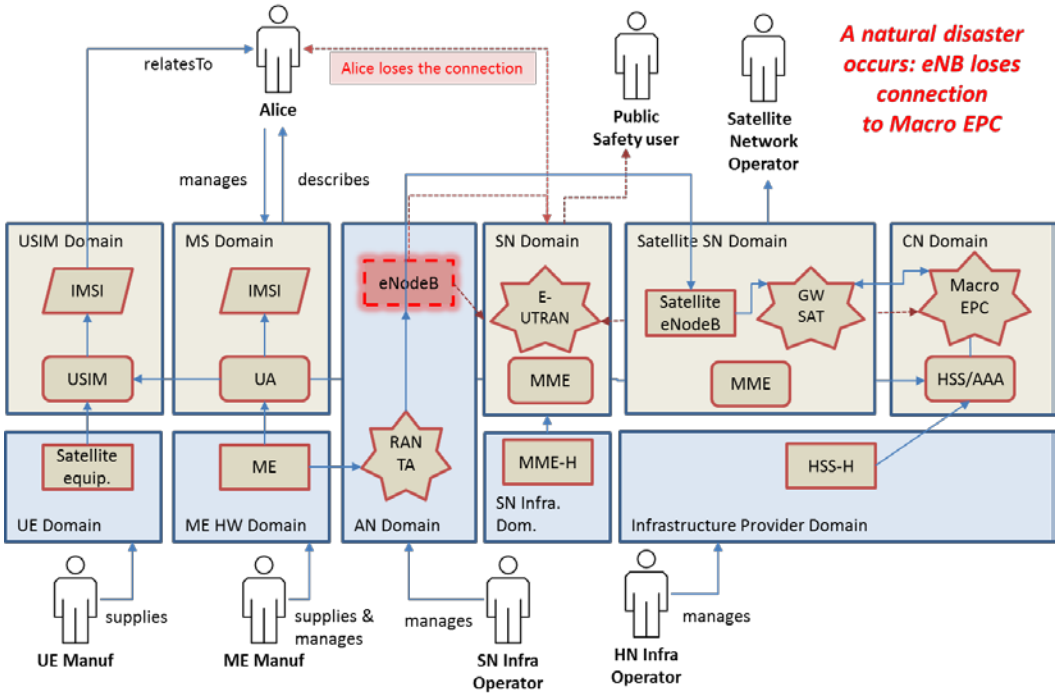

Figure A.74. Service failure over satellite capable eNB (T_UC8.1_1) – 'rainy day'

Main domains involved in this actions are shown in the Figure A.74, AN Domain cover the Radio Access network capabilities where traditional eNodeB are located, SN domain offers the connection between the Satellite SN Domain compose by Satellite eNodeB and GW Satellite shows the necessary components to provide satellite connections capabilities to the network increasing the recovery time and decreasing the service lost.

Without the mechanisms present, service lost time will be increasing, reliability of the system is decrease and mitigations actions are limited, presenting a potential point of failure in the network.

Trust implications

Potential Trust Implications:

- Customers can perceive a lack of trust based on the network availability and the capabilities for the VMNO to guarantee their service level agreements.
- The VMNO needs to demonstrate a trustable recovery actions regarding to guarantee the control over the VNO, offering detailed action plans that cover typical operations issues in sensible highly exposed locations.
- In this use case, the threat is not specially focus in an insider attack, but can be extrapolate from a service unavailability in the eNodeB as root case, actions and actor can be implemented in the same way from a trust implications perspective.

Threat mitigation strategy

Potential ways to mitigate this risk:

- Real time data gathering about network status and trends analysis can supply the foundations to accurate service lost detection.
- Establish clear action plans identifying critical elements and contentions actions as suggested in the rainy scenario can be key to mitigate the risks.

Generate pre-emptive configuration policies across the elements can decrease the reaction time and automatize the network recovery process, decreasing the SNO / VMNO actions and dependencies.

A.21 Standalone EPC (UC 8.2)

A.21.1 Use case description with architectural components

This use case concerns standalone-capable eNBs that have the capability of standalone mode of operation, which provides commercial local IP connectivity to the UEs via a Standalone EPC. This is assumed to be a commercial service, and connection to the Macro EPC is still possible.

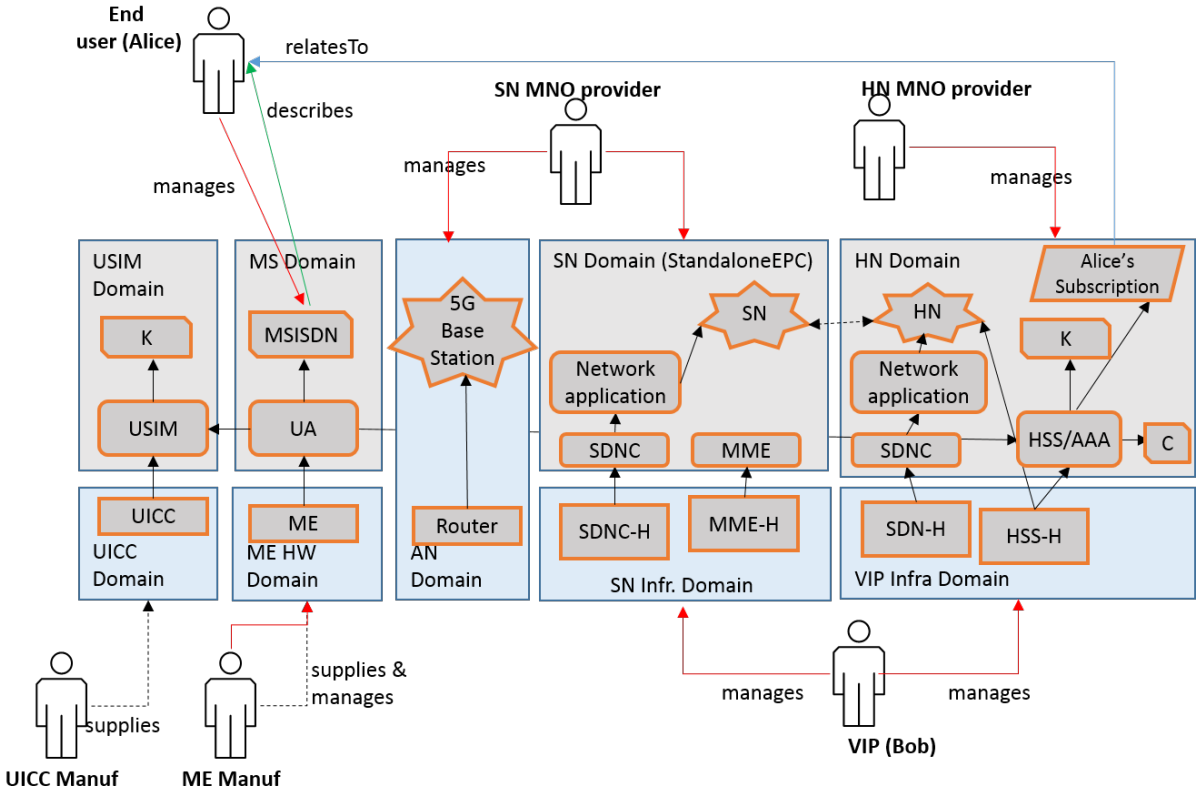

Figure A.75. Standalone EPC (UC 8.2): sunny day scenario

Figure A.75 shows this scenario in relation to the architecture, in the absence of any threat (the sunny day scenario). Alice is in a mega event with 100.000 other people. She wants to use the services that are available in the standalone EPC. When the mega event starts, the standalone-capable eNB starts to broadcast support of the ad-hoc roaming mode to the local EPC. Alice's phone attaches to the standalone-capable eNB of the standalone EPC. The standalone EPC authenticates Alice's USIM with the help of the HN. Alice's HN authorizes the ad-hoc roaming to the standalone EPC by sending Alice's subscription profile to standalone EPC. Alice's

phone does not lose the connection to the HN as the standalone EPC provides also connectivity to the HN. Alice uses the services in the standalone EPC, and also uses the services in the HN.

A.21.2 Identified threats

A.21.2.1 Standalone EPC loses connection to the Home Network (T_UC8.2_1)

The standalone-EPC-capable eNodeB fails to communicate to the subscriber's home network. This can be caused in a variety of ways, denial of service, system/hardware failure, or due to overloaded resources. By its nature this threat is can be exploited by a malicious attacker or an unintentional series of events. The crux of the threat is that some way the connection from the eNodeB to the Home Network will be disrupted, resulting in clients being unable to authenticate.

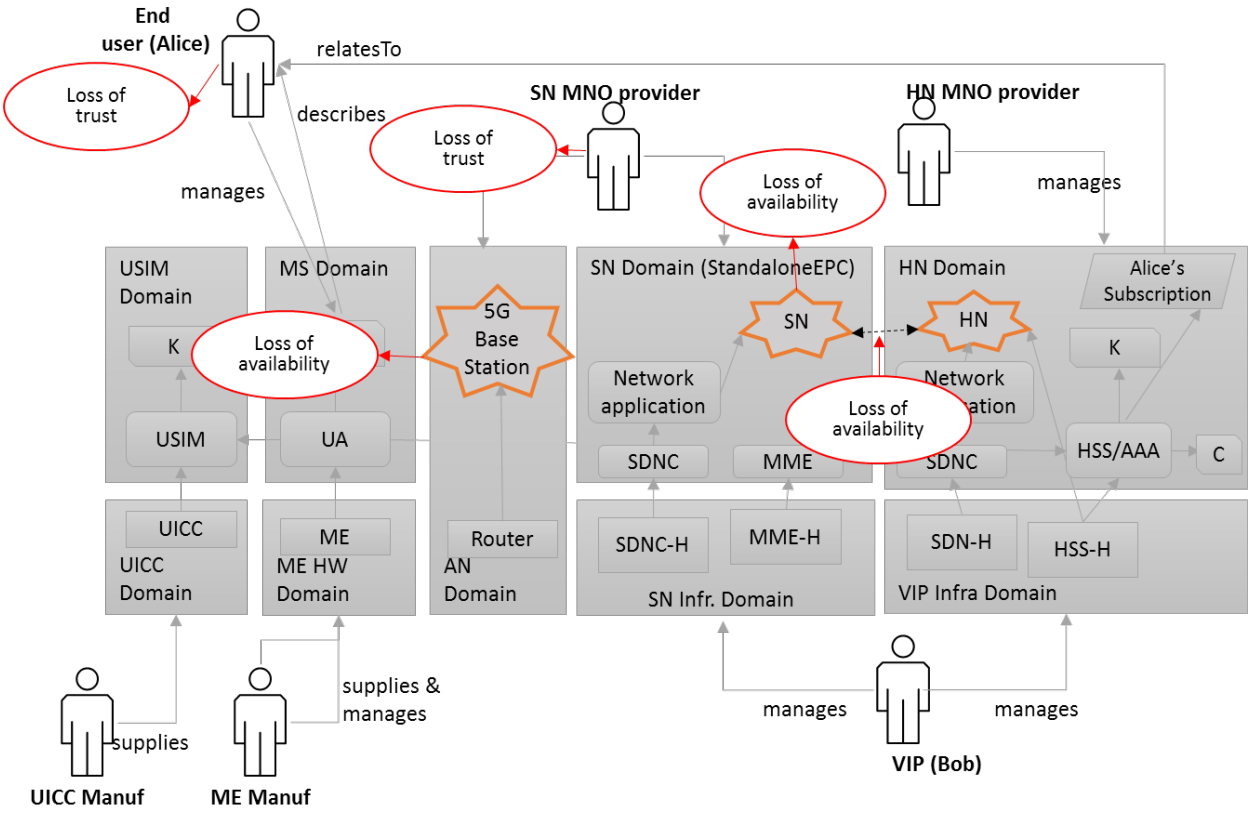

Figure A.76. Standalone EPC loses connection to the Home Network (T_UC8.2_1) – 'rainy day'

The threat is the loss of connectivity between the serving network and the home network, this could be caused maliciously, or by a misconfiguration. Typically it would be caused by an overload in capacity of the hardware used to communicate with the HN. In this case the standalone EPC.

Secondary effects are such that devices looking to authenticate with the network are denied authentication and will be unable to communicate with any other devices, unless it is possible to communicate with their peers. With the eNodeB unable to communicate with the Home Network, it prevents other clients, which might not be using the isolated EPC service, from working.

Trust implications

Potential Trust Implications:

- The end users of the network, will loss trust with their VMNO, who is meant to provide them with access to the EPC. This is also not limited to a single virtual mobile network operator, due the physical eNodeB being unavailable.
- The HN MNO will lose trust with the SN MNO, since they are the ones who are maintaining the eNodeB. And are bound by contract to allow other operator's customers to use their equipment.

Since the eNodeB is shared by range of operators and the use of which is provisioned by a virtual infrastructure provider (VIP), when the eNodeB is unavailable there.

A.22 Alternative Roaming in 5G (UC 9.1)

A.22.1 Use case description with architectural components

Legacy mobile networks (GSM, UMTS, LTE) use an interconnect network based on SS7 or Diameter. In such an interconnect network, network entities often rely on the assumption that the traffic originating from a certain network is authentic, without having any way of checking this assumption. Unfortunately, this assumption is not always true in today's heterogeneous landscape of networks. This has led to a variety of attacks on the interconnect network based on spoofing of messages. In this use case, messages are instead bound to the correct entities, so that spoofing cannot take place.

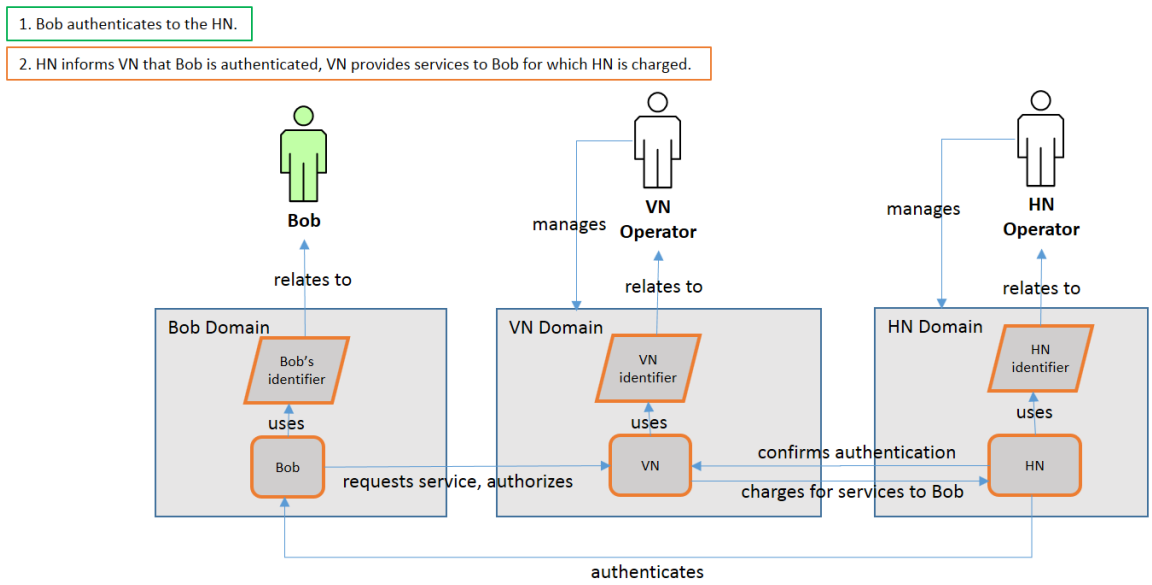

Figure A.77. Alternative Roaming in 5G (UC 9.1): sunny day scenario

Figure A.77 describes the use case in relation to the architecture, in the absence of any threat (sunny day scenario). The home network and the visited network have a roaming agreement. Bob needs the assistance of the home AAA infrastructure to authenticate himself to the visited network. The Home AAA issues the authentication challenge. This process also identifies both the visited network and the home network, so that the involved parties are identified. During this process, Bob also authorizes the visited network to provide services to him.

At the same time, accounting mechanisms are set up. The home network can therefore have assurance that any billing related information is tied to Bob. Thus, the visited network cannot make false claims. Similarly, Bob's false claims can be denied based on assured accounting information. Bob's device is involved in the process, so that there is transparency of the incurred costs to Bob as well.

A.22.2 Identified threats

A.22.2.1 Spoofed signalling messages (T_UC9.1_1)

If the authenticity of the messages related to the user cannot be verified, the integrity of the actions cannot be ensured. The actions can cause effects which lead to further compromises or have other unwanted consequences.

In Figure A.78, the threat is explained in relation to the architecture. Mallory impersonates the visited network and takes actions that were not authorized by the user. This could relate to billing (customer gets extra charges that were not caused by them) or it could cause messages (such as SMS) redirected to somewhere else (potentially leaking information). Alternatively, Mallory could spoof management messages which change the infrastructure, potentially in a devastating way. There are different ways how Mallory could impersonate the visited network: insider attacks, hacking into the visited network's interconnect access, or simply by buying access to the interconnect from a network provider.

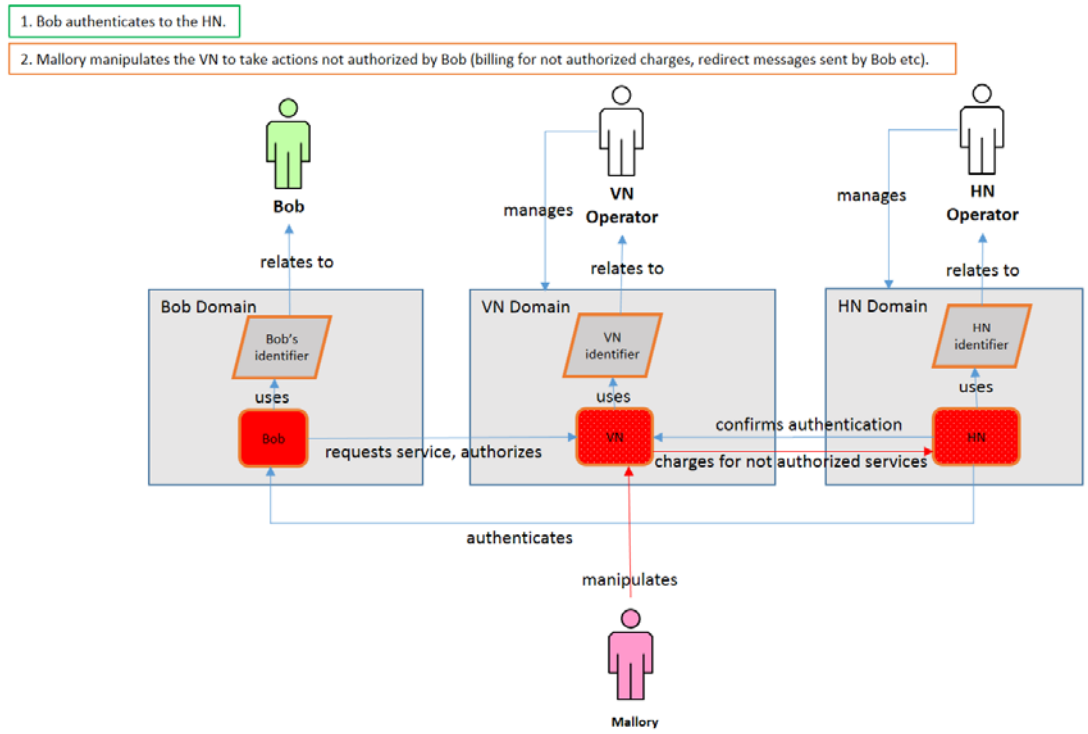

Figure A.78. Spoofed signalling messages (T_UC9.1_1) – 'rainy day'

Trust implications

This threat is based on an outdated trust model between network operators. As said in the description of the use case (Use Case 9.1), in today's heterogeneous landscape of network operators the authenticity of a message cannot be guaranteed even if it originates from a trusted roaming partner, because not all trusted roaming partners may be trustworthy.

Besides mutual trust between network operators, the threat has strong implications on the trust of users to network operators in general and especially their home network operator. The user has no way to prevent non-authorized actions on their behalf, such as intercepting messages sent to the user, impersonating the user and originating charging records on behalf of the user.

Threat mitigation strategy

All signalling messages should be integrity protected and bound to the correct entities. Using cryptographic identities for all entities (networks and users) would be one possible solution. Additionally, authorization methods need to be in place, both from the entity that sends the message but also from the entity that receives the message and needs to ensure that the sender is authorized to perform a certain action.

A.22.2.2 Disputes in charging (T_UC9.1_2)

This threat is a special case of T_UC9.1_1 above. A user could dispute charges or an attacker on behalf of an operator could place unfounded charges on the user actions. Basically, an attacker impersonating the operator can produce billing records, but the customer has no way of proving whether they are correct or not.

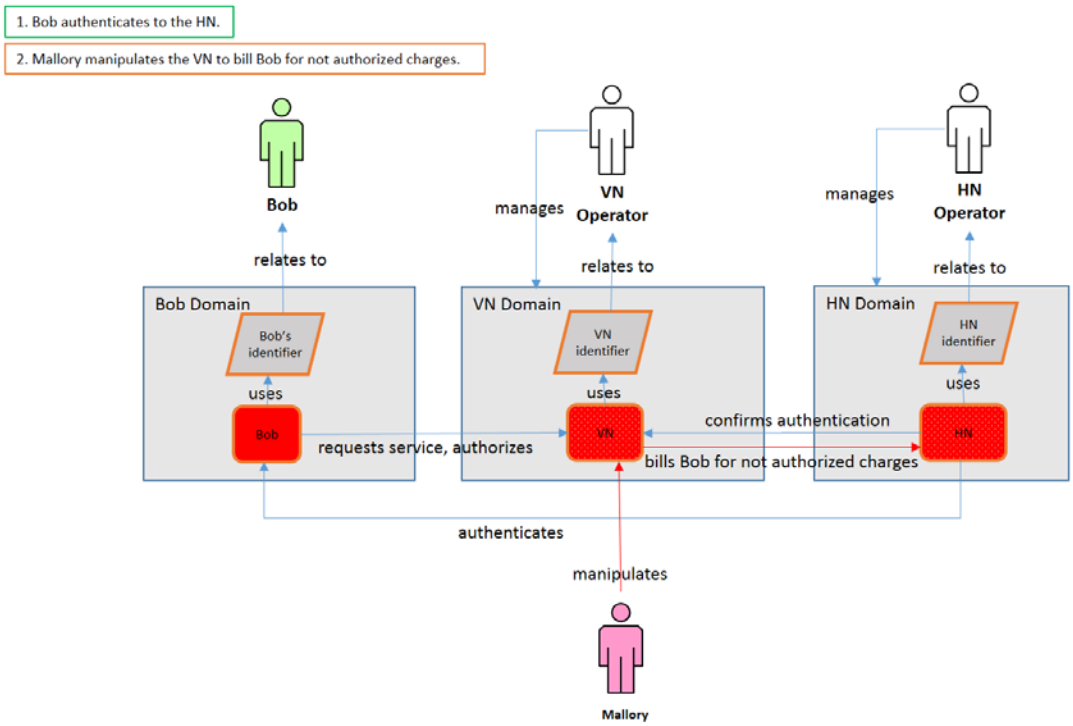

Figure A.79. Disputes in charging (T_UC9.1_2) – 'rainy day'

In Figure A.79, the threat is explained in relation to the architecture. Mallory impersonates the visited network and creates charging records not authorized by the user. As explained for the T_UC9.1_1 above, there are different ways for Mallory to impersonate the visited network.

Trust implications

This threat has mostly implications on the trust between user and home network operator. Users have no way to prove they have not originated the charging records, and the network has no way to check whether the user has originated the charging records.

Furthermore, this threat also has implications on the trust between network operators. A home network may realize that a trusted roaming partner was indeed not trustworthy.

Threat mitigation strategy

The charging related messages should have non-repudiation properties. Cryptographic identities could be one possible approach of creating records that are always strongly bound to the entity and cannot be disputed afterwards.

A.22.2.3 Disclose of sensitive data (T_UC9.1_3)

A request for sensitive information (such as authorization vectors) may come from non-trustworthy sources although they are received through a trusted channel. Obtaining sensitive information in unauthorized fashion could lead to further compromise of the network and possibly make it easier to spoof other entities.

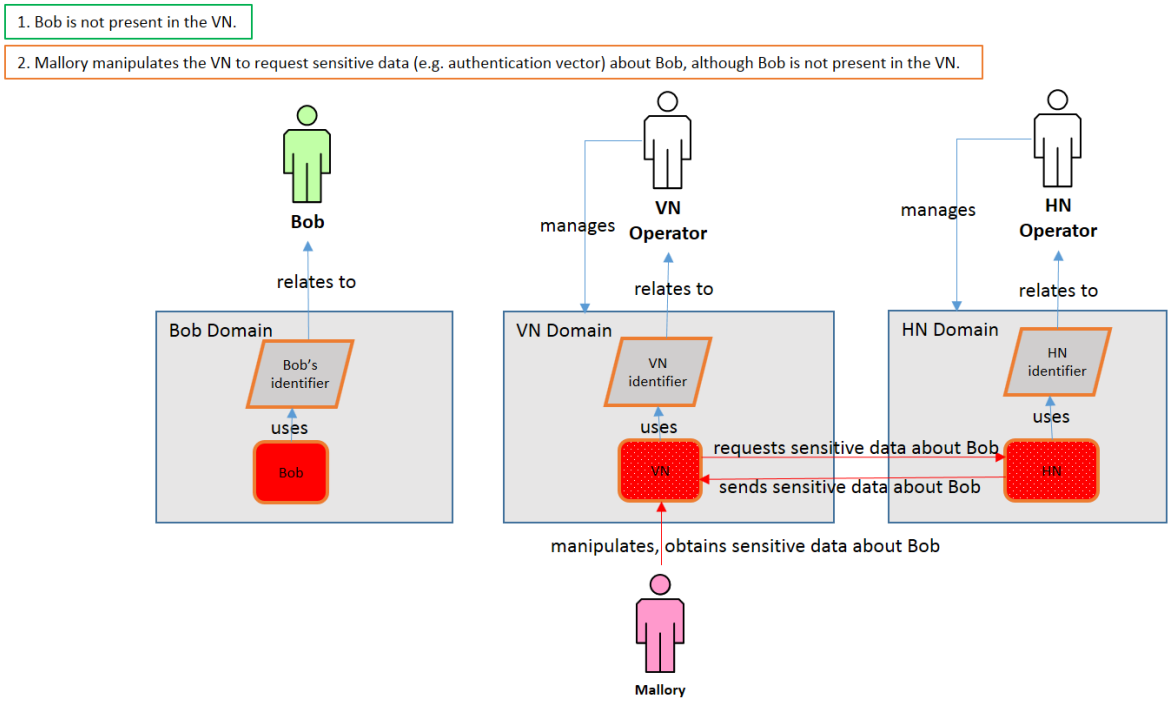

Figure A.80. Disclose of sensitive data (T_UC9.1_3) – 'rainy day'

In Figure A.80, the threat is explained in relation to the architecture. Mallory impersonates the visited network and manipulates the visited network to request sensitive data (e.g. authorization vectors) about Bob from the home network. Bob is not present in the visited network. Nevertheless, the home network sends the sensitive data to the visited network, and hence Mallory is able to obtain the sensitive data about Bob.

Trust implications

Similar as for the T_UC9.1_1 and T_UC9.1_2 above, this threat has implications for the mutual trust between operators as well as for the trust of users towards their home network operator and network operators in general.

Threat mitigation strategy

Similar as for the T_UC9.1_1 and T_UC9.1_2 above, the mitigation strategy should focus on providing authentication and authorization to the interconnect network.

A.23 Privacy in Context-Aware Services (UC 9.2)

A.23.1 Use case description with architectural components

The use case concerns the exchange of user context with third parties. User context can be used to provide enriched services to the user or otherwise communicate about his or her characteristics for the sake of network management in terms of flow semantics. This could especially take place in a roaming scenario, where the visited network and home network exchange information about the user. The user still needs to be in control of this disclosure of information so that the privacy of the user is not violated. Therefore, the users should be able to dictate the privacy policies to which they are willing to agree.

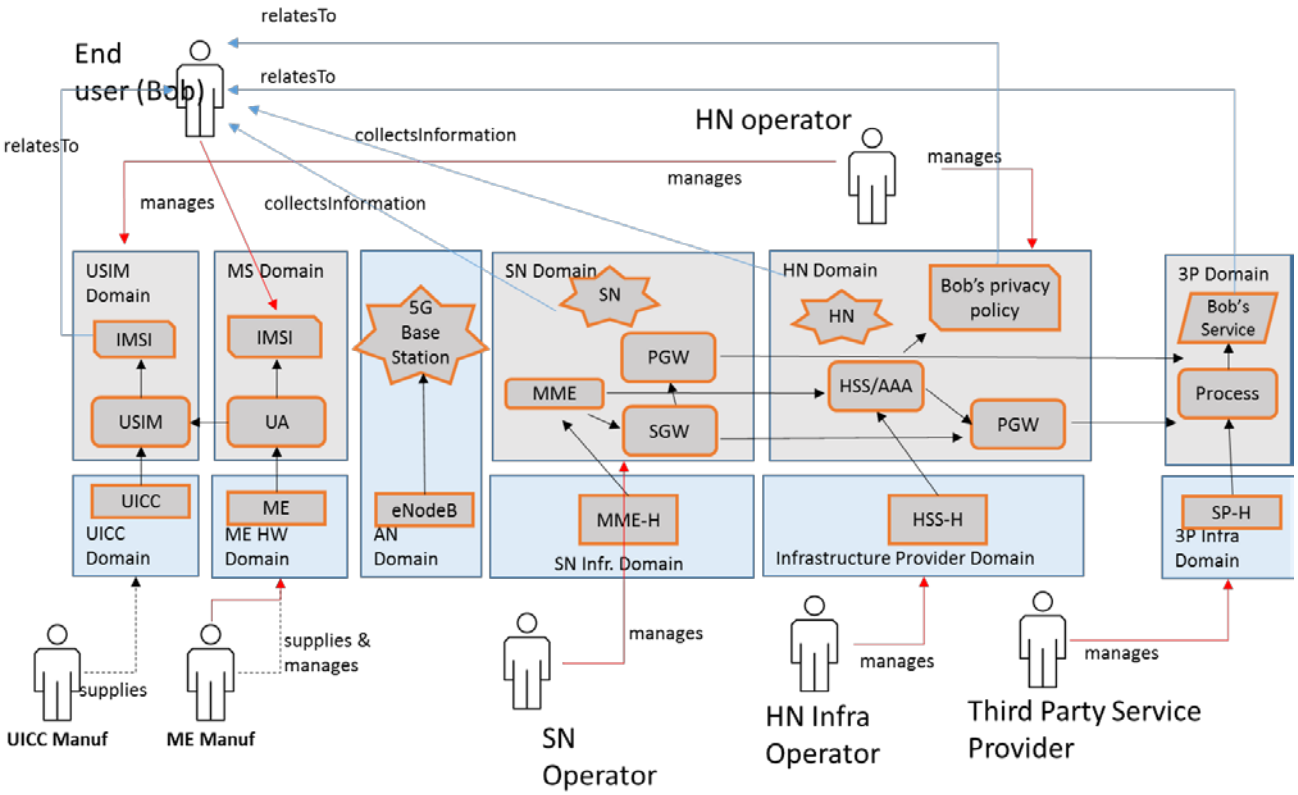

Figure A.81. Privacy in Context-Aware Services (UC 9.2): sunny day scenario

In the simplest case the exchange of flow semantics information takes place within the network or between the visited and home network to communicate about the user context. This information generally does not need to reach service providers. A more evolved use case is the case where user context information (in terms of network perspective) is disclosed to an external service provider in order to provide better user experience or evolved services. This disclosure takes place according to the privacy policies the user has defined. This could also be predefined by the home operator, but the user has to explicitly agree to it. The user trusts that the home operator does not violate these policies. In addition, the user expects that the home operator has appropriate filtering mechanisms in place to ensure that no network internal information is not disclosed accidentally (e.g., header enrichment mechanisms used between the visited and home operator). The previous also has to apply to visited networks that provide local breakout, i.e., data to third parties does not traverse via home network.

Note that the application level end-to-end communication can be encrypted, so the operator cannot provide any added value to the context, at least not in-band. This is not in the scope of this use case.

A.23.2 Identified threats

A.23.2.1 User privacy policies are not respected (T_UC9.2_1)

Privacy of the user in this use case can be endangered by the operator that does not respect the privacy policy of the user. This could relate to business decision (e.g., contracts with third party advertisers) or be just lack of proper filtering (e.g., misconfiguration of egress filtering).

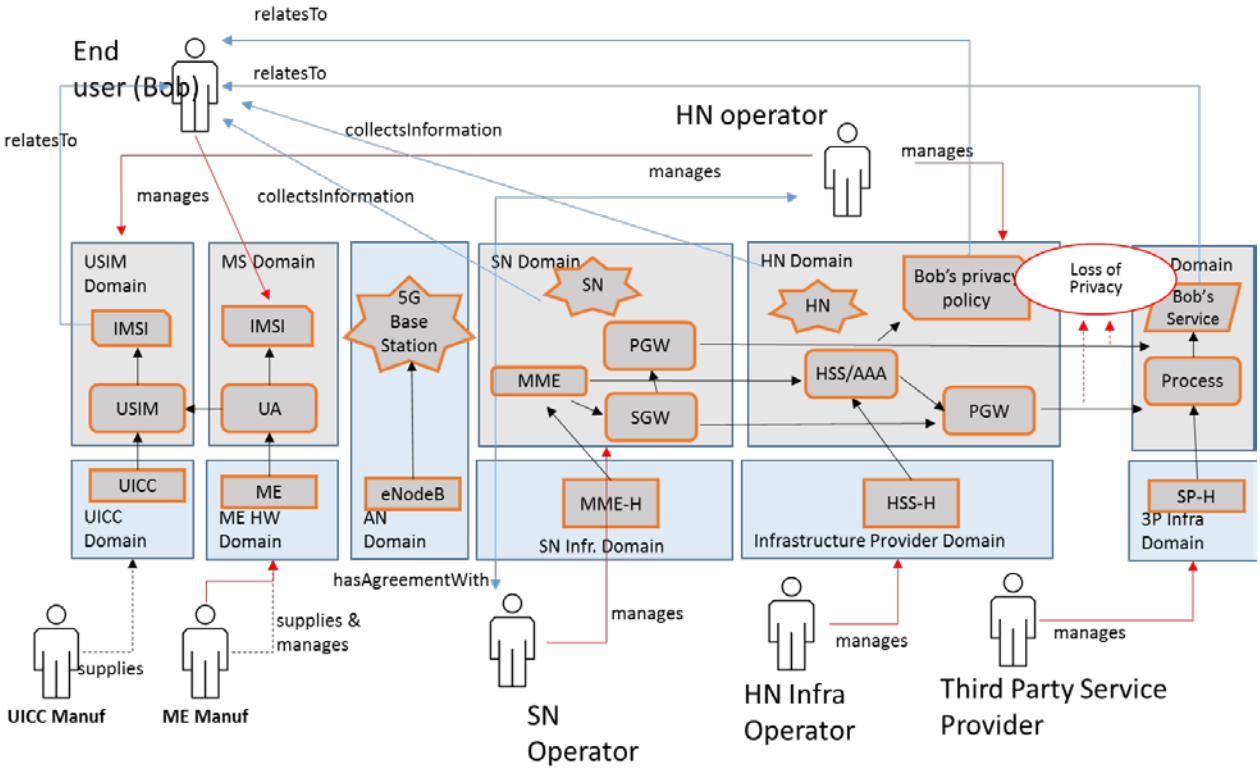

Figure A.82. User privacy policies are not respected (T_UC9.2_1) – 'rainy day'

The figure above describes the issue in terms of architectural components. While the egress components in the final 5G architecture might be termed differently, they most likely will be called gateways (e.g., BGW as currently). If they do not filter the traffic properly, privacy breach is possible. Naturally, it could be that those components intentionally do not do filtering or add additional context information to the flow of information to serve the interests of third party partners, with whom the operator might have a business agreement. This might not serve the interests of the user.

It is also possible that the third party service provider further discloses information about the user. However, the service in question ought to in any case have a separate privacy policy for dealing with the user and that is outside the scope of 5G system.

Trust implications

The outcome of above could be that the overall trust of the user to the 5G system or to the operator very least decreases. Naturally, there could be legal (and therefore societal) implications if it is found out that the privacy related information is disclosed in violation of the user's privacy policy. Another thing is if the user has agreed to too relaxed privacy policy, often inadvertently. Regulatory schemes might expect certain basic level of user protection to be in place, though.

In the use case the user trusts that the privacy policy is honoured. As the user has an agreement with the home operator, he or she expects that the home operator takes care of this. On the other hand, if visited network can do local breakout in the roaming scenario, then the home operator expects that the user's privacy policies are still followed. In other words, home operator places certain amount of trust to the visited operator. It is worth noting that the user generally does not have an agreement with the visited network (unless some dynamic roaming agreement mechanisms are introduced as suggested in the alternative roaming use case).

Breach of this trust can take place if the home or visited network does not adhere to these policies. It can either happen inadvertently or on purpose. It is also worth noting that the home and visited operators could be operating under different privacy legislation.

Threat mitigation strategy

As the network originated context information can be collected by the network, the user can do very little to mitigate the threat, i.e., the operators control the way infrastructure works. If the home operator cannot trust the visited operator to employ sufficient privacy protection, then local breakout should not be allowed. Regulatory schemes can be used to protect the user in these cases. For ensuring that regulatory controls are followed, external audit of the system could be used.

For improving the transparency of privacy policies to the users the 5G enabler "Privacy policy analysis" could be used. This could help users better understand what sort of privacy policies the operator offers and whether that matches their needs.

A.24 Authentication of new network elements (UC 9.3)

A.24.1 Use case description with architectural elements

The use case deals with cases where it is possible to install new elements into the network. This could be logical components, such as virtual network functions, or physical devices. These components need to be authentic so that rogue elements are not introduced into the network.

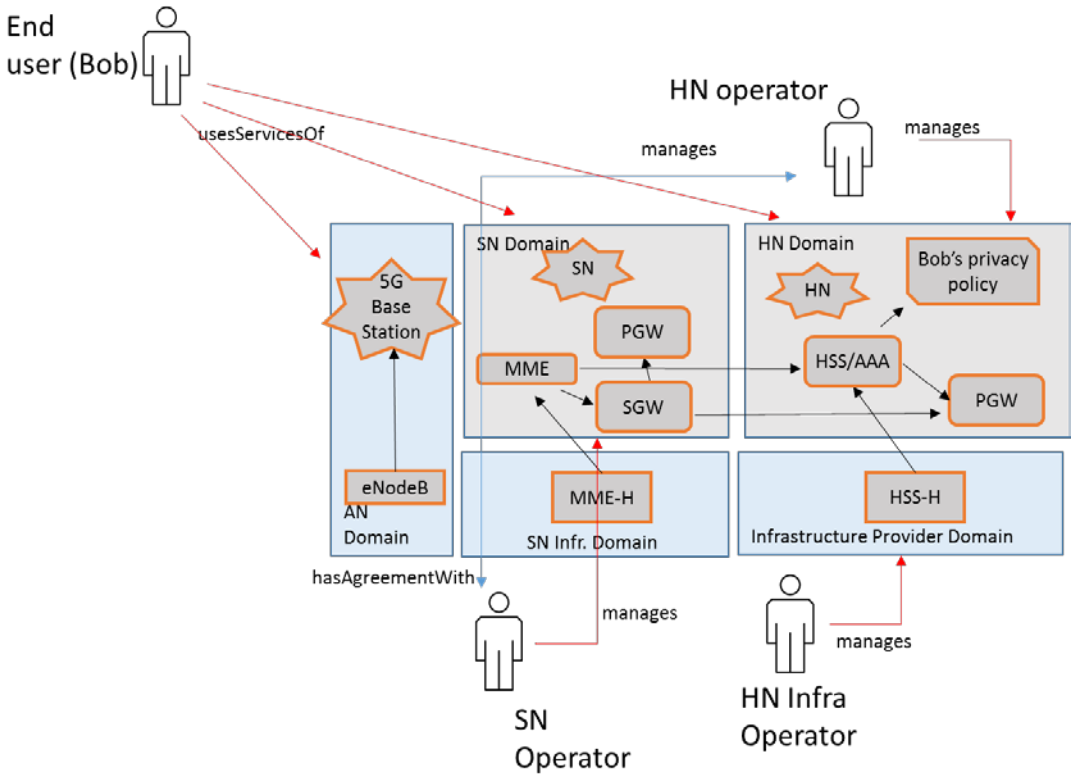

Figure A.83. Authentication of new network elements (UC 9.3): sunny day

In the "sunny day" scenario the installation of new network elements can be made only by authorized parties and with guarantees that these new elements cannot endanger the integrity of the network or network flows. In other words, they cannot compromise other elements in the same network or inject traffic that could be considered authentic by other entities. In essence, it is not possible to spoof other elements or other users.

A.24.2 Identified threats

A.24.2.1 Hardening or patching of systems is not done (T_UC9.3_1)

If the systems in the networks are not hardened sufficiently or do not contain the latest security patches, it is possible that they can be compromised. This could lead to installation of new functionality, which performs malicious actions in the network, or the current functionality could be subverted to perform undesirable results. Especially in the 5G environment it is envisaged that it is possible to install new virtual network functions to enhance the working of the network. This could be especially detrimental if this can be done in unauthentic fashion (e.g., due to misconfiguration or a vulnerability in the system).

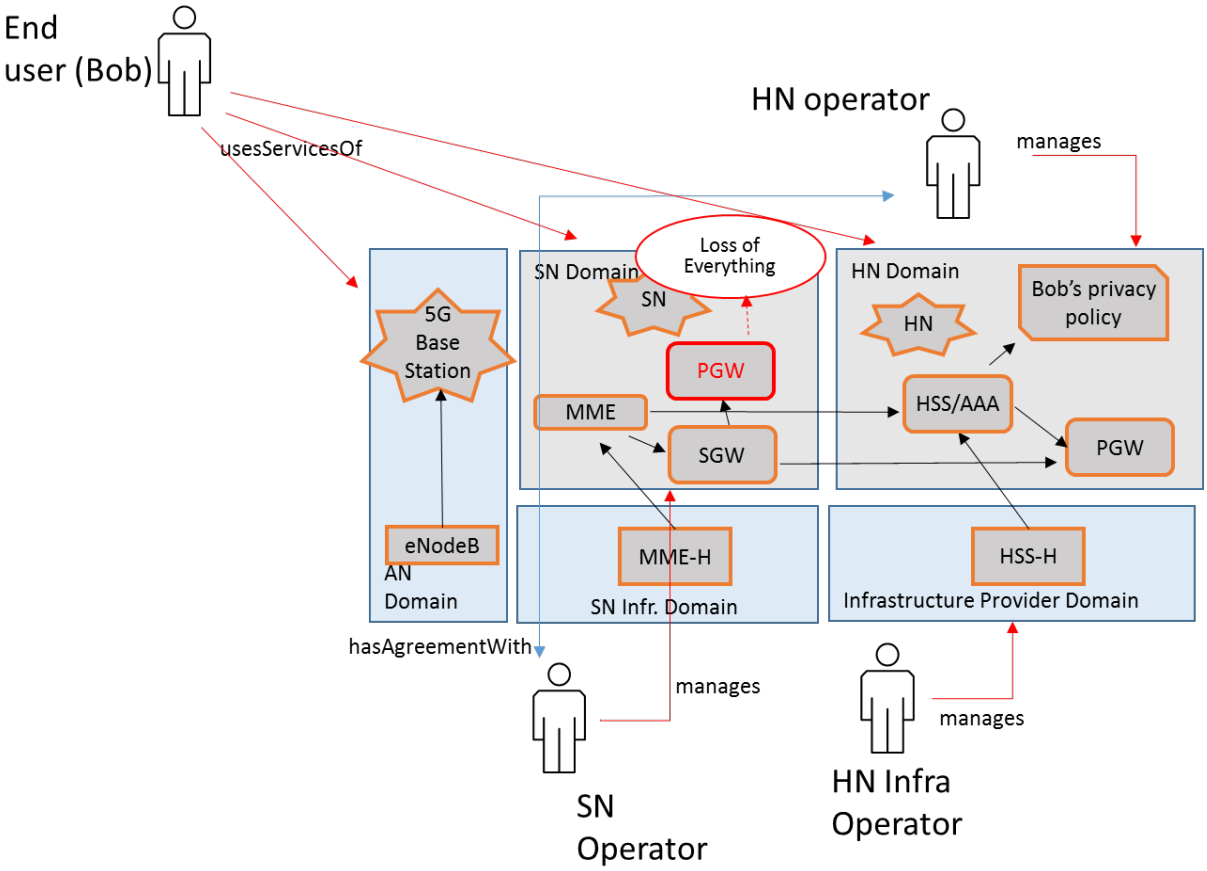

Figure A.84. Hardening or patching of systems is not done (T_UC9.3_1): rainy day

While the above diagram portrays that one specific network element is compromised (shown in red), the compromise could happen with any element that is not sufficiently hardened. This compromise basically renders the component untrusted in every way and the component can be used to launch attacks against other elements. The components that expose external interfaces are at most risk, but the risk could materialize through other vectors as well. For instance, poorly managed maintenance system of the operator could be compromised first and then the attack could pivot to the "inner" elements.

Trust implications

If a system is subverted, one no longer can rely on integrity of it. Any action that is performed by that system can lead to various adverse effects, e.g., additional malicious traffic could be generated and further compromise of other systems could be attempted. In essence, the whole network could end up being untrusted.

In the roaming scenarios, the compromise of the visited network leads to the fact that the traffic coming from the other operator to the home operator cannot be trusted and making decisions based on that (e.g., billing) could result in further problems in terms of liability.

Threat mitigation strategy

Systems should be properly maintained by introducing vulnerability management processes. The configuration management should ensure that the systems are consistently hardened and systems have most

up-to-date security patches installed. This is even more important with 5G systems, as there are going to be more software components present through virtualization.

Monitoring of systems can help in detecting breaches. This can potentially be cooperative actions between different operators, so that indicators of compromise are reported to the operator of the source traffic. Proper segmentation of systems can isolate the breach to only one system. Thus, other systems should be considered potentially hostile instead of implicitly trusting devices just based on their network location.

A new VNF that is introduced into the network could also introduce vulnerabilities. The enabler "VNF Certification" could help mitigate this risk, if through it a certain level of assurance with regard the security posture of a VNF can be gained. In other words, there has been a pre-evaluation of the security of the component before it is approved to be installed into the network.

Additionally, the monitoring enablers ("System Security State Repository", "Security Monitor for 5G Micro-Segments", "Generic Collector Interface", "PulSAR") and the virtualization isolation enablers ("Access Control Mechanisms", "Component-Interaction Audits", "Bootstrapping Trust", "Micro Segmentation") help in detecting potential integrity problems and limiting the amount of damage a subverted component can cause.

A.24.2.2 Unauthentic device installed into the system (T_UC9.3_2)

If the physical security is lax, then it might be possible to install an unauthorized device into the network environment of the operator. This could be an act of malicious insider, but equally it could be performed by an external actor, who manages to get access to the physical infrastructure, e.g., by posing as a maintenance personnel. Unauthentic device could send traffic to the network and pose to be an authentic entity. This could lead to various man-in-the-middle or spoofing attacks. Additional attacks could be also performed against other system elements as well (see previous threat).

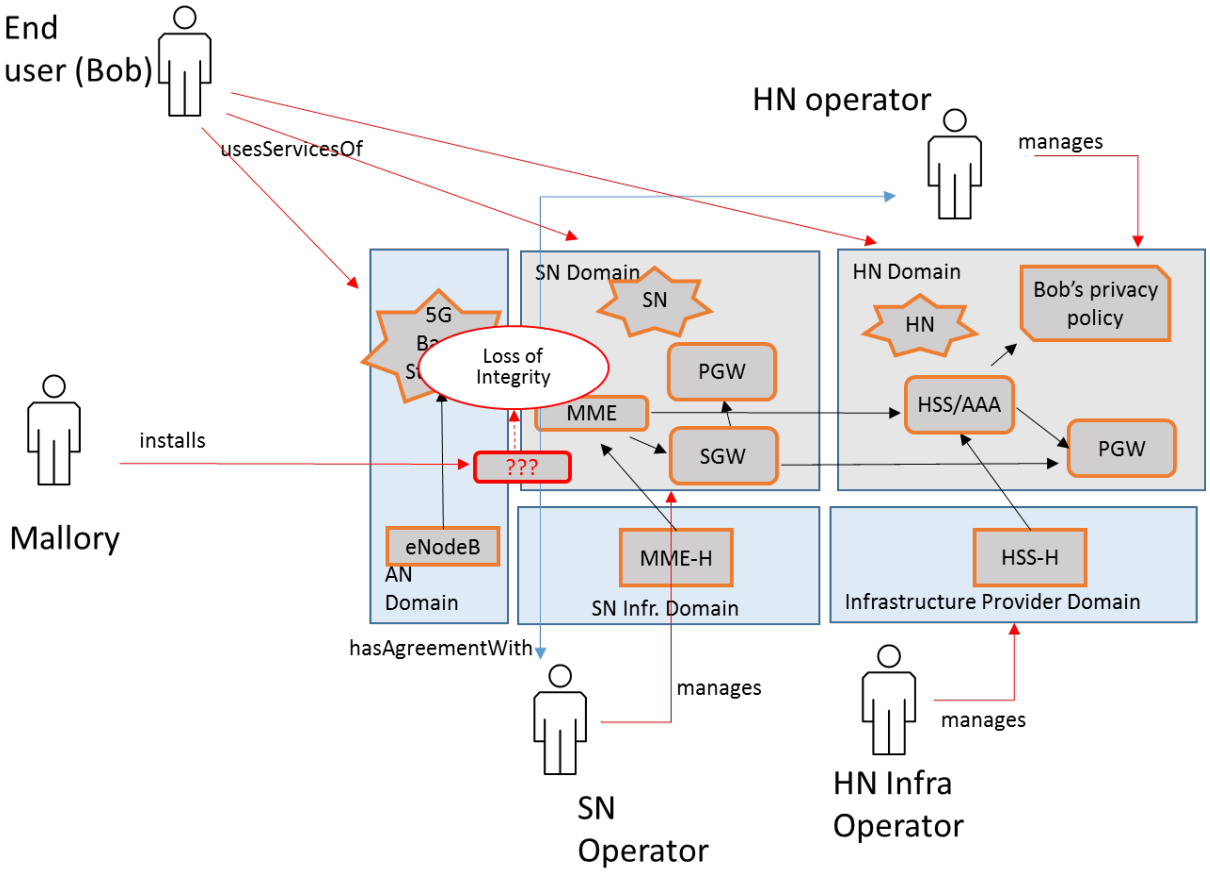

Figure A.85. Unauthentic device installed into the system (T_UC9.3_2): rainy day

Trust implications

If the trust is based on the network location of elements, then it can be possible to misuse that trust as traffic coming from certain interface can be deemed authentic. For instance, if there are no other authentication elements in the information flow, data received from another, hacked operator could be interpreted to be legitimate. This could lead to the situation where, for instance, a user is incurred additional costs for the traffic that does originate from the actions of that user.

Threat mitigation strategy

Monitoring of the systems can help in detecting breaches. Also, if only authentic elements are allowed to connect to the system, them it is harder to install physical elements into the networks. For instance, the network ports that are not in use are not enabled. The new elements should first authenticate themselves before allowing them to communicate with the rest of the network.

It is worth noting that in 5G the infrastructure elements might reside in "normal" data centers as the functions might be running in more commodity hardware. One ought to be aware that the level of physical security might not be in the same level as current telecom data centers. Regulatory schemes should ensure that the physical security is taken care of in such locations as well.

The monitoring enablers ("System Security State Repository", "Security Monitor for 5G Micro-Segments", "Generic Collector Interface", "PulSAR") and the virtualization isolation enablers ("Access Control

Mechanisms", "Component-Interaction Audits", "Bootstrapping Trust", "Micro Segmentation") help in detecting unauthentic components and limiting the amount of additional damage they can cause.

A.25 Botnet mitigation (UC 10.1)

A.25.1 Use case description with architectural components

A botnet is a network of hijacked agents/clients which are remotely controlled, often associated with introducing malicious software. Botnet infrastructure is increasingly being used for performing criminal activity that involves the use of computers or networks such as the Internet. Although the network operators are not highly impacted as yet, the situation will most likely change in the future, because of the rapidly growing trend of data traffic in mobile networks and increased capability of mobile devices. In this use case an attacker remotely instructs and end user mobile device to conduct malicious activities over MNO's network. This could, for instance, be scanning for additional victims, spamming, or directly attack other users.

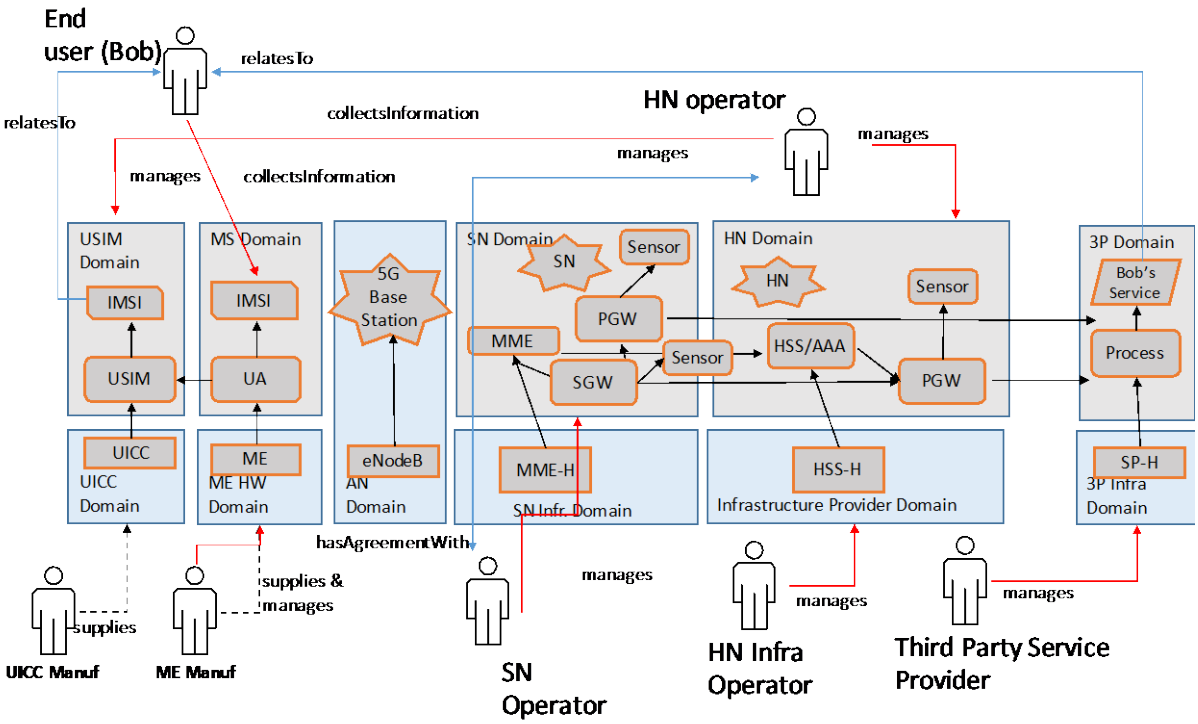

Figure A.86. Botnet mitigation (UC 10.1): sunny day scenario

In the sunny day scenario a typical user activity should not be disturbed. This means that the end user could perform normal activities like phone calls, browsing Internet or sending short messages uninterrupted. Of course one has to take into account that the previously described standard activities could also take place during a case where the user device has been subverted. However, in the normal case any additional protection elements installed by the operator should not degrade the quality the user experiences. These elements could be used to alert (or stop) in case malicious traffic is detected.

A.25.2 Identified threats

A.25.2.1 Subverted user equipment (T_UC10.1_1)

The user downloads and installs an application of untrusted origin. This could be a modified version of a well-known application, which adds functionality to the normal operation of the application. This functionality could perform malicious activity, which includes, but not limited to, possibility to remotely control the

application (and hence, the device itself) or perform actions that cause additional charges for the user, i.e., there is direct monetary impact.

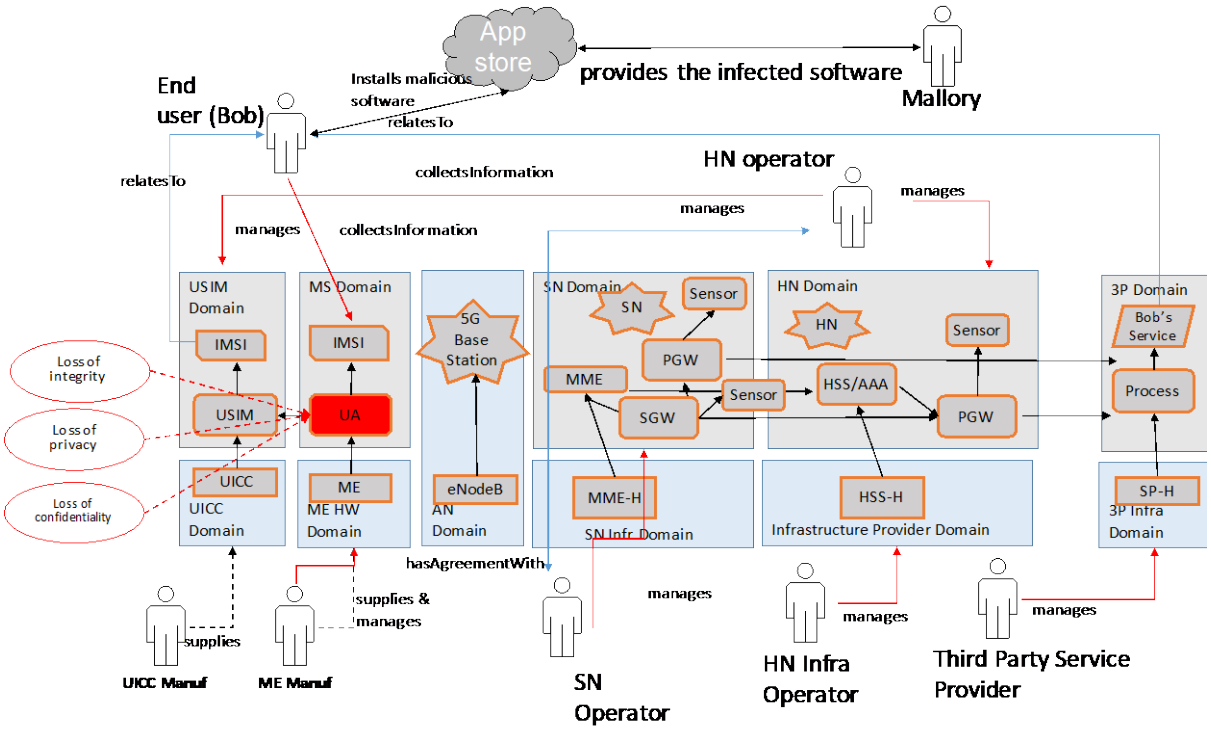

Figure A.87. Subverted user equipment (T_UC10.1.1) – 'rainy day'

The figure above describes the process how Bob gets infected. Bob is staying at home and browses his Google Play (App Store, Windows Market). He founds a free version of a popular and trendy game (other application) uploaded by unknown publisher (i.e. Mallory) and decides to give it a try. Bob downloads it and installs it after accepting everything the game (application) requires to run. As a result, Mallory now has a full (or partial) control of Bob's UE. Therefore, this leads of loss of privacy, integrity and confidentiality for Bob.

Furthermore, as secondary consequences:

- There is an infected device operating in the customer network of the MNO
- UEs remotely controlled by Mallory
- UEs used for malicious activities within the MNO as from the MNO
- Monetary loss for the end users through their monthly bills, regardless how insignificant the amount is for each individual is (in case the UE is instructed to send SMSs to premium numbers)

Trust implications

- Loss of authenticity for Bob, resulting in Mallory impersonating him in front of the other users and the MNO.

Threat mitigation strategy

One way to approach this problem from the MNO point of view is to employ the services of an anomaly-based network intrusion detection or prevention system within the core network, so that the system detects atypical individual behaviour.

Another solution could be providing the end user with visually represented historical data of their activity within the MNO, which, in addition to the targeted number and the party who owns it, and also contains a representation of which country and MNO that number is registered in. This would aid the users to identify anomalous activity from their mobile devices and to report this activity.

Furthermore, the MNO could offer services to the end users to define their own atypical behaviour in the MNO, so that users could, for instance, restrict any outgoing SMS to specific foreign countries, or display a message prior to sending any outgoing SMS.

A.26 Privacy Violation Mitigation (UC 10.2)

A.26.1 Use case description with architectural components

The use case relates to the use of an online service/application over the 5G network. Figure A.88 shows the scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

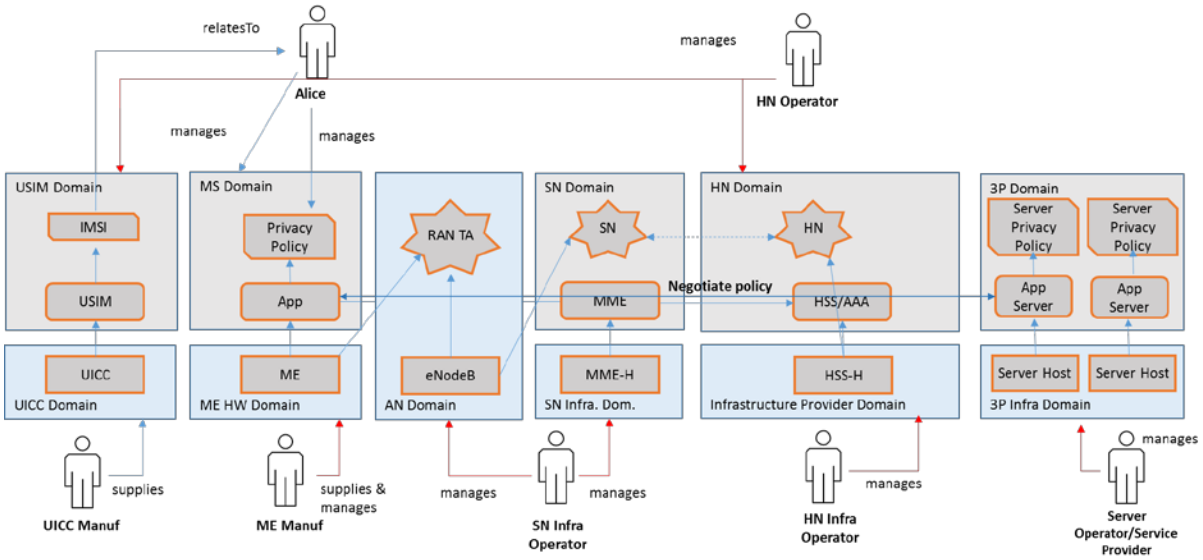

Figure A.88. Privacy Violation Mitigation (UC 10.2): sunny day scenario

Alice is connected to the 5G network through a mobile connection (AN in Figure A.88) thanks to a subscription (USIM domain) she has with her mobile operator (HN domain).

Alice get knowledge that a new technology company has created an inexpensive thermostat sensor for the house environment that learns about the temperature zone and movements around the house and potentially save the user's energy bill. It is programmable remotely.

Alice decides to buy this thermostat sensors. When Alice accesses via her ME the online service (provided by 3P domain) she is informed about the potential collection of some of her data as part of the privacy policy. Alice does not understand clearly the implication of these privacy policies. She uses the service and she is happy to be able to program and control by remote her house's temperature.

A.26.2 Identified threats

A.26.2.1 Nefarious activities (manipulation of information, interception of information): privacy violation (T_UC10.2_1)

Based on Figure A.89, Mallory is either the provider of the web thermostat service itself or is an attacker that took control of the service. As a consequence Mallory is able to retrieve data about some of the basic activities that take place in Alice's house like, when people are there and when they move from room to room. Additionally, Mallory also shares to third parties the data about Alice movements.

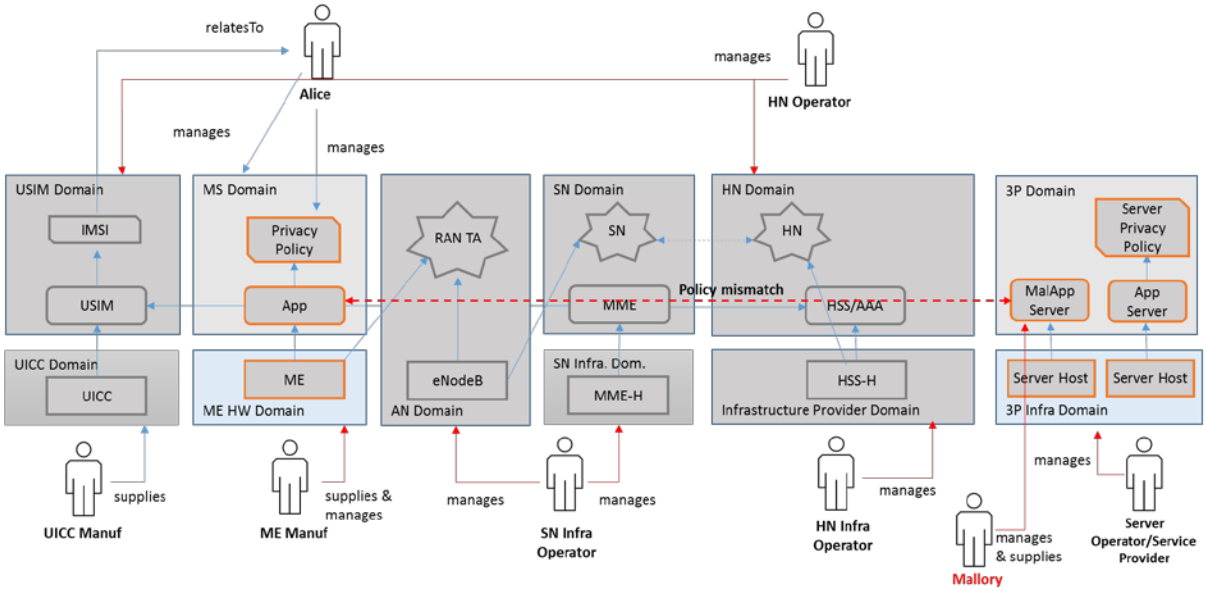

Figure A.89. Privacy Violation Mitigation (UC 10.2): rainy day scenario

The consequence is that the provider (in the 3P domain) of the online service accesses more information than the one required to perform the stated functions. This creates privacy problems, in terms of uncontrolled and unauthorized access to sensitive user data. Secondary effects are that users may not know that personal data are shared with third parties; they don't know if data are effectively transmitted and stored securely, and what further use is made of it.

Trust implications

The use case involves the following actors: service provider and mobile application developer, the user (the phone user and the App/Service Provider subscriber), user equipment operating system developer/provider, user equipment/phone manufacturer (ME).

The current trust model is based on the following relationships:

- The user trusts the provider of the service. He/she assumes that the provider follows the privacy policy of the user regarding the collected data, which implies that only the data required for the correct service operation are retrieved, and the data is not leaked to third parties. Therefore, the user trusts that the provider does not further disseminate the collected information to additional parties, if not explicitly allowed by the user to do so.

The implications related to the trust model are that if the user's privacy policies are not honoured, then the privacy of the user is endangered. The implications are:

- The user has no effective way to detect/measure the real trustworthiness of the service provider.
- It is sometimes difficult for a user to understand the privacy implications of using a service: privacy policies (where they exist) are often not easy for users to read and commonly not presented upfront to the user.
- The user cannot control how her/his data are protected and used after being retrieved and sent back to the provider's servers.
- The user has no way to specify his/her privacy preferences including what type of data they he/she is willing to share, for what purpose and for what period.

Trust mitigation strategy

The type of trust required in this use case can be ensured/guaranteed by providing the user a way to analyse the privacy policy of a service and compare it to his/her pre-defined preferences.

The user shall be able to specify his/her privacy preferences including what type of data he/she is willing to share, for what purpose and for what period. This allows the user to make privacy-aware decisions regarding the use of 5G networks and over-the-top 5G services. Ideally, the analysis would be carried out prior to the service being used, for example, at the client application installation time or at the point of connecting to a 5G network.

A provider of a commercial Web site or online service, that collects personally identifiable information about individual consumers who use or visit its commercial Web site or online service, shall post its privacy policy in understandable and clearly way informing the user at a minimum about what precise categories of personal data the service wants to collect and process, why the data processing is necessary (for what precise purposes), whether data will be disclosed to third parties, what rights users have, in terms of withdrawal of consent and deletion of data.

A.27 SIM-based and/or Device-based Anonymization (UC 10.3)

A.27.1 Use case description with architectural components

The use case relates to user's sensitive data accessed by online services and mobile applications. Application running on user devices constantly transmit a steady stream of information to third parties, often sensitive, private, and identifying data ranging from a device's serial number like IMEI, unique operating system identifiers, phone number, voice mail number, SIM ID and even location information. Some of these identifiers are personally identifiable and linked to the devices the user has. The constant transmission of identifying data is important to delivering seamless and tailored services and content to users.

Figure A.90. shows the scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

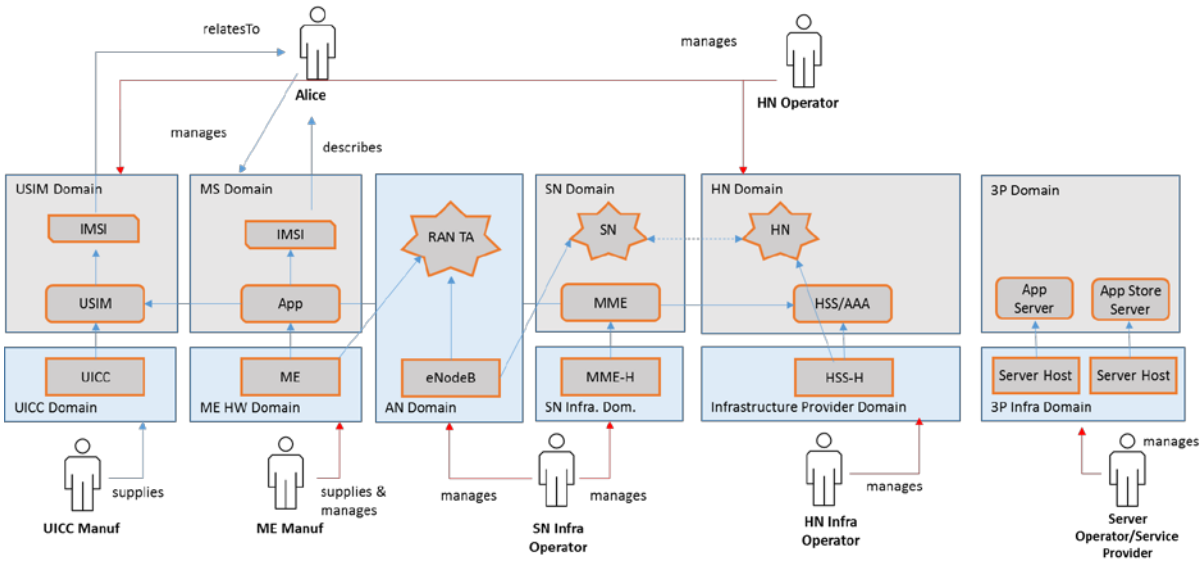

Figure A.90. SIM-based and/or Device-based Anonymization (UC 10.3): sunny day scenario

Alice is connected to the 5G network through a mobile connection (AN in Figure A.90.) thanks to a subscription (USIM domain) she has with her mobile operator (HN domain).

Alice needs to access via her ME an online service, e.g. a traffic road service to keep a check on the traffic situation and get real time information on traffic jams and road closures. Alice has to install on her ME the mobile application offered by the service provider (3P domain). During the installation process, the application notifies to Alice the data it needs to access as part of the 'permissions' list. Alice denies the permissions requested and the installation process fails. Few days later Alice travels away. She needs to reach a destination from the airport but since she does not have much time it is very useful for Alice to better plan the route and to know in real time any traffic situations that may affect her travel time. She tries to install again the application and this time she grants the permissions requested. The installation process ends successfully on the ME.

A.27.2 Identified threats

A.27.2.1 Nefarious activities (manipulation of information, interception of information): personal information disclosure (T_UC10.3_1)

Mallory can come into play in several places. Based on Figure A.91., Mallory is the application developer/provider of the service itself. He/she develops the application to access a range of identifiers while providing the service. This "abuse" is also possible since many mobile operating systems reveal subscription and device identifiers, such as phone number, IMSI, IMEI, together with a plethora of other personal data. In a more extended scenario, Mallory may partner with advertising networks or other third parties, and share Alice's identifiers or personal information with these other parties. As a result, in addition to the apparent collectors of identifiers (i.e. the app developer/service provider) there are largely hidden collectors, such as those belonging to advertisers and analytics or crash report companies. The consequence is that the real-time traffic application installed by Alice requests a wide range of information from Alice ME, not all of which is clearly necessary by the advertised functionality of the application. Many of these identifiers are transmitted, collected and shared without Alice's consent. Moreover, the average mobile phone user does not have tools to monitor or control such leaks.

In another scenario Mallory exploits weaknesses in the real-time traffic application to hack into Alice's ME and to retrieve sensitive data transmitted to remote servers.

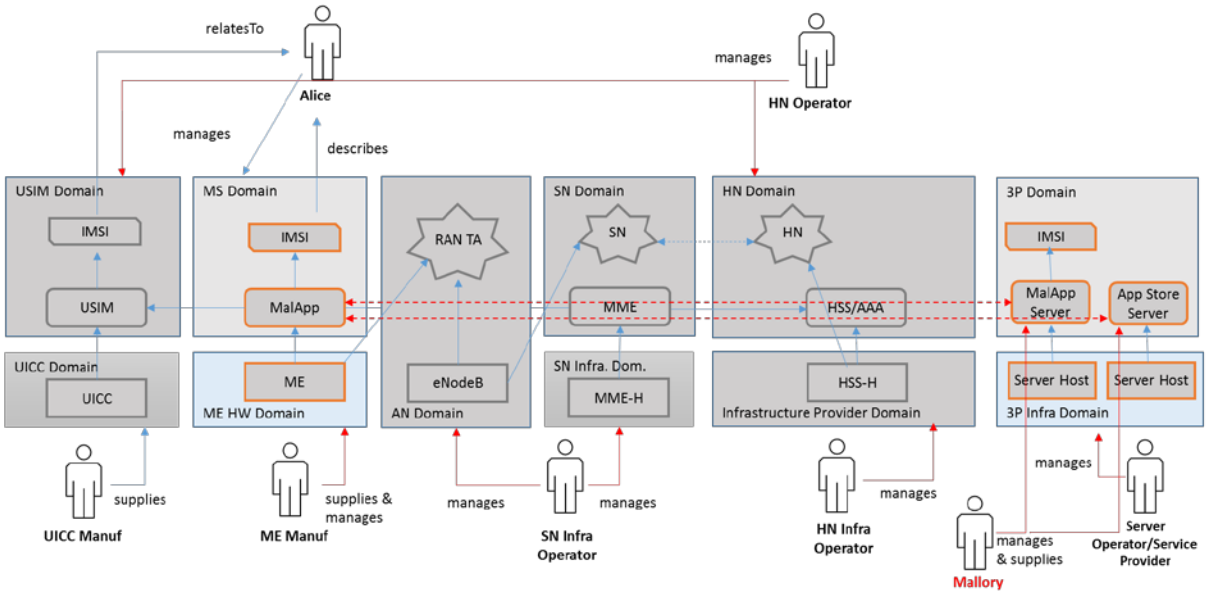

Figure A.91. SIM-based and/or Device-based Anonymization (UC 10.3): rainy day scenario

The consequence is that the application accesses more information than the one required to perform the stated functions. This creates privacy problems, in terms of uncontrolled and unauthorized access to sensitive user data. Secondary effects are that users may not know that personal data are shared with third parties; they don't know if data are effectively transmitted and stored securely.

Trust implications

The use case involves the following actors: app ecosystem (Application store provider or service provider and User equipment application developer), phone users (Service Provider subscriber), user equipment operating system developer/provider, user equipment/phone manufacturer (ME).

In this scenario:

- An application store provider trusts an application submitted to the store only after the adoption of vetting process, during which the app is tested to ensure that it does not crash in any obvious way and that it conforms to all the appropriate application store rules. This means that an application store does not implicitly trust an application but it gives the trust only if the vetting process is passed.
- A user trusts the application store provider or service provider offering the application based on the security controls like the vetting process put in place to ensure that the stored applications are not infected by malware. 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. Consequently the user implicitly assumes that applications downloaded from the trusted application store provider are trusted. Moreover, the user trusts the user equipment (ME) both in

the device manufacturer for firmware security, and, in particular, in 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.

The implication related to the trust model are:

- The user has no effective way to detect the real trustworthiness of the APP provider
- There isn't a direct trusted relationship between the user and the application. The user does not have a mechanism to control what data an application really access and if they are really necessary. A user cannot prevent an APP from retrieving her identifying data when identifying data would not be really necessary for the service provided by an APP to the user
- The user cannot control how her identifying data are protected and used after being retrieved and sent back to the APP provider's servers.
- 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.

Trust mitigation strategy

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. Potential solutions include an anonymization service that can be subscribed by 5G users needing it (5G users that have privacy concerns regarding their data). Network offers to subscribers a SIM (or a device) that implements anonymization algorithms like for example lightweight format preserving algorithms that can be implemented with little computational resources. Network offers to subscribers a means to configure their anonymization preferences.

The *Device-based Anonymization* enabler (R2) allows users to configure a fine grained data anonymization to distinguish between applications for which data needs to be protected and returned in an anonymized way to avoid unnecessary disclosure, and applications that need the real data (real IMSIs or MSISDNs) for their correct functioning. For example, some apps offer a mechanism to recover a lost password via SMS and therefore they need the real MSISDN of the user's profile. For compatibility with Internet services, format preserving encryption which generates the same pseudonym for the same identifier and service received in input should suffice. The enabler provides such an algorithm embedded in the mobile device OS, while being able to distinguish the calls coming from different applications installed on the user's device and apply data anonymization accordingly to the policy preferred by the user.

A.28 Lawful Interception in a Dynamic 5G Network (UC 11.1)

A.28.1 Use case description

In this use case, we attempt to show the implementation of a lawful interception. The sunny day is as follow (cf. D2.1 for further details). First, we assume that LEA identifies the suspected criminal (i.e., Bob) to be surveilled and that he (LEA) has an authorization from the court of justice in order to perform a lawful interception on Bob. On demand, the MNO should be able to answer any interception request regardless of the target entity / user or target service. At the beginning, LEA transmits the LI request and the granted authorization to the MNO to conduct the interception with regards to Bob. The MNO checks the validity of the request and depending on the intercept type and the service to be intercepted, the MNO instantiates, activates and initiates a Network function (we call it, in what follows, LI function) that will deliver to the authorities the required information. At the end of the authorized period, the MNO deactivates the LI function.

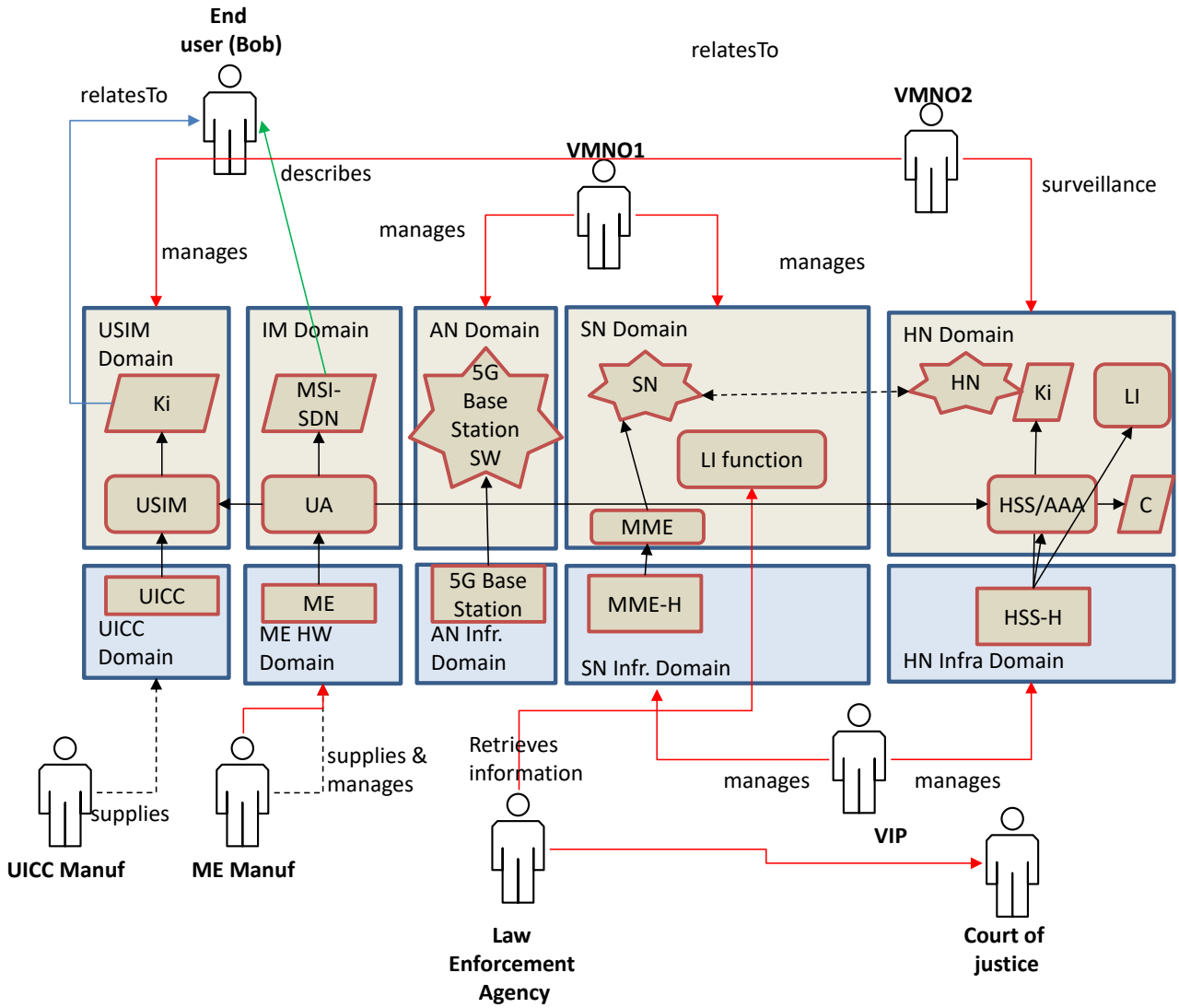

Figure A.92. Lawful Interception in a Dynamic 5G Network (UC 11.1): sunny day scenario

A.28.2 Identified threats

A.28.2.1 Compromised / malicious LI (Lawful Interception) function (T_UC11.1_1)

In this threat, we have an attacker that will target the LI function. Attacking the LI function may result in various issues. The attacker may act either against the authorities by compromising the LI function in such a way that it delivers fake information about Bob or correct information about another user instead of Bob. The attacker may also compromise the LI function such that its functioning is not any more transparent (like required by LI) because it causes disruption or degradation of the service. Finally, the attacker may target the user privacy by providing to the authority more information than what is authorised.

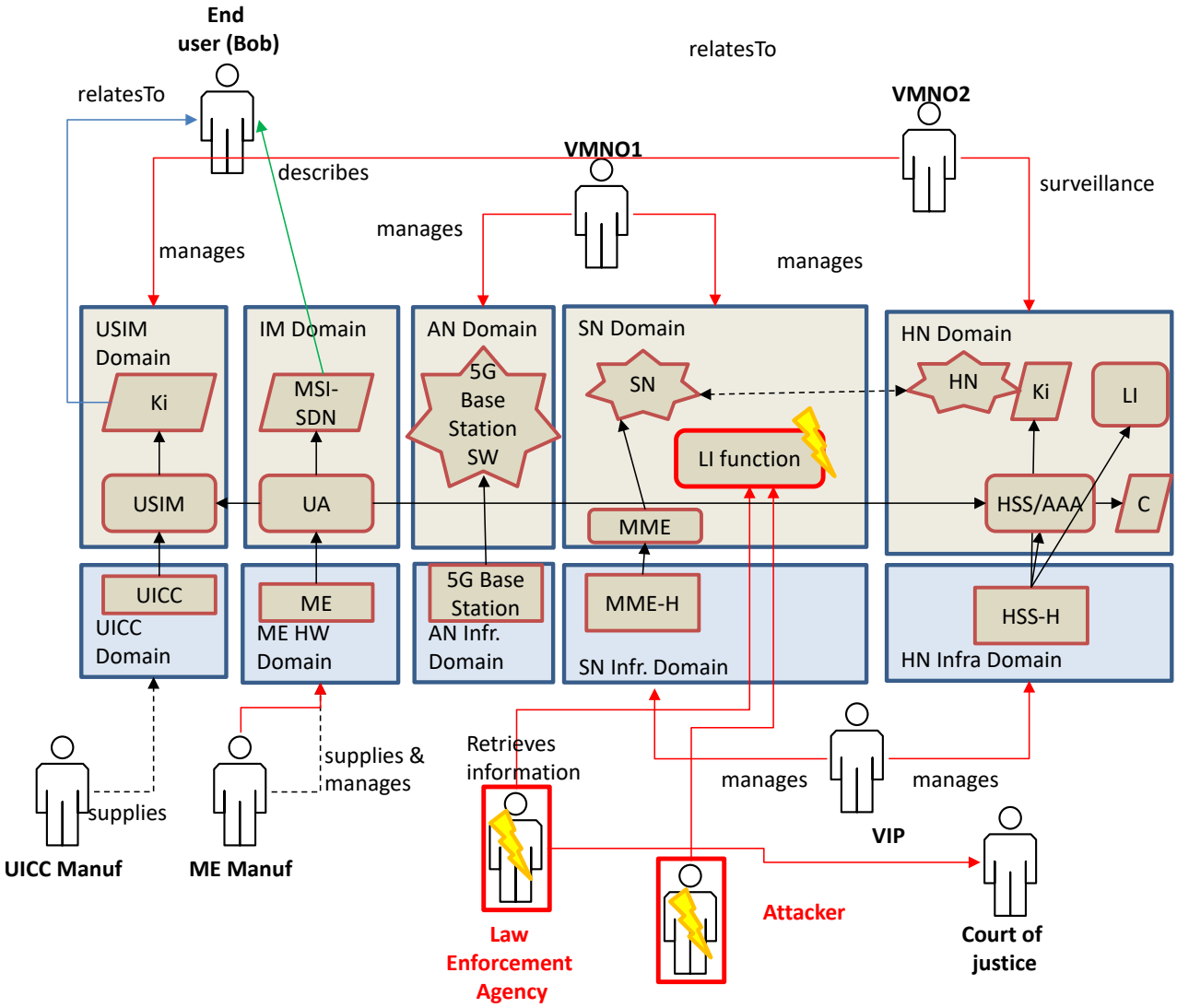

Figure A.93. Lawful Interception in a Dynamic 5G Network (UC 11.1): rainy day scenario

Trust implication

The user trusts the MNO that only authorized LI are executed and only authorized authorities have access to collected data during the LI. The user also trusts the MNO that an LI lasts only the time designated in the authorization and only on the users indicated in this authorization. The authorities trust that the MNO will provide correct data.

Threat mitigation strategy

In order to protect against this threat, the MNO needs to consider the validity of the LI function. We can consider the state of the art about remote attestation mechanism and software integrity verification.

A.29 End to end encryption in a LI aware network (UC 11.2)

A.29.1 Use case description with architectural components

The use case relates to the user communication over 5G network. Figure A.94. shows the scenario in relation to the architecture, in the absence of any threat (the sunny day scenario).

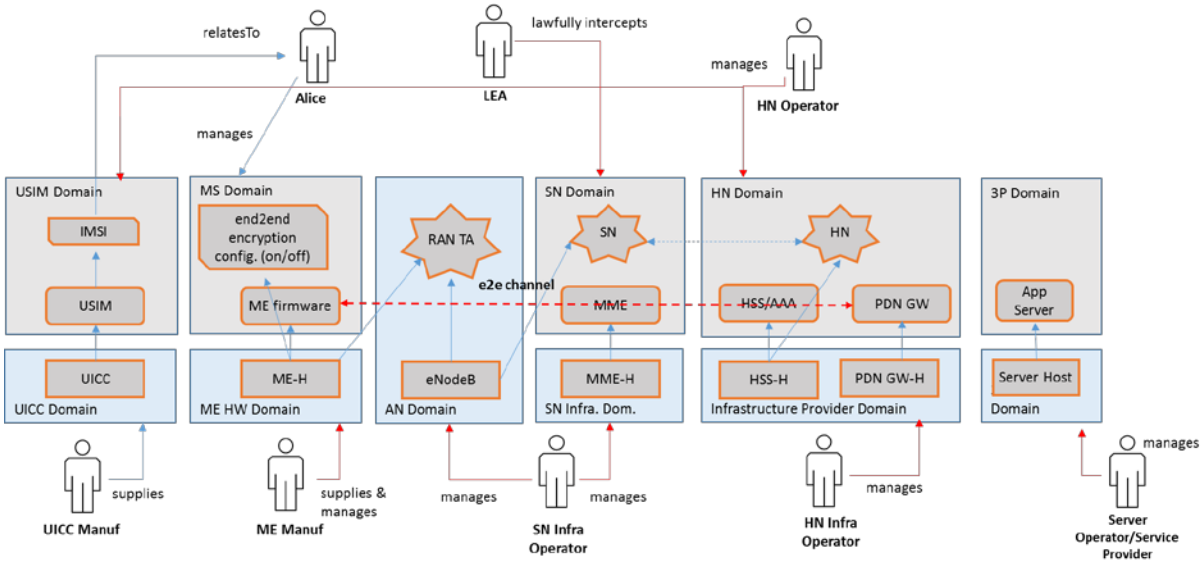

Figure A.94. End to end encryption in a LI aware network (UC 11.2): sunny day scenario

Alice is connected to the 5G network through a mobile connection (AN in Figure A.94.) thanks to a subscription (USIM domain) she has with her mobile operator (HN domain).

Alice needs to communicate in an encrypted manner with Bob. She wants her call or SMS/MMS to be encrypted but she does neither share a secret key with Bob nor an application to encrypt the communication. Alice uses the encryption service provided by the 5G Operator, as shown in Figure A.94..

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. One entity alone 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.

Therefore if LEA wants to intercept Alice's calls, LEA asks the 5G operator to provide access to the intercepted communications. 5G operator as provider of the encryption service acts as an escrow agent. The session key is retrieved or reconstructed and used by LEA to decrypt the session key and consequently Alice's communication by completely respecting the terms of the interception authorized by the court of justice.

A.29.2 Identified threats

A.29.2.1 Nefarious activities (manipulation of information, interception of information) over LI-aware network (T_UC11.2_1)

Based on Figure A.95., Mallory is a malicious LEA or a malicious key escrow actor. The main potential flaws of an end-to-end encryption service is to provide LEA (or any other key escrow agents, e.g., a 5G operator) full control of the decryption keys or to somehow enable a backdoor which might be used for undetectable mass surveillance. In such a case, the malicious LEA or any entity in control of the backdoor may get information exchanged by one of the users involved in LI out of the designated period in the authorization and/or about users not actually in the authorization list (Unauthorized disclosure).

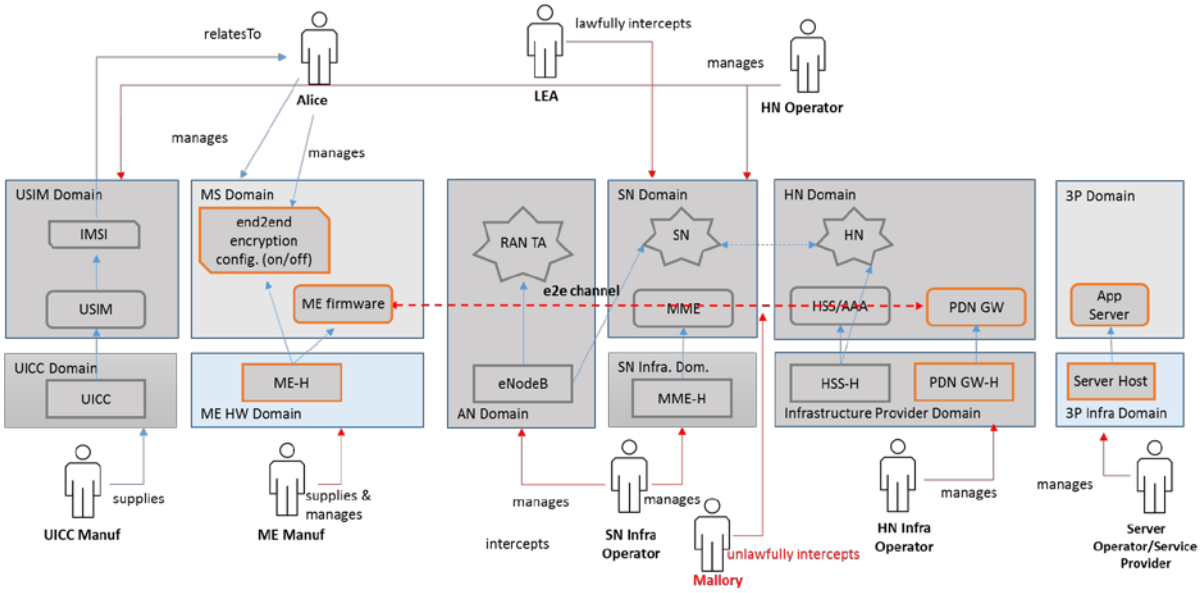

Figure A.95. End to end encryption in a LI aware network (UC 11.2): rainy day scenario

In this way the user data privacy is not guaranteed when the LI is active for an end to end encrypted communication.

Trust implications

The use case involves several actors: the end-user (e.g., Alice), the MNO (HN) to which the user has a subscription, the SN (and the AN) provider, the law enforcement agency (LEA) that needs to intercept a suspected user communications, the court of justice which delivers the lawful interception authorization. The current trust model is based on the following relationships.

- the user trusts its HN as part of the direct service agreement.
- The HN trusts the SN as part of the roaming agreement contract and it confers full trust in the SN with regards to its subscriber.
- Both HN and SN trust their interconnection provider.
- The user and the HN trusts the SN for the privacy aware implementation of LI. 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.

The implications related to the trust model are:

- The user has no way to detect the trustworthy of either the SN or the HN as far as the key escrow mechanism implementation is concerned.
- The user has no way to detect the trustworthy of LEA as far as the key escrow mechanism implementation is concerned.
- On the other hand if users trust the privacy fairness of the encryption service provided by the mobile network and this trust is broken, users may stop using this service.

Trust mitigation strategy

The type of trust required in this use case can be ensured/guaranteed through technical solutions (e.g. configurable end to end encryption) with privacy aware LI.

The properties that an end-to-end encryption service should satisfy are:

- *On-demand service*: The service should be turned on and off by the subscribers.
- *Backward secrecy*: LEA must not have access to exchanged information before the designated period in the authorization.
- *Forward secrecy*: LEA must not have access to exchanged information after the designated period in the authorization.
- *Security*: The end-to-end encryption service may be applicable on IP or higher layer independently by the type of UE using an application which is installed as part of the service.

The encryption key may be part of an escrow system provided by the 5G operator to enable secure communication and at the same time enable lawful interception. For example the session keys can be encrypted using a master key. To this end, we can use a threshold (k, n) secret sharing scheme. In such a case, less than k agents (e.g., LEA, 5G operator, etc.) cannot get any information about the master key and any k (possibly smaller than n) or more agents can recover the master key. In this way a malicious LEA cannot recover the session encryption key.

B Annex: User Attitudes Survey

B.1 Background of the survey

The survey focuses on human trust related to possible network threats, clarifying how people (non-professional and professional) conceive network related threats. The questionnaire was published as a web address (one link) on various locations.

- March 23 the link to the survey was sent to the members of EU project 5G-ENSURE
- March 27 the link to the survey was sent to the members of SIGCHI Finland (Special Interest Group of Human-Computer Interaction)
- March 31 the link to the survey was sent to several teams in VTT
- at the end of March/in the beginning of April the following was done in 5G-ENSURE:
    - the link to the survey was published in the LinkedIn community as a blog
    - the link to the survey was published in the project's website
    - the link was included in a newsletter of 5G-ENSURE
    - a tweet was posted about it
- March 31 the link to the survey was sent to some Ericsson departments

The responses were gathered by June 13. As a whole, 55 people took the survey.

B.2 Respondent qualities

B.2.1 Personal information

Regarding the respondents, there were 53 respondents who reported their age. On an average, the respondents were 46 years, the youngest having 25 years and oldest 61 years. Most (56%) were male some were females (39%), 5% did not want to provide their gender. Regarding education, most respondents were graduates (53%) (see Figure B.1).

	N	Percent
primary school	0	0%
secondary school	1	1,88%
college-level education	4	7,55%
undergraduate	1	1,89%
graduate	28	52,83%
PhD	19	35,85%

Figure B.1. The division of background education of respondents.

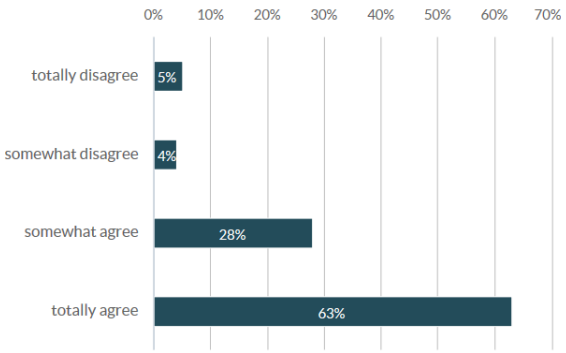

Figure B.2. The share of responses related to the statement 'I consider myself as an experienced Internet user'

Respondents were asked to write the country they live in as free text. Most of respondents were Finnish (21 respondents, 40% of all respondents) or Swedish (15 respondents, representing 28% of all respondents). 5 respondents (9%) were from Italy, 3 respondents (6%) from France, 2 respondents from Germany and Spain

each (both representing 4% of all respondents), and one respondent from UK, Malta and China. Additionally, one respondent had written UAE as the country to live in and one from Middle Europe.

The vast majority (73%) had technical education. The most usual education as the only or part of education was, not astonishingly, computer science (44% of all respondents). The average usage of Internet was, accordingly, high, the average being 21 years. The minimum number of years was 8 years and maximum 30 years (and one had reported the usage has continued over 20 years). Accordingly, most respondents considered themselves as truly experienced internet users (see Figure B.2). The average usage of Internet daily was 5 hours, with the minimum of one hour and maximum of 17 hours. The average usage of the Internet is, thus, not extremely high although used frequently. The most typical duration of the usage was 8 hours a day. All respondents used Internet both at work and for free-time activities. On an average, respondents had three devices to connect to the networks, the minimum being one and maximum 12 devices (but no respondent had named 12 devices). Most commonly, the respondent had two devices.

B.2.2 Network related general practices and attitudes

Respondents had relatively educated practices in using Internet as most respondents did not use the same passwords for many sites; 37% (20 respondents) totally disagreed with the statement of "I use the same password for many sites", and only 6% (3 respondents) agreed with it (see Figure B.3). On the other hand, based on the responses, seems to be that even if about a third of respondents were careful, the majority still used the same or perhaps a limited amount of passwords for several applications. Furthermore, the usage of the same password is not a severe threat in all situations. The same password can be used as enhancing memory capacity when that password is used in casual, not sensitive contexts.

About the same trend can be found in accepting invitations to use application sent via Internet, such as social media. For 43% (23) respondents, it was absolutely clear that invitations to use applications are not necessarily accepted. The hesitation to accept these invitations is quite clear as nobody totally agreed with this idea (see Figure B.4). On the other hand, the reason to not to accept invitations to use network applications may be based equally well on the fact not all applications are interesting as well as on distrust on these applications. All respondents except one did shopping on Internet and all but three used online banking.

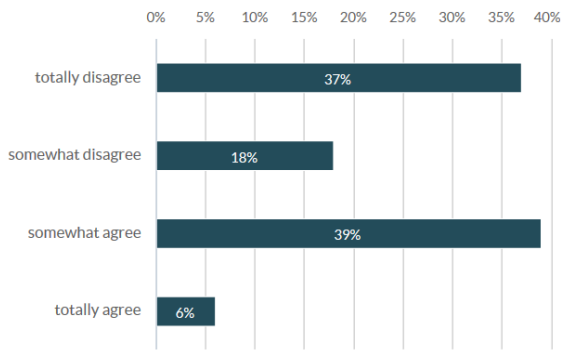

Figure B.3. The share of responses related to the statement 'I use the same password for many sites'. Thus, slightly more than half of respondents preferred using different passwords for different sites.

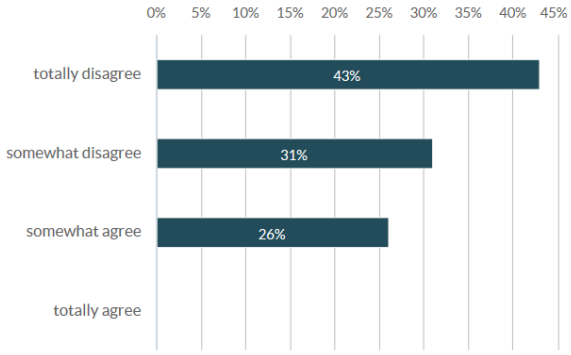

Figure B.4. The share of responses related to the statement 'I accept invitations to use applications sent via Internet, such as social media'. Thus, the vast majority of the respondents preferred not accepting all invitations.

Regarding attitudes related to Internet and intimacy, 20% (11 respondents) were totally against that shopping behaviour is analysed for marketing benefits of the companies, only 8% (4 respondents) finding it totally acceptable (see Figure B.5). In a large scale, the majority (59%) did not like being traced and analysed by companies behind the shops.

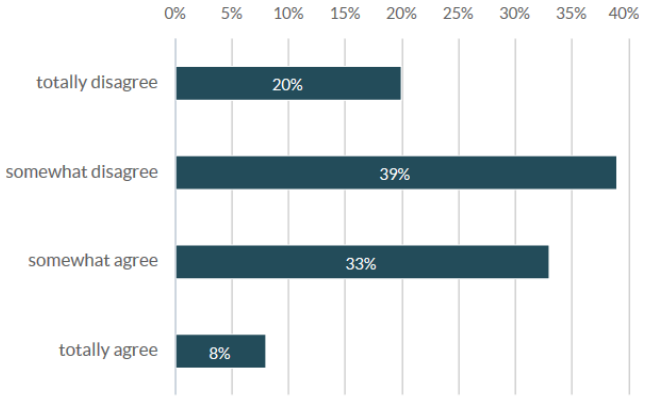

Figure B.5. The share of responses related to the statement 'I have no trouble in accepting my shopping behaviour is analyzed for marketing benefit of the companies'.

Attitudes towards being followed by an authority depended strongly on the reason (see Figures 6a and 6b). 58% (32 respondents) totally disagreed with the concept of being followed by some authority for an unknown reason; only 9% (5 respondents) somewhat agreed and 2% (1 respondent) totally agreed with it. The situation changed if the authority would perform the following as part of a campaign against terrorism. Then, the most common attitude was to somewhat agree on having no trouble with the idea (33%, 18 respondents). Only 27% (15 respondents) would totally disagree also with this, 25% (14 respondents) would somewhat disagree and as much as 15% (8 respondents) would totally agree with it.

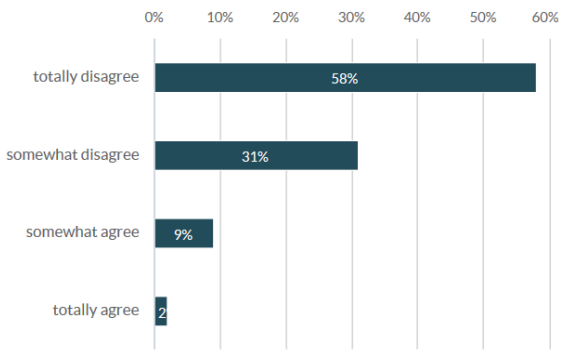

Figure B.6a. The share of responses related to the statement 'I have no trouble in accepting my behaviour (location, discussions etc.) would be followed by some authority for a reason I don't know'.

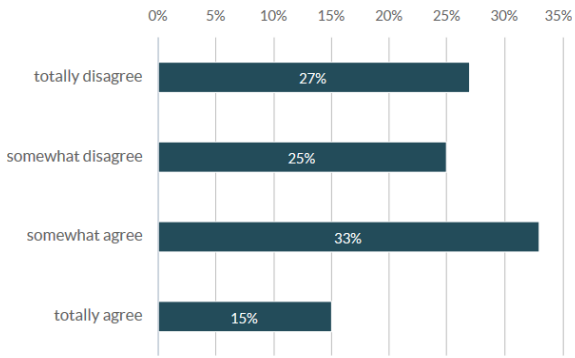

Figure B.6b. The share of responses related to the statement 'I have no trouble in accepting my behaviour (location, discussions etc.) would be followed by some authority as part of a campaign against terrorism'.

Regarding the trust on Internet and mobile networks, the majority (51%, 28 respondents) showed some trust but only 2 respondents had strong trust; the rest of respondents had some distrust (34%, 19 respondents), or strong distrust (11%, 6 respondents)(Figure B.7a). Looking at the results, seems to be that the usage of

Internet may be followed with some level of stress, taking into account the number of hours spent daily with Internet and the accompanying not so high level of trust on it. The trust on the questionnaire was similar (Figure B.7b): 43% (23 respondents) believed their identity is safe with the questionnaire and slightly more, making this group as a majority (57%, 31 respondents) did not believe this questionnaire keeps their identity safe.

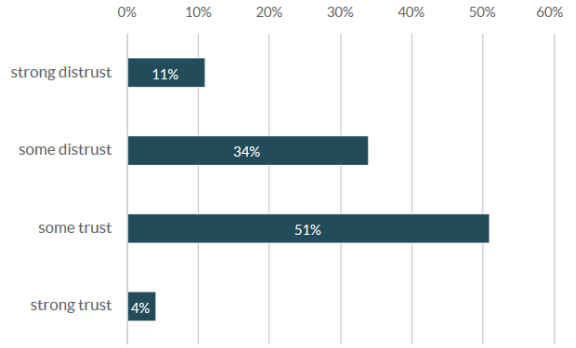

Figure B.7a. The level of trust on Internet among respondents.

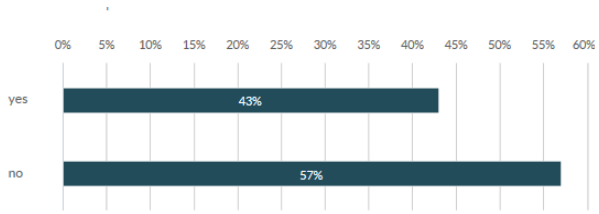

Figure B.7b. The share of responses to the statement 'I believe my identity is safe with this questionnaire'.

This can be, at least, due to the distrust related to the intentions of the organisers of this questionnaire or against the networks in general. Accordingly with the last possibility, most respondents (83%, 44 respondents) thought all operators are not equally secure and nobody totally agreed on the thought all operators are equally safe. – In reality, identity is safe with this questionnaire, to the point it is not possible to trace how some (unknown) individual has answered the questions as the results are provided in a graphical format whenever it is possible, providing only sums or percentages.

B.3 Attitudes related to networks related new technology

Regarding the idea of connecting heating system to be operated via network, it was not found attractive, even if it were affordable (Figure B.8). 59% of respondents considered this idea as something to totally disagree with (28%) or to somewhat disagree with it (31%). On the other hand, the most usual attitude was still somewhat agreeing with the idea, so these solutions could be attractive if the solutions are developed well enough; 35% (19 respondents) chose that option. Only 6% (3 respondents) did not hesitate at all with the idea of connecting their heating system to be operated via network as they totally agreed with the statement.

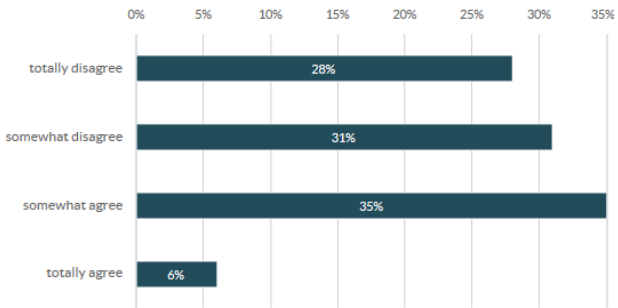

Figure B.8. The share of responses related to the statement 'If it were affordable, I would connect my heating system to be operated via network.'

Other responses related to new technology were similar. Most respondents (47%, 26 respondents) somewhat agreed with the statement that in the near future, it will be secure to use a car which navigates autonomously, based on traffic and other information mediated by networks (see Figure B.9).

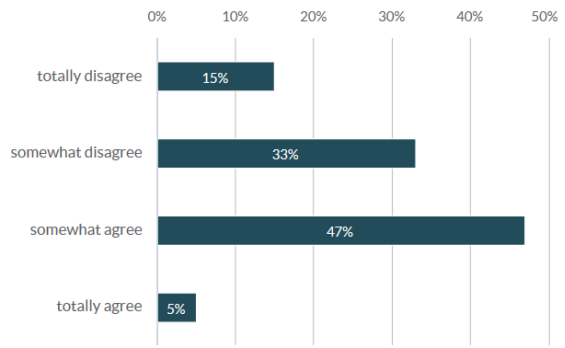

Figure B.9. The share of responses related to the statement 'In the near future, it will be secure to use a car which navigates autonomously, based on traffic and other information mediated by networks'.

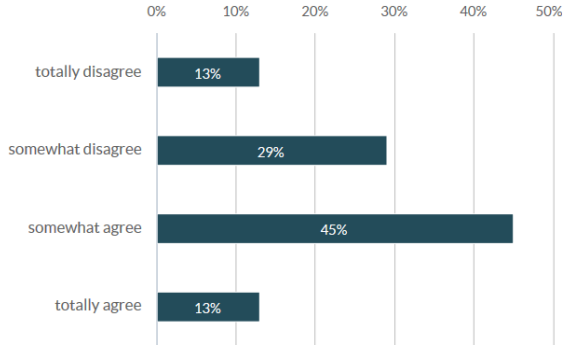

Figure B.10. The share of responses related to the statement 'The telemonitoring of health related functions for a patient living at home sounds safe to me'.

Also accordingly, most respondents (45%, 25 respondents) somewhat agreed with the statement according to which the telemonitoring of health related functions for a patient living at home sounds safe (see Figure B.10).

The scenario with a future fridge, ordering food from the store when needed, provoked less accepting attitudes; the most prominent answer to this statement (buying one when possible) is "somewhat disagree" (38%, 21 respondents) (see Figure B.11). The reason for that is probably the lack of trust as a fridge is not such a big investment as a, say, car. Of course, some respondents could have been thinking that when first appearing in the shops, the device may still have buggy features or that the system with the local stores is not necessarily functional. The most negative attitude was towards an electric key to home, controlled via Internet. Most respondents (40%, 22 respondents) totally disagreed with it as sounding interesting and trustworthy (see Figure B.12). This is rather understandable – if Internet is not to be trusted, why open the door to Internet-originating threats deliberately.

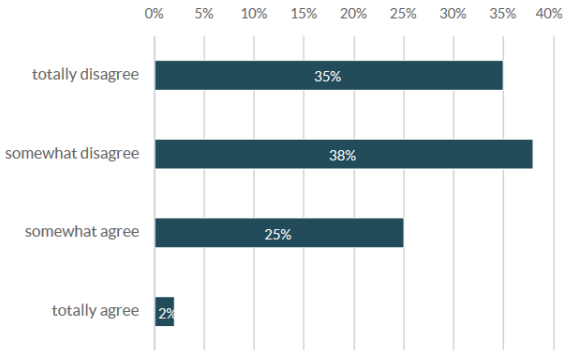

Figure B.11. The share of responses related to the statement 'If/when a fridge which orders food from the store when needed appears in the shops, I will buy one'.

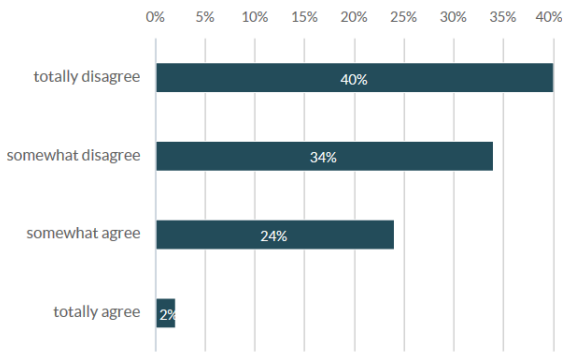

Figure B.12. The share of responses related to the statement 'An electric key to my home, controlled via Internet, sounds interesting and trustworthy to me'.

B.4 Threat and trust on networks

Respondents were asked to provide their conceptions related to some specific, short scenarios, which describe briefly some network related threat. The opinions varied in accordance with the scenario in question. As a whole, some usual trends, present with most scenarios, could be found.

- Firstly, usually more than half of respondents considered the threats to be avoidable or identifiable. This means that related to these threats, respondents felt (s)he has some control over the threat in question.
- Secondly, most threats were perceived as reflecting how networks are somewhat untrustworthy. As most respondents (51%) declared in a separate question having some trust (51%) or some distrust (34%) on Internet, this can be interpreted that even if some trust on Internet exists, the threats describe those instances which tend to lower the trust from higher to lower level.

In the following, each scenario is presented, followed by the related results.

B.4.1 Wiretapping

Scenario 1: Imagine that your phone call is being wiretapped.

Most respondents (43%) considered wiretapping as avoidable although this opinion was not very strong among respondents; 35% found it unavoidable and as much as 22% did not know whether wiretapping could be avoided (see Figure B.13). Regarding all scenarios in this survey, this result is a bit deviant in the sense that the percentage of respondents considering the avoidability of the threat is a bit lower here – usually the threat is considered to be avoidable by around 60-65% whereas when wiretapping is in question, less than half of respondents considered it is avoidable.

If being wiretapped, the awareness of it would affect most respondents' behaviour regarding phone calls (Figure B.14). The awareness would not have any effect for only 9% of respondents but, on the other hand, only 19% considered the awareness of being wiretapped to affect highly on phone call related behaviour.

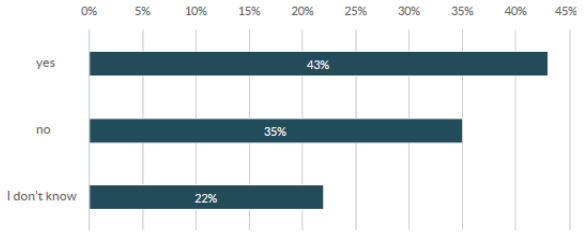

Figure B.13. The share of responses related to the question 'Do you think this would be avoidable?' [Scenario 1, wiretapping]

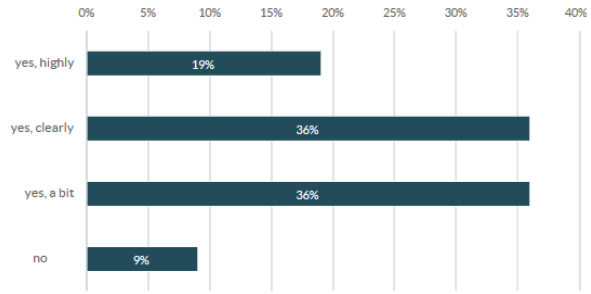

Figure B.14. The share of responses related to the question 'Would the awareness of this threat [Scenario 1] affect your behaviour regarding phone calls?'

Regarding trust, the same clear but moderate conception prevailed: most respondents considered that the possibility of wiretapping reflects how networks are somewhat untrustworthy. This conception is similar with most threats presented in this survey - about 50% of respondents think the threat as reflecting how networks are somewhat untrustworthy. Thus, it can be interpreted that wiretapping was considered as a real disadvantage but there is nothing really shocking about it - it just tells network is somewhat untrustworthy (see Figure B.12). The free comments provided in this context follow the same reasoning, for instance, "*all networks are open to regulatory and legal interception in my country - so ... I should be aware*" and "*Scenario 1 should happen only for valid reasons*".

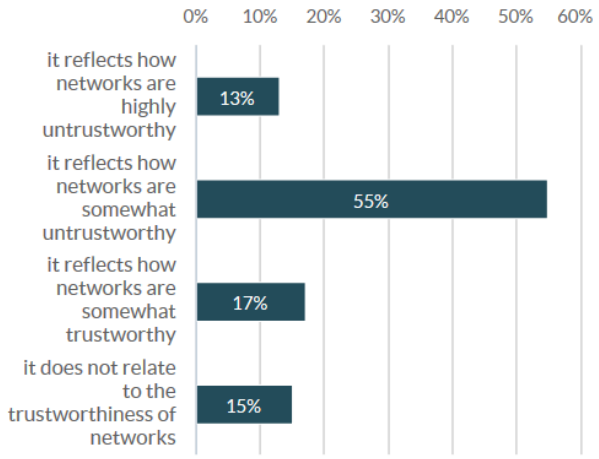

Figure B.15. The share of responses for the question 'How does this scenario [Scenario 1] relate to your trust on 5G/mobile networks?'

B.5 Burglar following your geological location

Scenario 2: Imagine that your geological location is followed (based on the location of your mobile device) by a burglar, planning to invade your house.

The vast majority, 62% of respondents, believed such as situation would be avoidable; only 22% thought nothing can be done and 16% did not know (Figure B.16). Thus, in this situation respondents tended to think the situation can be controlled, similarly with most scenarios in this survey.

The awareness of this threat would not necessarily decrease the usage of the mobile phone as again (Figure B.18), like in wiretapping, most respondents thought it would affect "a bit", decreasing the usage of networks. The reason for this could be, of course, that most respondents considered the situation avoidable if needed.

Again, similarly with most scenarios, this possibility was considered to reflect how networks are somewhat untrustworthy for about half of the respondents (see Figure B.19).

The comments provided support for the given responses. For instance, it was stated that "*I'd not put the blame on the provider of the network, but more the provider of the alarm system*" or "*I am more concerned about the fellow citizens who are constantly showing off their location in social media*", indicating that it is not necessarily a question about networks.

Some respondents perceived this problem being due to geolocation: "*Turn off geolocation :)*" or some other factors, such as "*Google knows it already*(…)", "*Problem is not the burglar but a) the Telco b) protocols leaking identifiers*" or "*location must be known to network (to be able to provide connectivity), and network is untrustworthy, software is buggy... That's why we have laws to punish and discourage exploiting this*".

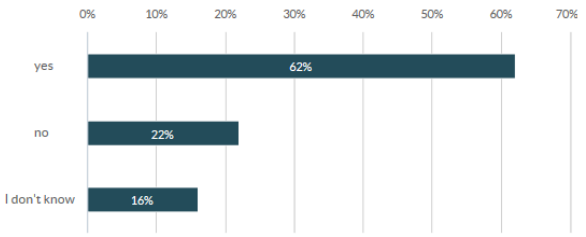

Figure B.16. Responses to question 'Do you think this would be avoidable [Scenario 2, geological location and burglars]?'

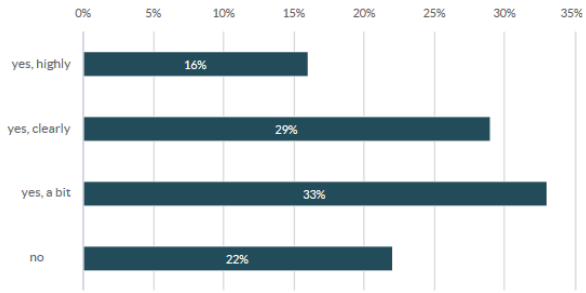

Figure B.17. Responses to question 'Would the awareness of this threat [Scenario 2] decrease your usage of your mobile 5G/networks?'

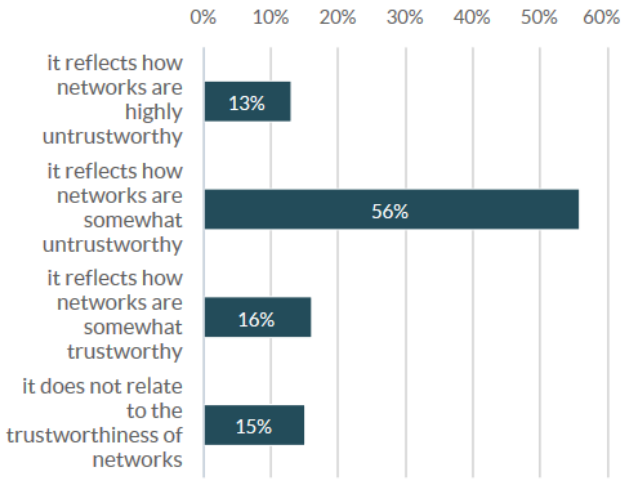

Figure B.19. The share of responses for the question 'How does this scenario [Scenario 2] relate to your trust on 5G/mobile networks?'

B.6 Leaking of identifiers

Scenario 3: Imagine that your mobile subscriber/device identifiers (i.e., IMSI, temporary IMSI, IMEI) linked to your personal identity are leaked because your identifiers are not adequately protected.

Identifier leakage was considered to be avoidable by most of the respondents (60%), only 16% believed it is not and 24% did not know (Figure B.20). This division of responses may reflect the fact most respondents were professionals or highly experienced with dealing with mobile networks. Similarly with the previous threats, also this threat would decrease the usage of mobile networks or mobile services for most respondents to only some extent (clearly for 33% and a bit for 40%), not for many highly (11%) or not at all (16%) (Figure B.21). The effect on trust is also similar; most respondents found it reflecting how somewhat untrustworthy networks are (see Figure B.22). All in all, all responses provided for the threat related to leaking identifiers were relatively similar with the ones for most threat scenarios in this survey.

Regarding free comments provided, many of them considered privacy lost already. For instance, "*Anonymity in this respect is not going to happen in 5G or in the next generation either. Maybe someday*." and "*Privacy is already lost, and by ourselves (e.g. by accepting rules of Facebook and it is hard or impossible to avoid Google)*".

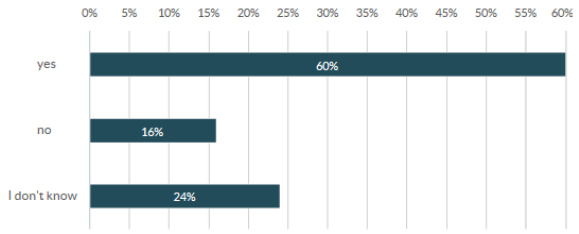

Figure B.20. Responses to question 'Do you think this would be avoidable?' [Scenario 3, leaking identifiers]

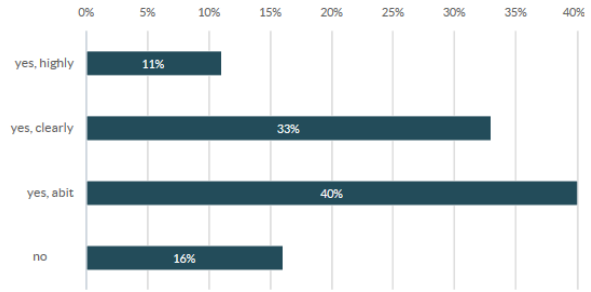

Figure B.21. Responses to question 'Would the awareness of this threat [Scenario 3] decrease your usage of the mobile networks (mobile services)'?

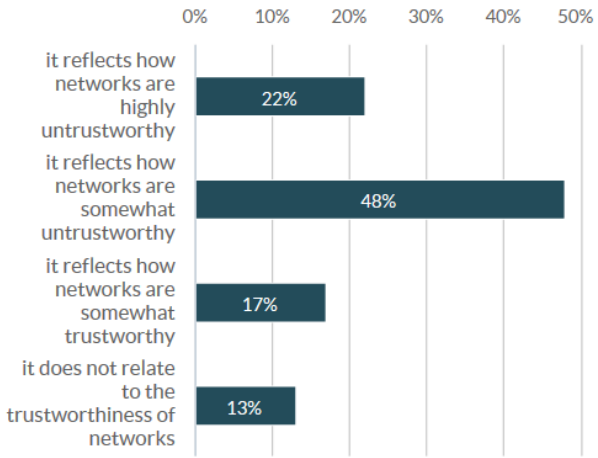

Figure B.22. The share of responses for the question 'How does this scenario [Scenario 3] relate to your trust on 5G/mobile networks?'

B.7 Malware in an e-mail attachment

Scenario 4: Imagine your mobile device is infected by malware. For instance, you open an email attachment which looks like it was sent by a familiar person, after that the data in your device becomes encrypted. Later you are asked for money to get your data back.

Respondents were asked whether they think it would be possible to identify malware in an e-mail attachment correctly and that way to avoid negative consequences. The responses (see Figure B.23) support the interpretation that most respondents were professionals who know, or think they know, what to do: 60% answered "yes" to this question, only 13% "no" and 27% did not know. The response is similar with the corresponding responses to most scenarios described in this survey.

Contrasting to most scenarios, though, this is the type of threat would affect highly respondents' behaviour with email messages (see Figure B.24), as the most typical responses were "yes, highly" (46% of responses) or "yes, clearly" (30%). Thus, the effect of this threat on behaviour is higher than the one related to most threats presented in this survey.

However, even if half of respondents considered that it reflects how networks are somewhat untrustworthy, somewhat similarly with most scenarios in this survey, as much as 32% considered that this threat does not relate to the trustworthiness of the networks at all (Figure B.25). Based on comments provided to this scenario, many respondents think that this threat depends on user behaviour. Also device or software based explanations were given, such as "*Nothing to do with the network; this is down to user behaviour and device set-up. It is also easily mitigated through the use of backup solutions*".

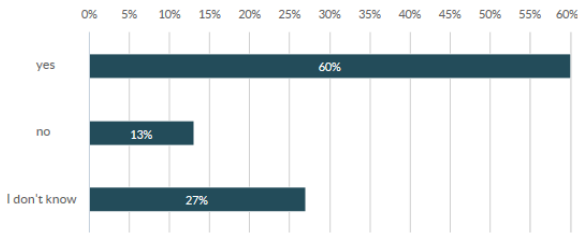

Figure B.23. Responses to question 'Do you think it would be possible to identify this type of situation correctly and that way to avoid negative consequences?' [Scenario 4, malware in an e-mail attachment]

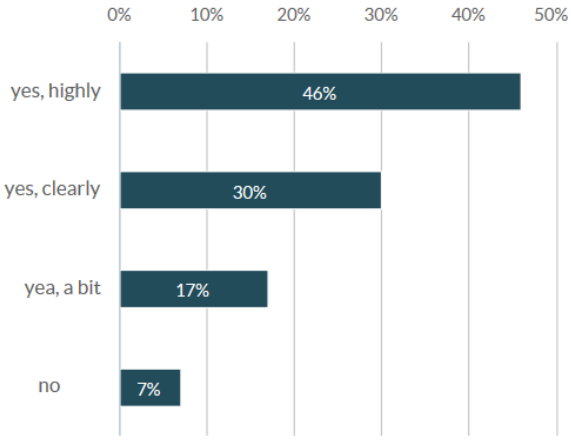

Figure B.24. The share of responses for the question 'Would the awareness of this threat [Scenario 4] affect your behaviour with email messages?'

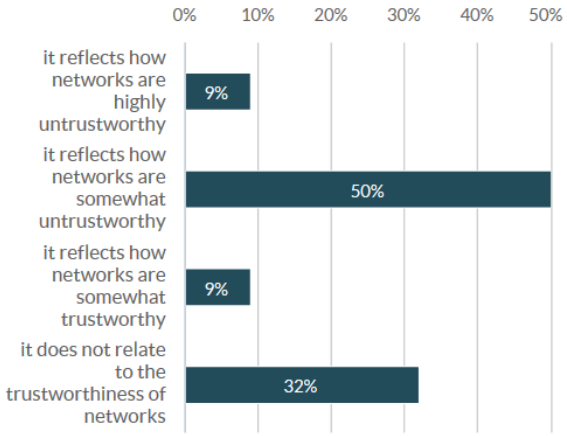

Figure B.25. The share of responses for the question 'How does this scenario [Scenario 4] relate to your trust on 5G/mobile networks?'

B.8 False hotel evaluations

Scenario 5: Imagine that in some evaluation in the Internet (such as hotel recommendations), several people seem to express extreme opinions whereas in fact there are only a few people commenting.

This is a rather mild threat regarding its possible consequences, at least in a first glace when compared with many threats described in this survey. The clear majority of respondents (64%) believed they could identify this type of situation correctly (Figure B.26), similarly with most scenarios in this survey.

Most respondents considered this decreases their usage of Internet originating evaluations (Figure B.27). This can be interpreted as using them only a little or not at all or that, if using, the evaluations are not valued or trusted.

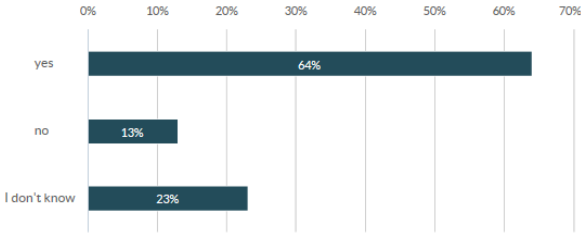

Figure B.26. Responses to question 'Do you think it would be possible to identify this type of situation correctly?' [Scenario 5, false hotel recommendations]

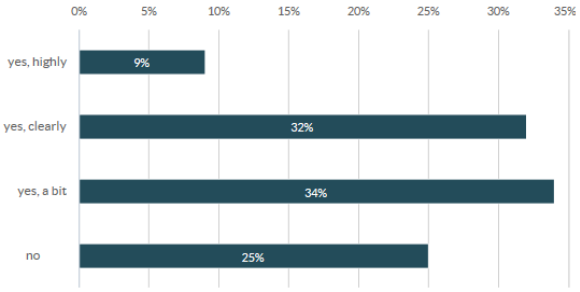

Figure B.27. Responses to question 'Would the awareness of this threat [Scenario 5] decrease your usage of Internet originating evaluations?'

Contrasting to all most scenarios, this phenomenon was not perceived to be related to the trustworthiness of networks (Figure B.28) by as much as almost half of the respondents (48%). Taking into account how these evaluations are created, it is understandable as in this case, technology only provides the platform but it is entirely up to people whether to be honest or not. The biasing effect can be created without specific technical skills. Correspondingly, a smaller amount of respondents thought this would reflect how networks are somewhat untrustworthy (usually around 50%, here only 35%).

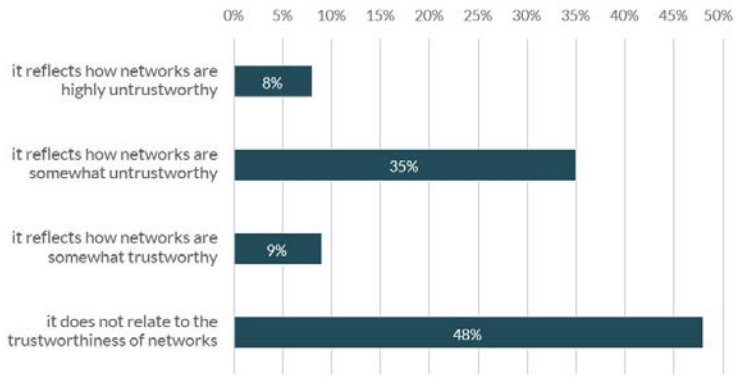

Figure B.28. The share of responses for the question 'How does this scenario [Scenario 5] relate to your trust on 5G/mobile networks?'

There were not many comments related to this scenario, perhaps because this was not considered personally very serious. Here are some examples: "*There is always possibility of fake ratings, but generally you can spot the trustworthy ratings*", "*It could be trolling if extreme views are only shown*", and "*this is a purely application specific scenario - may happen via any network and partly also in face to face situations*".

B.9 Voice calls disabled by hostile actors in the network

Scenario 6: Imagine that unexpectedly, due to hostile actors in the network, you cannot make voice calls using your operator.

Almost half of respondents (45%) thought they could avoid the prevention of making voice calls (Figure B.29). This is a smaller amount than related to most of the threats in this survey (usually around 60-65%).

Furthermore, the awareness of this threat would not decrease the calling to other people for most respondents (63%) (see Figure B.30) which is more than related to most threats in this survey. This may appear controversial at a first glance – the threat is considered relatively unavoidable but still it does not affect behaviour – but, on the other hand, people may think that whether it can be avoided or if not, the worst thing that happens is just that the calls cannot be made. The impossibility of calling can only be tested by making the calls so in practice, the awareness of this threat does not necessarily have any practical implications regarding calling.

However, experiencing this kind of event would probably degrade the relationship with the operator as only 11% of the respondents (Figure B.31) think the awareness of this threat does not increase the willingness to change the operator. Most respondents (60%) think this reflects the untrustworthiness of the networks (Figure B.32). Thus, this can be interpreted that respondents think that the context in which the operators provide services is not the easiest one, even if operators are expected to handle the situation so that there is not harm to the customer.

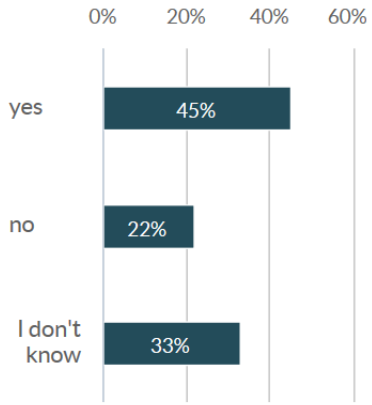

Figure B.29. Responses to question 'Do you think this would be avoidable?' [Scenario 6, disabled voice calls]

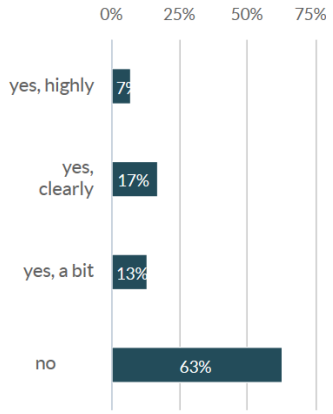

Figure B.30. Responses to question 'Would the awareness of this threat [Scenario 6] decrease your calling to other people?'

Most comments related to this scenario were operator centric, such as "*This type of DoS attack would not be specific to a network operator; it could happen to anyone. If it happened twice though, I would seek a new provider*" or "*If I would know that the other network has better security I may change*". Also other type of comments were presented, such as "*I don't think this is operator dependent. It is more about mobile device security in general*" or "*It is always your own behaviour that affects the situation*".

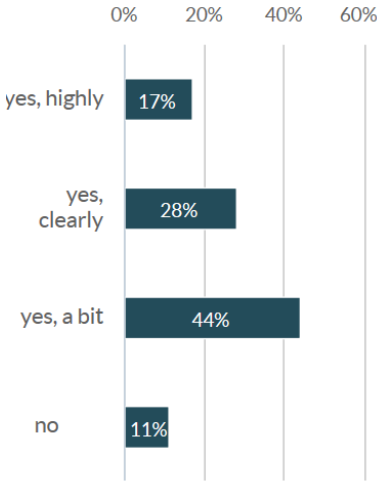

Figure B.31. Would the awareness of this threat [Scenario 6] increase your willingness to change the operator?

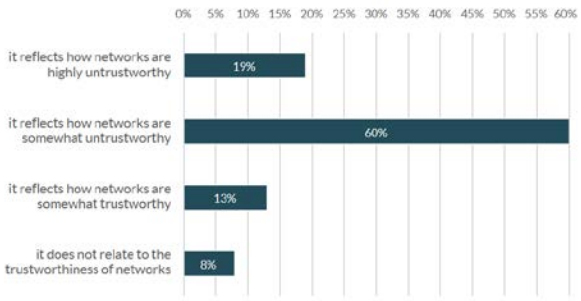

Figure B.32. 'How does this scenario [Scenario 6] relate to your trust on 5G/mobile networks?

B.10 Burglars interfering your home protection system

Scenario 7: Imagine that burglars are interfering with the radio signals of your home protection system so that it does not prevent them to break into your home.

The most usual response related to the possibility of avoiding the interfering with radio signals was positive ("yes", 46%) but compared to most threats presented in this survey, this percentage is a bit lower than usually (the usual being about 60-65%) (Figure B.33).

Somewhat correspondingly, most respondents considered the awareness of this threat to really decrease the usage of mobile networks based burglar system (decreased highly for 28% and clearly for 29% of respondents) (Figure B.34). If it is not possible to avoid, it is wiser to be cautious in behaviour.

Most respondents thought this to reflect how networks are somewhat untrustworthy (Figure B.35). The responses may reflect the severity of the threat to individuals, connected to difficulties in avoiding the threat. The comments were mostly about the way how to avoid this situation. Some concentrated in the design of the system, such as "*Man-in-the-middle and other repeating approaches should be considered in the design phase - whether some other protection than standard in the network should be included*", or "*Improvement of mobile communication protocols can help on this*".

Some comments focused on what an individual can do to protect his/her home: "*It is always your own behaviour that affects the situation*", or "*The key here is not around the mobile network, rather an idea of defence in depth. Is the mobile signal the only thing preventing the burglar breaking in? What about a siren? Or a security door. A burglar could defeat the network, but they should also have to overcome several other deterrence mechanisms*".

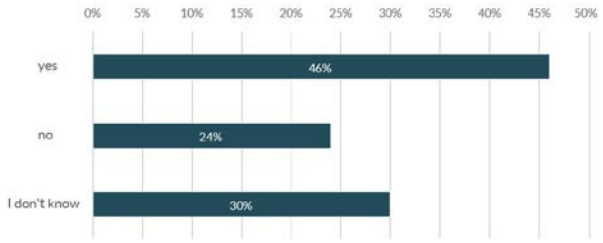

Figure B.33. Responses to question 'Do you think this would be avoidable?' [Scenario 7, burglars interfering home protection system]

Figure B.34. Responses to question 'Would the awareness of this threat [Scenario 7] decrease your usage of mobile networks based burglar system?'

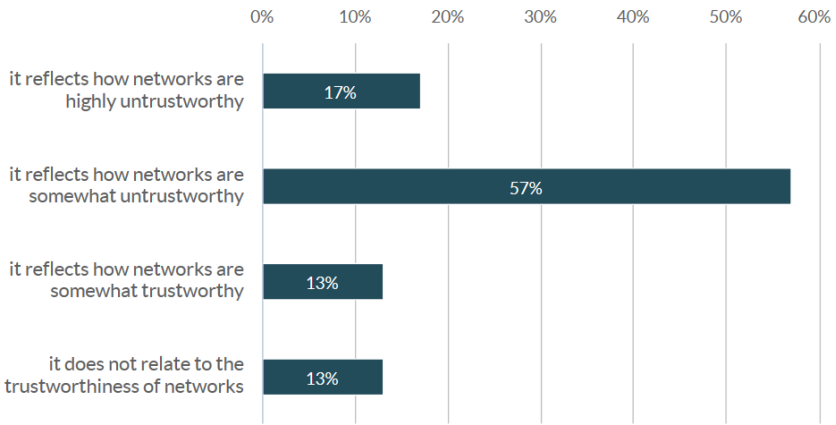

Figure B.35. Responses to question 'How does this scenario [Scenario 7] relate to your trust on 5G/mobile networks?'

B.11 High operator bill due to malicious application

Scenario 8: Imagine that your operator bill is unexpectedly high because the usage of some application has resulted in high data transfer deliberately.

Unlike all other threat scenarios, vast majority (83%) considered it is possible to avoid the threat (Figure B.36). Apparently, respondents were professionals or other type of experts who know how to handle mobile applications. In accordance with this, most respondents would decrease the usage of network applications (the usage would be affected by 26% highly and by 28% clearly, see Figure B.37) – why use the application if you know the threat is present?

This type of threat was not considered to be as much related to the trustworthiness of networks than most threats in this survey; only 41% thought this reflects how networks are somewhat untrustworthy and as much as 31% stated this threat does not relate to the trustworthiness of networks at all (Figure B.38).

Regarding comments provided, part dealt with own preferences, such as "*This is one reason why I prefer unlimited data plans*", "*to avoid I should only use trusted providers or free/flat rate connectivity ;-)*", or "*It is always your own behaviour that affects the situation*".

Others provided general statements (such as "*Creating application like that would create bad reputation for the application developer. It's not going to be a popular threat*") or an explanation (such as "*most likely an application layer issue, not a network issue*", or "*it's a question whether online accounting works in real time (in the order of few seconds lag, which it regularly does not) and timely information to the customer and/or configurable spending limits as well as whether traffic that a recipient (the mobile device) cannot influence/block is accounted/billed towards it*").

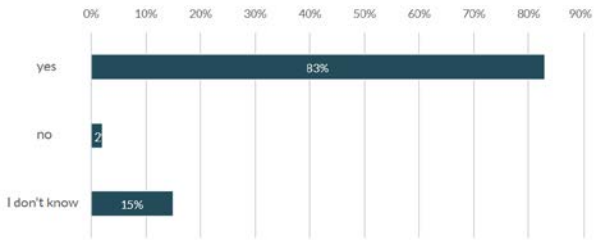

Figure B.36. Responses to question 'Do you think this would be avoidable?' [Scenario 8, malicious application raising operator bill]

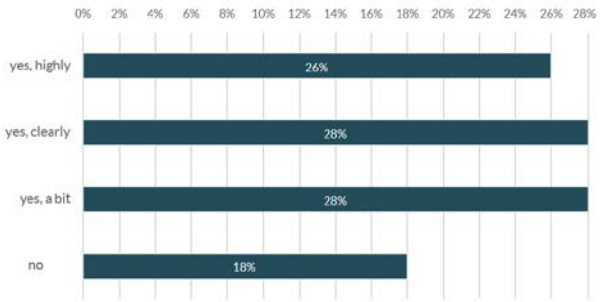

Figure B.37. Responses to question 'Would the awareness of this threat [Scenario 8] decrease your usage of network application?'

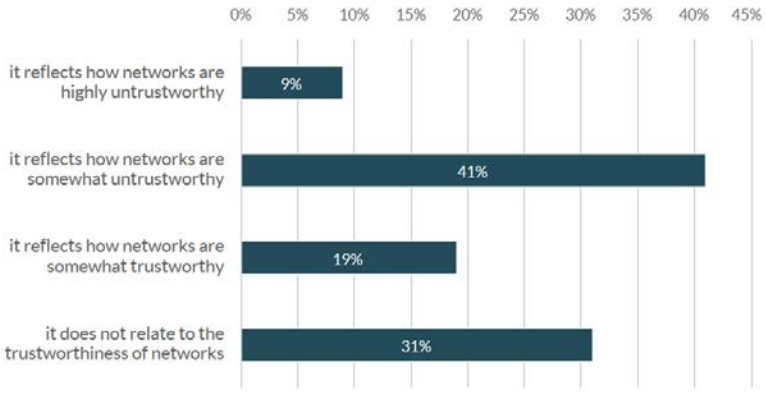

Figure B.38. Responses to question 'How does this scenario [Scenario 8] relate to your trust on 5G/mobile networks?'

B.12 Mobile battery drain due to network-based attack

Scenario 9: Imagine that your mobile device suddenly starts to drain battery excessively, due to a network-based attack.

In accordance with most threats presented in this survey, about 60% of respondents considered the threat (mobile battery drain due to network-based attack) is avoidable (Figure B.39). Probably this threat is not considered to have serious consequences as vast majority thinks this threat decreases only a bit (20%) or not at all (45%) the usage of mobile networks (Figure B.40).

This threat is considered to strongly reflect, though, how networks are somewhat untrustworthy (63%, see Figure B.41). Thus, this threat is conceived to be dependent on networks somewhat more than most threats in this survey as usually the percentage of responses dedicated to this option is around 50%.

Most comments vary again from the behaviour of the user, such as "*best protection to switch off*..."). Some provided technical contemplations, such as "*its a design choice; in 3GPP, network enforces when a mobile must Rx/Tx, so to mitigate the attack a mobile needs control/influence over how much/when/what it is willing to receive (DRX, packet filter) and send control signalling", "If phone is android based, scenario is not avoidable", or "most likely a application layer issue, not a network issue".*

Still some provided an operator related comment, such as "*As before, it is down to what sort of attack can an operator withstand? If it happens once, it is unfortunate, but it should be mitigated and prevented from happening again*" or "*User should pay attention, but a notification of this risk could be useful to decide*".

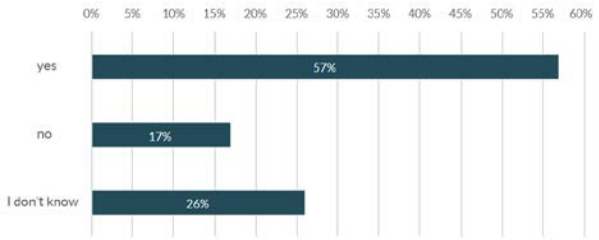

Figure B.39. Responses to question 'Do you think this would be avoidable?' [Scenario 9, battery drain due to an attack?'

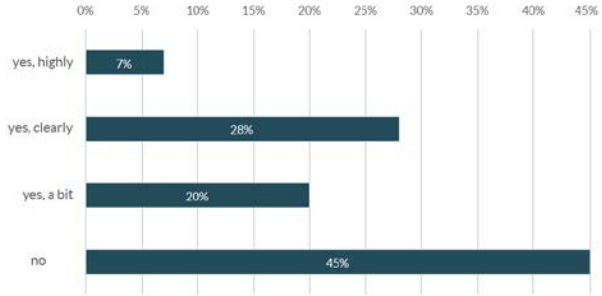

Figure B.40. Responses to the question 'Would the awareness of this threat [Scenario 9] decrease your usage of 5G/mobile networks?'

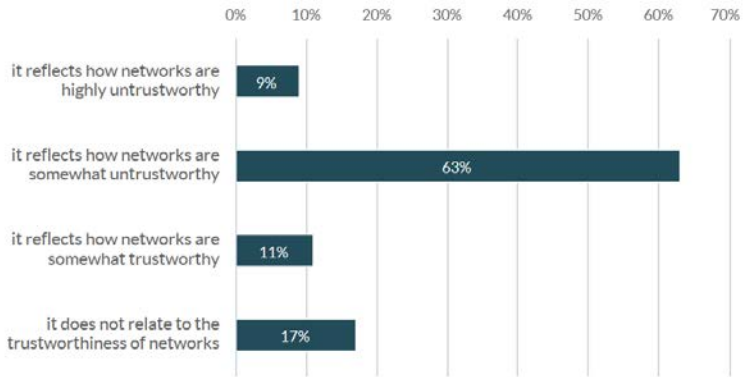

Figure B.41. Responses to question 'How does this scenario [Scenario 9] relate to your trust on 5G/mobile networks?'

B.13 Apparently legal party asks your password

Scenario 10: Imagine that your password is asked via mobile network by an apparently legal party but later it turns out your money is in danger to be stolen.

Most respondents (65%) thought that password stealing via asking about it in network is avoidable (Figure B.44) which is both according to common sense and also in accordance to most responses given to threats presented in this survey.

The amount of respondents contemplating this threat would highly decrease the amount of information provided in Internet (46%, see Figure B.45) is clearly higher than in most threats described in this survey. Also this is according to common sense – one should avoid providing such information.

The threat of being asked for password by an illegal party is not very strongly considered to be based on the trustworthiness of networks is only 41% think this reflects how networks are somewhat untrustworthy and as much as 31% state this does not related to the trustworthiness of networks at all (Figure B.46).

According to the percentages presented above, some respondents think this is a question of own behaviour, such as "*Never provide too much information on the internet*", "*Passwords are dead. They shouldn't be used, or given out to any party legal or not*" or "*It is always your own behaviour that affects the situation*".

Some respondents contemplated the nature of the legal party and/or technical reasons: "*if "apparently legal", I assume end-to-end security was comprised. A comprised communication peer won't relate to trustworthiness of networks, after all, there was no trust in the network in the first place anyway*", "*up to now all my legal parties tell me that they never ask for my password ... but on the other hand it may happen during authentication - I should only use known and reliable access services*", and "*It's a matter of application level security*".

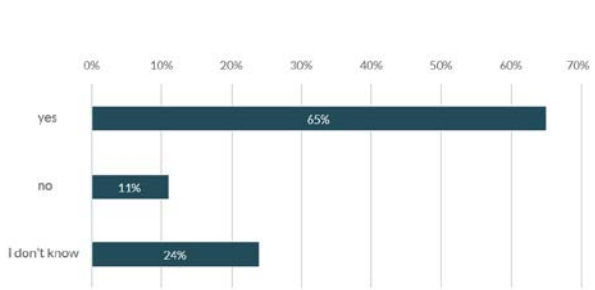

Figure B.44. Responses to question 'Do you think it would be possible to identify this type of situation correctly?' [Scenario 10, apparently legal party]

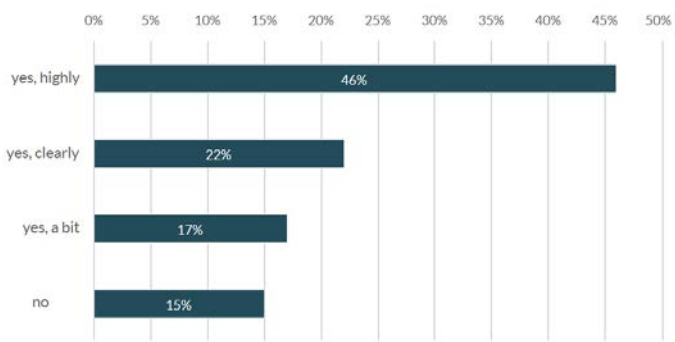

Figure B.45. Responses to question 'Would the awareness of this threat [Scenario 10] decrease the amount of information you provide in Internet?'

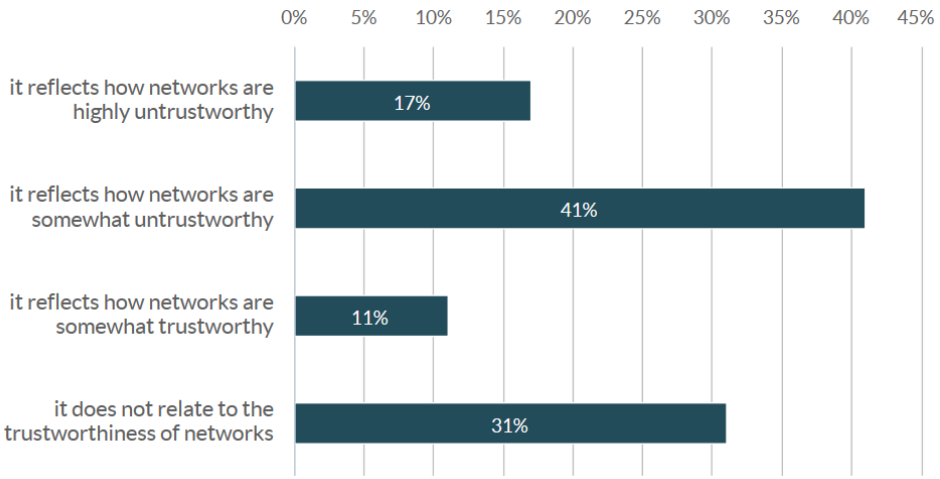

Figure B.46. Responses to question 'How does this scenario [Scenario 10] relate to your trust on 5G/mobile networks?'