Deliverable D2.3
Risk Assessment, Mitigation and Requirements (draft)

Project name	5G Enablers for Network and System Security and Resilience	
Short name	5G-ENSURE	
Grant agreement	671562	
Call	H2020-ICT-2014-2	
Delivery date	23/08/2016	
Lead beneficiary	ALBLF[1]	Linas Maknavicius <linas.maknavicius@nokia-bell-labs.com>
Authors	EAB: Mats Näslund IT Innovation: Stephen C. Phillips, Mike Surridge NEC: Mihai Moraru NIXU: Seppo Heikkinen, Tommi Pernila Orange: Ghada Arfaoui, José Manuel Sanchez Vilchez, Jean-Philippe Wary OXF: Piers O'Hanlon TASE: Ana Jalon Valero, Gorka Lendrino, Carla Salas TIIT: Madalina Baltatu, Luciana Costa, Pier Luigi Zaccone TS: Olivier Bettan, Edith Felix VTT: Jani Suomalainen, Pekka Ruuska	

[1] NOKIA Bell Labs since Jan 14, 2016

Executive summary

This first draft of the Risk Assessment, Mitigation and Requirements deliverable mainly addresses the first two aspects, by proposing a risk assessment and mitigation approach for the selected 5G- ENSURE security use cases. This document is not investigating in this first version the intrinsic risks of new 5G infrastructure and network (which is not yet fully defined). Those investigations will be delivered in subsequent iterations of this document, in particular to address such security issues as those related to the 5G network segments and trust boundaries, 5G slicing concept (RAN and core level and interaction between slices) and issues related to the level of isolation and associated proofs needed, along with efficient remediation capabilities.

This document takes the first steps towards the definition of a risk assessment and mitigation methodology to be followed for the specific task of evaluating the 5G security uses cases and architecture. Firstly we discuss and define terminology. This is essential, as common speech terminology can be quite inexact but in risk management we must be precise. We then review the state of the art in risk assessment and mitigation, understanding what existing methodology, or combination of, suits the evaluation of 5G-ENSURE proposed use cases.

To understand 5G networks we must first understand the proposed architectural framework and its differences when compared to the previous 4G networks. We therefore introduce the conceptual 5G security framework proposed until the present moment within the 5G-ENSURE project (work ongoing).

The Risk Management Context is then defined, looking first at the 5G assets and actors, which is followed by the identification of threats. The 5G-ENSURE risk evaluation methodology for use case analysis is also introduced with some possible approaches to risk likelihood estimation. Nevertheless, the methodology will be refined in the final version of this document (M24), after examination of each of the approaches, especially for factors such as risk severity, impact and the level of control of remediation.

The core chapter provides an initial threat analysis of representative use cases defined by the 5G ENSURE project, after the threat description formalism (template) is introduced. As agreed by the 5G-ENSURE partners, the focus is made on the ‘internal’ threats in this draft document, i.e. those derived from 5G-ENSURE specific use cases are only analyzed in this first version, as they capture the very essence of security and privacy aspects of 5G networks as seen by the project.

The chapter 6 gives some initial design recommendations with respect to the analyzed 5G threats.

As this document is a “draft” risk assessment methodology, the next steps to be done are set out alongside the conclusions chapter. In particular, the final version of the deliverable ‘D2.3 Risk Assessment, Mitigation and Requirements’ will comprise the following parts: full threat analysis (including ‘external’ threats coming from other sources than 5G-ENSURE use cases), their categorization, prioritization with regard to severity and impact, complete mitigation and remediation recommendations, functional requirements and architectural options (towards T2.4), definition of relevant metrics for use of security monitoring, as well as penetration tests over the security testbed and gap analysis (related to WP4).

Foreword

5G-ENSURE belongs to the first group of EU-funded projects which collaboratively develop 5G under the umbrella of the 5G Infrastructure Public Private Partnership (5G-PPP) in the Horizon 2020 Programme. The overall goal of 5G-ENSURE is to deliver strategic impact across technology and business enablement, standardisation and vision for a secure, resilient and viable 5G network. The project covers research & innovation - from technical solutions (5G security architecture and testbed with 5G security enablers) to market validation and stakeholders engagement - spanning various application domains.

The document has been written in cooperation with the D2.2 'Trust model (draft)' contributors (as for the common terminology and a sub-set of most important use cases covered). This draft version it is primarily nourished by D2.1 'Use cases' deliverable for the derivation of major 5G threats as seen by the consortium and, along with the trust model, feeds into the work on architecture currently under investigation and to be reported in D2.4. Of course, the risk assessment, mitigation and especially requirements also contribute to the work underway in WP3 in all tasks for security enabler definitions.

Disclaimer

Copyright notice

Contents

1 Introduction

5G network architecture is significantly different from the architectures of any previous generation network, where new network technologies are proposed both for the access and core network infrastructures, new actors (stakeholders) arise and novel business models are made possible. The attack surface is bigger because of massive number of connected devices, the virtualization techniques to be used in 5G, the support for open networks, etc. We foresee that 5G systems design and deployment will raise numerous security challenges and resulting risks, like:

- related to network virtualization (specific mobile and multi-tenant VNFs, sensitive data isolation etc.);
- risks induced by wireless network topology: multi-RAN, HetNets, multi-hop, D2D, unlicensed spectrum as alternative access…;
- new services (plain "old" communication services, utilities, mission-critical applications, M2M/IOT/sensors, V2X…) will co-exist and thus will necessitate devising particular end-to-end 5G security architecture allying optimization and complexity of the system.

Therefore the Risk assessment for 5G must be carefully studied and defined by examining the current methodologies and coming with a comprehensive model that will best adapt to the new network architecture, stakeholders and business models. Our approach is to perform a risk assessment and mitigation evaluation related to multi-stakeholder 5G system and NFV, comprising new risks and modifying existing ones. Those studies will be finalized in the second version of this document (M24).

2 Terminology

Risk assessment and mitigation is of interest in many different research IT disciplines, but also in military and civil industry, economics, etc. To avoid the problems of 'jargonised' terminology, we propose to follow a common definition alongside the whole 5G-ENSURE project, therefore a terminology which is also shared with the project's deliverable D2.2 'Trust model (draft)' [2].

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).

3 Methodology/related work

There are a number of documents from different standardization bodies addressing the issues of threat and risk assessment and mitigation in computer or telecommunication networks. In this document we provide a brief description of the standard well consolidated methodologies which have been taken into account by the 5G-ENSURE project.

ITU-T Recommendation X.805 "Security architecture for systems providing end-to-end communications" [3] has been developed by ITU-T SG 17 (ITU-T Lead Study Group on Telecommunication Security) and was published in October 2003. This architecture provides a structured framework that forces the consideration of all possible threats and attacks to provide comprehensive end-to-end network security. It is based on the concepts of:

- Security Layers (Infrastructure Security Layer, Services Security Layer, Applications Security Layer): they represent a hierarchical approach to securing a network. Each Security Layer has unique vulnerabilities, and specific threats. For this reason each of these layers must be addressed when creating an end-to-end security solution because at each point the network may be exposed to a new risk, threat or attack.
- Security Planes (End-User Security Plane, Management Security Plane, Control/Signaling Security Plane): they represent the types of activities that occur on a network. Different security vulnerabilities may exist in each of these planes and each plane along with the three layers must be secured in order to provide an effective security plan.
- Security dimensions (access control, authentication, Non-Repudiation, Data Confidentiality, Communication Security, data integrity, availability, privacy): they represent the classes of actions that can be taken or technologies that can be deployed in order to counteract threats or potential attacks present at each security layer and plane.

The ITU-T X.805 Security Architecture is illustrated in the following figure (Figure 1). In the ITU X.805 standard the definition of threats makes reference to another document (X.801) [4], which, in turn, does not contain any further useful threat description, at least as far as telecommunication networks are concerned.

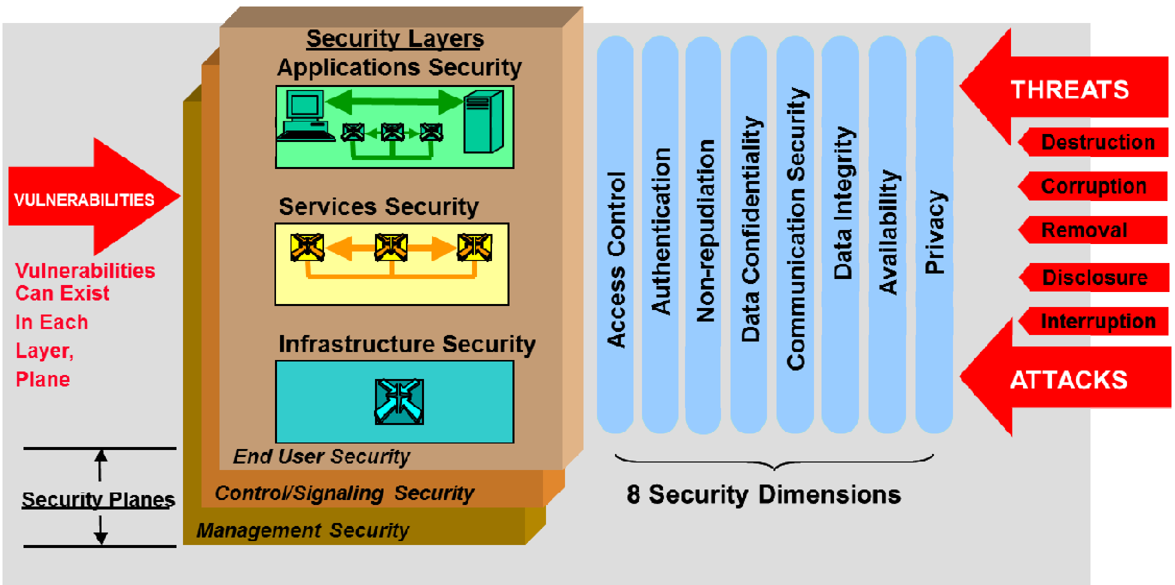

Figure 1. ITU-T X.805 Security Architecture for Systems Providing End-to-End Communications

A further document, NIST SP800-30, "Risk Management Guide for Information Technology Systems" delivered by NIST (National Institute of Standards and Technology) [5], presents a guide for risk assessment, evaluation and mitigation more specifically related to IT systems (networks included). The risk assessment process in SP 800-30 takes inputs from a preparatory step that establishes the context, scope, assumptions, and key information sources for the process, and then uses identified threats and vulnerabilities to determine their likelihood impact on assets and risk. Figure 2 gives an overview of the key steps required in order to complete a comprehensive risk assessment program as outlined in NIST SP 800-3.

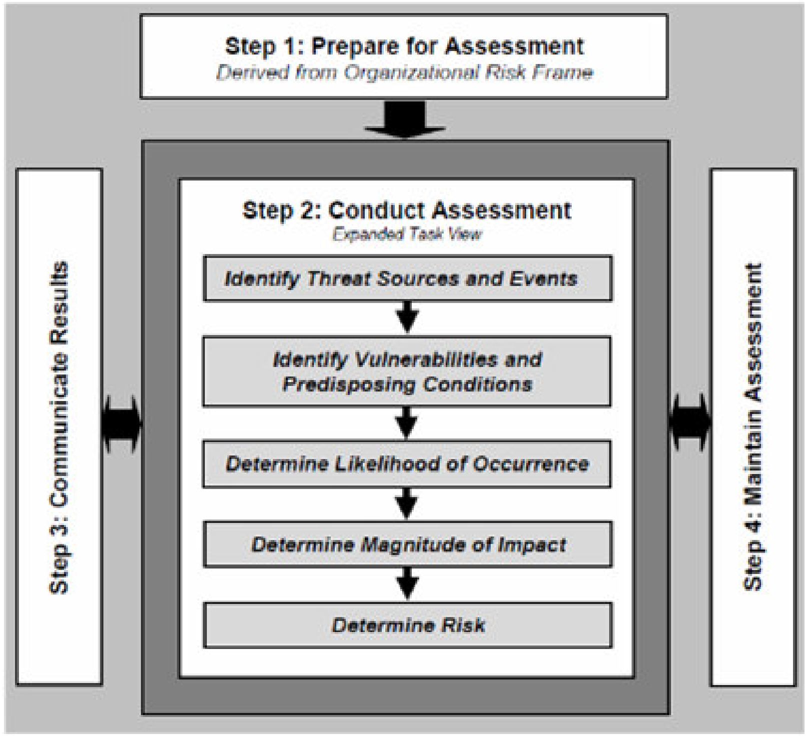

Figure 2. NIST SP800 -30 is "Risk Management Guide for Information Technology Systems"

Yet another standard, the ISO/IEC 27005:2011 'Information technology - Security techniques - Information security risk management' [6] contains the description of the information security risk management process and its activities, which include context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review.

The context establishment consists of:

- Setting the basic criteria such as the risk management approach, the risk evaluation criteria, the impact criteria and the risk acceptance criteria;
- Defining the scope and boundaries of the risk management;
- Defining the organisation and the responsibilities for information security risk management.

The risk assessment consists of:

- Identifying the risk by considering the assets within the defined scope, the threats, the vulnerabilities that can be abused by threats having a negative impact on the assets
- Estimating the risk by selecting the risk analysis methodology (which can be qualitative, quantitative or mixture of both) by defining the likelihood and determining the risk level for all relevant incident scenarios.
- Evaluating the risk evaluation by comparing the level of risk against the risk evaluation criteria and the risk acceptance criteria (defined in the context establishment).

The risk treatment consists of:

- Selecting four different options (risk removing, retention, avoidance, sharing) by considering the outcome of the risk assessment, the expected cost for implementing these options and the expected benefits from these options.

The purpose of ISO 27005 is to provide guidelines for information security risk management. It does not specify, recommend or even name any specific risk analysis method, although it does specify a structured, systematic and rigorous process from analysing risks to creating the risk treatment plan. For this reason the terminology and concepts used in ISO 27005 are widely accepted.

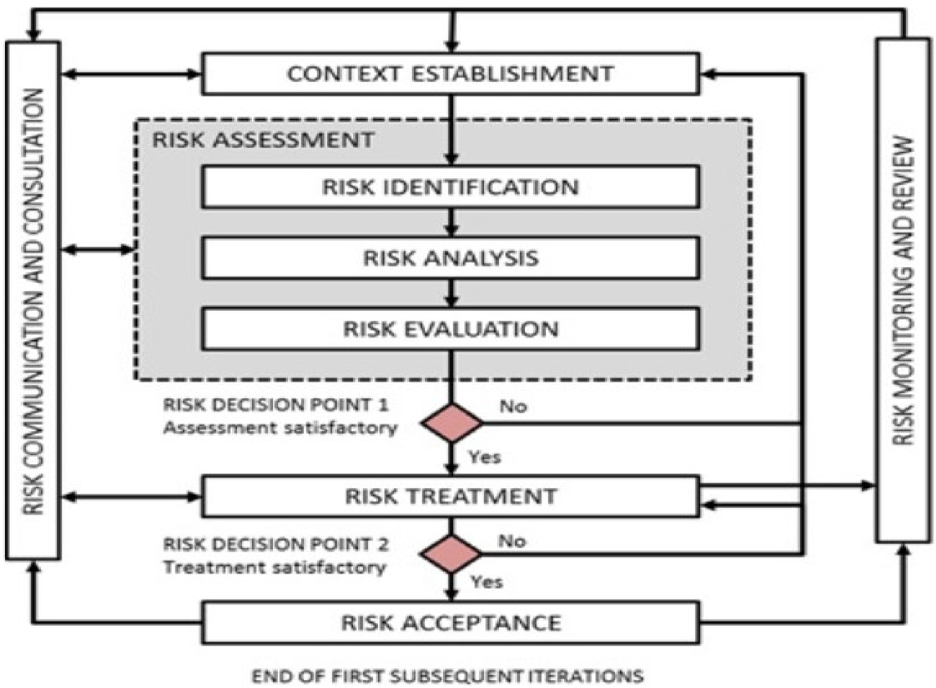

Figure 3. ISO/IEC 27005:2011 Information security risk management process

As a final remark on the methodologies, we want to outline that we have also considered the literature addressing the limits of the traditional well consolidated risk assessment methodologies we have considered herein [7]. It turns out that the traditional approaches, where assets are persistent items or properties of value and have owners, would work at their best in situations where the evaluated IT systems run in closed environment within an organization and therefore have unique owners, which is not always the case for 5G systems. For example, all roaming scenarios, and VMNOs which do not actually own the equipment (even though we can subdivide assets into the “service” of the operator and the actual hardware of the infrastructure owner). Nonetheless 5G-ENSURE adopts a traditional approach as the alternatives would require a larger consensus. For simplification the proposed methodology application will have to be reiterated for each security layer, and by each asset owner at the infrastructure layer. The higher services and application layers will have to take into consideration an inherent risk posed by threats/attacks at the infrastructure layer.

4 Risk Management Context – Threats in 5G-ENSURE Use Cases

The methodology which will be used within the 5G-ENSURE project for the risk assessment is based on the Risk Management Process (ISO 27005) and, especially, on its simplification represented by NIST SP-800-30. We have based the process on this standard mainly for its wide-spread acceptance and usage in the IT industry and because it provides a complete well-defined and consistent terminology and methodology for risk management.

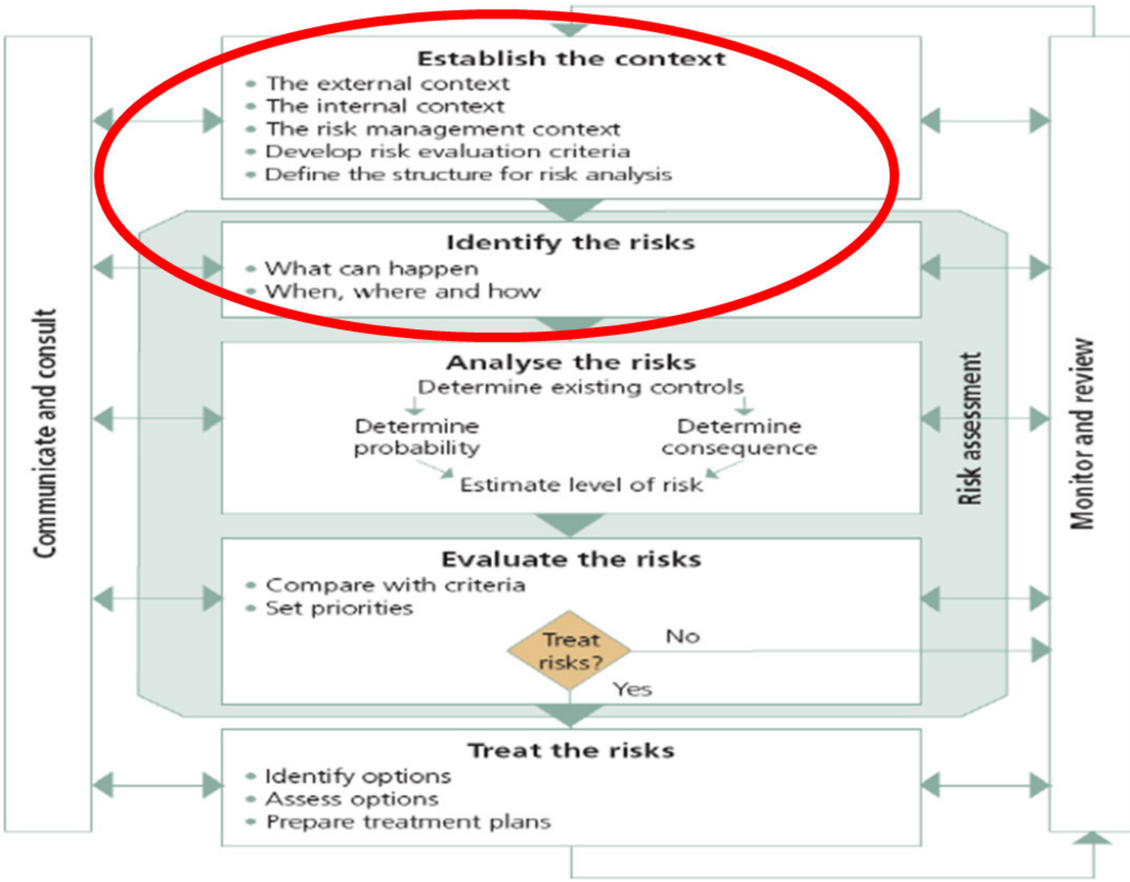

Figure 4. Complete Risk Assessment Procedure

According to the ISO 27005 standard, the Risk assessment process has 3 main parts, which will be detailed in the rest of the document:

- Risk identification
- Risk analysis
- Risk evaluation

Before going further, a reference 5G security architecture will be illustrated, even if we must keep in mind that this is ongoing work within 5G-ENSURE and could change during the project's life.

4.1 The reference 5G security framework

The reference 5G security architectural framework, where these risk assessment processes will be applied, is still under definition within the project's task 2.4. Nevertheless, we can already consider herein a first high level architectural considerations proposed by the 5G-ENSURE project for 5G.

In particular, the concept of domain in 5G network and system has to be defined. A domain is traditionally (3G and 4G networks) the highest-level group of physical entities. Reference points are defined between domains.

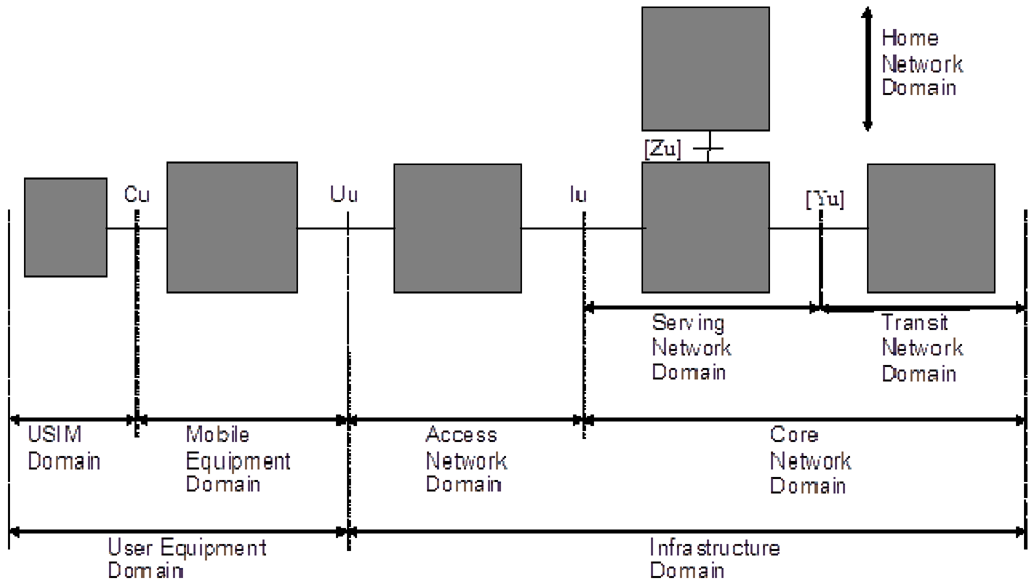

Figure 5. Domains defined in TS 23.101

This 4G domain structure may remain valid in 5G with the following considerations requiring adaptations and associated risk impact:

- in 5G we may have 3rd party ID providers (that may affect the home network domain)
- in 5G in the User Equipment domain we may have direct connections between UEs
- in 5G we may have several Infrastructure domains from different providers (owners), such as access/core/transit network or cloud infrastructure providers
- User Equipment and Infrastructure domain will remain as physical grouping
- the USIM, Mobile Equipment, Access Network and Core Network domains may to some degree remain as physical entities and will certainly remain valid as "trust domains".

The main concept not illustrated in the current domain's definition is the slicing concept introduced in 5G.

A draft security domains proposal for 5G which considers subdivision of domains and slicing is presented in Figure 6 (acronyms: "SN" = Serving Network, "AN" = Access network, "IM" = Identity Management, "ID" = Infrastructure providers e.g. ID2 could be Amazon EC2, "Rn" = Resource 1,2..n, etc.).

Specifically we use the following draft definition of **5G domain**:

- "A grouping of network entities according to physical *or logical* aspects, *relevant for 5G networks*."

Physical grouping is similar to 23.101. Logical groupings can be according to similarity in functionality (e.g. "RAN vs CN") or administrative/ownership related (e.g. "home vs serving", "operator vs 3rd party vertical" or "infrastructure provider vs tenant").

We propose to also add the concept of compound domains. **Slices**, as special services offered to 5G users seem to be an example of this since they may be "transversal" (e2e) to other domains. Slicing is indeed a major concern, on which strong security risk analysis has to be done.

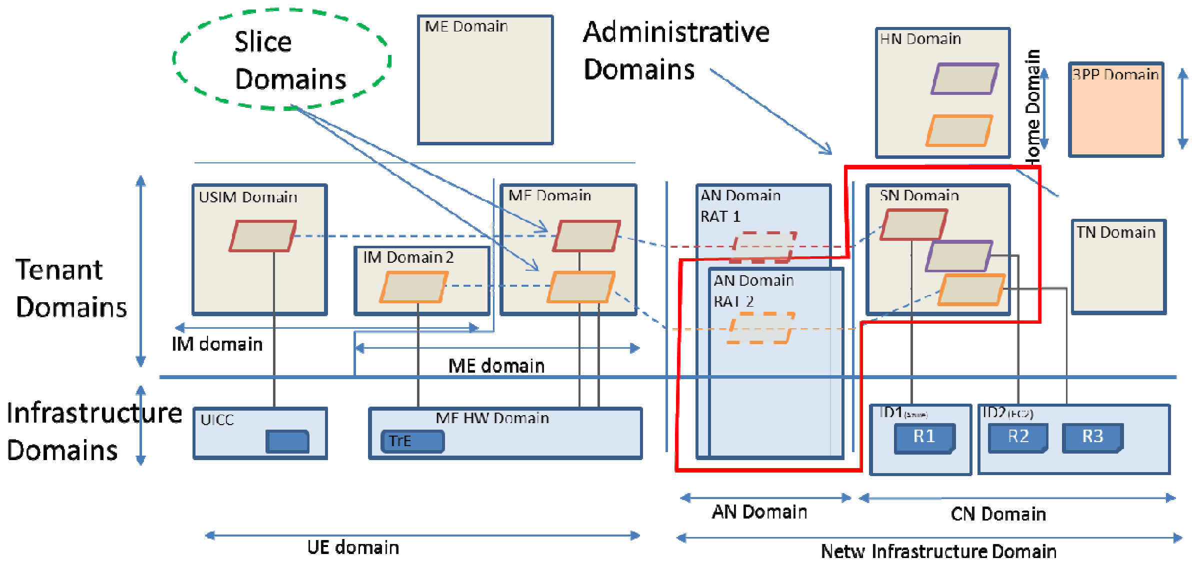

Figure 6. 5G-ENSURE Security domains proposal

The functionality and communication protocols used in this domains structure maps to the **functional/logical strata** shown in Figure 7. **A stratum** (in 23.101 parlance) is defined as "Grouping of protocols, *data and functions* related to one aspect of the services provided by one or several domains" (e.g. home stratum contains the protocols and functions related to the handling and storage of subscription data: functions related to subscription data management, customer care, including billing and charging, mobility management and authentication are located in this stratum).

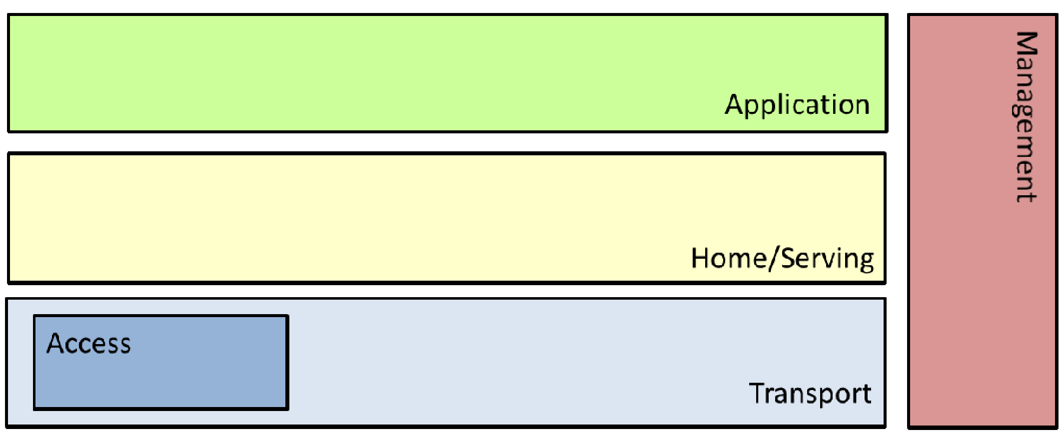

Figure 7. Strata

The application, home, serving and transport strata have been already identified within UMTS and remain the same in 5G, while the management stratum was not included before. **Management stratum** contains the protocols and functions related to network configuration: this includes the functions of creating and deleting virtualized networks and network slices. It also contains SDN specific protocols like OpenFlow and northbound APIs for network applications. Furthermore, network monitoring functionalities are also contained in the management stratum. Several issues are still to be addressed, e.g. if there is a need for a sub-stratum for security management or for monitoring (for detecting security anomalies, intrusion detection, lawful interception in a dynamic 5G network)? How to reflect multi-party trust issues? These are being discussed in ongoing D2.4 (5G-ENSURE security architecture) work.

For risk assessment purposes we note that these logical architectural views present a one to one mapping to the security planes defined in ITU-T X.805, which makes us more confident that the right approach is being followed in the initial steps of context establishment.

Further investigation of risk analysis with regard to 5G security architecture will be delivered for the next version of the present document.

4.2 Risk Identification

The purpose of risk identification is to determine what factors can cause a potential loss/damage, and where and how it might happen (ISO, 2011). In order to manage the risks, it is necessary to identify the assets, consider the threats that could compromise those assets, and estimate the damage that the realization of any threat could pose to them.

4.2.1 5G-ENSURE Assets Identification

The first step is the identification of all the assets, within the 5G scope, that need to be protected, with special attention to those that are considered most critical because they cause most damage if compromised.

As a first step towards the assets identification we looked at the available taxonomies and we found a very simplified but still useful one from ENISA [12], where the main assets of a mobile network are grouped into the following 7 categories:

- Data Plane Assets:
    - *Network Elements*
    - *Communication medium*
- Control Plane Assets:
    - *Software*
    - *Hardware*
    - *Data*
- Application Plane Assets:
    - *Software*
    - *Hardware*
- Service provider IT Infrastructure:
    - *IT Infrastructure*
    - *Billing systems*
    - *Operator data*
    - *End user data*
- Network service provider physical infrastructure:
    - *Facilities*
    - *Energy Power*
- SDN users:

    - *End user data*
    - *SLAs and regulations*
- Human agents:
    - *SDN Administrators*
    - *SDN Application Developers*
    - *Network Service Operators*
    - *End User Application Developers*
    - *End User Application Administrators*
    - *End User Service Providers*
    - *End Users.*

The approach adopted within the 5G-ENSURE project was to start with this high level set of assets and try to come with more specific assets by focusing on a generic 5G mobile network vision. This list has been extended to contain the assets related to SDN and NFV technologies, since they will be largely used to implement the 5G mobile network.

In the rest of this section, we provide an enriched 5G assets list with a focus on mobile network vision. Though, we also propose a list of assets related to SDN and NFV technologies which can be used to implement the 5G mobile network.

We distinguish three types of assets: “Primary assets” which are functions and components related to a mobile network, “Secondary assets” which are associated to the technologies used to implement the mobile network (i.e., SDN and NFV technologies), and “actors” which are users and organizations participating to the 5G security use cases mainly described in D2.1.

Note that in the threat description tables from Chapter 5 we will indicate the ENISA high level asset categories in order to keep the tables simple and legible. More detailed 5G-ENSURE asset specification can be provided by each use case by filling in the appropriate field in the “Other” category.

4.2.1.1 Primary assets

We consider the following primary assets [9], [10]:

- **Components:** these are physical machines and servers used to provide mobile network functions.
    - **User equipment:**
        - **Secure Element:** This is a tamper resistant platform, e.g. certified at EAL4+.
        - **Mobile Equipment**
    - **Access Network**
        - **Base Station:** This is the antenna and hardware running functions related to radio transmission and reception such as Radio resources management, Mobility management and Security (i.e., confidentiality and integrity protection).
    - **Core Network:** This includes hardware servers used to run core network functions (home or serving).
- **Functions**
    - **Radio Resources Management:** allocation and maintenance of radio resources
    - **Mobility Management:** handover and inter-working management
    - **Session Management**
    - **Accounting and Charging**

- **Security Management**
  - **Authentication and Authorization**
    - The authentication of mobile users
    - Authentication of “admin” personnel, network management , inter-network node authentication etc
  - **Confidentiality Protection**
    - core network encryption
    - air interface encryption
  - **Integrity Protection**
  - **Cryptographic Key Management**
    - Key Derivation: derivation of session and hierarchical keys
    - Key distribution: e.g. TLS keys for encryption of authentication protocols
    - Key Agreement

- **Services**
  - **IP connection:** Allocation and maintenance of IP addresses, naming resolution and, flow forwarding definition.
  - **Basics:** Voice / SMS
  - **Slice-specific service:** e.g. for critical MTC

4.2.1.2 Secondary assets

We consider the following secondary assets [11]:

- **SDN assets**
  - **Control Plane**
    - **Entities:** an entity has a given role(s) and performs one or several functions.
      - **SDN Controller**
    - **Functions** (realized by the entities)
      - **Network Topology discovery**
      - **Forwarding installation:** pushing forwarding rules from SDN controller to switches
    - **Components:** these are physical machines and servers over which an SDN controller can run.
  - **Data Plane**
    - **Components**
      - **Switches**
      - **Hosts**
    - **Functions**
      - **Forwarding execution**
- **NFV assets**
  - **Entities:** an entity has a given role(s) and performs one or several functions.
    - **NFV Orchestrator:** resource management of the NFV infrastructure and, lifecycle management of network services (e.g., instantiation, scale-out/in, performance measurement results, event collection and correlation, termination).
    - **VNF Manager:** life cycle management of VNF instances.

    - **VIM:** controlling and managing the NFV infrastructure compute, storage and network resources and, collection and forwarding of performance measurement results and faults/events information relative to virtualized resources.
  - **Functions** (realized by the entities)
    - **Resource management**
      - **Storage management**
        - **Isolation**
      - **Resource allocation**
        - **Virtual link allocation**
        - **VNF allocation**
      - **Post deployment VNF operations**
        - **VNF creation**
        - **VNF deletion**
        - **VNF scaling-out**
        - **VNF scaling-in**
        - **VNF scaling-up**
        - **VNF scaling-down**
        - **VNF updating**
    - **Security management**
      - **Confidentiality protection**
      - **Integrity protection**
      - **Trust boot (root of trust)**
  - **Components**

4.2.1.3 Actors

The actors are organizations and users that participate in use cases described in D2.1. They have been fully listed in the proposed 5G Trust model described in deliverable D2.2 [2]. We can summarize the 5G actors in the following succinct list and in Figure 8:

- Mobile/Satellite 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
  - Virtual mobile network operator (VMNO) who purchases SDN slices from an Infrastructure Provider
  - Factory or enterprise owner operating a AAA in a network linked to a (V)MNO
  - *Note that all (V)MNO entities submit to telecom regulation framework*
- Infrastructure Provider, including Virtual infrastructure provider (VIP), and satellite/HAPS provider
  - *those actors do not submit to telecom regulation framework, as they deliver technical services, as subcontractors, to operators (in the scope of their regulation framework)*
- Interconnect network provider
- Network access provider
- Service Provider including OTT/3rd Party service provider; commonly also the (V)MNO

- Network software provider, including VNF provider; commonly also the network equipment manufacturer
- Network equipment manufacturer
- User equipment manufacturer, including phone, USIM, sensor and robot
- User equipment software developer/provider, including OS, app and app store
- End user, including phone users, WSN owner/operator and enterprise employee
- Regulators, law enforcement agencies

An overall summary of 5G assets and actors is provided in Figure 8 below.

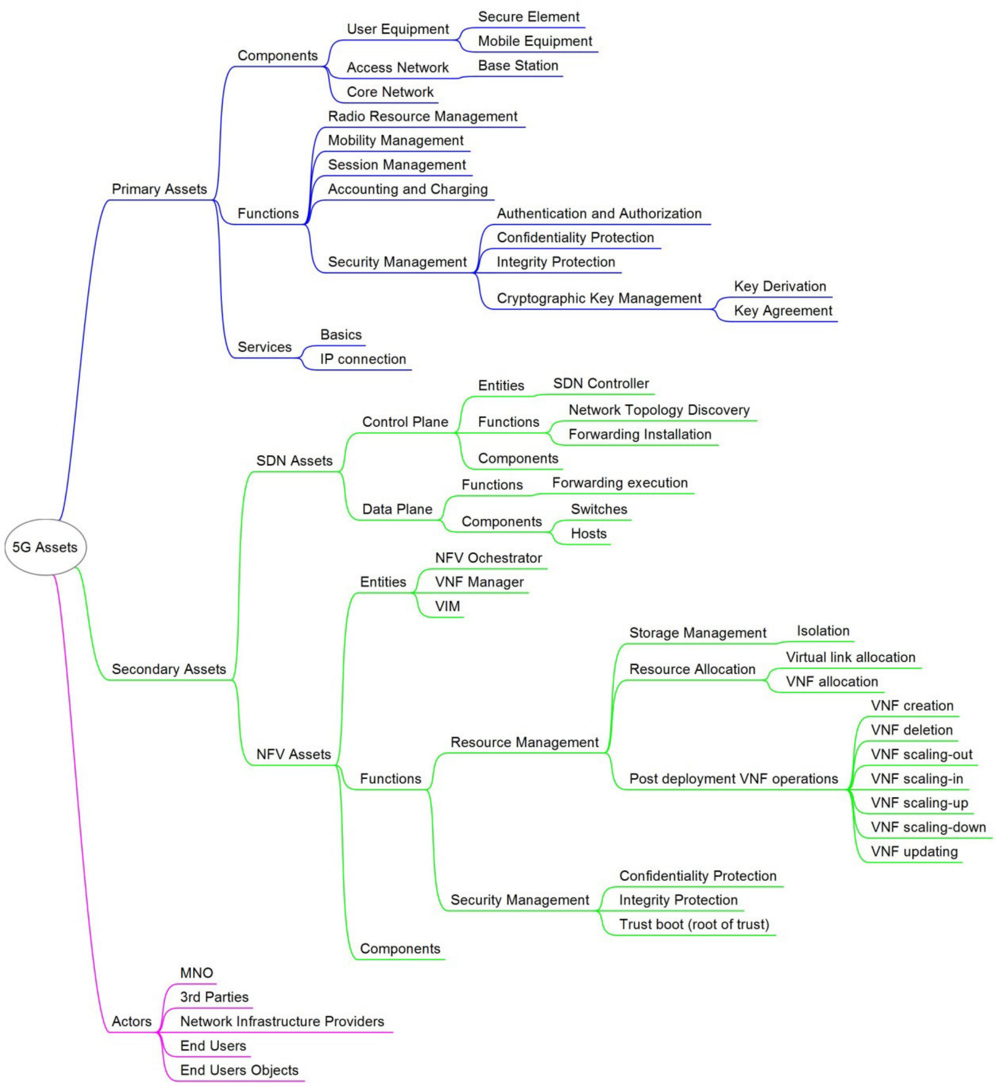

Figure 8. Summary of 5G Assets

4.2.2 5G-ENSURE Threat Identification and categorization

A threat analysis must start with a thorough threat taxonomy and identification in each specific context. A threat has a potential to exploit vulnerabilities and harm assets. Threat identification can be made based on history of previous incidents (if it exists) or an external threat catalogue. The approach adopted in this document has been to perform the identification of relevant threats through an assessment of a subset of use cases reported in the first technical deliverable of the project, D2.1. All use cases are evaluated regarding the possible threats to the list of asset reported in section 2.1.1. The advantage of this approach if compared to the one based on a predefined list of threats is that it can allow one to address the 'known unknown' or the 'unknown unknown' threats and therefore it allows for identification of individual threats depending on the specific context.

For this reason a set of the 5G use cases defined in D2.1 has been used to drive the threat analysis. The use cases have been analysed to gain an understanding of:

- the main threat/s the use case is exposed to
- the vulnerability exploited by the threat (threat's description)
- the category the threat belongs to
- the impact caused by the threats
- the assets the attacker would be interested in
- the entry point where a potential attacker could interact with the service and/or business-model described in the use case
- possible mitigation that is the set of controls or measures that could prevent the threat from causing impacts

The threat analysis based on 5G-ENSURE use cases is carried out using a clearly defined structure, to ensure that the correct information has been collected. For this purpose a specific template has been defined to derive threat descriptions from 5G-ENSURE use cases and facilitate the risk analysis associated with each threat. The template is illustrated in the following Figure 9.

ID: Unique ID # of the threat	*Numbering scheme: <T_UC-number_associated-threat-number>,* *e.g.* T_UC1.3_1, T_UC1.3_2, T_UC5.3_1, …
Name: Brief name of the threat	
Description: Detailed description of threat and its importance	
Category: ITU-T X.805 security dimension(s) – tick the appropriate box(es)	☐ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☐ Privacy

Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	
Assets impacted: What assets could be damaged? – from ENISA 5G/SDN asset categories, and/or others	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	

Entry Points (optional, if known): What possible means does an adversary have?	
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

Figure 9. Threat description template

There are various ways to classify the threats to a given system. A threat classification identified to be useful for the purpose of the 5G-ENSURE project is the one provided by ENISA in the *Threat Landscape for SDN/5G* [12]. The threat taxonomies in the form of a mind map is shown in the following figure.

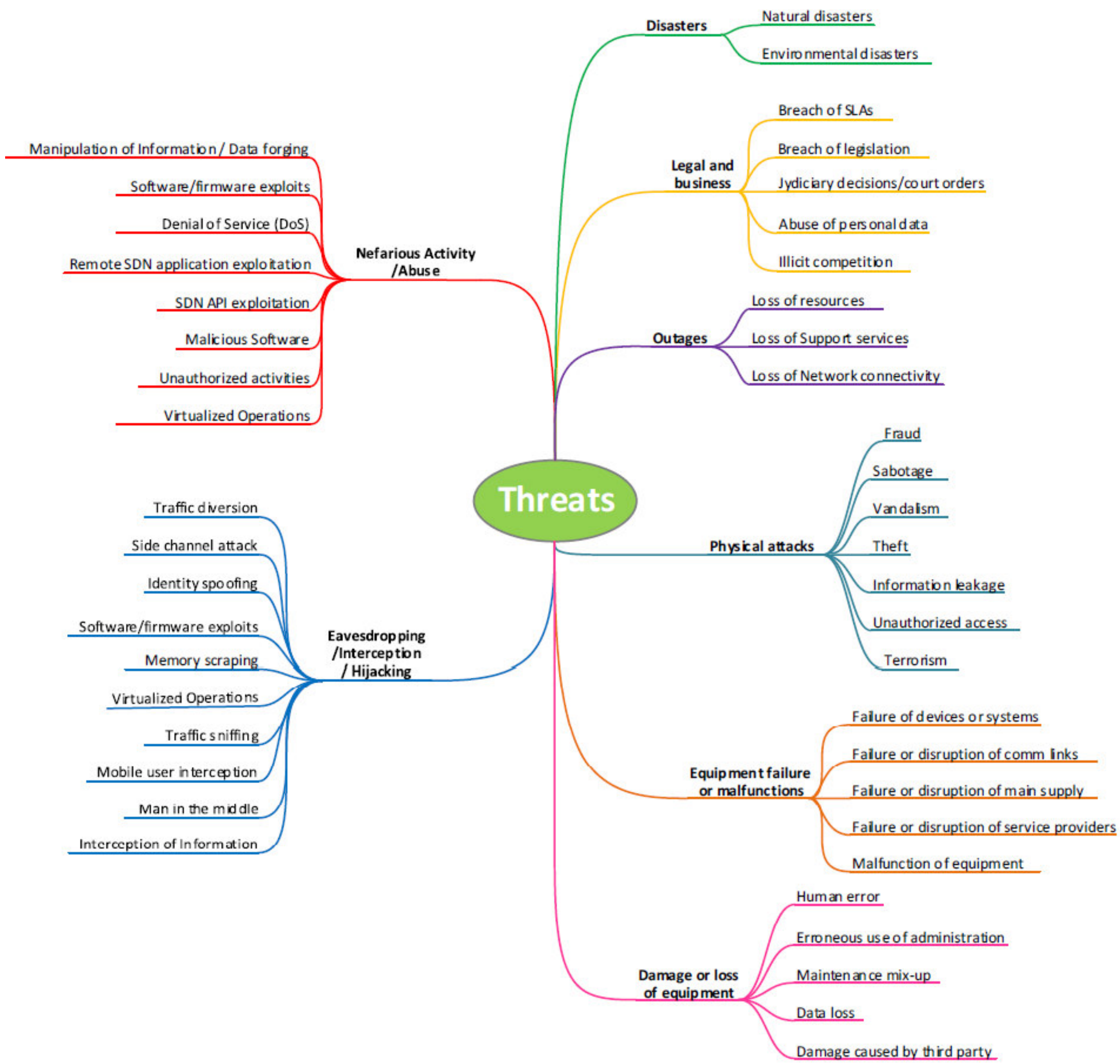

Figure 10. Lists of SDN/NFV/5G and Generic Network Threats (source ENISA)

The left side of the map lists the *threats specific to SDN/NFV/5G* referring to the categories:

- Nefarious Activity/Abuse
- Eavesdropping/Interception/ Hijacking.

The right side of the map lists the *generic network threats* referring to the categories:

- Disasters
- Legal and business
- Physical Attacks
- Outages
- Equipment Failure or malfunctions
- Damage or loss of equipment

The threat taxonomy from ENISA that is considered useful for the scope of the project is the one related to SDN/NFV/5G threats. Since having only two categories was considered too restrictive for the inclusion of the threats identified with the use cases analysis, it was decided to categorize the threats based on the ITU-T X.805 "security dimensions" herein reported:

- Access control
- Authentication
- Non-repudiation
- Data confidentiality
- Communication security
- Data integrity
- Availability
- Privacy

The list of threats derived from the analysis of the subset of 5G-ENSURE use cases (see full threat description in Chapter 5) and categorized based on the ITU-T X.805 security dimensions is reported in the following table.

Threat Category	Threats derived from 5G-ENSURE use cases in D2.1
Access Control	• *Unauthorised activities related to satellite devices or (satellite) network resources* • *Fake roaming from terrestrial network into satellite network (and vice versa)* • *Compromised authentication gateway* • *Unauthorized data access* • *Misbehaving control plane* • *Add malicious nodes into core network* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Hardening or patching of systems is not done* • *Unauthentic device installed into the system*
Authentication	• *Fake roaming from terrestrial network into satellite network (and vice versa)* • *Compromised authentication gateway* • *Leaking keys* • *Unauthorized data access*

	• *Misbehaving control plane* • *Security threats in a satellite network* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Spoofed signalling messages*
Non-repudiation	• *Compromised authentication gateway* • *Manipulation of forwarding logic* • *Security threats in a satellite network* • *Service failure over satellite capable eNB* • *Spoofed signalling messages* • *Disputes in charging* • *Compromised / malicious LI (Lawful Interception) function*
Data confidentiality	• *Fake roaming from terrestrial network into satellite network (and vice versa)* • *Mobile user interception and information interception* • *Compromised data* • *Compromised authentication gateway* • *Leaking keys* • *Unauthorized data access* • *Misbehaving control plane* • *Add malicious nodes into core network* • *Forwarding logic leakage* • *Manipulation of forwarding logic* • *Security threats in a satellite network* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Spoofed signalling messages* • *Disclose of sensitive data* • *Nefarious activities (malicious software, unauthorized activities, interception of information): privacy violations* • *Nefarious activities (manipulation of information, interception of information): personal information disclosure* • *Compromised / malicious LI (Lawful Interception) function* • *Nefarious activities (manipulation of information, interception of information) over LI-aware network*
Communication security	• *Mobile user interception and information interception* • *Compromised data* • *Compromised authentication gateway* • *Leaking keys* • *Unauthorized data access* • *Misbehaving control plane* • *Add malicious nodes into core network* • *Forwarding logic leakage* • *Manipulation of forwarding logic* • *Misuse of open control and monitoring interfaces* • *Unauthorized access to a network slice*

	• *Bogus monitoring data* • *No control of Cyber-attacks by the Service providers* • *Compromise the availability and integrity of the radio interface* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Hardening or patching of systems is not done* • *Unauthentic device installed into the system* • *Nefarious activities (manipulation of information, interception of information) over LI-aware network*
Data integrity	• *Compromised data* • *Compromised authentication gateway* • *Leaking keys* • *Unauthorized data access* • *Misbehaving control plane* • *Add malicious nodes into core network* • *Manipulation of forwarding logic* • *Security threats in a satellite network* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Spoofed signalling messages* • *Disclose of sensitive data* • *Compromised / malicious LI (Lawful Interception) function* • *Nefarious activities (manipulation of information, interception of information) over LI-aware network*
Availability	• *Fake roaming from terrestrial network into satellite network (and vice versa)* • *Authentication traffic spikes* • *Compromised authentication gateway* • *Unauthorized data access* • *Misbehaving control plane* • *Add malicious nodes into core network* • *Manipulation of forwarding logic* • *Fingerprinting attack* • *Misuse of open control and monitoring interfaces* • *Unauthorized access to a network slice* • *Bogus monitoring data* • *Security threats in a satellite network* • *Compromise the availability and integrity of the radio interface* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *Service failure over satellite capable eNB* • *Spoofed signalling messages*
Privacy	• *Fake roaming from terrestrial network into satellite network (and vice versa)* • *User's privacy attack* • *Mobile user interception and information interception*

	• *Compromised authentication gateway* • *Leaking keys* • *Unauthorized data access* • *Misbehaving control plane* • *Add malicious nodes into core network* • *Misuse of open control and monitoring interfaces* • *Security threats in a satellite network* • *Denial of service due to Unprotected Mobility Management Exposes Network* • *User privacy policies are not respected* • *Nefarious activities (manipulation of information, interception of information): privacy violations* • *Nefarious activities (manipulation of information, interception of information): personal information disclosure* • *Compromised / malicious LI (Lawful Interception) function* • *Nefarious activities (manipulation of information, interception of information) over LI-aware network*

The analysis of each specific 5G use cases is reported in Section 5, while the use cases themselves are briefly summarized in the Appendix 1.

4.3 5G-ENSURE Risk Evaluation methodology

The risk evaluation procedure is based on the identification of risk criteria and the definition of metrics for risk quantification based on likelihood and impact.

- **Risk criteria**: Decide on the acceptable level of risk for each activity / use case / asset
    - One can define a threshold of 'acceptable' risks (after their quantification as product of likelihood and impact), stating that only risks above value e.g. {4} should be treated...
- Define risk **Likelihood** & **Impact** metrics:
    - An even number of range of values is recommended, e.g. { low, medium, high, extreme/critical }, so as to avoid classical pitfall to evaluate likelihood and impact to the 'middle' value;
    - A likelihood range of values could be based on the periodicity of possible risk occurrence;
    - There is currently a debate within risk management community about the very concept of categorizing likelihoods, consequences (impact), risks and acceptability *vs.* simply ranking them on continuous scales…

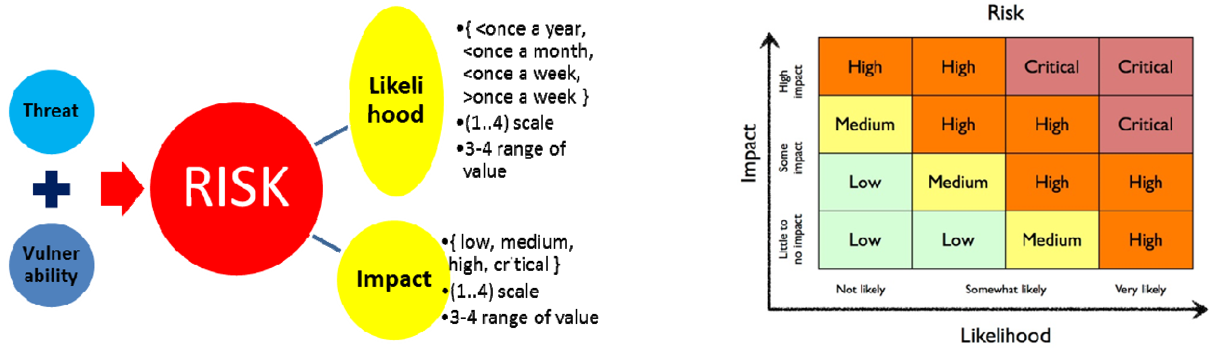

Figure 11. Risk Evaluation Procedure

Computing risk likelihood and impact for 5G assets is quite a challenge, since the system is not actually active and used yet. Three main approaches can be used:

1. Based on our evaluation on estimations performed for 4G systems
2. Provide a theoretical value based on existing literature (again for 4G networks)
3. Based on our evaluation of values provided by the experts present in the 5G PPP projects

Each approach will be examined by 5G ENSURE and a clear methodology will be proposed and followed during the project's lifetime, and reported in the next version of the present document.

5 'Internal' threat description/analysis (from Use Cases)

The 5G-ENSURE project has proposed and analyzed use cases covering a wide variety of 5G deployment scenarios including Internet of Things, Software Defined Networks and virtualization, ultra-reliable and standalone operations. The analysis has produced 31 security relevant use cases grouped in 11 security clusters described in detail in the project's deliverable 2.1 [1], which highlight security issues inherited from current generation networks, as well as security and privacy functionality needed to support the new scenarios introduced in 5G. Most of the clusters focus on the availability, reliability and integrity of the network and the supported services. An initial threat analysis of the major use cases is provided as the basis. A more detailed analysis and risk remediation recommendations will be provided in the final version of this deliverable.

The reader is invited to refer to [1] for use case settings from which the threats are derived. Use case descriptions are not reproduced here.

Note that in the threat description tables we indicate the high level asset categories in order to keep the tables simple and legible. More detailed asset specification can be provided by each use case by filling in the appropriate field in the "Other" category.

5.1 Threat descriptions Use Cases cluster 1 - Identity Management

ID: Unique ID # of the threat	**T_UC1.3_1**
Name: Brief name of the threat	Unauthorised activities related to satellite devices or (satellite) network resources
Description: Detailed description of threat and its importance	Network Operators (e.g. SatNO) and M2M communications (e.g. updated satellite device SW) require fine-grained access to network resources (e.g. satellite device, eNB…). Also, satellite devices shall be authenticated to access satellite services (e.g. broadband access, direct-to-home services…). These network components and devices are distributed in a wide-area large enough that other wired or wireless network connectivity is not feasible. In this scenario, main threats are related to Unauthorised activities: • Unauthorised access • Unauthorised administration of devices and systems • Falsifications of configurations
Category: ITU-T X.805 security dimension(s)	☒ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Information integrity. Information destruction. Service availability.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☒ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems*

	☐ *Operator data* ☐ *End user data* ☒ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☒ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Fine-grained access control focusing on the application level. In case of resource constrain devices (e.g. satellite devices), the fine-grained access control can be based on tokens evaluated directly in the device.
Entry Points (optional, if known): What possible means does an adversary have?	Non updated network components or satellite devices compromise system security/functionality. Wide-area distributed network composed of resource constrained devices (i.e. satellite devices) with high latency.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Fine-grained Authorization enabler.

ID: Unique ID # of the threat	**T_UC1.3_2**
Name: Brief name of the threat	Fake roaming from terrestrial network into satellite network (and vice versa)
Description: Detailed description of threat and its importance	Due to the fact that 5G is of multi-operator nature, 5G devices shall be connected to different networks. These 5G devices could be identified in either the satellite network or the terrestrial network with a set of credentials that allows access to both networks. Then due to coverage issues the 5G

	device performs a roaming to the other network. Non-repudiation of SLAs between integrated satellite and terrestrial networks and different operators should be considered. In this scenario, main threats are related to Legal and business category: • Breach of SLAs • Abuse of personal data from not honestly operators • Identity theft: a customer of MNO A (authenticated by A), present an identity of MNO B inside MNO B network thank to the roaming agreement (SIP fraud over VoIP interconnect) Thread agents could be dishonest external operators.
Category: ITU-T X.805 security dimension(s)	☒ Access control ☒ Authentication ☐ Non-repudiation ☒ Data confidentiality ☐ Communication security ☐ Data integrity ☒ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Service availability. Information confidentiality.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☒ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users:

	☐ *End user data* ☐ *SLAs and regulations* ☒ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Integrating the envisaged 5G AAA system mechanisms with satellite authentication function using standard interfaces.
Entry Points (optional, if known): What possible means does an adversary have?	Heterogeneous security levels between network operators may allow fraudulent behaviours and permits customers to gain unauthorised access to content, services and resources.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Fine-grained Authorization enabler R2.

ID: Unique ID # of the threat	**T_UC1.4_1**
Name: Brief name of the threat	Compromised data
Description: Detailed description of threat and its importance	In this use case, the MNO needs to collect data about a user from the mobile network (step (c) in Figure 5 of Deliverable D2.1). If the user device or any network component is compromised, this can tamper with the integrity and confidentiality of the collected data. As the metrics provided to the service provider are cryptographically computed based on the collected data, collecting fake data may compromise the metrics, hence, the provided service.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☒ Communication security

	☒ Data integrity ☐ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	In order to provide this enhanced service, the MNO needs to have an assurance about the validity of the collected data. This may imply the use of attestation protocols between the collect points (in the network) and the MNO.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☒ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☒ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐

Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	In order to protect against this threat, the MNO needs to perform validity checks on the collected data. The solution may include remote attestation protocols and investigation in statistics data processing.
Entry Points (optional, if known): What possible means does an adversary have?	An adversary can have one or all the following means: Communication channels, user equipment and a network component
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Generic collector interface enabler can be part of the solution.

ID: Unique ID # of the threat	**T_UC1.4_2**
Name: Brief name of the threat	User's privacy attack
Description: Detailed description of threat and its importance	The MNO 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 metric do not properly anonymize user's data, this can break the user's privacy.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The MNO must carefully choose the cryptographic mechanisms used to compute the shared metrics.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data*

	☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	A solution can consider the state of the art about secure attribute sharing mechanisms and perhaps enhancements or adaptations of these mechanisms to the mobile network context.
Entry Points (optional, if known): What possible means does an adversary have?	In order to get the shared metrics between the MNO and the service provider, an adversary can control the communication channel or compromise the service provider.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

5.2 Threat descriptions Use Cases cluster 2 - Enhanced Identity Protection and Authentication

ID: Unique ID # of the threat	**T_UC2.1_1**
Name: Brief name of the threat	Mobile user interception and information interception
Description: Detailed description of threat and its importance	In some situations in current mobile networks (GSM and UMTS and in all networks during an emergency call setup) the IMEI is sent to the network in plain text. This opens the door to device identity disclosure and unauthorized device tracking attacks.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☒ Communication security ☐ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, end users, end devices …) or e2e effect…	User privacy violation through IMEI (International Mobile Equipment Identity) interception and tracking.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities*

	☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	The solution space includes exploration of protocol enhancements and investigation into state-of-the art end-to-end encryption/anonymization techniques, offering protection against device identity disclosure and unauthorized device tracking. Therefore 5G should ensure that the IMEI is sent only in a confidentiality protected message (e.g., through encryption). In addition the enhancement should aim to also address the emergency call case where the IMEI is sent over the network unprotected. This may imply the implementation of additional possibly public key-based cryptographic techniques
Entry Points (optional, if known): What possible means does an adversary have?	Communication channel (IMEI sniffing over the air)
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	The Enhanced Identity Protection Enabler and Device Identifier(s) Protection may be employed to provide IMEI encryption as well.

ID: Unique ID # of the threat	**T_UC2.2_1**
Name: Brief name of the threat	Tracking of device's (user's) location
Description: Detailed description of threat and its importance	Terminals' (and users owning them) location can be tracked by eavesdropping identifiers transmitted between a base station and user terminal. [1, 2] The location can be tracked using either permanent identifiers, which may be transmitted when device joins the network, or using temporary identifiers (pseudonyms like GUTI or TMSI). Such identifiers are broadcasted in clear text so that devices identify which communication is targeted for whom. If such

	identifiers are not changed (re-pseudonymized) before an adversary is able determine which identifier belongs to a victim, so the victim's location can be tracked. Broadcasting a temporary identifier, which is known or suspected to belong to Alice, is an indication that Alice is close to the broadcasting base station. By analysing signal directions, Mallory may be able to determine UE's location more accurately.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☐ Communication security; ☐ Data integrity; ☐ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	5G network is not able to protect end-user's privacy and will be considered less trustworthy by the end-users.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators*

	☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Using of encrypted identifiers when possible. However, devices need to be aware that the communication is targeted for them, so encrypted identifier will become a pseudo-identifier that can be mapped to the device. Frequent changing of temporary identifiers. This solution may add complexity or signalling.
Entry Points (if known): What possible means does an adversary have?	Adversaries must link terminals identifiers to the users' identity. This can be achieved by triggering the mobile network into initiating the generation of paging messages to the victim (and thus to victim's terminal). For instance, adversaries may connect users with using social media application to initiate unobtrusive communications. Location tracking can be done at the granularity of base station's coverage or in more detail if the adversary has capabilities to analyse signal directions. Also, detailed location tracking is possible by eavesdropping plaintext signal measurement reports.

ID: Unique ID # of the threat	**T_UC2.2_2**
Name: Brief name of the threat	Mobile user interception and information interception.
Description: Detailed description of threat and its importance	In some situations in all current mobile networks the IMSI is sent to the network in clear text. This opens the door to subscriber's identity interception/disclosure and unauthorized user tracking attacks.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☒ Communication security ☐ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	User privacy violation through IMSI (International Mobile Subscriber Identity) interception and tracking.
Assets impacted:	☐ Data Plane Assets:

What assets could be damaged?	☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Potential solutions to provide for subscriber privacy include encryption of the IMSI and/or use of improved pseudo-identifiers. Anonymisation systems may be investigated to provide for unlinkability of subscriber and device identities.
Entry Points (optional, if known): What possible means does an adversary have?	Communication channel (IMSI sniffing over the air, rogue eNBs)
5G-ENSURE enablers (optional, if covered for	The Enhanced Identity Protection Enabler may be employed to provide IMSI protection through encryption and improved anonymization to temporary

given threat): What possible means does an adversary have?	identifiers.

5.3 Threat descriptions Use Cases cluster 3 - IoT Device Authentication and Key Management

ID: Unique ID # of the threat	**T_UC3.1_1**
Name: Brief name of the threat	Authentication traffic spikes
Description: Detailed description of threat and its importance	Simultaneous or periodic authentication events may cause excessive amount of traffic for network. Adversaries – aiming to perform a denial-of-service attack - may try to initiate traffic spikes or emphasize the effects of natural traffic spikes with IoT application specific means. As a consequence, the network will experience more signalling and authentication functions needs to perform more processing. Potentially, the authentication of devices may fail and devices may lose connectivity.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☐ Communication security; ☐ Data integrity; ☒ Availability; ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The 5G network must be over-resourced in order to handle large short-term traffic amounts.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data*

	☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☒ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Different means may be utilized to mitigate traffic spikes. Methods include relying gateway or one group member to perform authentication on the behalf of individual devices. For instance, using group authentication schemes such as [3]. Monitoring and filtering approaches can be used to mitigate effects.
Entry Points (if known): What possible means does an adversary have?	The traffic spikes may emerge naturally in the IoT network as devices may be programmed e.g. to join the network at the same time. However, an adversary may try to guide this behaviour with different means, for instance, by tampering network time or causing power outages to get large amount devices to authenticate at the same time.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC3.1_2**
Name: Brief name of the threat	Compromised authentication gateway
Description: Detailed description of threat and its importance	Compromised and maliciously acting node providing authentication on the behalf of a group – an IoT gateway or a mobile phone - may endanger IoT devices' security. Authenticating node may act as a man-in-the-middle – tamper or eavesdrop communication – or provide tampered security configurations. As a result, data collected from IoT devices may leak from to wrong parties and IoT devices may receive commands from malicious party.
Category: ITU-T X.805 security	☒ Access control; ☒ Authentication;

dimension(s)	☒ Non-repudiation; ☒ Data confidentiality; ☒ Communication security; ☒ Data integrity; ☒ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	5G network will have more potentially misbehaving end-points. Application services cannot rely on strong authentication of individual nodes.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☒ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐

Possible Mitigation Hints (if known): How can we protect against the threat?	
Entry Points (if known): What possible means does an adversary have?	
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC3.2_1**
Name: Brief name of the threat	Leaking keys
Description: Detailed description of threat and its importance	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 gain an access to the end-points. The may e.g. provide false information to application services or send malicious commands to IoT devices.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☒ Authentication; ☐ Non-repudiation; ☒ Data confidentiality; ☒ Communication security; ☒ Data integrity; ☐ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The leaking keys will compromise the security (confidentiality and integrity) of those applications that are end-to-end secured.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware*

	☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☒ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☒ *End User Application Developers* ☒ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	The key server could be used only for authentication purposes and not for delivering the sessions keys. This would make attacks more difficult as the attacker would be required to compromise the server to provide wrong (asymmetric) authentication keys and then mount an interception attack on the end-to-end communication. However, all IoT devices may not be computationally capable to asymmetric key operations. The key server should be hardened to withstand attacks. The server cannot be isolated from the open internet as it needs to be available for the clients. However, some isolation techniques – e.g. micro-segmentation – may be utilized to control which applications may access the server.
Entry Points (if known): What possible means does an adversary have?	Attacker may compromise the key server in various ways. For instance, the attacker may utilize vulnerabilities in server interfaces to gain an access to the service. Lawful interception mechanisms may be vulnerable and leak keys for third-party attackers or authorities that are misusing their privileges.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

5.4 Threat descriptions Use Cases cluster 4 - Authorization of Device-to-Device Interactions

Complete coverage of use cases from this cluster will be provided in the next version of this document.

ID: Unique ID # of the threat	**T_UC4.1_1**
Name: Brief name of the threat	Unauthorized data access
Description: Detailed description of threat and its importance	The main threats are due to a malicious user who may want to access the sensors' data without authorization. Such a malicious user may either try to generate a fake token or try to modify the security policy to get access to the sensors. Moreover, the AAA server may introduce several vulnerabilities in the 5G network infrastructure, which have to be carefully investigated. In any case, an investigation of liabilities between parties will have to be performed (AAA owner, sensor owner and 5G operator).
Category: ITU-T X.805 security dimension(s)	☒ Access control; ☒ Authentication; ☐ Non-repudiation; ☒ Data confidentiality; ☒ Communication security; ☒ Data integrity; ☒ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The sensors become vulnerable to information leakage and tampering as well as denial-of-service attacks.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☒ Application Plane Assets: ☐ *Software* ☒ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☒ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power*

	☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Use of authorization mechanisms, for example based on tokens. The generation of the authorization token should be based both on the security policy, as defined by the sensor owner, and on the 5G credentials which provides the overall trust. The AAA server activities should not affect the security of the 5G Network to which it is connected (for example not contribute to other attacks such as cloning, eavesdrop of communication, network element compromise, etc.).
Entry Points (if known): What possible means does an adversary have?	To compromise a sensor: • Adversaries may send malicious commands / policies to the sensor or sensor controller/gw, can install malicious software. • Alternatively, adversaries may compromise sensor's traffic.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Task T3.1 AAA enablers

5.5 Threat descriptions Use Cases cluster 5 - Software-Defined Networks, Virtualization and Monitoring

ID: Unique ID # of the threat	**T_UC5.1_1**
Name: Brief name of the threat	Misbehaving control plane
Description: Detailed description of threat and its importance	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.
Category: ITU-T X.805 security dimension(s)	☒ Access control; ☒ Authentication; ☐ Non-repudiation; ☒ Data confidentiality; ☒ Communication security; ☒ Data integrity; ☒ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The network and applications become vulnerable to eavesdropping and tampering as well as denial-of-service attacks.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☒ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☒ *SDN Administrators* ☐ *SDN Application Developers* ☒ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users*

	☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Strong protection should be provided for control plane components. They should authenticate and authorize commands and support up-to-date trusted interfaces.
Entry Points (if known): What possible means does an adversary have?	To compromise control plane: • Adversaries may send malicious commands / policies to the controller, if controller does not strongly authenticate and authorize the source of the policies. As a consequence, a legitimate controller will behave maliciously according to adversaries' policies. • Alternatively, adversaries may compromise legitimate control plane component, for instance, by utilizing weaknesses in the controller and its interfaces. • Adversaries may also get credentials to provide the controller policies using e.g. social engineering attacks against the operator. A data plane may be misconfigured so that it accepts control commands also from other slices or external parties. If data plane does not authenticate commands from the controllers, an adversary may masquerade as legitimate control plane component and send malicious southbound control messages.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC5.2_1**
Name: Brief name of the threat	Add malicious nodes into core network
Description: Detailed description of threat and its importance	Malicious nodes may e.g. eavesdrop, tamper, and prevent data flows.
Category: ITU-T X.805 security dimension(s)	☒ Access control; ☐ Authentication; ☐ Non-repudiation; ☒ Data confidentiality; ☒ Communication security; ☒ Data integrity; ☒ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Confidentiality, integrity and availability of e2e communication are compromised.
Assets impacted:	☒ Data Plane Assets:

What assets could be damaged?	☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☒ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☒ *SDN Administrators* ☐ *SDN Application Developers* ☒ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Applying security verification procedures – technical and organisational - for assuring that the added nodes are trustworthy. Only authenticated and authorized entities should be allowed to add nodes. Security monitoring of behaviour of added nodes as well as communication over the network.
Entry Points (if known): What possible means does an adversary have?	Software, image used for deploying new nodes may be compromised. Forwarding logic may be misconfigured so that illegitimate node, switch is able to get access to data flows. In this case, the malicious node is unintentionally added to the core network.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC5.2_2**
Name: Brief name of the threat	Forwarding logic leakage
Description: Detailed description of threat and its importance	A network application running on the controller is able to see the forwarding logic of another application (i.e.: the OpenFlow rules installed in the switches). The applications can belong to different virtual network operators who do not want to leaking sensitive information about how their virtual nodes are located or migrated. The leakage can happen in two directions. Controller-to-switch contains rules that have been installed in the switches. A malicious application can not only intercept the OpenFlow messages as they are sent, it can also request information from the switch about installed rules and related statistics belonging to other applications. Eavesdropping on switch-to-controller (e.g.: OFPT_PACKET_IN) messages can also leak information not only about the forwarding logic, but about application data that might be confidential.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☒ Communication security ☐ Data integrity ☐ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Information about forwarding logic is leaked: positioning of network elements like DNS or other services provided through VNFs and how they are migrated which can be used to infer user population, reliability information etc.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure*

	☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☒ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Insert a reference monitor at the southbound interface.
Entry Points (optional, if known): What possible means does an adversary have?	Deploy an application on the controller in a multi-tenant virtualized network.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Enabler 6.2 “Access Control Mechanisms”

ID: Unique ID # of the threat	**T_UC5.2_3**
Name: Brief name of the threat	Manipulation of forwarding logic
Description: Detailed description of threat and its importance	The setting is the same as T_UC5.2_2, however this time the attacker decides to become active. Instead of simply gleaning information about the forwarding logic of a competing application running on top of the same

	controller, it modifies the flow entries.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☒ Non-repudiation ☒ Data confidentiality ☒ Communication security ☒ Data integrity ☒ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	In order of increasing attacker power and severity: • Overflow the switch table causing the switch to act much slower (due to limited TCAM), causing degraded performance • Evict or delete rules, causing denial of service • Modify rules to redirect data plane traffic through attacker's listening point, causing all data to be intercepted (instead of just the initial PACKET_IN from the passive case) • Modify rules to intercept and tamper data.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers*

	☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	See T_UC5.2_2
Entry Points (optional, if known): What possible means does an adversary have?	See T_UC5.2_2
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	See T_UC5.2_2

ID: Unique ID # of the threat	**T_UC5.3_1**
Name: Brief name of the threat	Fingerprinting attack
Description: Detailed description of threat and its importance	Unlike T_UC5.2_2, the attacker is external to the controller. The attacker can measure the time of reconfiguring the physical network. This way, the attacker can gain information about which and when a network packet triggers a reconfiguration of network components.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☒ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts,	The attacker can exploit the obtained information to mount DoS attacks by overloading the controller with packets that will most likely trigger a reconfiguration of the network. Furthermore, installing flow rules in current SDN switches is a costly operation. This means that even the performance of

applications, e2e effect…)	the physical network can be impacted.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☒ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☒ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	
Entry Points (optional, if known): What possible means does an adversary have?	

5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Enabler 6.1 "Anti-fingerprinting"

ID: Unique ID # of the threat	**T_UC5.5_1**
Name: Brief name of the threat	Misuse of open control and monitoring interfaces
Description: Detailed description of threat and its importance	Third-party service providers may misuse the access to control and monitoring interfaces and cause service disruptions for the operator or attack against data flows. For instance, monitoring information on flowing data may be captured in order to profile end-users. While interfaces are opened for service providers they may also become available for other adversaries.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☒ Communication security; ☐ Data integrity; ☒ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Resources and user data become available for larger amount of parties. More trusted parties means that there may be parties that do not provide good enough security and follow good security practises.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data*

	☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☒ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Service providers should be required to protect the monitoring data they acquire. Service providers should protect their own resources sufficiently, so that adversary cannot access slices through service providers' systems. Strong isolation is needed to prevent service providers from accessing resource outside a slice. Service providers should be allowed to access only those control interfaces that are required to minimize service providers potential to escape
Entry Points (if known): What possible means does an adversary have?	Control interfaces can be enable access to operator's functions either directly (if not sufficient fine-grained protection is available) or the interfaces may contain vulnerabilities that may be utilized to gain additional privileges. A service provider itself may be untrustworthy. Alternatively, an adversary may compromise service providers systems in order to gain access to the slice.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC5.5_2**
Name: Brief name of the threat	Unauthorized access to a network slice
Description: Detailed description of threat and its importance	Isolation of the slice may fail allowing a service provider to gain an access to resources belonging to the operator or other slices. This may jeopardize availability and security of the operators and other services providers' network services.

Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☒ Communication security; ☐ Data integrity; ☒ Availability; ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Availability and security of operators' resources and service provider's resources jeopardized. This may prevent opportunities that are gained by opening operator's network to third-party service providers.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☒ *SDN Administrators* ☒ *SDN Application Developers* ☒ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐

	☐
Possible Mitigation Hints (if known): How can we protect against the threat?	Strong isolation between slices is needed. Authentication and authorization over the access to control and data plane. Security monitoring is needed to detect ongoing incidents.
Entry Points (if known): What possible means does an adversary have?	Failing or misconfigured authentication and authorization both in the control or data plane may enable access to slices.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC5.5_3**
Name: Brief name of the threat	Bogus monitoring data
Description: Detailed description of threat and its importance	False monitoring data / measurements may cause monitoring / 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.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☒ Communication security; ☐ Data integrity; ☒ Availability; ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The threat in impairs availability of the network services and may ease eavesdropping and tampering attacks against the data flows. The threat also makes security monitoring (or security countermeasures that are based on monitoring) less effective.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software*

	☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☒ *SDN Administrators* ☒ *SDN Application Developers* ☒ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	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, e.g. 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 e.g. against correlated data sources.
Entry Points (if known): What possible means does an adversary have?	Adversaries may produce bogus information easily if the measurement sources are not authenticated. If sources are authenticated, an adversary may try to invade and compromise an authentic measurement source.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC5.5_4**
Name: Brief name of the threat	No control of Cyber-attacks by the Service providers
Description:	The use case features a Service Provider (SP) offering its Massively Multiplayer

Detailed description of threat and its importance	Online Game service to gamers. The Service Provider buys its network service to Virtual Mobile Network Operator (VMNO) which itself relies on an Infrastructure Provider. The VMNO supplies a sub-slice to the SP with the required QoS. The service of the SP is subject to cyber-attacks. The SP wants to manage the cyber-security of its service. It signs a contract with a third party Security Service Operator (SSO) to monitor and remediate to 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 it has not the information about the configuration of the NVF and their vulnerabilities, it cannot build a classical attack graph to monitor the cyber-attacks.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☒ Communication security; ☐ Data integrity; ☐ Availability; ☐ Privacy
Potential effect: What effect it will have on 5G system (network, hosts, applications…)	The Service Provider has no control over the cyber-attacks on its slice.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☒ *Network Elements* ☒ *Communication medium* ☒ Control Plane Assets: ☒ *Software* ☒ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☒ *IT Infrastructure* ☒ *Billing systems* ☒ *Operator data* ☒ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users:

	☒ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	A possible mitigation hint would be to enable the SSO to get access to the information from the infrastructure domain, especially the type of software used for NVF in order to establish the vulnerabilities of it. Another way to mitigate this is to separate the responsibilities by contract between the infrastructure domain and the VMNO. The SP will have to rely on the VMNO interface and will only control its cyber-threats at application level.
Entry Points (if known): What possible means does an adversary have?	An adversary could attack the VNFs, hypervisor or orchestrator of the Infrastructure Provider to compromise the Service Provider's service.

ID: Unique ID # of the threat	**T_UC5.6_1**
Name: Brief name of the threat	Security threats in a satellite network
Description: Detailed description of threat and its importance	Security client-side agents are deployed over the satellite network components in order to periodically collect information related to the security dimensions. Once registered, these components deliver to the security monitoring (server-side) the compiled information. This information is supervised in the security monitor that carry out a security analysis to detect attacks and malicious behaviour. The origin of most fraudulent accesses or security breaches can be summarized as either technical identity alteration (after an illegal or illegitimate privilege augmentation) or signalling messages received outside of the normal sequences. These systems are exposed to new threats in 5G that must be mitigated. …). Some of the threats identified are: • Attack on network components: RF interference, power or communications lines… • Attack on the network management system: intruding the system by hijacking, blackmailing, placing or impersonating the operator, to obtain credentials or/and gain control of the system… • Denial of service: flood the network with dummy indicators to make the network unusable, preventing any useful communications with

	the network management system.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☒ Authentication ☒ Non-repudiation ☒ Data confidentiality ☐ Communication security ☒ Data integrity ☒ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	The security properties that this threat can compromise are: • Service availability • Outages • Information confidentiality
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☒ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☒ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☒ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators*

	☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	System can be protected against these threats acting on three levels: • Client-side: Generic secure interface to provide indicators from a heterogeneous network. • Server-side: Data analytics and intelligence-driven security to detect threats based on security metrics. • Network-side: Partitioning the satellite network into virtual private networks.
Entry Points (optional, if known): What possible means does an adversary have?	Heterogeneous networks (satellite and terrestrial) which components are geographically widespread distributed. Some of these network components (e.g. eNBs) are outside the MNO facilities and even on the customer's premises (e.g. satellite device).
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Satellite Network Monitoring

5.6 Threat descriptions Use Cases cluster 6 - Radio Interface Protection

Complete coverage of use cases from this cluster will be provided in the next version of this document.

ID: Unique ID # of the threat	**T_UC6.1_1**
Name: Brief name of the threat	Compromise the availability and integrity of the radio interface
Description: Detailed description of threat and its importance	A critical communication device D, e.g. serving critical infrastructure or used by user Bob in an emergency situation, is trying to attach to the MNO's network. The network is busy serving many other attach requests so D does not get immediate access to the network. Even devices which are attached but lose radio synchronization are required to perform the random access procedure and may become locked out of the network in these situations.
Category: ITU-T X.805 security dimension(s)	☐ Access control; ☐ Authentication; ☐ Non-repudiation; ☐ Data confidentiality; ☒ Communication security; ☐ Data integrity; ☒ Availability; ☐ Privacy

Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Potential consequences include: • Disrupted availability of critical communications network. Deceptive illegitimate requests may cause disruption in network access • Emergency and critical communication requests cannot get higher priority than non-urgent attachment requests
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☒ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect against the threat?	• A secure method for priority of access requests • Save resources by rejecting illegitimate or non-prioritized request at early stage, i.e. enable integrity protection at a low layer in the radio network stack • Give priority for re-attachment to devices losing radio synchronization • Threats of cyber-attacks directly targeting 5G networks needs to be

	dealt with in the 5G design
Entry Points (if known): What possible means does an adversary have?	Access to the radio interface is required, for example by means of a fake BTS.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Task T3.1 AAA enablers

5.7 Threat descriptions Use Cases cluster 7 - Mobility Management Protection

Complete coverage of use cases from this cluster will be provided in the next version of this document.

ID: Unique ID # of the threat	**T_UC7.1_1**
Name: Brief name of the threat	Denial of service due to Unprotected Mobility Management Exposes Network
Description: Detailed description of threat and its importance	User powers on his phone, as part of the LTE specification [TS33.401] the phone will initiate an *"Attach request"* to the base station (eNB). Once connected to the MNO, the user equipment (UE) will send periodic tracking area update (TAU) request messages intended for the MNO's Mobility Management Entity (MME). 1. Attacker intercepts the TAU request and responds with a TAU Reject with EMM cause number 7 "*LTE Services not allowed*" or cause number 8 "*LTE and non-LTE services not allowed".* 2. User's phone accepts the TAU Reject message and acts accordingly a. If EMM cause number 7, user's phone will consider itself invalid for LTE services. If supported the phone will connect to available 3G or 2G networks b. If EMM cause number 8, user's phone will consider itself invalid for all services and enter the state EMM-DEREGISTERED.
Category: ITU-T X.805 security dimension(s)	☒ Access control; ☒ Authentication; ☐ Non-repudiation; ☒ Data confidentiality; ☒ Communication security; ☒ Data integrity; ☒ Availability; ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	• The TAU Request is sent without confidentiality protection, hence the attacker can decode it. • The TAU Reject message is accepted by the UE without integrity protection and without an established security context between the UE and network.

	• The “*Attach request”* is sent unprotected, hence the list of the network capabilities can be altered by the attacker. • The “*Forbidden PLMN”* are accepted by the UE without integrity protection and without an established security context between the UE and network. These vulnerabilities can be used to perform a denial of service or downgrade attacks, which persists until the user reinserts the USIM, reboots the UE, or in one case, physically moves the UE to a new tracking area.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☒ *Communication medium* ☒ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (if known): How can we protect	Security monitoring could be one solution to capture those attacks where UE is denied service or forced to use weaker services. UE that previously has been able to use full services, typically does not downgrade its own

against the threat?	capabilities. If the TAU Reject messages were digitally signed, which are verified by the UE, an adversary's messages would be rejected by the UE. This would require the introduction of MNO specific public keys. A mitigation that makes it more difficult to implement a persistent denial of service attack would be to introduce a mechanism based on a timer or counter value, to allow the UE to re-attach itself to the network after a certain time. To mitigate the man-in-the-middle attack on the *Attach* request, the 5G network could require an identical integrity protected reconfirmation of the network capabilities as is required for the security capabilities in LTE.
Entry Points (if known): What possible means does an adversary have?	Access to the radio interface is required, for example by means of a fake BTS.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Task T3.1 AAA enablers

5.8 Threat descriptions Use Cases cluster 8 - Ultra-Reliable and Standalone Operations

ID: Unique ID # of the threat	**T_UC8.1_1**
Name: Brief name of the threat	Service failure over satellite capable eNB
Description: Detailed description of threat and its importance	Main threats that may cause a service failure are related to the following activities: • Failures or malfunctions: o Failure or disruption of communication links o Failure or disruption of main supply o Failure or disruption of service providers o Malfunction of equipment • Outages: o Network connectivity o Loss of physical resources o Support services (Internet provider or Electricity provider) • Disasters: o Natural disasters o Environmental disaster • Physical attacks: o Sabotage o Vandalism o Terrorists attack 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, military scenarios…).
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☒ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☒ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Service availability or traffic congestion
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☒ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☒ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☒ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers*

	☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Allowing the Service Provider to have some degree of control over their micro-slice or sub network enabling dynamic allocations and network reconfigurations on the fly. Evolving the Transport Network Architecture (TNA) by combining both satellite and terrestrial transport architectures. Once a link failure has been detected, new topology is forwarded to base stations with satellite links and smart antennas, enabling topology reconfiguration according to traffic failures and traffic demands.
Entry Points (optional, if known): What possible means does an adversary have?	4G backhaul networks are fixed topologies, therefore the network barely manages accidental/deliberate link failures or traffic congestion. An exhaustive radio planning is needed before base station deployment and new backhaul nodes cannot be easily added.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Once a link failure/congestion is detected, Satellite Network Monitoring provides a Topology algorithm to reconfigure the network components.

5.9 Threat descriptions in Use Cases of Cluster 9 - Trusted Core Network and Interconnect

ID: Unique ID # of the threat	**T_UC9.1_1**
Name: Brief name of the threat	Spoofed signalling messages
Description: Detailed description of threat and its importance	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. This applies to other signalling messages as well, e.g., management related.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☒ Authentication ☒ Non-repudiation ☒ Data confidentiality

	☐ Communication security ☒ Data integrity ☒ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Network could take actions that were not really 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). Also, if management messages are spoofed, this could change the infrastructure, potentially in a devastating way.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☒ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☒ *Billing systems* ☒ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐

Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	All signalling messages should be integrity protected and bound to correct entities. Cryptographic identities is one possible approach.
Entry Points (optional, if known): What possible means does an adversary have?	Adversary can try to inject signalling traffic into the core by either subverting a node inside the core or bypassing the filtering of ingress traffic.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC9.1_2**
Name: Brief name of the threat	Disputes in charging
Description: Detailed description of threat and its importance	The user could dispute charges or operator could place unfounded charging on the user actions. Basically, the operator can produce billing records, but the customer has no way of proving whether they are correct or not.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☒ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Decrease of trust into the system and loss of revenue.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets:

	☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☒ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☒ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	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.
Entry Points (optional, if known): What possible means does an adversary have?	
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC9.1_3**
Name: Brief name of the threat	Disclose of sensitive data
Description: Detailed description of threat and its importance	If visited network is not well-established operator, e.g., this could be a mall network, then there is an amount of certainty regarding the trust level of the interconnect party for the home network. In order to provide service to the end user, the visited network needs to obtain, e.g., authentication vectors from the home network. In general, the requests for such sensitive information should come only from verified source (and not necessary just relying on network topology).
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☐ Communication security ☒ Data integrity ☐ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Obtaining sensitive information in unauthorized fashion could lead to further compromise of the network and possibly make it easier to spoof other entities.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data*

	☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Interconnect networks need to be authenticated and authorized. One should not rely on requests coming from a certain network address (e.g., coming through an established IPsec tunnel).
Entry Points (optional, if known): What possible means does an adversary have?	Potentially malicious interconnect partner or other malicious entity within operator network.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC9.2_1**
Name: Brief name of the threat	User privacy policies are not respected
Description: Detailed description of threat and its importance	If the system provides the possibility for the user to dictate user specific privacy policy to be handed over to the visited or home network, nothing prevents the operator from not honouring this policy. This could lead to the breach of user privacy.

Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	User trust to the system is decreased.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☒ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☒ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users*

	☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Regulatory sanctions and oversight could decrease the incentives to engage in disclosing user information to third parties. Audit programs could be used to monitor compliance.
Entry Points (optional, if known): What possible means does an adversary have?	
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC9.3_1**
Name: Brief name of the threat	Hardening or patching of systems is not done
Description: Detailed description of threat and its importance	If the systems are not hardened correctly or if the patching processes do not keep the systems up-to-date, the systems could be compromised through the vulnerabilities existing in the systems.
Category: ITU-T X.805 security dimension(s)	☒ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☒ Communication security ☐ Data integrity ☐ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Systems can be compromised through the vulnerabilities and elevated privileges gained. Thus, total control of a node can be achieved.
Assets impacted: What assets could be	☐ Data Plane Assets: ☒ *Network Elements*

damaged?	☐ *Communication medium* ☐ Control Plane Assets: ☒ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☒ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	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.
Entry Points (optional, if known): What possible means does an adversary have?	Abuse of software vulnerabilities in the software
5G-ENSURE enablers	Proactive security analysis and remediation

(optional, if covered for given threat): What possible means does an adversary have?	Microsegmentation

ID: Unique ID # of the threat	**T_UC9.3_2**
Name: Brief name of the threat	Unauthentic device installed into the system
Description: Detailed description of threat and its importance	Breach of physical security could result in an unauthentic device to be installed into the network.
Category: ITU-T X.805 security dimension(s)	☒ Access control ☐ Authentication ☐ Non-repudiation ☐ Data confidentiality ☒ Communication security ☐ Data integrity ☐ Availability ☐ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	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.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☒ *Network Elements* ☒ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☒ *Hardware* ☒ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☒ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data*

	☐ Network service provider physical infrastructure: ☒ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☐ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Proper physical security measures are needed to prevent access to the communication equipment. Logical access control also needs to be in place to ensure that no unauthorized device can be just plugged into any open port. Hence, devices need to be authenticated before allowed to access the network. Monitoring can be used to detect unauthentic devices or traffic that does not match the typical usage pattern of the network.
Entry Points (optional, if known): What possible means does an adversary have?	Physical plugging in of the device
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	Proactive security analysis and remediation Microsegmentation

5.10 Threat descriptions in Use Cases of Cluster 10 - 5G Enhanced Security Services

ID: Unique ID # of the threat	**T_UC10.2_1**
Name: Brief name of the threat	Nefarious activities (malicious software, unauthorized activities, interception of information): privacy violations

Description: Detailed description of threat and its importance	Mobile devices and the installed applications disclose a large amount of private information both personal and device related information mostly through misbehaving apps, PUAs (Potentially Unwanted Applications), adware and ransomware.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☐ Communication security ☐ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, end users, end devices, e2e effect…)	Threat effect: information leakage, disclosure of sensitive info, privacy violation in general.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☒ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers*

	☐ *Network Service Operators* ☒ *End User Application Developers* ☒ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	Potential solutions include means to protect the user's privacy at the application layer. The 5G network adopts a privacy policy containing various privacy parameters (related to device and apps activity on user data) that can be controlled on user's demand or upon some anomalous event detection. The 5G network offers to subscribers a service that checks the privacy risk of devices and their installed apps. A useful tool for this service is to require the mobile applications and servers to declare a human readable privacy policy and to offer a tool to the user's device to verify it. 5G should support an application level service that provides privacy policy analysis.
Entry Points (optional, if known): What possible means does an adversary have?	Compromised devices by malicious app.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	The enabler is Policy Privacy Analysis

ID: Unique ID # of the threat	**T_UC10.3_1**
Name: Brief name of the threat	Nefarious activities (manipulation of information, interception of information): personal information disclosure
Description: Detailed description of threat and its importance	Mobile devices and/or the installed applications (malware/spyware, misbehaving applications and also common applications) disclose a large amount of personal and device identifying information (e.g., IMSI, phone number, location data, IMEI etc.).
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☐ Communication security ☐ Data integrity

	☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Threat effect: information leakage, disclosure of sensitive identifying info, privacy violation in general.
Assets impacted: What assets could be damaged?	☐ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☒ *End User Application Developers* ☐ *End User Application Administrators* ☒ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect	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

against the threat?	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.
Entry Points (optional, if known): What possible means does an adversary have?	Mobile Device
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	The enabler is SIM or device-based Anonymization.

5.11 Threat descriptions in Use Cases of Cluster 11 - Lawful Interception

ID: Unique ID # of the threat	**T_UC11.1_1**
Name: Brief name of the threat	Compromised / malicious LI (Lawful Interception) function
Description: Detailed description of threat and its importance	Attacking the LI function may result in to various issues: unauthorized disclosure of user's data / communications, a disruption or degradation of the service used by the user, and reporting fake or compromised information about the suspected data.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☒ Non-repudiation ☒ Data confidentiality ☐ Communication security ☒ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	A solution may encompass mechanisms to check the validity of the reported data and mechanism to check the validity of the LI function.
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☐ *Communication medium* ☐ Control Plane Assets: ☐ *Software*

	☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☐ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents: ☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	We can consider the state of the art about remote attestation mechanism and perhaps investigate enhancements of these mechanisms.
Entry Points (optional, if known): What possible means does an adversary have?	An adversary may attack the LI function.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	

ID: Unique ID # of the threat	**T_UC11.2_1**
Name: Brief name of the threat	Nefarious activities (manipulation of information, interception of information) over LI-aware network
Description: Detailed description of threat and its importance	The user data traffic can be eavesdropped and manipulated on some possible paths if there is no end-to-end protection. In this way the user data privacy is not guaranteed completely from its source to the final destination.
Category: ITU-T X.805 security dimension(s)	☐ Access control ☐ Authentication ☐ Non-repudiation ☒ Data confidentiality ☒ Communication security ☒ Data integrity ☐ Availability ☒ Privacy
Potential effect: What global effect it will have on major 5G system domains (network, hosts, applications, e2e effect…)	Data disclosure, data manipulation with e2e effect
Assets impacted: What assets could be damaged?	☒ Data Plane Assets: ☐ *Network Elements* ☒ *Communication medium* ☐ Control Plane Assets: ☐ *Software* ☐ *Hardware* ☐ *Data* ☐ Application Plane Assets: ☐ *Software* ☐ *Hardware* ☐ Service provider IT Infrastructure: ☐ *IT Infrastructure* ☐ *Billing systems* ☐ *Operator data* ☒ *End user data* ☐ Network service provider physical infrastructure: ☐ *Facilities* ☐ *Energy Power* ☐ SDN users: ☐ *End user data* ☐ *SLAs and regulations* ☐ Human agents:

	☐ *SDN Administrators* ☐ *SDN Application Developers* ☐ *Network Service Operators* ☐ *End User Application Developers* ☐ *End User Application Administrators* ☐ *End User Service Providers* ☒ *End Users* ☐ Others (please specify): ☐ ☐
Possible Mitigation Hints (optional, if foreseen): How can we protect against the threat?	5G should provide an optional end to end encryption service Potential solutions include an end-to-end encryption service 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.
Entry Points (optional, if known): What possible means does an adversary have?	Communication medium using a fake access node or a compromised mobile device.
5G-ENSURE enablers (optional, if covered for given threat): What possible means does an adversary have?	The enabler is end to end encryption.

6 Analysis: Functional design recommendations

We can observe some interesting 5G usage patterns from the previous threat descriptions. They imply the following early (non-exhaustive) recommendations for 5G system security design.

The first one comes from the very essence of multi-stakeholder setting of 5G, e.g. how to ensure integrity and confidentiality of data collected/exchanged between infrastructure providers, MNOs, service providers or even third-party operators such as SSO (threats T_UC1.4_1, T_UC1.4_2, T_UC5.5_4). Also, liabilities between involved parties can be performed (as for the threat T_UC4.1_1) or multi-tenant interfaces can be hardened (as between different VNO network applications and controllers to avoid leakage or manipulation of the forwarding logic as in threats T_UC5.2_2 and T_UC5.2_3).

Also, complex 5G network and system topology needs careful design of technical interfaces between and inside the domains, e.g. how to avoid data leakage through vulnerable or misbehaving end-points (threats T_UC3.1_2, T_UC1.4_1) or how to protect SDN control plane components through trusted interfaces (threat T_UC5.1_1). Indeed, while control and monitoring interfaces are opened for third- party service providers they may also become available for other adversaries (threat T_UC5.5_1).

Also, specific 5G radio interface protection schemes need to be devised so as to ensure availability of critical communication network, e.g. by prioritizing attach requests (threat T_UC6.1_1).

End-to-end encryption techniques emerge several times, e.g. to avoid user data eavesdropping but at the same time to enable lawful interception (threat T_UC11.2_1) or against device identity disclosure (threat T_UC2.1_1).

Moreover, appropriate security monitoring measures appear to be important in 5G networks (threats T_UC5.5_2, T_UC5.5_3, T_UC7.1_1, T_UC9.3_1) in order to detect security incidents/attacks and to perform corrective actions.

This chapter will be extended in the final version of the present document for more complete 5G system design options and will feed architecture work in D2.4.

7 Conclusions and Next Steps

This document provides a first draft of the Risk Assessment, Mitigation and Requirements deliverable and mainly addresses the first two aspects, by proposing a risk assessment approach for 5G-ENSURE specific security use cases.

While risk management context definition, assets identification and threats categorization are aspects already addressed herein, the next steps will focus on: the thorough definition of the risk evaluation methodology, the "external" risk analysis which will result in the formulation of mitigation recommendations and definition of the security requirements for the 5G security architecture. Note that potential mitigation/security solutions are already indicated in the use cases threat analysis, our main task in future will be to provide a complete and systematic definition.

8 References

[1] 5G-ENSURE Deliverable D2.1 "Use Cases"

[2] 5G-ENSURE Deliverable D2.2 "Trust model (draft)"

[3] ITU-T Recommendation X.805 "Security architecture for systems providing end-to-end communications"

[4] ITU-T Recommendation X.801

[5] NIST SP800-30, "Risk Management Guide for Information Technology Systems", NIST (National Institute of Standards and Technology)

[6] ISO/IEC 27005:2011 "Information technology - Security techniques - Information security risk management"

[7] A. Roller, S. Turpe, K. Kinder-Kurlanda, "An Asset to Security Modeling? Analyzing Stakeholder Collaborations Instead of Threats to Assets"

[8] ETSI TS 123 101 V3.1.0 (2000-12), http://www.etsi.org/deliver/etsi_ts/123100_123199/123101/03.01.00_60/ts_123101v030100p.pdf

[9] ASMONIA Project, http://www.asmonia.de/index.php?page=20

[10] ETSI TS 133 401 V10.3.0 (2012-07), http://www.etsi.org/deliver/etsi_ts/133400_133499/133401/10.03.00_60/ts_133401v100300p.pdf

[11] ETSI NFV, http://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.01.01_60/gs_nfv002v010101p.pdf

[12] "Threat Landscape and Good Practice Guide for Software Defined Networks/5G", ENISA, December 2015, https://www.enisa.europa.eu/publications/sdn-threat-landscape

9 Appendix 1: Use cases threats Identification

The following set of use cases in D2.1 [1] are used to derive threats description for 5G networks:

Cluster no.	Cluster name/topic	Use case no.	Use case name
1	Identity Management	1.1	Factory Device Identity Management for 5G Access
		1.2	Using Enterprise Identity Management for Bootstrapping 5G Access
		1.3	Satellite Identity Management for 5G Access
		1.4	MNO Identity Management Service
2	Enhanced Identity Protection and Authentication	2.1	Device Identity Privacy
		2.2	Subscriber Identity Privacy
		2.3	Enhanced Communication Privacy
3	IoT Device Authentication and Key Management	3.1	Authentication of IoT Devices in 5G
		3.2	Network-based Key Management for End-to-End Security
4	Authorization of Device-to-Device Interactions	4.1	Authorization in Resource-Constrained Devices Supported by 5G Network
		4.2	Authorization for End-to-End IP Connections
		4.3	Vehicle-to-Everything (V2X)
5	Software-Defined Networks, Virtualization and Monitoring	5.1	Virtualized Core Networks, and Network Slicing
		5.2	Adding a 5G Node to a Virtualized Core Network
		5.3	Reactive Traffic Routing in a Virtualized Core Network
		5.4	Verification of the Virtualized Node and the Virtualization Platform
		5.5	Control and Monitoring of Slice by a Service Provider
		5.6	Integrated Satellite and Terrestrial Systems Security Monitor
6	Radio Interface Protection	6.1	Attach Request During Overload
		6.2	Unprotected User Plane on Radio Interface
7	Mobility Management Protection	7.1	Unprotected Mobility Management Exposes Network for Denial-of-Service
8	Ultra-Reliable and Standalone Operations	8.1	Satellite-Capable eNB
		8.2	Standalone EPC
9	Trusted Core Network and Interconnect	9.1	Alternative Roaming in 5G
		9.2	Privacy in Context-Aware Services
		9.3	Authentication of New Network Elements
10	5G Enhanced Security Services	10.1	Botnet Mitigation
		10.2	Privacy Violation Mitigation
		10.3	SIM-based and/or Device-based Anonymization
11	Lawful Interception	11.1	Lawful Interception in a Dynamic 5G Network
		11.2	End-to-End Encryption for Device-to-Device Communications

10 Appendix 2: Abbreviations

List of abbreviations used throughout this document.

AAA	Authentication, Authorization and Accounting
AKA	Authentication and Key Agreement
AN	Access network
BTS	Base Transceiver Station
CN	Core Network
D2D	Device-to-Device
DNS	Domain Name System
(D)DoS	(Distributed) Denial of Service attack
EAL	Evaluation Assurance Level (EAL1 through EAL7)
EAP	Enhanced Authentication Protocol
eNB	Evolved Node B
ENISA	European Union Agency for Network and Information Security
EPC	Evolved Packet Core
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary UE Identity
HAPS	High Altitude Platforms
HSS	Home Subscriber Server
ID	Identifier
IM	Identity Management
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IOT	Internet of Things
ITU-T	ITU (International Telecommunication Union) Telecommunication Standardization Sector
LI	Lawful Interception
LTE	Long Term Evolution
M2M	Machine-to-Machine
MBB	Mobile Broadband
MME	Mobility Management Entity
(m)MTC	(Massive) Machine-Type Communication
MNO	Mobile Network Operator
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
OTT	Over-the-Top (Provider)
PLMN	Public Land Mobile Network
PUA	Potentially Unwanted Application
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
SatAN	Satellite Access Network
SatNO	Satellite Network Operator
SDN	Software Defined Networks
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement

SMS	Short Message Service
SN	Serving Network
SP	Service Provider
SSO	Security Service Operator
SW	Software
TAU	Tracking Area Update
TCAM	Ternary Content Addressable Memory
TMSI	Temporary Mobile Subscriber Identity
TNA	Transport Network Architecture
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
V2X	Vehicle-to-Everything
VMNO	Virtual Mobile Network Operator
VIP	Virtual infrastructure provider
VNF	Virtualized Network Function(s)
WSN	Wireless Sensor Network