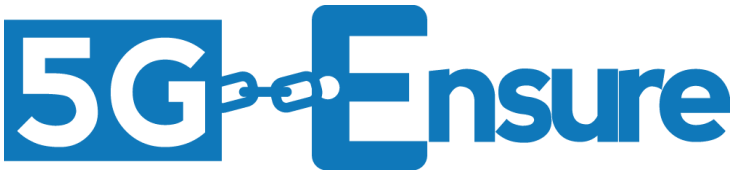

Deliverable D2.7
Security Architecture (Final)

Project name	5G Enablers for Network and System Security and Resilience	
Short name	5G-ENSURE	
Grant agreement	671562	
Call	H2020-ICT-2014-2	
Delivery date	31.10.2017	
Dissemination Level:	Public	
Lead beneficiary	SICS (RISE SICS)	Rolf Blom, rolf.blom@ri.se
Authors	EAB: Håkan Englund, Alexander Maximov, Prajwol Kumar Nakarmi, Mats Näslund, Christian Schaefer, Per Ståhl IT Innov: Gianluca Correndo, Vadims Krivcovs, Stephen Philips LMF: Vesa Lehtovirta, Vesa Torvinen NEC: Felix Klaedtke Nixu: Seppo Heikkinen, Tommi Pernila Nokia: Hon-Yon Lach, Linas Maknavicius Orange: Ghada Arfaoui, Jean-Philippe Wary Oxford: Ravishankar Borgaonkar, Piers O'Hanlon SICS: Rolf Blom, Martin Svensson TCS: Sébastien Keller TS: Edith Felix, Pascal Bisson VTT: Petteri Manersalo, Pekka Ruuska, Jani Suomalainen, Janne Vehkaperä	

Executive summary

This deliverable (D2.7) of the 5G-ENSURE project describes a security architecture for 5G networks. The focus lies on a logical and functional architecture and omits (most) aspects related to physical/deployment architecture. This focus is motivated by general trends such as network de-perimeterization as well as 5G systems' strong dependency on software defined networking and virtualization in general.

The presented 5G security architecture builds on and extends the current 3GPP security architecture. The "logical dimension" of our architecture first of all captures the security aspects associated with the various domains that are involved in delivering services over 5G networks. This part is therefore also strongly associated with the project's trust model. Additionally, the logical part captures the security aspects associated with network layers and/or special types of network traffic which, in our architecture, are associated with different strata. The "functional dimension" of our architecture comprises a set of security capabilities required to protect and uphold the security of the various domains and strata. In the functional dimension, we build on the 3GPP defined security feature groups and introduce security realms. We extend and refine these concepts to adapt to a 5G context.

A goal of the architecture work within 5G-ENSURE has been to clearly provide rationale for the architecture's structure and features. We seek to motivate which high level security problems are relevant in a 5G context, and then break that down into a manageable set of security objectives for a 5G security architecture. From these objectives the high-level architecture is derived and only after that stage do detailed requirements enter the discussion (many of them defined in the work on risk assessment, mitigation and requirements).

The presented 5G security architecture models the network and its security functionality in terms of domains, strata, security realms and security control classes. The security architecture design is based on security objectives related to the architecture itself. The security architecture is extensible and flexible and can be adapted to the future developments in 5G networking as new domains, strata, security realms and security control classes can be defined as required to capture new network architectures, services and functions.

The applicability of the security architecture has been demonstrated by mapping the 3GPP 5G logical network architecture and the 5G-ENSURE developed enablers onto the security architecture.

Guidance on how to implement required security controls is also given in a discussion of design principles and recommendations.

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.

This deliverable, "Security Architecture (final)" (D2.7), presents an overarching security architecture, suitable for 5G networks, produced by task T2.4 in work package WP2 "Security requirements and architecture" of 5G-ENSURE. There is an interdependency on the tasks T2.1, T2.2, and T2.3. Trask T2.1 (use cases) was completed before this work started, T2.2 (Trust model) and T2.3 (Risk analysis and requirements) have been running in parallel. In addition, T2.2 and T2.3 are dependent on the results of T2.4. Therefore, it has been necessary to structure the work to allow taking the results from the other tasks into account during the whole project. This has in part been achieved by have draft deliverables and in part by a strong personnel interaction between the tasks.

We firmly believe that this architecture will provide useful guidance for creating a shared 5G security architecture vision within the 5G-PPP as well as providing a useful basis for ongoing standardization discussions. To ensure cross-coordination between the security and network architecture work within the 5G-PPP, we have participated in the 5G-PPP Security and the 5G-PPP Architecture Working Groups. In particular we have provided the section on "5G Security Architecture" in the "5G PPP 5G Architecture White Paper".

To make this report self-contained we have included material from deliverable D2.4 [d2.4]

Disclaimer

Copyright notice

Contents

Abbreviations

3GPP	3rd Generation Partnership Project
3P	3rd party
5G-PPP	5G Infrastructure Public Private Partnership
AAA	Authentication, authorization and accounting
AN	Access Network
APT	Advanced Persistent Threat
AuC	Authentication Centre
AS	Access stratum
BEREC	Body of European Regulators for Electronic Communications
CN	Core Network
CVE	Common Vulnerabilities and Exposures
DoS	Denial-of-service
DDoS	Distributed Denial-of-service
eNodeB	E-UTRAN Node B (LTE base station)
eSIM	Embedded-SIM
E-UTRA	Evolved UMTS Radio Access Network
HAPS	High Altitude Platform Stations
HLR	Home Location Register
HN	Home Network
HSS	Home Subscription Server
ICT	Information and Communications Technology
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identifier
IMSI	International Mobile Subscriber Identity
IoT	Internet-of-things
IP	Infrastructure Provider
ITU	International Telecommunication Union
IWF	InterWorking Function
LTE	Long-term Evolution
M2M	Machine to Machine
ME	Mobile Equipment
MEC	Mobile-edge computing
MNO	Mobile Network Operator

MT	Mobile terminal
MTC	Machine-type Communication
NAS	Non-access stratum
NFV	Network Function Virtualization
NVD	National Vulnerability Database
ProSe	Proximity-based services
QoS	Quality-of-service
RAN	Radio access network
RAT	Radio access technology
SDN	Software defined networking
SDR	Software defined radio
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SS7	Signalling System 7
TAU	Tracking Area Update
TE	Terminal equipment
TN	Transit network
TRL	Technology readiness level
VLR	Visited Location Register
TVRA	Threat, Vulnerability and Risk Analysis
UE	User equipment
UICC	Universal integrated circuit card
USIM	Universal subscriber identity module
V2X	Vehicle-to-Everything
VLR	Visited Location Register
VMNO	Virtual mobile network operator
VNF	Virtual network function
VoLTE	Voice over LTE
VS	

1 Introduction

This deliverable, produced by the partners of the 5G-ENSURE project, describes a security architecture for 5G networks. Leveraging the draft security architecture presented in the previous deliverable D2.4, [d2.4], the security architecture is an extension and enhancement of current 3GPP 3G and 4G security architectures to cover the 5G context. The focus of the work lies in the security relevant modelling of 5G networks. The modelling results in a logical and functional security architecture aligned with the 5G network architecture developed within 3GPP, see TS 23.501 [ts23.501].

In this final version, we look upon a security architecture as a methodology for instantiation of secure systems, comprising a toolbox for security relevant modelling of a system, a set of security design principles and a set of security functions and mechanisms implementing the controls needed to achieve the predefined security objectives for the system. This view of a security architecture is corroborated by the security architecture defined in X.805 [x805]*;* in particular, X.805 states that "*the security architecture logically divides a complex set of end-to-end network security-related features into separate architectural components"* and *"this separation allows for a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing networks".*

The important qualities of a security architecture are thus, in a simple and straightforward way, to help identify where security controls are required and which the required security controls are. Furthermore, the security architecture should enable finding valid trade-offs between security and other essential requirements like performance and functionality. Here we note that there is an interplay between the network architecture and the required security controls. A poorly designed network architecture can make it impossible (or at least very expensive) to implement the security controls required to adequately protect the network. Conversely, making unfortunate choices in the selection of applied security controls may result in a highly secure network, but at the same time have a negative impact on the service performance of the network and in extreme cases, even may prevent them from working. For mobile networks, the security architecture also plays an important role in that, due to the regulatory aspects of telecommunications and spectrum usage, many aspects of the security architecture are strongly correlated with a network's ability to fulfil contractual and legal obligations, and to settle liabilities, etc.

To ensure cross-coordination between the security and network architecture work within the 5G-PPP, 5G-ENSURE has participated in the 5G-PPP Security and the 5G-PPP Architecture Working Groups. In particular 5G-ENSURE has provided the section on "5G Security Architecture" in the "5G PPP 5G Architecture White Paper" [5GPPPArchWP] and made the 5G security architecture part of the overall 5G architecture design contributing to the overall success of the 5G-PPP initiative.

1.1 Why a New Security Architecture?

The current 3G and 4G networks have security architectures defined in 3GPP TS 33.102 and TS 33.401 [ts33.102, ts33.401]. These architectures are discussed in detail in Section 4. Let us here just highlight the most important reasons why we simply cannot re-use them as is and why a new security architecture for 5G is needed. The security landscape of 5G will be further discussed in Chapter 2.

New Business models: Services for different vertical markets with specific service requirements will be built from both physical and virtualised network functions running on underlying infrastructure

resources in 5G. Many actors will be involved in providing services, functions and resources. A security architecture for 5G must be able to capture the needs of secure interactions, the appropriate isolation of components, and the management of actor's different functions and services.

Threat environment: The threat environment for ICT in general and consequently also for 5G networks exhibits more and more advanced threats to network functions and services. This situation may act as a "magnet" for more general and more advanced cyber threats when many new services, some mission critical, such as health, transport, industrial automation, etc. will rely on 5G networks. The damage done (even loss of life) may then go far beyond the worst imaginable impact on the "mobile broadband" type services that we see today. It is thus critical that the security architecture correctly models the network and can help capture current and future security needs.

Trust model: There is no explicit and complete trust model documented for 3G and 4G networks. This does not imply in any way that they are insecure for their designed purpose, but it does produce an issue in a 5G context where we have new actors entering the value chain with new business models, new services and new types of devices. Thus, there is a strong need to have a security architecture in which trust relations between actors and other entities in the network are visible and can be taken into account in the security design of the network.

Network Softwarization: A security architecture for 5G needs to take into account the use of virtualization and software defined networking and the security needs following the use of them. These technologies are fundamental for achieving the overarching objectives for 5G to provide a flexible and extensible infrastructure for all types of communication services on top of which a dynamic service and business environment can evolve. These aspects are not explicitly considered in the existing 3G and 4G security architectures.

Management: Management is almost completely left outside the scope of the security discussions for 3G and 4G, see e.g. [ts33.401], as it was considered implementation and operator dependent. In 5G, technologies will be blended; new roles, actors and types of services will appear. This will require a unified view on management to guarantee smooth interworking between network services and functions and also to enable delegation of management responsibilities to actors providing specific services. In particular secure orchestration and management of virtualization, general forms of security management (e.g. monitoring) are absolutely fundamental for 5G to operate robustly. Without it, we cannot achieve the robustness required by telecom regulatory constraints.

1.2 Contributions

A 5G (or any other) security architecture does not in itself provide answers to what the security threats to the network are, or which threats need to be mitigated by specific countermeasures. The basis for answering these questions must be a multi-stakeholder Threat, Vulnerability and Risk Analysis (TVRA), see e.g. [d2.6 Chapter 3], taking the security objectives for the network into account. The TVRA should result in a risk treatment plan defining which threats to handle where and how. A high-level illustration of dependencies between work performed in 5G-ENSURE and the TVRA is found in Figure 1.

The security architecture presented in this deliverable provides a toolbox for modelling 5G networks in a security relevant way. This model is of course essential in the TVRA but should also be taken as a starting point for the trust modelling and the risk assessment, mitigation and requirements work. The security controls in the security architecture are the means for protection of assets in the risk

treatment plan. Finally, the security design principles guide in selecting the security controls in the risk treatment plan and in the actual implementation.

In the deliverable "Risk assessment, mitigation and requirements (final)" [d2.6] a TVRA procedure is described and discussed together with security requirements for the 5G-ENSURE use cases. The risk assessment performed and the resulting security requirements are also part of the basis for the compilation of security objectives for the security architecture presented in this document.

The deliverable "Trust model (final)" [d2.5] describes a trust model which can be used in the TVRA to determine where security controls should be implemented. In particular the trust modelling work is essential for understanding where and how identified threats should be treated.

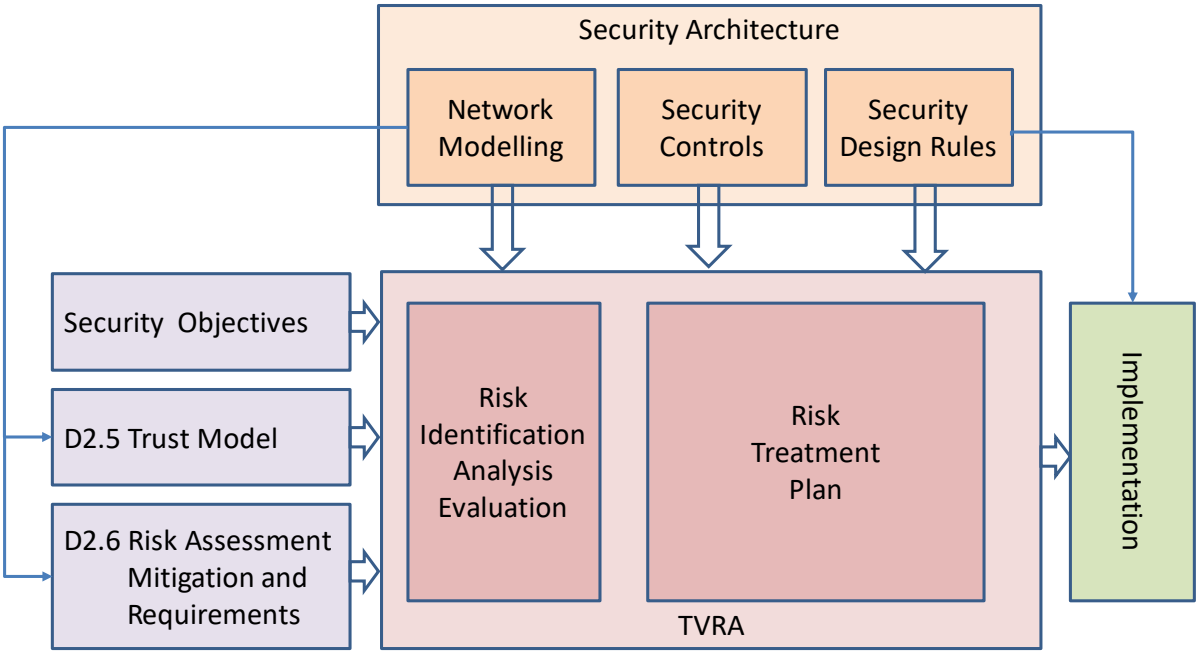

Figure 1: Illustration of dependencies between work performed in 5G-ENSURE and the TVRA.

The security architecture, the trust model and the risk assessment, mitigation and requirements work are all related to the use-cases analysed in deliverable D2.1 "Use Cases" [d2.1]. Here a relevant question to ask is if there is a risk that use-cases that might have led to a slightly different trust model and/or slightly different risks/requirements have not been considered, which in turn may have led to a slightly different architecture. Of course, such risk cannot be denied. However, the 5G-ENSURE project is confident that such a risk is minimal. Deliverable D2.1 covered 31 use cases and even though there is no "safety in numbers", it is not the quantity of use-cases that is critical but their quality. The use-cases have been selected because they seem to "span" the 5G Security problem space well, just as a small number of vectors can still span an "exponentially large" vector space. Furthermore, there has been no censorship: the 31 use-cases comprise all use cases suggested by the 5G-ENSURE partners. The expertise available in the 5G-ENSURE consortium makes it highly unlikely that an important corner of the security problem space is missing. Secondly, the 5G-ENSURE use-cases do not constitute the only background material. For example, the 3GPP "SMARTER" study [tr22.891] comprises over 70 uses cases and the overall 5G-PPP consortium has produced hundreds of use cases.

A special use-case harmonization activity has taken place in the 5G-PPP, with representation from 5G-ENSURE, in which no gaps were identified.

1.3 Updates and changes

Here we describe the major changes and updates of the security architecture in this report compared to the draft version [d2.4] published earlier.

TS33.102 and TS33.401 introduces a categorization of security mechanisms by defining so called *security feature groups,* see also D2.4 Section 4.4. This naming of security features groups was used in D2.4 but has been changed in this final version of the architecture. The categories are now called security realms; the reason for this change is that these realms are more or less orthogonal in spanning the security space of 5G. The naming and definition of the security realms have also been updated to provide a more precise tool for handling different security aspects.

Furthermore, the security architecture has been updated to include security control classes, i.e. groupings of security mechanisms and functions for different types of protection mechanisms. A section on how the security architecture should be used has also been added. In Chapter 7, Table 3 illustrates how the 5G-ENSURE enablers are mapped on the security architecture.

In deliverable D2.4 it was proposed to adopt a methodology similar to the one used in the Common Criteria assurance standard [cc] starting with a security problem definition, followed by a definition of security objectives and then verification that all objectives are met and covered by the proposed security architecture. It turned out that this approach was really not viable because of the amount of work required to cover a system as big as 5G network. However, the security problem definition is kept and a list of security objectives for the security architecture has been compiled, see Chapter 3.

1.4 Report Layout

In Chapter 2 we present aspects of the general setting for our work to define a security architecture for 5G. We highlight new security characteristics of 5G capabilities, i.e. technologies adopted, new concepts and usage, with major impact on security considerations. We also summarise the 5G business and trust model developed and the high-level threats to 5G systems considered by 5G-ENSURE, which are relevant for the design of the security architecture. We also discuss the important regulatory aspects of 5G and their implications for security and implementation.

In Chapter 3, we present the 5G security problem statement then detail the objectives for the security architecture and the security of 5G networks. These objectives are derived from the study of the use cases relevant to 5G security (see [d2.1]), security threats detailed in [d2.3] and TR 33.899[1] [tr33.899], which contains a study on the security aspects of the next generation system (i.e. 5G).

Chapter 4 presents the concepts in the security architecture comprising security domains, strata, security realms and security control classes. Domains group network entities according to physical or logical aspects that are relevant for 5G networks. A stratum is concerned with the grouping of protocols, data, and functions related to one aspect of the services provided by one or several domains. A security realm captures the security needs of one or more strata or domains and a security

[1] TR33.899 has been withdrawn, but its content is still relevant for the security design of 5G networks

control class is a collection of security functions. Additionally, we map 3GPP 5G network functions onto our domains and show how our security architecture can be used to secure a 5G use case.

Chapter 5 reviews the objectives for the security architecture and analyses how they are met. It also contains a discussion on security enforcement in domains and strata.

Chapter 6 addresses the high-level security design principles for the architecture and recommendations as to how to proceed. We make recommendations as to how to apply these principles in a 5G architecture.

Chapter 7 presents the mapping of 5G-ENSURE security enablers towards 5G-ENSURE Security architecture. Secondly, it proposes a way to use the 5G-ENSURE Security architecture to map a practical use case and deduce the Security controls needed in this context.

Section 8 covers existing work in the area of security procedures for 5G systems. In particular, we discuss 5G security related work from various entities such as 5G-PPP, 3GPP, ITU, NGMN, IETF, and OMA.

Chapter 9 summarizes the reported achievement.

2 The Security Landscape of 5G

5G is being developed with new concepts and capabilities to enable new business models for mobile operators to provide enhanced applications and services to mobile network subscribers. In order to ensure that 5G fulfils its promise, all security matters accompanying the 5G architecture need to be addressed. 5G networks will require complex security requirements at different layers within the system. 5G networks must support a very high level of security and privacy for their users (not restricted to humans, but also tailored to machines, systems etc.) and their traffic. At the same time, networks must be highly resistant to all kinds of cyber-attacks. To address this two-fold challenge, security cannot be regarded as an add-on; instead, security must be considered as part of the overall architecture and start with a security by design approach be built into the architecture right from the start. This approach will protect subscribers, devices and their communications, as well as the integrity of the network itself, whatever the use case.

This section intends to highlight the security characteristics of 5G capabilities; 5G's business and trust model; high-level threats to 5G systems; the regulatory aspects of 5G; and provide a 5G security problem definition.

2.1 Security Characteristics of 5G Capabilities

5G will embrace new technologies and concepts as a significant evolution from 4G. It will employ virtualisation technologies to enhance its infrastructure's flexibility and scalability. Thanks to SDN, it is also refining its network slicing concept to more dynamically offer various kinds of services to VMNOs and users. Besides, 5G aims to enhance its support for low-latency, location-aware, and network-aware applications with mobile edge computing, as well as its support for various kinds of IoT applications. Finally, 5G will incorporate the support, to a higher extent, of other non-3GPP network access technologies to enlarge its service reach to various UEs.

All these new capabilities are exciting and will bring significant benefits to operators, application services and end users. However, they also bring new security challenges and characteristics that needs to be addressed to ensure a successful deployment of these capabilities. This section will discuss the security characteristics of the 5G capabilities.

2.1.1 Virtualisation

5G intends to leverage virtualisation to be cost-effective in infrastructure deployment, flexible in scaling, and dynamic in providing new services. Virtualisation is the underlying enabling technology for network function virtualisation, network slicing, and mobile edge computing in 5G. The current security support for virtualisation, developed and deployed in public and private clouds, serves as the fundamental protection of 5G's virtualised infrastructures, functions and services. However, as a mobile network has a more stringent security requirement than a typical cloud provider in terms of service availability and data privacy, 5G observes in particular the following security characteristics of virtualisation.

- Integrity of virtualisation platform: The integrity of virtualisation platform is the root of trust for virtualised functions and services in 5G.

- Authentication of software entities: It is important to authenticate virtualised network functions, mobile edge applications, and other software entities running in the virtualisation platform to protect against attacks by impersonating software entities.
- Isolation of resources: Runtime memory, data, I/O and other assets of each software process needs to be isolated from the others to ensure that they are not leaked, misused, or corrupted.
- Compliance monitoring of resources: While technical monitoring of resources is self-evident, there could be compliance requirements that the virtualised resources also have to meet. These could, for instance, relate to the geographical locations of the resources and whether such locations are acceptable for the service in question. One might also need to get assurance that certain level of security is offered, instead of resorting to a configuration with weaker security requirements. Some components, such as VNFs, might also need to be certified in order to get the assurance of their proper functions.

2.1.2 Network Slicing

Network slicing (and further sub-slicing) could be used to create portions of the underlying network to provide network services with particular properties.

Slicing can be utilized in such complicated cases where more than one Virtual Mobile Network Operator (VMNO) shares the same 5G physical network which is operated by a provider of virtualized infrastructure. The VMNO's may control their own slices while they provide sub-slices to their customers. The main security characteristics for network slicing are listed hereunder.

- Micro-segmentation to control and prevent anomalies: Anomalous behaviour in an SDN network can be easier to detect and to respond, if the 5G network system is (virtually) divided into smaller parts, i.e., network slices, sub-slices and micro-segments. Through this approach the surface for attacks and threats can be reduced significantly.
- Extremely secure services: Micro-segmentation could provide an even more fine-grained approach than traditional network slicing and with micro-segmentation it can be possible to create extremely secure segments where more granular access controls and stricter security policies can be enforced.
- Trustworthiness of sliced system: For advancing security of the sliced system, the authenticity and integrity of the received data and commands in each slice must be ensured. Furthermore, to control the access between slices, security mechanisms must be able to check, if the received data/commands, originated from within the slice or not (from a legitimate entity). In other words, it must be able to check its trustworthiness, to prevent access from other slices.
- Satisfying SLA objectives: The security system must also ensure that the different SLA objectives for the different slices are met. The SLA objectives will be different depending on the slice's use case (e.g. autonomous driving, health applications, massive IoT, real-time 4K video broadcasting, etc.). To control the varying and sometimes conflicting SLA objectives, the SDN controller should support policy-checking functions.
- Slice isolation: In a 5G network, the isolation of slices (isolation assurance within 5G nodes) must be ensured. This assurance must be provided at two levels, at security level (threats propagating through the slices) and at resiliency level (faults in the physical infrastructure propagating through the slices).

- Physical isolation: A compromised slice may compromise the security of other slices sharing the same physical 5G nodes.
- Limited physical resources: Unavailability of a physical network resource (physical 5G node) serving the slices, due to intentional or accidental disruption, may propagate to unavailability of those slices (a.k.a. cascade effect).
- Data integrity and authenticity: Integrity and authenticity of the data/commands uploaded/downloaded by a 5G controller/object must be ensured to avoid any security issues.
- Resiliency through real-time monitoring and controlling: Resiliency of a sliced system should be ensured to prevent cascade effects between different slices. This can be done by checking in real time which part of the physical infrastructure is ensuring the integrity of a given slice topology and by proposing migrations upon detection of vulnerable, attacked, compromised or affected physical resources. For that, it is necessary to support on-the-fly retrieval of the dynamic dependencies between the slices and the physical infrastructure in order to assess the propagation of faults and attacks in a given slice.
- Secure Slice management: 5G networks will provide capabilities for third parties to create and manage network slice configurations (e.g. scale slices). The network also provides capabilities for operators to manage slices, e.g. set parameters for resource sharing or dynamically create network slice. The capabilities to manage network slices should be under control of authorized third parties to avoid illegal access and prevent possible attacks to slices (e.g. terminate a slice or a compromised critical network function). Also, security with interacting parties should be provided in terms of the API used to access the slice management system

2.1.3 Mobile Edge Computing

Mobile edge computing (MEC) is a capability of hosting third-party applications at the edge of a mobile network on edge hosts deployed at radio nodes, on aggregation points, or on the edge of the core network. MEC creates new opportunities for 5G operators and applications. First, it allows better support of low-latency applications by placing them in close proximity of their users, avoiding having application traffic traverse the core network. Second, mobile operators can provide mobile edge services, such as location and radio information, to third-party mobile edge applications so that they can optimise their performance and responsiveness. The security characteristics of MEC can be observed in the following aspects.

- Mobile edge hosts outside the mobile operator's premises: Since the data traffic of mobile edge applications do not go through the core network, it seems that lawful interception and traffic accounting need to be performed at the mobile edge hosts. If the mobile edge hosts are deployed at radio nodes or aggregation points, lawful interception and traffic accounting would very likely have to be conducted outside the mobile operator's premises, in a stadium, in a shopping mall, on a campus, on a hill, on a rooftop, etc. This increases the risks of exposing the lawful interception and traffic accounting functions to attacks for illegal eavesdropping, fraudulent billing, etc. Besides, with numerous cloudlets (mobile edge hosts) outside the operator's premises, the physical protection of MEC's virtualisation environment is more challenging than a standard cloud environment.
- Provision of mobile edge services: In MEC, the mobile operator can provide mobile edge services to third-party mobile edge applications. It is necessary that the mobile edge services

are capable of authenticating the mobile edge applications to ensure legitimate access to their services. This may in turn pose threats to credentials exposed outside the core network.

- Service continuity of mobile edge applications upon UE handover: In the event of UE handover, to maintain the low-latency communication and context awareness of the mobile edge application, it is necessary that the UE be served by the closest instance of the mobile edge application. Thus, service continuity has to be supported either by an application context transfer from the current instance of the mobile edge application to the next instance, or by the transfer of the mobile application instance itself from the current mobile edge host to the next one. In either case, it is necessary to assure that the source and the destination mutually authenticate each other, and that the transfer is secure.
- UE authentication and re-authentication: Low-latency communication is one of MEC's key promises. The current UE authentication and re-authentication approach in pre-5G mobile networks may need to be enhanced to minimise or eliminate their disruption to low-latency communication, in particular during a UE handover.

2.1.4 Internet of Things

One of 5G's key objectives is to support Internet of Things use cases. IoT use cases often involve a potentially large number of IoT devices, from a few home network devices to hundreds of thousands of smart meters. For 5G, IoT presents the following security characteristics.

- Surge of network signalling: In many IoT use cases, the IoT devices behave similarly and very often act simultaneously. When such IoT devices are numerous, this could pose a security challenge to 5G because the 5G network must deal with sudden surges of network signalling and application traffic. The network needs to gracefully sustain the overload without breaking down.
- Distributed denial of services (DDoS): IoT is becoming a new attack vector for DDoS. Whether the attack target is the mobile network or an application, the mobile network will face a flood of network signalling and application traffic. As indicated above, such behaviour is very typical of IoT use cases. Even non-malicious device malfunctions could result in attacks. Thus, it is important that 5G can distinguish DDoS from normal IoT behaviours to protect the network resources.
- Extremely constrained devices in a network with strong security algorithms: IoT devices are often designed to operate with extremely low power. Therefore, their processing power and memory size can be limited and they may not be able to support strong security algorithms. Even their radio interface can be non-3GPP, supporting only ZigBee, Bluetooth, or WiFi. Such constrained IoT devices may not be able to access 5G networks directly themselves, and in that case special 5G user equipment may act as IoT gateways for groups of IoT devices. With this approach, each IoT device may still establish itself a point of presence and unique identity in the 5G network and enable itself a service differentiation (such as specific QoS). 3GPP specifies MTC-IWF and Service Capability Server (SCS) to support MTC.
- Group-based authentication and security: In many cases IoT devices may advantageously be treated as groups based on their physical location, type of sensors or actuators, type of application, or other factors. Such device groups could perform simultaneous authentication through an IoT gateway or a mobile device which acts as a relay. This approach could strongly reduce the AAA overheads since each device need not execute the complete protocol

individually. In group communication setting also arises the need for securing multicast and broadcast traffic with specific security requirements.

- Impact of high latencies and low access priorities on authentication: For supporting IoT, 3GPP now develops specifications for low access priority, extended access barring and high latency communication. The UEs can be configured with low access priority, which means that much longer delays are tolerated when accessing the network, while high latency communication allows mobile-terminated communication with UEs running in power saving mode. These changes may require enhancement of current authentication procedures.

2.1.5 Heterogeneous Network Access

5G is expected to bring more flexibility to network access. Not only several different kinds of technologies could be used to provide the radio access, but also authentication would be more dynamic and local for access to 5G services.

- Enhanced identity protection: While Internet of Things is one major driving force for the convoluted radio access, satellite is also likely to play part in providing heterogeneous access, especially in sparsely populated or hard-to-reach locations. A challenge is to ensure the same level of protection in terms of authenticity and identity protection to these complementary technologies. Pseudo-identifiers could be used to provide better anonymity against tracking of clear text device identifiers, but more advanced key management solutions with perfect forward secrecy could also be used to mitigate any effects of key leakage.
- Identity services interoperability: When it comes to identifying the subscriber identities, there is likely to be more interactions with different kinds of identity providers. MNO could interact with the AAA services of an enterprise or a satellite provider to authenticate the users, while it could also provide identity management services to third parties.
- Dynamic roaming: Dynamic roaming would allow access even in the cases where static roaming agreements do not exist between the home operator and the serving network. In other words, a subscriber might have service needs which could not be covered by the current agreements of the home operator. Such use cases could involve, for example, satellite networks to provide resiliency to improve the decreased level of service due to disruptive environmental conditions such as earthquakes, or capacity overload such as temporary surge of number of users. This calls for mechanisms to establish sufficient trust and assurance of compensation between the network entities.
- Strong accountability: In order to address spoofing concerns, there should be a stronger linkage between the use and the identities. For instance, in the above mentioned dynamic roaming use case, the home operator could get assurance that a subscriber trying to get access to the network is genuine (the same non-repudiation assertion regarding compensation could be then given to the visited network as well). One way of achieving this could be through cryptographic identifiers. Such identifiers also make it easier to bind user related signalling messages to the user, so that it is harder to try to spoof user identity in order to incur costs which are not legitimate. The introduction of cryptographic identifiers and digital signing of signalling could also be used to mitigate DoS concerns in cases due to spoofed signalling messages.

2.1.6 Critical Service Support

Since 5G targets applications related to industrial automation, public safety, vehicle-to-vehicle, and communication with cyber-physical systems, the needs in the area of robustness, resilience high availability and fault-tolerance will be more profound, ranging all the way from radio-access to back-bone transport. For example, security mechanisms used for ultra-low latency, mission-critical applications may not be suitable in massive IoT deployments where mobile devices are inexpensive sensors that transmit data only occasionally. Latency critical services will require distribution of the core to edge data centres, while new services will require more flexible application management and automated delivery. Such new service use cases, as vehicular traffic control or industry control, place the highest demands on the dependability of the network. Indeed, human safety and even human lives depend on the availability and integrity of the network service.

2.2 Business and Trust Model Summary

5G will be about connecting people and things profitably. These are entirely different business models, yet the flexibility of 5G radio and architecture will enable operators to be profitable in both.

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

As a result, 5G will bring radical changes to mobile communication. Applications for 5G are not only driven by the Internet and telecommunication industry, but also by other industries such as automotive, healthcare, industrial networking, manufacturing and logistics, financial and the public sector. These kinds of industry applications may have very different reliability and latency requirements when compared to traditional telecommunication applications in 4G.

One new possibility for 5G is that due to virtualization a network operator might opt to run parts of its network functions and applications for example on an external cloud infrastructure. One could imagine that for example parts of the subscriber database is run on an external cloud. In this case, a new actor is the external cloud provider who is not part of the existing 4G trust model.

Another new domain for 5G is the possibility to “insource” network functions from third parties in order to enhance the network and/or the services it offers. One could imagine that a content distribution network (CDN) provider integrates caches in a network operator’s network. Another way to extend the network offerings could be that for example a factory is allowed to provide its own identity and authentication mechanism for the devices in the factory and that these devices, authenticated in a non-3GPP way, are then authorized to use, say a slice of the operator’s network.

It therefore makes sense to consider the different possible 5G network actors. The following list of 5G actors is reproduced from deliverable D2.5. New actors compared to the 4G setting are highlighted with a “[5G]” label.

- **Network equipment manufacturer**
    - Terrestrial equipment manufacturer
    - [5G] Satellite equipment manufacturer
- **Infrastructure Provider**
    - [5G] Virtual Infrastructure Provider (VIP), providing Infrastructure as a Service (IaaS)

    - [5G] Satellite/ High Altitude Platform Stations (HAPS) provider
- **Network software provider;** commonly also the network equipment manufacturer
    - [5G] Virtual Network Function (VNF) provider
- **Interconnect network provider** (provides a network linking one network operator to another)
- **Mobile Network Operator** (MNO) (taking the role of "home" or "serving" operator); commonly also the infrastructure provider
    - Virtual Mobile Network Operator (VMNO) who purchases bulk capacity from MNOs and may (or may not) have their own HSS
    - [5G] Virtual Mobile Network Operator (VMNO) who purchases SDN slices from an Infrastructure Provider
    - [5G] Factory or enterprise owner operating a AAA in a network linked to a (V)MNO
- [5G] **Satellite Network Operator**; commonly also the satellite/HAPS provider
- [5G] **Network access provider** (uses the services from one or more Satellite/Mobile Network Operators to provide bulk transmission resources to Service Providers)
- **Service Provider**; commonly also the (V)MNO
    - [5G] Over-the-Top (OTT) service provider
- **User equipment manufacturer**
    - Phone manufacturer
    - UICC manufacturer
    - [5G] Sensor manufacturer
    - [5G] Robot manufacturer
    - [5G] Vehicle Manufacturer
- **User equipment software developer/provider**
    - User equipment operating system developer/provider
    - User equipment application developer
    - Application store provider
- **End user**
    - Common phone users (Service Provider subscriber)
    - [5G] Wireless Sensor Network (WSN) owner/operator
    - [5G] Employee of enterprise
    - [5G] Vehicle owner/driver/lease company
- **Regulators**, law enforcement agencies

Different business offerings will require different combinations of the above actors, and therefore understanding the relationships between these actors is vital. Typically, an actor will rely upon other actors, and the services they provide, in order to deliver their own business offering. Given the potential consequences for a business, if a third-party fail to deliver a service that is required in order to meet their own customer obligations, it is vitally important that a business knows who or what they are trusting, and why.

Trust as a concept is often discussed in the 5G community. At the ETSI Security Week in 2017 [etsi-sw-2017], the need for a well-defined trust model was highlighted by several speakers as one of two major technical challenges, along with isolation between virtual networks running over the same infrastructure. These were identified as the biggest remaining barriers to realising the 5G vision of agile, flexible networks that can be provisioned rapidly and operated safely by traditional

telecommunications operators and (most significantly) by vertical consortia in specific sectors. A VMNO may be a vertical integrator such as an automotive manufacturer or a health care administration with no prior experience of large scale network operation. Even virtual mobile networks run by traditional operators may depend on customer or third-party services for functions such as AAA, as well as a range of virtualised network functions. One cannot assume that new actors operating 5G networks or critical network components have the same understanding of security challenges or their responsibilities in protecting networks and users from security breaches.

The approach taken in 5G-ENSURE recognises that trust (i.e. a firm belief in the reliability, truth, or ability of someone or something) is actually a response to a perceived risk. In fact, when faced with a risk, the possible responses to it are:

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

These actions all involve trust decisions; either choosing to trust someone or something, or choosing not to trust at all.

The 5G-ENSURE project provides a high-level architecture describing the different domains and strata, aligned with the equivalent 3GPP concepts. It also defines two further concepts: security realms which capture security requirements in one or more domains or strata, and security control classes which refer to security measures that may be used to reduce risks. The 5G-ENSURE security enablers provide a means to implement selected security control classes that are particularly relevant for 5G networks. Other security control classes may (in many cases) be implemented using off-the-shelf solutions found in previous generation networks.

However, within the 5G-ENSURE architecture it is not possible for a stakeholder to implement all the security control classes needed to address every risk that is relevant to their specific security realm. In many cases the necessary control features must be implemented in domains over which that stakeholder has no influence. In general, this creates security dependencies between domains, and forces stakeholders to trust each other to implement appropriate security measures in each domain.

In deliverable D2.5 [d2.5] a model of the trust relationships between the different 5G actors is developed from a careful analysis of the 5G use cases defined in deliverable D2.1 [d2.1]. A formal model of the different assets, actors, and relationships in a 5G network was constructed using Trust Builder, a 5G-ENSURE security enabler (see deliverable D3.6 [d3.6] for more details on Trust Builder). From this formal model, the trust relationships between the 5G actors was mechanically computed using machine reasoning in a series of steps:

1. Threats were identified by finding vulnerable design patterns in the 5G-ENSURE architecture. This included 5G specific threats found in use cases as analysed in deliverable D2.1 [d2.1].
2. Risk mitigation measures to counteract these threats were added to the model, based on the analysis of risk mitigation in deliverable D2.6 [d2.6], except where the risk is likely to be acceptable to the affected stakeholder(s).

3. The resulting model was then queried to determine which stakeholder(s) would need to be responsible for implementing mitigation measures.

Note that in any given vertical application, it will be possible to accept some risks that are unlikely or have minimal impact given the nature of the application. Which risks are acceptable will of course depend on the application, so we expect there will be some trust assumptions that stakeholders may choose to leave implicit. However, the output of the last step will tell us which trust assumptions must be made explicit between the stakeholders in that (vertical) application.

In practice, each security control class will contribute to mitigation against multiple threats, e.g. by using mutual authentication one can address spoofing threats and go some way towards addressing snooping threats (although authentication alone is not sufficient to address snooping threats). We therefore expect the trust model expressing the assumptions made by a given stakeholder will be in two parts:

- a statement of security control classes that should be implemented by other stakeholders in each domain: essentially, this expresses assumptions about what security is provided; and
- a statement of how risk is shared for (groups of) threats that are not addressed.

Threats that are not addressed may include those the stakeholder has chosen to accept (in which case they will normally bear the consequences), and those for which other stakeholder(s) failed to deploy the necessary security measures. Note that in the latter case compensation need not be linked to who is at fault, not least because a formal business relationship may not be appropriate between every pair of stakeholders. For example, a subscriber will normally only have a contractual relationship with their VMNO, so if they need to be compensated for (say) a privacy breach, this may have to be done by the VMNO in the first instance. Of course, one would expect the VMNO in turn to have transferred this risk to other stakeholders where they are responsible for implementing the necessary security.

2.3 High Level Threats to 5G Systems

Wireless communication is inherently vulnerable and needs specific protection against interception and tampering. Ever since GSM—the second generation of mobile networks—encryption has been used on the radio interface to secure the user communication. In the next two generations of mobile networks, UMTS and LTE, respectively, the security measures against threats was significantly enhanced. Besides encryption of user traffic, these networks have also provided mutual authentication between mobile terminals and the network, as well as integrity protection and encryption for all control and management traffic. Overall, UMTS and LTE security features ensure not only a high level of security and privacy for subscribers, but, very importantly, also assure the resilience required to combat various forms of attacks against the integrity and availability of the services these networks provide.

The LTE security concepts have not shown any major flaws since they were specified 10 years ago. This raises the question: Are new security concepts required for the next mobile network generation to circumvent existing and new threats? The answer is yes. On the one hand, the support of a variety of new use cases and, on the other, the adoption of new networking paradigms has made it necessary to reconsider some current elements in risk management. Figure 2 visualizes the main drivers for 5G security.

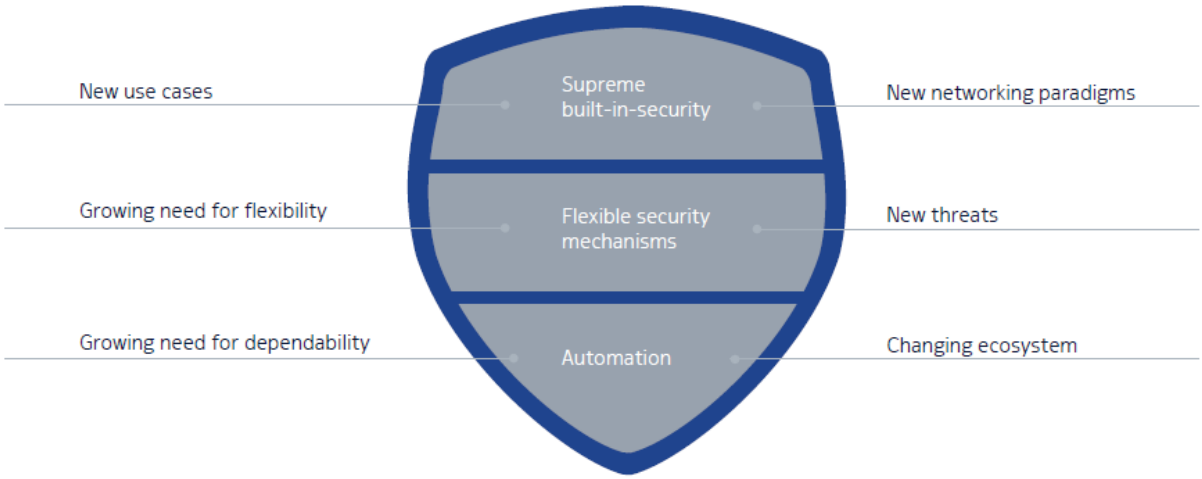

Figure 2. 5G security drivers and new threats

While LTE was designed primarily to support the mobile broadband use case (i.e., broadband access to the Internet), 5G targets a variety of additional use cases with a variety of specific requirements, inducing bigger attack surface. These cases include support of an enormous density of mobile devices or the need for ultra-low latency in the user communication. Use cases, such as vehicular traffic control or industry control, place the highest demands on the dependability of the network.

To support each use case in an optimal way, security concepts will also need to be more flexible. For example, security mechanisms used for ultra-low latency, mission-critical applications may not be suitable in massive Internet of Things (IoT) deployments where mobile devices are inexpensive sensors that have a very limited energy budget and transmit data only occasionally.

To efficiently support the new levels of performance and flexibility required for 5G networks, it is understood that new networking paradigms must be adopted, such as Network Functions Virtualization (NFV) and Software Defined Networking (SDN). At the same time, though, these new techniques also bring new threats. For example, when applying NFV, the integrity of virtual network functions (VNFs) and the confidentiality of their data may depend to a larger degree on the isolation properties of a hypervisor. More generally, they will also depend on the whole cloud software stack. Vulnerabilities in such software components have surfaced in the past quite often. In fact, it remains a major challenge to provide a fully dependable, secure NFV environment. SDN, for its part, bears the threat that control applications may wreak havoc on a large scale by erroneously or maliciously interacting with a central network controller.

5G-PPP security White Paper [5GPPPSecurity], as the result of a joint effort across the various 5G-PPP Phase 1 projects, lists the following major 5G security risks:

- Unauthorized access or usage of assets, e.g. 5G Identity thefts or cloning, opportunistic and fraudulent usages of shared resources, unauthorized access and/or modification of 5G connected devices critical data, etc.;
- Weak slices isolation and connectivity, e.g. sensitive data, managed inside a slice, could be exposed to applications running in other slices services, through side channel attacks;
- Traffic embezzlement due to recursive/additive virtualization;
- Insufficient technology level readiness (TRL);

- Difficulties to manage vertical SLA and regulation compliance, e.g. difficulties to address, manage and deliver, from an E2E perspective, the verticals' SLA and to comply with actual present regulations and known evolutions of the regulatory framework;
- Slicing VS Neutrality risks, i.e. slicing concept seems not to be fully compatible with network neutrality concept, while both, however, are regulated by the EU Regulation;
- Trust Management Complexity and liabilities between parties in complex 5G infrastructures;
- Provisions to facilitate change of service provider Domain Lock-in, i.e. lack of common security standards and guarantees across multiple domains could lead to provider lock-ins, a slice owner being unable to easily and flexibly migrate all or parts of its virtual service infrastructure from one provider to the other, without affecting or degrading the security requirements and the expected levels of security SLAs.

2.4 Regulatory Aspects

Regulation is not a new aspect for mobile networks. 5G network, like the previous mobile network generations, must therefore undergo a set of regulations including new and old ones. Its implementation can be different. In this section, we first discuss the spectrum regulations. Then, we highlight the 5G ecosystem /environment in order to show that a responsibility re-allocation is needed and a new perception of neutrality is required. We also consider the roaming example to demonstrate the importance of responsibility re-allocation and liability chains. Finally, we provide the main security Lawful Interception requirements namely the privacy of users' data and confidentiality of communication.

The new 5G use cases like broadband access in dense area or Massive IoT, are expected to dramatically increase exchanged data. This is one of the main reasons to have a new spectrum for 5G. However, the frequency bands are very densely used and free spaces are rare. In the US and Europe, a major source could be the spectrum released by the migration from analogue to digital television. The frequency bands are designated by the ITU-R or by individual regulatory bodies. For 5G, the choices include new spectrum below 6GHz, as well as spectrum in higher frequency bands [bt], [ericsson]. The choice of spectrum either for licensed or unlicensed use is important because it affects the cost of equipment, hence the price of services, coverage and interoperability.

The 5G is assumed to be the future Internet. Unlike the previous mobile network generation, so called 4G/LTE, that provides homogeneous connectivity to customers, 5G is expected to be versatile: it will encompass various access network technologies, i.e., Fixed access, Radio Access (3GPP RANs and Non-3GPP RANs), and provide connectivity to heterogeneous services such as mass market, IoT and Public Safety. In this context, "*the telecom Industry warns, in what they called "5G Manifesto", that the current Net Neutrality guidelines, as put forward by BEREC, create significant uncertainties around 5G return on investment, concurs with Industry verticals that the implementation of Net Neutrality Laws should allow for both innovative specialised services required by industrial applications and the Internet Access quality expected by all consumers",* and points out *"the danger of restrictive Net Neutrality rules".* In addition, they consider the new *"concept of "Network Slicing" to accommodate a wide-variety of industry verticals' business models on a common platform, at scale and with services guarantees"* [bt]. In addition, 5G would imply new technologies, like virtualization, SDN and NFV. Thus, a new 5G ecosystem and new actors / roles / entities are emerging. In addition to traditional roles,

namely Mobile Network Operators (MNO), Service Providers (SP) and end users, we may have new roles such as Network Infrastructure Provider, Virtualized Infrastructure owner, Virtualized function provider or Slice owner. All those roles can be for instance assured by the MNO. In this case, we end up in the same case as previous mobile network generations where the MNO is the main owner of the mobile network and also main responsible for any issue (financially responsible). In the other case, where the roles are allocated to different entities / actors, main-owner-responsible system (applied in the previous mobile network generations) is not any more relevant. Consider for instance a VNF running within the network, this VNF is provided by a VNF provider A, runs within a slice that belongs to a Slice-owner B and managed by a slice provider C, is managed by a VNF manager D and runs over hardware from infrastructure provider E. If this VNF has a security or functional issue (e.g., unavailability, underperformance, security breaches, isolation breaches, non-compliance with security policies), is the responsible A or B or C or D or E or, A and B, or etc. How can we designate the responsible? In such a complex environment, it is important to set a traceability system that enables to identify the source of an issue and whom responsibility. Thus, Liability chains are important. This system can be based on remote / local attestation of a given property like the code integrity, the trustworthiness of the execution environment, the isolation of a slice and so forth. Certifications can also be a tool to build liability chains. Naturally, in addition to the technical solutions, agreements between different actors are needed.

Now consider the example of roaming, in the previous mobile network generations, we distinguish domestic and international roaming. Domestic roaming is used between national operators to offer a better coverage to end users in the same country. International roaming is used between mobile network operators from different countries. Whatever is roaming type, the roaming operator must rely on the choices made by the 'visited' operator running the network in that area. In a 5G context, roaming takes new dimensions. We can have roaming agreements at different level, e.g., between slice owner, between slice provider, between infrastructure provider, etc. For instance, we can have a roaming agreement between two slice owners even if they are running over the same infrastructure.

Whatever is the ecosystem, Lawful Interception (LI) requirements remain the same as in Section 13 of [d2.1]. Indeed, the LI dilemma is ensuring the end user and services privacy (namely the confidentiality) vice versa the ability to answer any LI requirement. This mainly results in the following elements. The mobile network operator must ensure that only those under surveillance are wiretapped, e.g., Authorities cannot wiretap users / entities not on the list. Only the mobile network operator must be able to trigger a LI action. These imply a strong isolation requirement in the mobile network to prevent fraudulent network access and abusive use of resources. In addition, only concerned entities (i.e., the mobile network operator, the LI service and the Law Enforcement Agency) have access to the list of the wiretapped and collected data. The mobile network operator must be able to answer any LI request without requiring any third party. This operation must not be detectable through observation or quality of service. Finally, in case of an end-to-end encryption managed by the network, the mobile network operator should be able to deliver plain data or the encrypted data along with the decryption key.

3 5G Security problem statement and Objectives

Here we aim to capture the core essence of 5G security as a problem statement, summarizing the security landscape and its threat situation as laid out above. Obviously, when facing the new 5G security challenges we must not neglect to provide at least the same level of security that users have been able to obtain in existing 2G-4G systems. This leads us to the following problem statement.

> *In 5G, maintain 4G success as a trustworthy mobile broadband service, and extend the security functions against a landscape of advanced cyber-security threats evolving from new use cases, such as critical communication services and IoT. Create highly scalable, flexible and efficient security infrastructure and security protocol design that fulfils the security needs of various stakeholders of the 5G ecosystem, including the needs of the traditional telecom stakeholders such as subscribers, network operators, and regulators, as well as the needs of emerging new stakeholder such as virtual mobile operators, and telecom-cloud infrastructure providers. Allow this multitude of 5G user categories to securely share common, virtualized network infrastructures.*
>
> *Build solid security for the new 5G radio technology, the new 5G access networks composed of a diverse set of different access technologies, the virtualized 5G core networks, and the global network-of-networks composed of virtual network components. Separate the security of access and core networks[2] allowing future-proof independent evolution of new radio, access network and core network technologies.*
>
> *Pay special attention to present and new types of end-user equipment such as sensors, actuators, groups of small devices, relay-nodes, smart phones, or any other end-user equipment, and make unauthorized tracking, interception or any other violation of privacy of the subscribers infeasible.*

Below, we present a break-down of this problem statement into more fine-grained *security objectives*. The first group of security objectives relates to the security architecture itself, i.e. which features does the security architecture have to exhibit to be able to capture all security relevant aspect of 5G networks. The following groups of security objectives are related to the security requirements of a 5G network. They are grouped according to the Security Realms defined as part of the security architecture, see Section 4.4. These objectives are mainly coming from the study of the use cases relevant to 5G security described in [d2.1] and the 5G-security threats detailed in [d2.3]. We have also included security objectives based on TR 33.899 [tr33.899], which contains a study on the security aspects of the next generation system (i.e., 5G). Note that the security objectives related to the implementation of a secure 5G network is not a complete list but rather it is a collection of security objectives relevant for the design of the 5G-ENSURE enablers. In Annex A we present a mapping between the 5G-ENSURE enablers and the security objectives we have listed.

3.1 Objectives related to the design of the security architecture

O1.1 5G security architecture should be able to group network entities based on ownership and functionality.

[2] This does not imply breaking "end-to-end principles" since it only affects lower layers. End to end security at e.g. IP or transport level is still possible.

O1.2 5G security architecture should enable consideration of future network solutions with new functionalities and services and re-evaluation of threats and security solutions not known or considered at design time (i.e., flexibility, adaptability and evolvability).

O1.3 5G security architecture should enable the description and analysis of the 3G and 4G network security as they will be an integral part of future 5G networks (i.e. backward compatibility).

O1.4 5G security architecture should make explicit trust relations between 5G actors and between 5G network entities.

O1.5 5G security architecture should enable depiction of the boundaries and interfaces of a 5G network.

O1.6 5G security architecture should identify security relevant protocols and network functions used and offered in a 5G network in order to build effective protection.

O1.7 5G security architecture should capture virtualization and slicing.

O1.8 5G security architecture should consider the management aspects.

O1.9 5G system should enable seamless interworking of different network technologies, mobile, fixed as well as satellite without downgrading the security.

O1.10 5G security architecture should enable structuring and modelling the mobile network functions and needs into areas with specific security concerns.

O1.11 Where possible, 5G security should be decoupled from specific physical deployments, focusing on defence-in-depth, in particular self-protection of assets, limiting dependency on protection at network, site, or node perimeter.

3.2 General security objectives

3.2.1 New Business and Use-cases

O2.1 5G system must be able to deliver and maintain SLAs to verticals in terms of: security, latency, bandwidth, access control from an end to end perspective.

O2.2 5G systems must allow secure interworking with external AAA, e.g. provided by a vertical

3.2.2 Security-relation to Legacy Systems

O2.3 5G system must improve the level of security and privacy compared to 4G.

O2.4 5G security and privacy should not negatively affect the security and privacy of the legacy systems.

3.2.3 Regulatory Aspects

O2.5 5G systems must comply with regulatory aspect, e.g. those related to Lawful Intercept and user privacy.

3.3 Access Network

O3.1 5G Access Networks should have resistance and resilience to false base station type of attacks and other DoS attacks.

O3.2 5G Access Networks should not introduce security or privacy issues. 5G system must not have security and privacy vulnerabilities identified in the previous mobile network generations such as the IMSI and IMEI unauthorized tracking or the denial of service provoked by the unsecured mobility messages (i.e., TAU messages).

O3.3 5G Access Networks security should allow for high efficiency in authentication and security set-up, supporting ultralow latency services.

O3.4 5G Access Networks should not grant access to non-authenticated or non-authorized users and devices.

O3.5 5G Access Networks should operate only approved software (liability of supplier).

O3.6 5G Access Networks should be designed to prevent any attempt to alter or modify (through parameters or software modification) its behaviour.

3.4 Management

O4.1 5G management systems should provide strong mutual authentication and authorization to nodes and functions.

O4.2 5G systems should provide functionality to mutually assess the trustworthiness before, and during interactions.

O4.3 Management communication should be secured and only manage licit requests or commands (authenticated).

O4.4 Management of subscriber credentials must support traditional UICC/USIM.

O4.5 Management of alternative credentials by an external vertical AAA must be done with a security level commensurate with both that of the vertical application as well as the operator business partner.

O4.6 5G systems must support security monitoring capable of detecting advanced cyber security threats and support coordinated monitoring between different domains and systems (e.g. mobile and satellite).

O4.7 5G management interactions must be auditable and produce evidence of liabilities.

O4.8 Management of network slices' resources should be securely authenticated and authorized.

O4.9 In a logical or physical part of the network, governed by a specific security policy, further fine-grained security policy enforcement should be possible based on mechanism such as e.g. micro-segmentation.

3.5 User Equipment

O5.1 Storage of subscriber and device identifiers should be secure in terms of integrity.

O5.2 5G security protocols must scale to support massive IoT.

O5.3 5G security protocols must be efficient enough for resource and energy constrained devices.

O5.4 Connected devices must be able to adequately protect critical data such as subscriber credentials.

3.6 Network

O6.1 5G networks should have resilience to DoS type of attacks.

O6.2 5G networks should have resilience to fraud type of attacks.

O6.3 5G networks should have resilience to attacks (privacy in particular) coming from interconnects.

O6.4 Interfaces between entities, nodes, or functions should be secured.

O6.5 Storage of security sensitive network information should be secured.

3.7 Infrastructure and virtualization

3.7.1 General

O7.1 5G system should enable a secure, reliable, and traceable sharing of network resources (i.e., compute, storage and network) between the various services having vastly different requirements such as reliability and low latency for tactile remote surgery and availability for massive IoT services.

O7.2 5G system should be dynamically scalable in order to easily and securely implement and confirm different security requirements, trust models and assurances for different network slices.

O7.3 5G infrastructure components should support necessary root-of-trust functionality.

3.7.2 Slicing

O7.4 5G system should deliver isolated slices, not sensitive to whatever perturbation coming from the others slices or the infrastructures itself (DoS, saturation of resources, side-channel between slices).

O7.5 5G system should prevent low level security slice to expose whatever part of the 5G system.

O7.6 5G system should enable configurable security of slices and be able to provide slice-unique security services as required by specific services and applications.

O7.7 5G system should be able to detect and confine any potential attack or damage to the attacked or compromised network slice.

4 5G Security Architecture Overview

This section defines and explains the main building blocks of the 5G-ENSURE security architecture. The core of our proposed security architecture for 5G networks extends and revises the domain and stratum concepts from 3GPP TS23.101 [ts23.101] and takes the 5G security objectives from Chapter 3 into account. We first elaborate in Section 4.1 on our rationale of choosing TS23.101 as a basis for the 5G-ENSURE security architecture. Then the domain and stratum concepts are described in Sections 4.2 and 4.3. They provide different viewpoints of a network and model different network aspects. Both concepts provide a general partitioning of aspects of a system so we introduce a partitioning based on security aspects in Sections 4.4 and 4.5 by introducing security realms and security control classes. Finally, we show how our security architecture can be used to design a secure network.

4.1 Rationale

TS23.101 identifies and names the reference points and functional groupings appearing in the general UMTS architecture at a high level, from both physical and functional viewpoints. Namely, the physical aspects are modelled using the *domain* concept and the functional aspects are modelled using the *stratum* concept. These viewpoints and concepts proved very useful and are widely used. For instance, the 3GPP system and security architecture defined in TS33.401 [ts33.401] builds upon these two viewpoints and concepts. However, we note that TS33.401 focuses on the functional aspects by using the stratum concept and uses less of the domain concept. This is one reason for lacking a solid anchoring in the trust model. TS33.401 also adds a categorization of security mechanisms by introducing so called *security feature groups*, which are loosely connected to the domains. Details are provided in the forthcoming subsections.

Although 5G networks will be in some regards very different from their predecessors, e.g., through the use of virtualization and support for diverse and critical non-telecom oriented services, they will still share similarities and they will reuse and extend concepts that have proved successful and that are widely adopted. Furthermore, 5G networks must provide some backward compatibility and will use existing network infrastructure to some extent, i.e., standard mobile broadband services will continue to be important and mobile operators will continue to have business agreements among themselves, offering users the ability to roam between home and serving networks, using USIM-equipped smartphones, etc. Reusing and building upon the accepted and well-known concepts and terminology in TS23.101 (also TS33.401 and other standards) helps to understand the similarities and differences better. In particular, the advanced features and capabilities of 5G networks are highlighted. Furthermore, it is more likely to quickly reach a common and coherent understanding, which results in consensus and new or revised standards. Finally, it provides us with the opportunity to clarify or correct earlier work by eliminating some of its misunderstandings or shortcomings that we have identified as part of our work.

4.2 Domains

We begin by quoting and briefly recalling the domain definition from TS23.101.

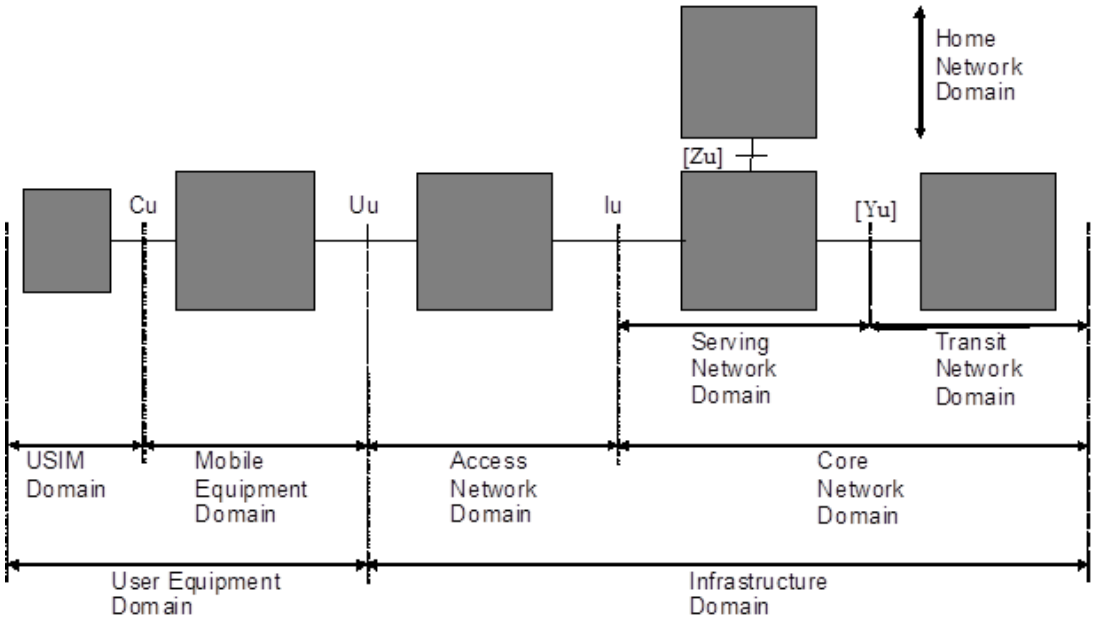

Figure 3: Domains and reference points as defined in TS23.101.

According to TS23.101 (Clause 3.1, p. 5), a *domain* is "the highest-level group of physical entities". Furthermore, "reference points are defined between these domains". Figure 3, also taken from TS23.101 (Clause 5), provides an overview of the domains and the reference points between them. The following list provides a short description of these domains. Note that domains can have subdomains to provide a more fine-grained grouping of entities.

1. **User Equipment Domain.** User equipment (UE) is the equipment used by the user to access network services.
    a. **Mobile Equipment Domain.** The Mobile Equipment (ME) performs radio transmission and contains applications. The mobile equipment may be further sub-divided into several entities, e.g. the one which performs the radio transmission and related functions, Mobile Termination (MT), and the one which contains the end-to-end application or (e.g. laptop connected to a mobile phone), Terminal Equipment (TE).
    b. **USIM Domain.** The USIM contains data and procedures which unambiguously and securely identify itself. These functions are typically embedded in a standalone smart card. The USIM device is associated to a given user, and as such allows one to identify this user regardless of the used ME.
2. **Infrastructure Domain[3].** The infrastructure consists of the physical nodes which perform the various functions required to terminate the radio interface and to support the telecommunication services requirements of the users. The infrastructure is a shared resource that provides services to all authorized end users within its coverage area.

[3] This domain name is introduced and used in TS23.101. In recent work however, namely [etsi_nfv], the same domain name is used with a different meaning. We decided to rename this domain of TS23.101 into Network Domain.

a. **Access Network Domain.** This domain consists of the physical entities which manage the resources of the access network and provides the user with a mechanism to access the core network domain.

b. **Core Network Domain.** This domain consists of the physical entities which provide support for the network features and telecommunication services. The support provided includes functionality such as the management of user location information, control of network features and services, the transfer (switching and transmission) mechanisms for signalling and for user generated information.

    i. **Serving Domain.** This domain represents the core network functions that are local to the user's access point and thus their location changes when the user moves. The serving network domain is responsible for routing calls and transport user data/information from source to destination. It has the ability to interact with the home domain to cater for user specific data/services and with the transit domain for non-user specific data/services purposes.

    ii. **Transit Network Domain.** This domain is located on the communication path between the serving network domain and the remote party. If, for a given call, the remote party is located inside the same network as the originating UE, then no particular instance of the transit domain is activated.

    iii. **Home Network Domain.** This domain represents the core network functions that are conducted at a permanent location regardless of the location of the user's access point.

The above definition from TS23.101 of the term *domain* is obviously too narrow for 5G networks. In particular, it limits itself to physical network entities and does not account for virtualized network entities, which will play a dominant role in 5G networks. We therefore broaden the scope of a domain as follows.

Definition. A *domain* is a grouping of network entities according to physical or logical aspects that are relevant for a 5G network.

The phrase "relevant for a 5G network" has been added to prevent the introduction of domains covering all sorts of logical aspects, which are however unrelated or only marginally related to 5G and/or networking aspects. A large number of domains would most likely result in a confusing and complicated architecture. Keeping in mind that complexity is usually unfavourable for security considerations, we seek to stop at a small number of domains, which are however already sufficient for capturing the gist of security in 5G networks. Examples of relevant aspects can include type of functionality, trust, (geographical) location, etc.

Furthermore, the respective domains User Equipment Domain, Infrastructure Domain, etc. as defined in TS23.101 also need to be revised and extended. Table 1 provides an overview of the domains we foresee in 5G networks. It uses the following abbreviations.

Table 1: List of domains foreseen in 5G networks.

Abbreviation	Meaning
UE Domain	User Equipment Domain
ME Domain	Mobile Equipment Domain
MEHW Domain	Mobile Equipment Hardware Domain
UICC Domain	Universal Integrated Circuit Card Domain
USIM Domain	Universal Subscriber Identity Module Domain
IM Domain	Identity Module Domain
A Domain	Access Domain
H Domain	Home Domain
S Domain	Serving Domain
CN Domain	Core Network Domain
IP Domain	Infrastructure Provider Domain
T Domain	Transit Domain
3P Domain	3rd Party Domain
IPS Domain	Internet Protocol Service Domain

In the following, we describe the domains of Figure 4 in more detail.

The horizontal lines H1, H2 and the vertical lines V1, V2 give a first high-level classification of domains. The ones above H1 represent the logical network aspects, called Tenant domains; the ones between H1 and H2 represent the physical network aspects, called Infrastructure domains; and the ones below H2 represent higher order groupings based on several aspects, e.g., ownership, called Compound domains. V1 separates the user equipment from the network, and V2 further separates the operator network from the external network, e.g., Internet services used by the operator network.

Note that Figure 4 also contains additional features for domains to account for network slices and trust issues between domains. Slice domains are, for example, depicted as solid and dashed parallelograms inside domains in Figure 4, which usually transverse several other domains. We refer to the forthcoming sections for additional details.

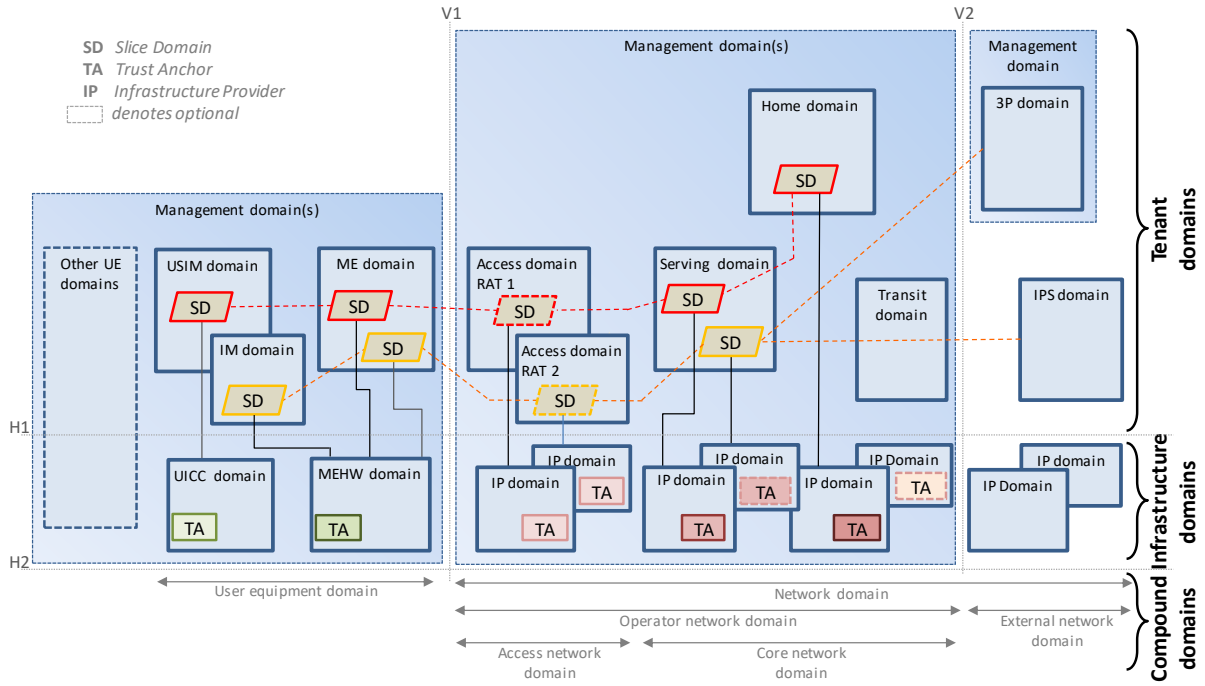

Figure 4: Domains of the 5G security architecture. The dashed lines H1, H2 and V1, V2 are used to mark logical or physical communication interfaces between domains. Rhombic shapes denote Slice Domains and lines from slice domains down to Infrastructure Domains denotes that VNFs allocated to a slice make use of certain physical resources.

4.2.1 Domain Types

With reference to Figure 4, we can make a first classification of domains according to whether they are physical or logical, by considering the horizontal line H1 separating *tenant domains* from *infrastructure domains*. These domains have direct correspondences in the ETSI NFV work [etsi_nfv]. We urge the reader to note that this means that "infrastructure domain" now gets a new meaning, different than the one it had in the previous 3GPP work (as the collection of network-side domains). For this reason, the domain corresponding to the infrastructure domain of TS23.101 is now assigned the new name Network Domain.

We also define the concept of *compound domain*. This is simply a collection of other domains, grouped together according to some 5G relevant aspect, e.g. ownership, joint administration or the like. For the time being, we foresee two new types of compound domains, slice domains and administrative domains, which we will elaborate more in detail below. The different types of domains are summarized as:

- An **Infrastructure Domain** focusses on the relevant physical network aspects, i.e. it contains the HW and (low level) SW providing infrastructure platform services, including hypervisors and trust anchors.
- A **Tenant Domain** is a logical domain executing in an infrastructure domain.
- A **Compound Domain** is a collection of other domains, grouped together according to some 5G relevant aspects, e.g. ownership, joint administration or the like.
- A **Slice Domain** is special type of compound domain. It is a collection of sub domains and/or domains grouped together to offer a specific 5G service environment.

4.2.2 Infrastructure Domains

The infrastructure domains focus on the relevant physical network aspects, similar to TS23.101. In other words, the infrastructure domains contain the "hardware" required by both the network domain and the UE domain.

4.2.2.1 Universal Integrated Circuit Card (UICC) Domain

A **Universal Integrated Circuit Card (UICC) Domain** contains the conventional tamper-resistant module offering protected storage and processing of long-term subscriber credentials required to access a 5G infrastructure and other security sensitive information. The UICC domain is under 5G Infrastructure Operator control.

4.2.2.2 Mobile Equipment Hardware (MEHW) Domain

A **Mobile Equipment Hardware (MEHW) Domain** contains the hardware support for the ME. The ME HW may include Trusted Execution Environments (TEE) supporting e.g. secure storage of other forms of credentials such as certificates.

4.2.2.3 Infrastructure Provider Domain

An **Infrastructure Provider (IP) Domain** contains the hardware platforms for the compute, storage, and networking resources required by both the network/telecom functionality and the access (radio) specific hardware.

4.2.3 Tenant Domains

4.2.3.1 Mobile Equipment (ME) Domain

A **Mobile Equipment (ME) Domain** contains the logical functionality required for using access network services, for the operation of access protocols by users and for user applications. (It is thus analogous to the ME domain of TS23.101, though it only contains the software parts.)

4.2.3.2 USIM Domain

A **USIM Domain** contains the logical functionality for USIM operation together with other hosted security services. (It is analogous to the USIM domain of TS23.101 but only contains the logical functionality.)

4.2.3.3 Access (A) Domain

An **Access (A) Domain** contains the logical functionality which manages the resources of the access network and provides users with mechanisms to access the core network domain.

4.2.3.4 Serving (S) Domain

A **Serving (S) Domain** contains the logical functionality which is local to the user's access point. It also routes calls and transports user data/information from source to destination. It has the ability to interact with the home domain to cater for user specific data/services and with the transit domain for non-user specific data/services purposes.

4.2.3.5 Home (H) Domain

A **Home (H) Domain** contains the logical functionality situated at a permanent location regardless of the location of the user's access point. The USIM is related by subscription to the home domain. The

home domain therefore contains user specific data and is responsible for management of subscription information. It may also handle home specific services, potentially not offered by the serving domain.

4.2.3.6 Transport (T) Domain

A **Transport (T) Domain** contains the logical core network functionality in the communication path between the serving domain and external remote parties.

4.2.3.7 Identity Management (IM) Domain

An **Identity Management (IM) Domain** contains functionality to support alternatives to USIM-based authentication, e.g. for industry automation use cases. (The IM domain may contain for example public key certificates. The IM domain preferable obtains security support from a UICC or from a TEE in the ME HW as discussed above.)

4.2.3.8 3rd Party (3P) Domain

A **3rd Party (3P) Domain** contains functionality for use cases where a (semi-)trusted third party provides services normally performed by an operator, e.g. when a factory/industry vertical provides its own authentication services for its M2M devices like industry robots and IoT-devices.

4.2.3.9 Internet Protocol Service (IPS) Domain

An **Internet Protocol Service (IPS) Domain** represents operator-external IP networks such as the public Internet and/or various corporate networks. Such networks may be partially or fully non-trusted.

4.2.4 Management Domain

A **Management Domain** contains the logical functionality required for management of specific aspects of a 5G network. Management domains may cover security management (i.e. ensure that the security services providing protection of network and user assets are in place and operational, e.g. setting up IPsec tunnels or other security mechanisms), management of security (i.e. management of the security mechanisms including e.g. identity, key and credential provisioning, configuration), traditional network management, orchestration of SDN and virtualized environments, and management of user equipment domains etc.

4.2.5 Compound Domains

As in TS23.101, and also for other, more 5G-specific reasons, we may also group domains together according to various criteria, thus creating *compound domains* as mentioned above.

4.2.5.1 User Equipment (UE) Domain

A **User Equipment (UE) Domain** is defined by MEHW, ME, UICC, USIM and IM domains included, i.e. it consists of the equipment used by a user to access network services.

4.2.5.2 Access Network (AN) Domain

An **Access Network (AN) Domain** is defined by both the A and IP domains, i.e. it consists of the entities that manage the resources of the access network and provides the user with a mechanism to access the network. It may comprise different types of access technologies, e.g. both WLAN and 5G-radio.

4.2.5.3 Core Network (CN) Domain

A **Core Network (CN) Domain** is defined by the H, S, T and IP domains included, i.e. it consists of the entities that provide functionalities to support the network features and telecommunication services such as user location information, control of network features and services, transfer (switching and transmission) mechanisms for signalling and for user generated information.

4.2.5.4 Operator Network (ON) Domain

An **Operator Network (ON) Domain** is defined by the AN and CN domains included, i.e. it consists of the physical nodes together with their various functions required to terminate the radio interface and to support the telecommunication services requirements of the users.

4.2.5.5 External Network (EN) Domain

An **External Network (EN) Domain** is defined by the 3P, IPS and IP domains included.

4.2.5.6 Network (N) Domain

A **Network (N) Domain** is defined by the ON and EN domains included.

4.2.5.7 Slice Domains

A central feature of 5G is network slicing, which we capture with a special form of compound domains.

Slice domains enable the network to provide virtual networks, optimized for delivering specific types of services, e.g. an ultra-low latency slice for critical industry automation, a slice optimized for real-time multimedia, etc. Indeed, specific slices could be defined to offer special security services, e.g. allowing special AAA solutions, unified threat management services, strong isolation of information etc. A slice can cover only parts of the network (i.e. part of the CN domain only) but may in other cases be defined end-to-end. It may therefore happen that while the slice is (logically) defined end-to-end, parts of the network are not implementing all the slice-support functions, for example, in a part of the network that uses some legacy equipment. We use the term *slice-aware* to signify if a particular part of the network has full support for slicing. A legacy part of the network, which may thus happen to not be slice-aware could still have functionality relevant for slicing. For example, (legacy) functions related to QoS could provide useful slicing support, even if other aspects of slicing (e.g. strong data isolation) is not present. In other words, slice related orchestration may still be performed in parts of the network that lacks full slice support. In Figure 5 we use dotted lines around parts of slices which are located in sections of the network that are not fully adapted to be slice aware. We use a solid line, drawn from the “slice box” to the IP domain, showing that for slice-aware domains, the slice is “anchored” in the domain.

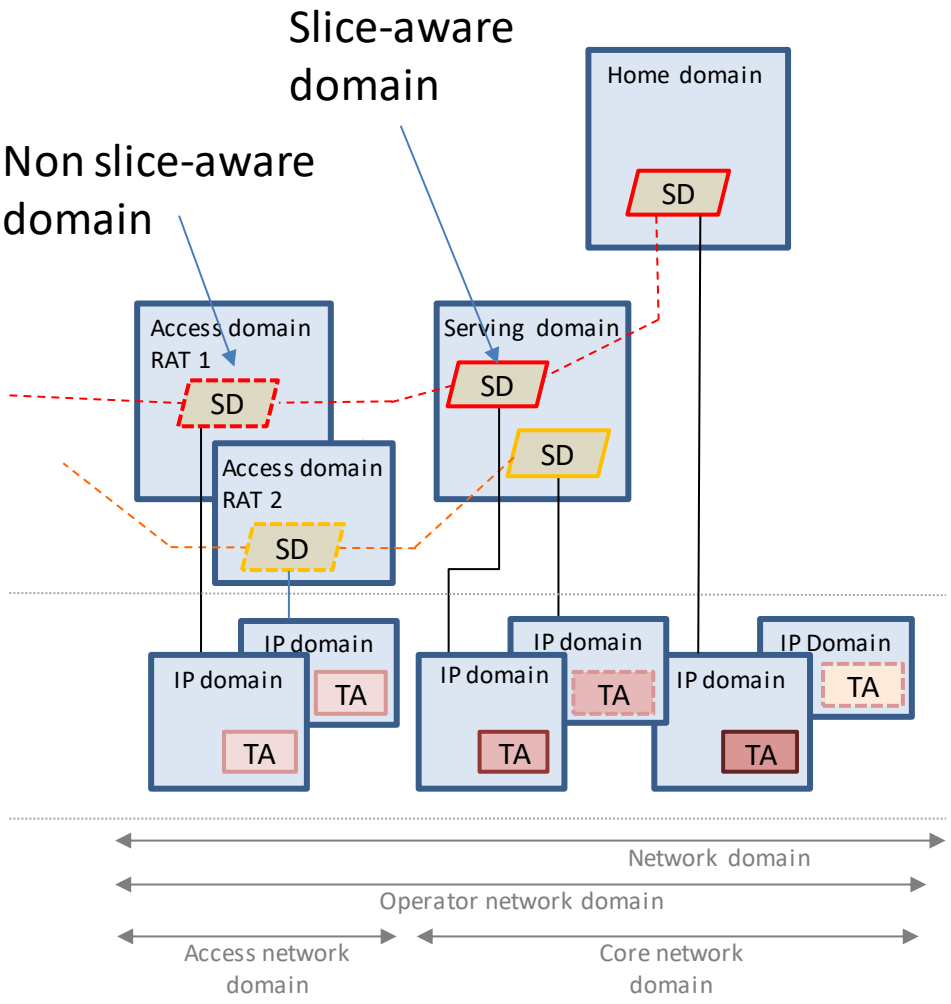

Figure 5: Slice-aware and non-slice aware domains.

Though not shown in Figure 5, it is conceivable that also some Management Domains may contain slices, separating different aspects of management.

4.2.5.8 Administrative Domain

An *administrative domain* is a special case of a compound domain defined not by the presence of a special functionality, but by ownership and/or administration. This is again borrowed from ETSI NFV. While not shown in Figure 4, an administrative domain is simply a collection of other domains, defined by ownership and/or administration. For example, a Serving (S) domain and Access (A) domain may jointly define an administrative domain if owned by the same mobile network operator.

Note that there is no direct coupling between administrative domains and management domains. For example, an A domain together with a S domain may form one administrative domain, denoted AD, e.g. defined by ownership of one single operator. That operator may however outsource the management of AD to a 3rd party (with liability regulated in contract). Thus, management of AD may be provided by a management domain belonging to a separate administrative domain, denoted BD.

4.2.6 Mapping of 3GPP 5G network functions

The 3GPP working group SA WG2[4] is in charge of defining the 5G architecture which comprises identifying which the main network functions of a 5G network are, how these functions are linked to each other, and which information they exchange. The SA WG2 is currently working on its TS 23.501[5] which will be the 3GPP's standard governing the "System Architecture for the 5G System". We take the opportunity to map the network functions defined in the 3GPP TS 23.501 onto the domains defined in 5G-ENSURE's security architecture. Note that, at the time of this writing, the 3GPP TS 23.501 is at version 1.2.0.

Figure 6 is a diagram that shows the 3GPP 5G network functions, denoted by "numbered" yellow circles, on top of the 5G-ENSURE domains. The corresponding network functions are described later. The "starred" pink circles denote the 5G-ENSURE domains that currently do not have any corresponding 3GPP 5G network function. The “starred” circles in the IP domain are in the scope of ETSI NFV (e.g., [etsi_nfv] also defines infrastructure and tenant domains as 5G-ENSURE) as 3GPP generally does not cover virtualization aspects. 5G-ENSURE’s scope is broader and has envisioned and covered both 3GPP’s and ETSI NFV’s scope. Note that the mapping shown in the Figure 6 is simplistic, e.g., only a non-roaming scenario has been assumed, single network function has been mapped only to a single domain, etc.

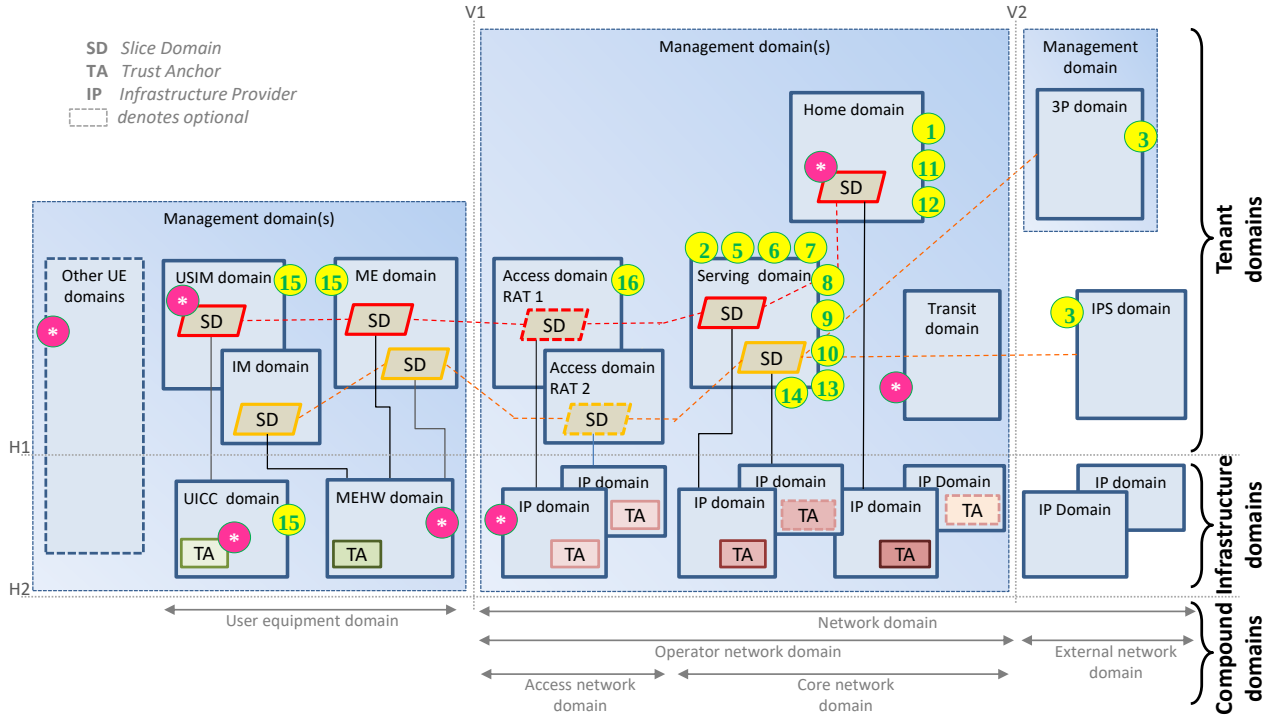

Figure 6: 3GPP 5G network functions mapped onto the domains defined in 5G-ENSURE's security architecture

The 3GPP "numbered" circles denote the following network functions as defined in the 3GPP TS 23.501 v1.2.0:

[4] http://www.3gpp.org/Specifications-groups/sa-plenary/53-sa2-architecture
[5] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

(1) Authentication Server Function (AUSF), which provides unified user authentication.

(2) Core Access and Mobility Management Function (AMF), which provides authentication, authorization, registration and mobility management, termination of non-access stratum security etc.

(3) Data network (DN), which provides data services, e.g. operator services, Internet access or 3rd party services, etc. Notably, the 3GPP's DN network function has been mapped onto the 5G-ENSURE's 3P domain because of secondary authentication provided by a DN-AAA. In 5G-ENSURE's terms, the DN-AAA could be considered as semi-trusted third party whose scope of authentication service is restricted only to the secondary authentication.

(4) Structured Data Storage network function (SDSF), is currently not defined therefor no mapping is possible.

(5) Unstructured Data Storage network function (UDSF), which provides storage and retrieval of information as unstructured data by any network function.

(6) Network Exposure Function (NEF), which provides secure exposure of services and capabilities in 3GPP network functions, etc.

(7) NF Repository Function (NRF), which provides service discovery, maintains network function's profiles, etc.

(8) Network Slice Selection Function (NSSF), which provides selection of network slice, determining allowed slices, etc.

(9) Policy Control function (PCF), which provides unified policy framework governing network behaviour, retrieving subscription information relevant for policy decision, etc.

(10) Session Management Function (SMF), which provides session management, IP address allocation, configuring traffic steering, downlink data notification, etc.

(11) Unified Data Management (UDM), which provides user identification, subscription management, processing of authentication credentials, etc.

(12) Unified Data Repository (UDR), which provides storage of subscription and policy data, retrieval of subscription and policy data, etc.

(13) User plane Function (UPF), which provides packet routing and forwarding, traffic usage reporting, etc.

(14) Application Function (AF), which provides application influence on traffic routing, interaction with policy framework and network exposure function, etc.

(15) User Equipment (UE), which provides registering and accessing the network, etc.

(16) (Radio) Access Network ((R)AN), which provides access to the network, etc.

Note that above (3) and (4) are slightly modified ((3) with added text starting with "Notably…" and (4) with text being removed for editorial reasons) compared to the original text from 3GPP.

4.3 Strata

Similar to Section 4.2, we begin by quoting the stratum definition from TS23.101. Furthermore, we briefly recall the strata introduced in TS23.101.

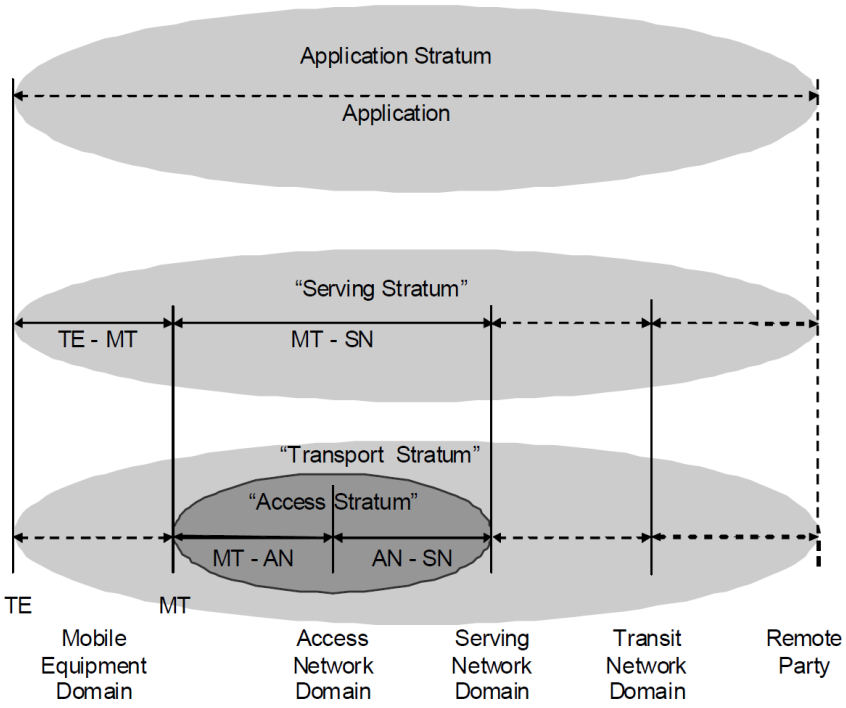

Figure 7: Functional flow between TE, MT, Access Network, Serving Network, Transit Network Domains and the remote party.

According to TS23.101 (Clause 3.1, p. 5), a *stratum* is a "grouping of protocols related to one aspect of the services provided by one or several domains". Figure 7, which is again taken from TS23.101 (Clause 6), shows the five strata defined for UMTS. These strata are used in the security architecture descriptions of TS33.102 (3G) and 33.401 (4G).

Considering the applicability of these strata in 5G networks, one can immediately notice that no stratum is defined for management aspects. In the 5G case, all the (security critical) functionality related to orchestration, virtualization management, security management (monitoring, key distribution, etc.) strongly speak for the introduction of a management stratum in 5G. We need to be able to model the specific (and usually very stringent) security requirements of the management aspect.

Another issue is that the definition of stratum as "grouping of *protocols* related to one aspect of the services provided by one or several domains", seems to include only communication/signalling aspects through the usage of the word "protocols". Clearly, end-points of a protocol must reside in some stratum (usually the same stratum as that of the "protocol"). Therefore, end-point *functionality* can also be considered to fall inside some stratum. (In fact, this is the real intention also in TS23.101 can be seen in later discussions in that specification.) Finally, one can note that (big) data, being an important aspect of 5G should be highlighted in the 5G architecture. For example, data communicated within a stratum may require protection not only during communication, but also when stored/processed in the end-points. This leads to the following revised (clarified) definition of stratum.

Definition. A *stratum* is a grouping of protocols, data, and functions related to one aspect of the services provided by one or several domains.

In the rest of the document, we will use the following strata (as illustrated in Figure 8):

- The **Application Stratum** represents the application process itself, provided to the end-user. It includes end-to-end protocols and functions which make use of services provided by the home, serving and transport strata and infrastructure to support services and/or value-added services. End-to-end functions are applications which are consumed by users at the edge of/outside the overall network.
- The **Home Stratum** contains the protocols and functions related to the handling and storage of subscription data and home network specific services. It also includes functions to allow domains other than the home domain to act on behalf of the home network. Functions related to subscription data management, customer care, including billing and charging, mobility management and authentication are located in this stratum when end-users are at the home network. When end-users are roaming, then the serving domain is allowed to do mobility management at serving network level.
- The **Serving Stratum** is a sub-stratum of the home stratum and consists of protocols and functions to route and forward data/information, user or network generated, from source to destination. The source and destination may be within the same or different networks. Functions related to telecommunication services are located in this stratum, such as session management.
- The **Transport Stratum** supports the transport of user data and network control signalling from other strata through the network. It includes consideration of the physical transmission, e.g., physical transmission format, error correction/recovery, data encryption, resource allocation, etc.
- The **Access Stratum** is a sub-stratum of the transport stratum. It is located between the edge node of the serving network domain and the UE domain. It provides services related to the transmission of data over the radio interface and the management of the radio interface.
- The **Management Stratum** comprises aspects related to conventional network management (configuration, software upgrades, user account management, log collection/analysis) and, in particular, *security management* aspects (security monitoring audit, key and certificate management, etc.). In addition, aspects related to *management of virtualization* and service creation/composition (orchestration, network slice management, isolation and VM management, etc.) belong to this stratum.

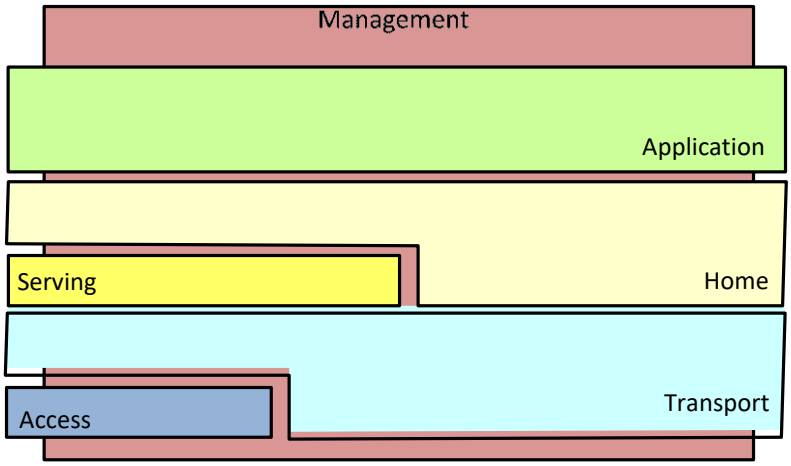

Figure 8: Strata of the 5G Security Architecture.

4.4 Security Realms

Domains and strata as previously discussed, are general partitioning of aspects of the 3GPP system. However, as we are looking at it from a security perspective, it is beneficial to look at a system partitioning based on security aspects.

4.4.1 Security Feature Groups

TS33.102 and TS33.401 introduces a categorization of security mechanisms by defining so called *security feature groups*. The following five security feature groups are defined.

- **Network access security (I)**: the set of security features that provide users with secure access to services, and which in particular protect against attacks on the (radio) access link.
- **Network domain security (II)**: the set of security features that enable nodes to securely exchange signalling data, user data (between AN and SN and within AN), and protect against attacks on the wireline network.
- **User domain security (III)**: the set of security features that secure access to mobile stations.
- **Application domain security (IV)**: the set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **Visibility and configurability of security (V)**: the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

In TS33.102 and TS33.401, it is illustrated in what strata and between which domains the security features belonging to the different security feature groups are present. This is shown in Figure 9 that

is borrowed from TS33.401. This is the primary use of the security feature groups in TS33.102 and TS33.401.

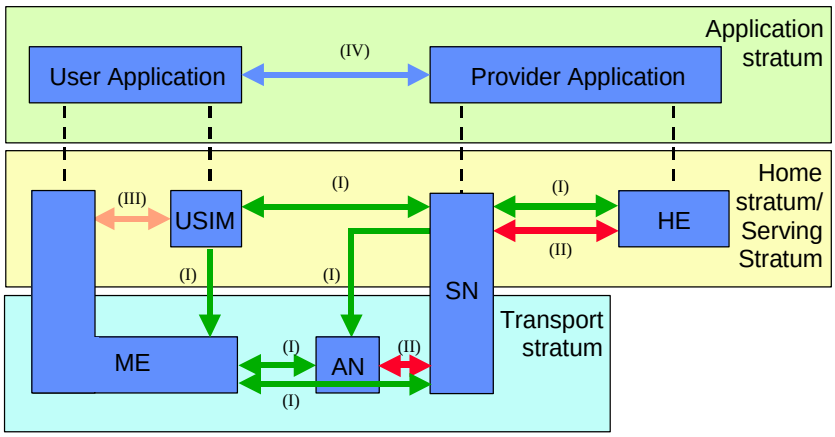

Figure 9: Security feature groups, domains, and strata from TS33.401.

The security feature groups described above are relevant also for 5G but the groups are insufficient and do not fully fit 5G security features such as management, monitoring, and virtualization aspects. Furthermore, the visibility of security in group V is focused only on the user, but in 5G this is relevant also for network nodes that needs to know whether security of other entities with which they communicate is properly enabled/configured of the entities to which it is communicating.

4.4.2 Security Realms

To cover the gaps identified above and considering management and virtualization aspects, we hence introduce security realms.

Definition. A **Security Realm (SR)** captures security needs of one or more strata or domains.

We have identified the following Security Realms that are of interest for the 5G architecture:

- **The Access Network (AN) SR** captures security needs of the access domain and access stratum as part of the transport stratum, in particular aspects related to end-users securely accessing 5G services over 3GPP (5G radio) and certain non-3GPP (e.g. WLAN) access technologies.
- The **Application (App) SR** captures security needs of the application stratum. That is, end-user applications/services provided over the 5G network, either as operator provided services (from H or S domain), or provided from external network domains (3P or IPS domain). Note that when the service is hosted by an external network domain, the service may not always be fully trusted by 5G network operators. Examples of applications/services include: VoIP, VoLTE, V2X, ProSe, HTTP-based services, etc.
- **The Management (Mgmt) SR** captures security needs of the management stratum and management domains, including secure management (secure upgrades, secure orchestration etc.) and management of security (monitoring, key and access management, etc.). Thus, Management Security is either a concern related to communication between a management domain and some other (semi-)trusted domain, or, related to security of the management domain itself.

- The **User Equipment (UE) SR** captures security needs of user equipment (UE) domain comprising the ME, MEHW, UICC, USIM, and IM domains, e.g. visibility and configurability and security aspects related to communication between these domains.
- **The Network (Ntw) SR** captures security needs of communication in core network domains and between the core network domains and external network domains - including aspects related to securely exchanging signalling and end-user data between nodes in the operator and external network domain.
- The **Infrastructure and virtualization (I&V) SR** captures security needs of IP Domains, e.g. for attestation, secure slicing/isolation, and trust issues between tenant domains and between tenant domains and infrastructure domains.

4.5 Security Control Classes

In this section, we will discuss security concepts (for further details see Section 6.1) for the protection of information. The most well-known model is the CIA triad, standing for Confidentiality, Integrity and Availability. Another model is the CAIN, which extends the CIA triad with Non-repudiation. However, in many cases these models fail to describe all important security aspects of a system. We hence give our definition of what we denote as security control classes and provide classes that are of interest for 5G.

Definition. A **Security Control Class (SCC)** is a concept that refers to a collection of security functions and mechanisms (including safeguards and countermeasures) for one security aspect like e.g. integrity. Security classes contain security functions and mechanisms to avoid, detect, deter, counteract or minimize security risks to 5G networks, in particular, risks to a network's physical and logical infrastructure, its services, the user equipment, signalling and data.

The Security Control Class is a concept that is inspired by the security dimensions in X.805 and the security controls found in security standards, e.g., by ISO [iso27001] and NIST [nist]. The purpose of the security control classes is to provide a breakdown of the needed security functions and mechanisms in terms of security concerns e.g. authentication, confidentiality, availability, privacy. Actual controls that are needed are not always the same, given the domain/strata/realm we consider.

The following Security Control Classes have been identified as important for the 5G architecture:

- The **ID & Access Management SCC** is a collection of security functions addressing access control (authorization), management of credentials and roles, etc.
- The **Authentication SCC** is a collection of security functions serving to verify the validity of an attribute, e.g. a claimed identity.
- The **Non-repudiation SCC** is a collection of security functions serving to protect against false denial of involvement in a particular action.
- The **Confidentiality SCC** is a collection of security functions protecting data against unauthorized disclosure.
- The **Integrity SCC** is a collection of security functions protecting data against unauthorized creation or modification.
- The **Availability SCC** is a collection of security functions serving to ensure availability of resources, even in the presence of attacks. Disaster recovery solutions are included in this category.

- The **Privacy SCC** is a collection of security functions serving to the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact and share its personal information with its environment.
- The **Audit SCC** is a collection of security functions providing review and examination of a system's records and activities to determine the adequacy of system controls and detect breaches in system security services and controls. The necessary data collection to enable audit (e.g. logging) is also included.
- The **Trust & Assurance SCC** is a collection of security functions serving to convey information about the trustworthiness of a system. For a trustor such information constitutes a claim which may or may not persuade them to trust the system, while a trustee would see such information as evidence of the security level achieved.
- The **Compliance SCC** is a collection of security functions provided to allow an entity or system to fulfil contractual or legal obligations.

4.6 How to use the architecture?

Our security architecture has been described in the sections before. We continue by elaborating the process to secure a use case using this defined security architecture. Several steps should be followed:

1. The use case to be secured should be modelled by first introducing the top level physical and logical domains. These domains are characterized by ownership, management control and functional area. This step also includes the definition of the slice domains which should be supported. The resulting top-level domain model should be based on the functional architecture of the network to be secured.
2. After the domain model has been established, the reference points (interfaces) between the defined domains are to be introduced. The reference points define the dependencies and interactions between the domains. The information carried over the reference points should be characterized according to the defined strata and the used protocols. Then the information flows should be characterized with respect to which security realms they belong.
3. Then, for each reference point the trust assumptions between the domains have to be defined. An analysis has been made to identify trust assumptions that are implied by the 5G-ENSURE architecture. However, some dependencies exist in which stakeholders can choose how to distribute responsibilities, based on application sector requirements.
4. In the next step, a risk treatment plan with required security controls should be derived by performing a TVRA. As part of the TVRA it should be determined where and by whom the required protective measures should be implemented. The trust model from the step before provides a sound basis for these decisions. The analysis in the TVRA itself should be structured based on domain (see 4.2), strata (see 4.3) and security realm (see 4.4) concepts. 5G-ENSURE has created a trust enabler called Trust Builder to help adopters identify risks and model their decisions about which countermeasures are applied by operators in each domain. This is the same tool that was used to find dependencies and define trust assumptions (see above).
5. The definition of required security controls should follow established security by design principles and best practises (see Chapter 6).
6. The last step is to implement defined security controls and validate achieved network security objectives (Chapter 3.2).

5 Architecture Enforcement

In this Chapter, we analyse how well the objectives for the design of the security architecture were achieved. Then, we describe and discuss security enforcement in domains and strata.

5.1 Introduction

By *architecture enforcement* we refer to the problem of ensuring that the logical domains and strata of the architecture are properly upheld in an instantiation of a 5G network. Security controls should be in place to ensure isolation and to secure and control information flow between domains. Similarly, strata must implement security controls to appropriately protect user traffic and signalling. In other words, for the architectural components to be useful beyond a mere "abstract thought experiment", they must also be reflected in operational networks.

Architecture enforcement of security and privacy objectives is based on implementation of required security controls. The required security controls must be implemented in all domains and strata, i.e. in all 5G entities, network functions and the platforms on top of which they execute. Their implementation in the network should provide strong assurance that the security controls cannot be circumvented. The controls should also ensure that 5G entities, networks and network functions are legitimate, can be authenticated and integrity verified and provide privacy and confidentiality for data and users.

The toolbox for 5G security architecture enforcement will comprise the different security functions and mechanisms contained in the security control classes, the 5G-ENSURE security enablers and (when appropriate) already existing security controls developed for 4G networks, possibly with some enhancements. Examples of existing controls are the 4G security features developed to cope with threats to radio base stations in physically exposed locations (e.g. when the AN Domain is E-UTRA), and tampering threats to user credentials in devices (the USIM Domain is protected by the UICC). The specification of the of required security controls and their implementation should follow the security design recommendations in Chapter 6.

For a description of the 5G-ENSURE security enablers we refer to [d3.6]. In Chapter 7, Table 3 specifies how the enablers are related to the security architecture. In the description of security enforcement in this Chapter we will only give some important examples of where 5G-ENSURE enablers are located.

5.2 Review of objectives for the security architecture

Before discussing the security architecture enforcement in more detail, we review the fulfilment of the objectives for the security architecture itself (Chapter 3.1). If these objectives are not achieved, it would be of no use to discuss security enforcement according to the security architecture as the overall targets would not be achieved. Fulfilment of security realm security objectives is more or less just a question of availability and application of security defined controls and security enablers. In Table 2 we list the objectives and comment on the fulfilment of each one of them.

Table 2. Fulfilment of objectives for the security architecture

Obj. #	Description	Fulfilment
O1.1	5G security architecture should be able to group network entities based on ownership and functionality.	A key concept in the security architecture is to use domains to model 5G networks. These domains are grouping of network entities according to physical or logical aspects, including management and ownership aspects, that are relevant for a 5G network.
O1.2	5G security architecture should enable considering future network solutions with new functionalities and services and re-evaluating threats and security solutions not known or considered at design time, (i.e. flexibility, adaptability and evolvability).	The security architecture is flexible, adaptable and evolvable as domains, strata, security realms and security controls can be combined in numerous ways to cover very diverse network configurations. When needed to cover future network designs, new domains, strata, security realms and security controls can also be defined.
O1.3	5G security architecture should enable the description and analysis of the 3G and 4G networks security as they will be an integral part of future 5G networks (i.e., backward compatibility).	The security architecture will be applicable for 3G and 4G networks as it extends and enhances the 3G and 4G security architectures.
O1.4	5G security architecture should make explicit trust relations between 5G actors.	The security architecture relies on describing the interfaces and interactions between domains and as domains belong to actors the trust relations becomes visible.
O1.5	5G security architecture should enable depiction of the boundaries and interfaces of a 5G network.	The boundaries of the a 5G network will be determined by the boundaries of the domains.
O1.6	5G security architecture should identify security relevant protocols and network functions used and offered in a 5G network in order to build effective protection.	The security architecture relies on describing the interfaces and interactions between domains and will thus identify used protocols and network functions.
O1.7	5G security architecture should capture virtualization and slicing.	Tenant and infrastructure domains are basic concepts in the security architecture used to capture virtualization. Slice domains are defined to handle slicing aspects
O1.8	5G security architecture should consider the management aspects.	The security architecture defines management domains, a management stratum and a management security realm to cover all management aspects.
O1.9	5G system must enable seamless interworking of different network	The security architecture can model and be applied on networks within which different

	technologies, mobile, fixed as well as satellite without downgrading the security.	network technologies are used simultaneously.
O1.10	5G security architecture should enable structuring and modelling the mobile network functions and needs into areas with specific security concerns.	The security realms define areas with similar security needs. The security control classes provide a structure for expressing security needs.
O1.11	Where possible, 5G security should be decoupled from specific physical deployments, focusing on defence-in-depth, in particular self-protection of assets, limiting dependency on protection at network, site, or node perimeter.	The security architecture can model and be applied on networks within which different network technologies are used simultaneously.

5.3 5G Domain Security Enforcement

Domains should be isolated and have well defined entry points where security controls can be implemented so that only legitimate traffic and signalling can take place. However, as domains in many cases are virtualized the isolation properties and controlled entry points must be enforced by logical means. It should also be defined how domains are securely deployed, integrity verified, protected from outside threats and from threats coming from other domains. Clearly, with this usage of virtualization and much more interaction between domains, this is a more challenging task than guaranteeing security in previous generations. In the following discussion on security enforcement in the defined domains we give examples of enablers that these domains should support.

5.3.1 Infrastructure Domains

As mentioned in Chapter 4, the Infrastructure Domains contain the “hardware” and this hardware shall in many cases provide a platform for network function virtualisation, network slicing, and mobile edge computing. This will require new security services like for example trust anchoring of services and verification of platform integrity as discussed in Section 5.3.1.3

5.3.1.1 UICC Domain

The UICC Domain will in essence be unchanged in 5G as it already in its current form provides all essential security controls like tamper resistance, protected storage for long-term subscriber credentials, use of trusted execution environments, and optionally secure communication over its interfaces. The only new feature in 5G is if the UICC Domain is required to support slicing and thus it needs to provide a shared trusted execution environment. This shared environment will most likely be based on virtualization using a secure hypervisor which can guarantee isolation between slices and provide proof of its integrity.

5.3.1.2 MEHW Domain

The MEHW Domain may be required to host one or more IM Domains in addition to the ME Domain. These domains may be slice aware and thus require to be run in a shared trusted execution environment. The security requirements for at least part of the MEHW Domain will thus be similar to

the requirements for the UICC domain with tamper resistance, protected storage for long-term subscriber credentials, and secure communication over its interfaces.

5.3.1.3 Infrastructure Provider Domain

Most of the security requirements for support of network function virtualisation, network slicing, and mobile edge computing impact the Infrastructure Provider Domain (IPD). The domain must implement a number of new security controls and enablers. The most prominent ones being providing proof of platform integrity, isolation between slices and control of services deployment, execution and migration. Specific security and trust guidance for NFV can be found in [etsi_nfv]. We note that the following 5G-ENSURE enablers will need to be supported: 1) the VNF Certification enabler, 2) Security Monitoring Enablers in that certain events and data have to be collected and made available, 3) Network management and virtualisation isolation enablers.

5.3.2 Tenant Domains

A first general security requirement for tenant domains, which will become very important in 5G, is that tenant domains should be bound to the infrastructure domain on which they are deployed, where in some cases, more than one infrastructure provider domain may be involved. The form of binding will vary depending on the characteristics of the tenant domain as well as the infrastructure domain employed, typically mutual authentication between a deployed VNF and the underlying HW would be a relevant requirement.

A second general security requirement for tenant domains is that they should implement 5G-ENSURE trust enabler features enabling users, management systems and network nodes to inform themselves whether a security feature is in operation or not and whether the use and provision of services will/should depend on the security feature. In virtualized environments, this will require support for the VNF certification enabler.

A third general security requirement for tenant domains that are slice aware is that they have to be able to provide strong isolation of and between slices.

A fourth set of general security requirements, which already should be in place by current best-practices, is to apply common best practices in IT security, e.g. that domains should implement authentication, authorization and access controls, have encrypted communication interfaces, use separation of traffic and perform systems monitoring and logging.

5.3.2.1 ME Domain

The ME domain may be slice aware and usually handles an application environment for services hosted by the ME, 5G communication services and the radio interface. Many of the provided services are critical from a security point of view and should be performed in a trusted and isolated environment. The control of the radio interface is of course of particular importance as manipulation of the radio stack may incur serious disturbances and malfunctioning in the access domain. The ME domain will support 5G-ENSURE AAA and privacy enablers.

5.3.2.2 USIM Domain

The USIM domain provides the USIM application, other security services or services requiring security, which are hosted on the UICC. The USIM domain is slice aware and thus has to provide isolation of and between slices. As mentioned, this may be supported by virtualization in the UICC Domain. The

USIM domain will host support for 5G-ENSURE enablers, e.g. the basic AAA enablers, vertical GBA and group-based authentication. It will also support the enabler privacy enhanced identity protection.

5.3.2.3 IM Domain

The IM domain supports alternative means to USIM based authentication and will thus benefit from execution in a trusted execution environment and secure storage of security credentials, provided by the MEHW Domain. The IM Domain will implement e.g. support for the 5G-ENSURE AAA Security Enablers Authentication of USIM-less devices.

5.3.2.4 Access Domain

The access domain plays a key role in providing efficient and secure services in native 5G systems. It will support a large number of security controls inherited from 4G systems together with new security enablers. Its orchestration plays a key role in the creation of e.g. slices and microsegments even if it in itself isn't slice aware. Trust has to be established with subdomains in the UE Domain and mediated to the SN domain. Furthermore, the access domain should support Security Monitoring Enablers and the Trust Metric Enabler.

5.3.2.5 Serving Domain

The Serving Domain has traditionally been considered trusted and mainly, from a standardization point of view been protected by well-defined interfaces and protected communication towards other domains. In 5G the serving domain may be slice aware and rely on VNFs and must thus also support Security Monitoring Enablers and the Trust Metric Enabler. Furthermore, the serving domain will support the Privacy Enhanced Identity Protection Enabler and Network management and virtualization isolation enablers.

5.3.2.6 Home Domain

The home domain is from a security point of view one of the most sensitive domains as it hosts HSS (AuC and HLR) functionality. Still, it has mainly been up to the operator to implement appropriate security measures to protect its operation. From a 5G perspective it will require at least the same security controls as the serving domain and support the same security enablers. In particular it can be worth mentioning that SS7/IMAP vulnerabilities occurring when used for control communication between HSS and VLR in 3G networks must be handled to counter threats aiming at theft of user credentials and identities. The home domain should e.g. support many AAA enablers.

5.3.2.7 Transit Domain

The transit domain may not be slice aware. Still, it may play a role in micro-segmentation as it may have to provide services with specified performance and quality to support the features wanted by the introduction of micro-segmentations. It should in all other respect fulfil the same requirements as the serving domain.

5.3.2.8 3P Domain

The 3rd party (3P) Domain is a domain which is "untrusted" from a 5G system point of view. Such a domain should only be allowed to interact with native 5G domains via special policy enforcement points having gateway functionality, e.g. application level gateways, and only be able to access well defined services. It is up to the 5G operator to determine the exact security requirements that a 3P

domain should fulfil to be allowed to interact with the 5G system. If e.g. the 3P domain provides AAA based authentication services, the interactions could be limited to accepting authentication requests using the Diameter protocol.

5.3.2.9 IP Service Domain

The IP service domain represents operator external IP networks such as the public Internet and/or various corporate networks and are as such partially or fully non-trusted. No security architecture enforcement is thus in general possible in this domain.

5.3.2.10 Management Domain

Note that in a 5G network there may be many management domains to cater for the management of different administrative domains, vertical services and in this context also for the corresponding slices. A management domain will in many cases provide security critical services to the operation of the network and management of all or a subset of the network domains. It may include security management, i.e. ensure that the security services in its managed domains are in place and operational, but it may also do management of the security services including configuration and installation of credentials and keys. Furthermore, a management domain may be directly involved in the operation of 5G Security Monitoring Enablers, Trust Enablers, and Network Management and Virtualisation Isolation Enablers.

5.3.3 Compound Domains

The security of compound domains is specified by the requirements on the individual domains comprising it. In certain cases, the security controls for communication within a compound domain could be relaxed if they e.g. are collocated in a physically secured environment. However, if the compound domain comprises VNFs, relaxation of security controls should only be considered after a thorough analysis of the threat environment. Below we only discuss some aspects related to specific compound domains.

5.3.3.1 Administrative Domain

As an administrative domain is a special case of compound domain, defined not by the presence of special functionalities, but by ownership and/or administration, it does not imply any additional security requirements compared to those of the individual domains comprising it.

5.3.3.2 Slice Domain

A slice domain usually involves slices in more than one of the defined single domain types. Typically, a slice domain is partially managed by the slice “owner”. As a slice domain is hosted in other domains, the slice domain has to trust the hosting domains and that they provide the isolation and integrity support required. The slice owner should have the possibility to verify this which means that hosting domains and slice management services must support the 5G-ENSURE VNF Certification enabler and/or be given access to some slice-specific API of Trust Enablers. In general, the slice owner should have the possibility to configure the security offered by a slice.

5.3.3.3 (Additional) UE Domain

The UE and the additional UE domain shall fulfil the same security requirements. These compound domains include MEHW, UICC, ME, IM and USIM domains. As interaction between two UEs may

expose a UE to threats not existing when accessing an AN domain, additional security controls may be required.

5.3.4 Domain Interactions

Domains can be characterized in terms of their relationship to different stakeholders, how they are managed, if they are slice aware, and who owns them. These characteristics determine how interactions can take place.

Most stakeholders will be in some way dependent on the way domains are constructed and operated. These dependencies leave stakeholders exposed to certain risks. As discussed in Section 2.2, one of the possible response to risk is to decide to trust other entities. In 5G-ENSURE an automated approach was used to find risks and identify trust decisions that should or in some cases could be taken by each stakeholder. Broadly speaking, each stakeholder has to decide what risk mitigation they expect other stakeholders to implement within each domain (i.e. which security control classes are assumed to be addressed). This determines how much the stakeholder can trust each domain, and with respect to which of the potential risks should security in a domain be lacking.

For example, in most cases there are risks associated with impersonation (spoofing) of stakeholders or their technology components. If a domain is trusted with respect to these risks, it means the trustor believes that authentication measures in that domain are adequate for their needs, and will accept credentials issued or verified in that domain. They accept risks of impersonation that can be mitigated by security measures in the trusted domain, and will operate their own domain(s) on that basis. Risks associated with data disclosure (loss of confidentiality) require different types of security measures, e.g. to control access and detect and deflect attacks on the integrity of key system components. It is possible that a stakeholder may trust a domain with respect to one set of risks but not another. For example, they may feel that access control and integrity protection provided in a domain are strong enough, but nevertheless decide to issue and verify their own credentials.

If a domain is untrusted then no security critical interactions should be allowed. If a domain is semi-trusted then the scope of offered services is restricted. To give another example, a transit network domain may be trusted to forward data, but not access it. Trust is often associated with administrative ownership of a domain. A high-level view of trust in different domains is a as follows

- 5G-operator domains trust each other as they comply with provisions of the 5G security architecture. However, in 5G setting the need to verify the operator domain authenticity is more outspoken.
- Management domains are trusted by the domains they manage. It is assumed that the owner of a managed domain ensures that management is performed by a trusted entity, even in the case where management is outsourced.
- 3P domains with a 5G operator SLA are semi-trusted in the sense that only the agreed services are allowed and subject to use of agreed security mechanisms.
- Access (network) domains that use other technologies than standardized by 3GPP are generally referred to as “Non-3GPP access” (includes for instance Wi-Fi and fixed networks) and are in general considered untrusted. Note however that tight 3GPP integration of e.g. WLAN access may render the WLAN to be considered as “Trusted non-3GPP access”.
- A slice domain is semi-trusted by the hosting domain(s).

- Any A, S, H, T, or slice domain trusts any underlying infrastructure provider domain. This is generally necessary simply because these domains ultimately rely on the underlying infrastructure. Of course, this requires prior trust establishment through aforementioned controls such as authentication and authorization and potential use of additional trust enablers. Clearly, some additional security controls such as attestation and end-to-end encryption may relax the trust on the semi-trusted level.
- Slice domains are untrusted by other slice domains.

As mentioned above, most domains in the 5G security architecture need to be trusted by at least some other domains. They may however belong to different management and administrative domains. This may mean some form of verification is needed, e.g. to allocate responsibilities or liabilities for data disclosure, or an out-of-band exchange of trust anchors to allow mutual recognition of credentials.

Security measures within a trusted domain are generally left to the domain owner except when interoperability or specific security requirements have to be fulfilled. Interactions between domains have to be protected. In all cases, the involved entities in an interaction between domains should be authenticated and the communication protected:

- If there is mutual trust between two domains, then the domains should be mutually authenticated and exchanged traffic and/or signalling should be adequately protected.
- If a domain is semi-trusted, the interacting domains should be mutually authenticated, exchanged traffic and/or signalling should be adequately protected and it should be filtered in an application level gateway to limit available services. An example of this situation is a 3P domain interacting with a serving network domain via an Industrial Automation Control (IAC) server for industry robot authentication.
- If a domain is untrusted then it should only be allowed to tunnel traffic and signalling through it.

Tenant and infrastructure domain interactions are mainly concerned with trust anchoring in the sense that tenant domains should be able to authenticate the infrastructure domain used and verify its integrity. In the same way, the infrastructure domain should authenticate the launched domain and check that it is an authorized entity. Specific security and trust guidance for NFV can be found in [etsi_nfv]. These guidelines are of particular interest for network domain virtualization and slice domains and should be adhered to. As mentioned earlier the VNF Certification enabler is relevant here.

Slice domains should in addition to authenticating the infrastructure domain also authenticate the hosting tenant domain.

5.4 5G Strata Security Enforcement

A stratum is a grouping of protocols, data, and functions related to one aspect of the services provided by one or several domains. The most prominent parts to consider in the security enforcement are the interfaces and protocols used for interactions and invocation of functions. The protocols should be used with appropriate security controls to guarantee that the information flow, signalling, data and commands are protected and that the security objectives for the network are achieved.

In general, all security control classes contain some security functions relevant for a given security realm. Which security controls that are required depends on the security objectives relevant for the given security realm which makes it difficult to make but very general statements. An overview of how the 5G-ENSURE security enablers maps on the security architecture can be found in Chapter 7.

5.4.1 Application Stratum

For the application stratum, there are no or possibly only minor differences compared to 4G. However, it is worth noting that the application stratum may depend on slices and e.g. edge computing to deliver special services and that in such cases end-to-end security might not always be possible and that special security measures have to be installed. Such measures will strongly rely on the management security realm for their installation, maintenance and security management.

5.4.2 Home Stratum

The home stratum will mainly change as it must support the 5G-ENSURE AAA Security Enablers. The security control class involved for these enablers would be that of authentication.

5.4.3 Serving Stratum

In the serving stratum, there will be some major changes as the network domain and transport domain will be virtualized and based on SDN controls for routing. These SDN controls will be key in e.g. implementing slices and micro segments. It also should support the 5G-ENSURE Privacy security enablers.

5.4.4 Transport Stratum

In the transport stratum, there will also be major changes as the serving and transit domains will be virtualized and based on SDN controls.

5.4.4.1 The Access Stratum

The access stratum is a substratum to the transport stratum and is in principle the stratum for the control and data mediated in an access (network) domain and has specific security controls per radio access technology.

5.4.5 Management Stratum

The definition of the management stratum is new and many new management and monitoring services will belong to this stratum. The management stratum must support the 5G-ENSURE Security Monitoring Enablers and Network Management and Virtualisation Isolation Enablers. It will be used for SDN and VNF orchestration and it will be the stratum used for configuration of networks security mechanism and transfer of security credentials.

Management actions must be secure, traceable down to the persons authorizing and performing them, and they must be non-repudiable. This will be of the utmost importance in sliced and virtualized networks as here trust in the network will rely on the implemented security controls and the possibility to audit them and their use.

6 5G Security Design Principles and Recommendations

This section addresses the high-level security design principles for the implementation of a secure network following the application of the security architecture. We take as our basis the set of security building blocks needed to meet the security objectives, not only in terms of the 5G architecture enforcement (Section 5) but also to address explicit requirements (coming from the work on Risk analysis and requirements reported in D2.6) and building blocks related to "common best practices". We put them into context with reference to the security features. We make recommendations as to how to apply these principles in a 5G architecture.

6.1 Security Concepts

The high-level design principles for the architecture are more general principles which should be applied when designing and deploying mobile systems.

Here we outline the key security concepts that are relevant in the design of most systems. The NIST *Computer Security Handbook [nist-sec]* defines the term *computer security* as follows:

> "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information, data, and telecommunications)."

These three basic concepts Confidentiality, Integrity, and Availability, commonly referred to as the CIA-triad are key aspects in design of secure systems. Though there are other key concepts such as authentication, non-repudiation, and privacy which are also important characteristics of secure system design. Together these concepts make up the security control classes.

Furthermore, with an evolving architecture one has to bear in mind the backwards compatibility issues, and in particular the design needs to be careful to avoid 'downgrade attacks' when attempting to maintain compatibility with older protocols (e.g. key compromise, tunnelled authentication attacks, and cross-layer attacks).

In a mobile network, there are a number of layers at which the security mechanisms may operate particularly with advent of Internet of Things devices which rely on a plethora of different radio technologies. The deployment across multiple layers requires careful consideration as the system needs so as to balance the various factors, such as efficiency, security and compliance with local regulations, to create an optimum system.

6.1.1 Authentication

Authentication involves the process of providing and assuring identity of communicating entities. Once the authentication phase has completed then the provided identity may be used to grant authorization to utilise certain assigned resources. In the case of the mobile networks the Authentication and Key Agreement (AKA) phase will allow for an authorized user to securely access the mobile network for transport of data for communication purposes. A user's mobile subscription identity is today defined by their International Mobile Subscriber Identity (IMSI) and an associated 128-bit secret authentication key (K_i), which are usually stored in the USIM on a Universal Integrated Circuit Card (UICC).

The process of subscriber authentication should employ identity protection preferably through the use of confidentiality and integrity mechanisms. The design of the network should be such that unauthorized entities cannot access, nor put a significant stress/load on drain resources, of the core network services.

In the new multi-actor environment of 5G, we need to ensure that all entities utilise authentication where appropriate.

6.1.2 Confidentiality

Confidentiality provides for concealing of communication content usually through the use of cryptographic algorithms. The use of cryptography is also one of the important techniques to enable privacy for communications and data. Modern mobile networks are now primarily providing for Internet based transport and the main sources of traffic are at the application level which usually employs its own encryption. It could be argued that one layer of encryption is sufficient but it is important to maintain a secured transport for a number of reasons. Firstly, one cannot rely upon every single application layer service providing for secure connectivity (e.g. DNS is not yet widely secured), and secondly there are many attacks that may be facilitated by an unsecured transport layer.

There are two basic forms of cryptography. Firstly, there is symmetric encryption which uses a single secret key to both encrypt and decrypt communications. The symmetric secret authentication key K_i is used to generate material for use in the AKA protocol which subsequently generate keying material for encrypting the user's communications. Whilst in today's mobile systems 128-bit symmetric keys are typically used, there are plans to deploy 256-bit keys though no algorithms have yet been specified. Secondly, there is asymmetric cryptography which employs two keys one of which may be used to encrypt and the other to decrypt. This approach is also known as public key cryptography, as one of the key pair may be made public, which forms the basis for the use of public certificates which are used in securing key agreement for Transport Layer Security (TLS) and IPsec communications.

The management of keys is a crucial aspect of implementing encryption which for some protocols is separate phase. Furthermore, there are certain properties of key generation and management that can provide for features such as Perfect Forward Secrecy (PFS). The provision of PFS in mobile systems is becoming more important but needs to be implemented so that it operates appropriately in conjunction with other services such Lawful Intercept.

We recommend that all communications should be encrypted, preferably on an end-to-end basis. The encryption should also aim to provide for perfect forward secrecy. For future-proofness, 256 bit keys should be supported[6] and random number sources used in cryptography should be indistinguishable from a truly random source.

6.1.3 Integrity

Integrity protection provides for a defence against modification of communication content. This is usually achieved through the use of Message Authentication Codes (MACs), many of which are based upon a range of cryptographic hashing algorithms, though the latest Secure Hashing Algorithm (SHA-3) from NIST employs a cryptographic sponge function. A MAC has the dual purpose of an integrity

[6] A new "Study on Supporting 256-bit Algorithms for 5G" has been discussed by SA3 during the SA3#88bis meeting in Singapore, 9-13 October 2017.

and authentication check of communication content. Current 3G and 4G standards lack the ability to integrity protect the data plane, something which would provide enhanced security e.g. for critical machine-type communication (MTC), and needs to be a part of the 5G design.

6.1.4 Availability

Availability is the property of a system, or a resource, being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system. A number of attack types can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures, such as authentication and encryption, whereas others require some sort of physical action to prevent or recover from loss of availability of elements of a distributed system. In 5G the introduction of Software Defined Networks (SDN) and Network Functions Virtualization (NFV) and cloud computing will aid in providing scalable service deployment to maximise availability.

6.1.5 Non-repudiation

Non-repudiation provides for proof of the origin of a message such that a sender cannot denying having transmitted a message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver also received the message. Stronger requirements on non-repudiation arise from a need to provide strong liability chains. Non-repudiation is an important feature when addressing issues relating to inter-operator trust when attempting to tackle potentially fraudulent activities. Networks should provide for non-repudiation functionalities to tackle fraud.

6.1.6 Legacy compatibility

Care must be taken when handling backward compatibility and interworking with legacy systems. We must ensure protection against “bidding-down” attacks and securely handle e.g. inter-RAT handovers, preventing legacy systems (with potentially lower security) being able to impact the security of 5G.

6.2 Standards Based Security

An important principle in designing and building secure systems is to choose proven security algorithms and protocols from standardised sources such as those organisations listed below to avoid security and interoperability problems. Clearly new standards will need to be developed but where ever possible they should utilise and build upon existing security standards in preference to developing their own.

6.2.1 ETSI/3GPP

The European Telecommunications Standards Institute (ETSI) is an independent, not-for-profit, standardization organization in the telecommunications industry in Europe. ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. ETSI supports the 3GPP international standards body.

6.2.2 NIST

The National Institute of Standards and Technology (NIST) is a national laboratory, which is an agency of the United States Department of Commerce, which provides for the development of technology,

measurement, and standards. Despite its national scope, the NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have worldwide impact. NIST has standardised various widely used cryptographic algorithms (e.g. AES, SHA-2).

6.2.3 IETF

The Internet Engineering Task Force (IETF) is the main body for standardisation of Internet based protocols and some associated security algorithms many of which are in use today's in mobile networks and are proposed for use in 5G (e.g. IPsec, TLS, SCTP, DIAMETER, SIP, HTTP, COAP). It is supported by the Internet Society (ISOC) which is an international non-profit organization founded to provide leadership in Internet related standards, education, access, and policy. ISOC has a worldwide membership including both organizations and individuals. The organization develops Internet standards and related specifications, which are published as *Requests for Comments* (RFCs).

6.2.4 ITU-T

The International Telecommunication Union (ITU) is an international organization, which is part of the United Nations System, where governments and commercial entities participate to globally coordinate and standardize telecom networks and services. The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the ITU. The ITU-T mission is to produce standards covering all fields of telecommunications. The international standards produced by the ITU-T are known as *Recommendations*.

6.2.5 ISO

The International Organization for Standardization (ISO) is a global federation of national standards bodies. ISO is a non-governmental organization that promotes the development of standardization and related activities that aims to facilitate the international exchange of goods and services and to develop cooperation in the areas of intellectual, scientific, technological, and economic activity. The work of ISO results in international agreements that are published as International Standards. ISO standards cover a wide range of areas such as smart card interfaces (e.g. ISO 7816).

6.3 Lesson learned from enabler development

During the course of the project there were 17 enablers specified as part of software release 1.0 [d3.2] and a further 25 specified as part of software release 2.0 [d3.6], which were either extensions of R1 enablers or as new enablers. During this process, the partners worked together in varying sized teams from single institutions to multi-party collaborations. As part of the project many of these enablers also needed integration onto the project's 5G testbed and testing facilities. These collaborations brought the project together in considering how the enablers fit together with respect to other components in network.

In terms of input into the design of the architecture the work on the enablers has provided an understanding that it is important to be able to develop and test software components both separately and in conjunction with others. Whilst this is a well-recognised principle, it is particularly important with 5G systems as they will be largely centred around flexible software based approaches (e.g. SDN, NFV etc).

Quite a number of the enablers have also been based upon open source software which has proved to be a valuable resource that enables entities to build upon the work of others and potentially

contribute back to the original open source projects. The other benefit of open source approaches is that it enables the potential for crowdsourced approaches to security assessment of software. For example, this has been highlighted with advent of high profile vulnerabilities in widely used security libraries such as OpenSSL which resulted in a number of stakeholders performing security reviews on OpenSSL.

6.4 Further Recommendations

Although we have strived to make the security architecture complete, there are obviously issues that fall outside the scope of the architecture itself, for example how to implement and operate the architecture. In the following, some recommendations are provided.

6.4.1 Implementing Security

Whilst we covered security concepts in the previous section, here we examine the ways in which security systems may be implemented. These may just be implemented on general purpose computing entities but increasingly many of these algorithms are abstracted into virtualised services or into specific hardware implementations, or a combination of the two. Making the appropriate design choice as to how to implement security mechanisms can lead to dramatic improvements in security, performance, scalability, and availability.

Hardware based security has been used in the mobile sector for some time now. The Universal Integrated Circuit Card (UICC), or SIM card, is an early example of this trend, which originates from the 2G era, that provides for physical tamper-resistant protection of the user subscriber credentials, including the International Mobile Subscriber Identity (IMSI) and the secret authentication key (K_i). Although the external physical interface of the UICC has existed almost unchanged since the 2G days, internally the software implementation has changed significantly where it has evolved to provide to support for multiple applications, and security improvements like the mutual authentication and use of longer encryption keys. Furthermore, with the advent of the embedded-SIM (eSIM), which allows for remote provisioning of subscriber identities, there are new possibilities particularly for embedded devices which may be too inaccessible, or too small to physically host a UICC card. The flexibility afforded by the eSIM has now attracted consumer manufacturers such as Apple, who have already begun to include it in a number of their devices. eSIM or other forms of trusted execution environments will be key to support large scale IoT and other credential alternatives to (U)SIM.

Trusted Systems in one form or another have now become available in many smartphones. This is largely down to the fact that many now utilise CPUs based upon the ARM chip design which has included ARM's TrustZone for a couple of generations. TrustZone is the marketing name for ARM's Security Extensions, which provides two virtual processors backed by hardware based access control. This lets the application core switch between two states, referred to as worlds, in order to prevent information from leaking from the more trusted world to the less trusted world. TrustZone, and related technologies such as Apple's secure enclave, may be used for storing critical credentials such as biometric data and credit card details, or for running stronger process sandboxing (e.g. Samsung's KNOX). There are range of existing and emerging trusted computing technologies that are making their way into the mobile arena (e.g. Intel's TXT & SGX), which may be employed in the user equipment or the core network. Additional alternatives may be needed for some IoT devices.

Virtualisation has yet to have a serious bearing on end user devices, but it is having major impacts on the core network services infrastructure. There are a range of different applications of Virtualisation in the infrastructure. One major aspect of virtualisation is on the use of virtual machines which removes many of the physical restrictions that may be imposed by running software on specific hardware at a particular location. Virtual machines allow for the seamless migration of software services from one place to other for a variety of reasons including scalability, reliability and redundancy. Another important aspect of virtualisation is the rise of Network Function Virtualization (NFV) which also builds upon Software Defined Network (SDN) to provide for virtualisation of networked resources and services. The combination of these technologies provides for slicing, a key 5G technology. However, whilst these technologies provide a range of advantages they also introduce new security issues which need to be addressed, such as ensuring that the security policy is also implemented in the network management entities.

6.4.2 Design Phases

Here we briefly discuss design considerations for 5G networks. The aspects of risk assessment, mitigation and requirements are covered in other project deliverables [d2.3, d2.6] thus will only lightly touch on them here.

Threat analysis. A comprehensive list of all possible threats against the system needs to be compiled along with the cost of carrying out an attack that can lead to a particular threat. This has been addressed in [d2.3].

Risk analysis. The impact of each threat is measured as discussed in [d2.3]. Estimates are required for both the probability of various attacks and the potential gain for the attacker and/or damage to the attacked side caused by them.

Requirements capture. The results of risk and threat analysis will be taken to formulate the security requirements for the system [d2.6].

Design phase. The security protection mechanisms are designed in order to meet the requirements. The security architecture is constructed using as pre-existing building blocks such as security protocols or primitives, with new mechanisms defined if necessary. The constraints need to be taken into account, although it is possible that not all requirements can be met. This may require re-visiting the earlier phases, such as the risk analysis phase.

Security analysis. This phase should be performed independently from the other phases so that the system may be correctly evaluated. It may be possible to use automatic verification tools for certain parts of the evaluation but a good deal of the work would need to be performed by experts in the field to properly assess the security of the entire system.

Monitoring. In order to cover the whole life-cycle of cyber-security threats from design vulnerabilities to alerts triggered by SIEMs (Security Information and Event Management), the design of cyber-security monitoring function shall follow a continuous process starting at the design of a network and looping continuously at run-time in a Deming wheel way. A plan phase consists initially at checking the design of a network. If vulnerabilities are found, a remediation is proposed in a do phase. The remediation is then checked itself to see if it verifies the QoS contracts. Then, the remediation is deployed in an act phase. At run-time, the cycle continues: various sensors and SIEMs trigger alerts, and countermeasures or new remediation are proposed in a do phase, which are checked towards

the QoS contracts in a check phase. Then the countermeasure or the new remediation is deployed in an act phase.

In terms of component, this chain relies on the following different components:

- Sensors are placed throughout the network in order to send back events or measures.
- Aggregators such as SIEMs correlate the rough information of the sensors and trigger alerts.
- Attack graph engine processes the alert and builds an attack tree where the progression of the threat is clearly shown.
- Remediation and/or countermeasures are proposed in order to stop the attack.
- A verification process checks if the remediation or countermeasure proposed is consistent with the QoS contracts of the Service Level Agreement.
- Then, the remediation or countermeasure is deployed by the security administrator.

Since 5G infrastructure is a metamorphic network, a true issue leads in the changes to be performed on the network in an ad hoc manner at run-time to enforce security functions such as mainly sensors, remediation and countermeasures. Challenges can be either to:

- Place a new security function such as a sensor or a security enforcement point,
- Create, delete or change a flow,
- Move, create, delete or add QoS constraints to a VNF or a VM
- Etc.

Reaction phase. While planning of the system management and operation can be seen as part of the mechanism design phase, reaction to all unexpected security breaches cannot be planned beforehand. In the reaction phase, it is vital that the original design of the system is flexible enough and allows enhancements; it is useful to have a certain amount of safety margin in the mechanisms. These margins tend to be useful in cases where new attack methodologies appear faster than expected.

6.4.3 Monitoring

As any IT infrastructure, 5G infrastructures are subject to cyber-attacks which could impact the availability of the services, the confidentiality and the privacy of the users' data as well as the integrity of the data transmitted. A specificity of 5G infrastructure lies in the stack of virtualized services, each of them depending on (or coming from) potentially different players. The details of the software used underneath do not have to necessarily be accessible to the upper tenants. All parties of the 5G infrastructure, from the infrastructure operator to the verticals tenant, shall collaborate to endorse cyber-security monitoring in their perimeter of responsibility. Indeed, considering that cyber-security monitoring is one aspect of the service security, and considering that service security performance is part of the Quality of Service [e860, section 2.6], the one-stop-responsibility principle developed in [p806] and re-used in [e860 section 4], can present the right framework to handle this issue. As a recall, the one-stop-responsibility principle states that "*a single provider is considered as responsible for aspects of the service delivery as seen from a user's point of view ("one-stop-responsibility"). That is, a given user should not need to go beyond the nearest provider for the given aspects of the service. On the other hand, the provider might depend on proper delivery from other providers in order to fulfil its commitments.*"

Vulnerabilities and Threats analysis

Classical IT cyber-attack graph engines are based upon the knowledge of both the topology of the network and the software and versions used in order to induce the software vulnerabilities from databases such as the National Vulnerability Database (NVD) or Common Vulnerabilities and Exposures (CVE). In order to define a node in an attack graph, one needs to use an exploit of a vulnerability, leading to a compromising of a host or a privilege elevation.

5G infrastructures bring new threats and attack surfaces:

1. Virtualization in 5G infrastructures brings with it specific threats due to the concentration of the command centres on the SDN controllers, the Orchestrators, the VNF managers and the Hypervisors. If one of those is compromised, it could impact all the entities controlled by each of them, that is to say VNFs and VMs.
2. Organization of the 5G domains in new paradigms such as slices and micro-segments brings new QoS metrics which need to be monitored. Contracts guarantying their respect are at threats when the network is under attack. Monitoring should be oriented in order to fit and serve such new entities.
3. In the context of 5G virtualization involving a hierarchy of different operators, it is not obvious for the tenant to obtain the software versions used by the infrastructure provider, nor the topology of the network, which are the elements needed for a classical cyber-security monitoring through attack graphs, as mentioned above. Nevertheless, it is probably possible to model malevolent activities at another level such as it is done for Advanced Persistent Threats (APT) where social engineering is involved.

Response

Security issues are detected either at design time according to the knowledge of the topology and of known vulnerabilities, or at run time through alerts sent by products such as Security Information and Event Management (SIEM) which correlates security information at a first level, showing in real-time which software or machine is compromised. Responses to this different kind of detection can scale from a proposal of remediation which will consist of a total re-design of the network, to lighter countermeasures such as cutting a route to an identified attacker. Other intermediary responses are also useful, such as migrating a Virtual Machine, upgrading a version of software or applying a patch.

6.4.4 Orchestration

In order to address business requirements related to the security of the operation, 5G providers will have to operate their network as metamorphic entities which can adapt to counteract on-going threats and changing needs of their customers. The convergence of ICT and telecommunication is on its way but needs new achievements to provide a smooth management framework.

Virtual Network Functions principle has been standardised to help such a convergence [etsi_mano]. Then, a language like TOSCA [tosca1] [tosca2], defines ways to describe objects such as Network Services (NS), Virtual Network Functions (VNF), Virtual Links (VL), Connection Points (CP), VNF Forwarding Graphs (VNFFG), Virtual Network Forwarding Paths (VNFP), Virtual Deployment Units (VDU). TOSCA descriptors regroup these concepts to describe the following entities:

- Network Service Descriptor (VNF, CP, VL, VNFFG, VNFP),
- Virtual Network Function Descriptor (VDUs (CPU, RAM, images), CPs, internal VLs),

- Virtual Link Descriptor (CPs, Type (E-LAN[7], E-Line[7], E-Tree[7] …),
- VNF Forwarding Graph Descriptor (VLs, VNFs, NFP (routing policies)),
- Physical Network Function Descriptor (external CPs, linked VLs or PLs).

Such a language enables basically a good description of these entities, as well as VLs and VDUs capabilities and requirements. Nevertheless,

1. Extension of this description shall be made possible to express security specific dimensions to meet Quality of Service requirements,
2. Actual interpreters like Tacker from the OpenStack environment only interpret these descriptors before the deployment of the components, but not at run-time. This is a big limitation for security dynamicity requirements. The schema in Figure 10 below presents Tacker's ecosystem.

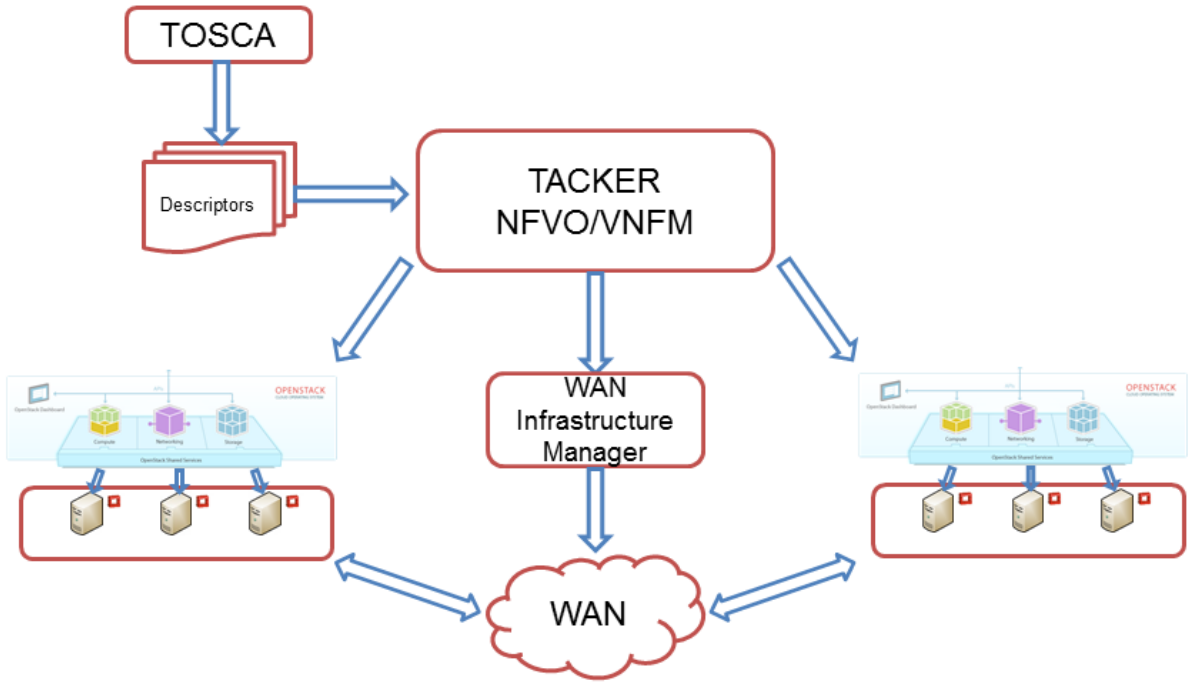

Figure 10: Tacker's ecosystem

In order to counter this limitation for dynamicity, a partial solution can be found in SDN controller's capacity to enable dynamically new routes. Therefore, for example in case of a DDoS attack, a flow can be rerouted dynamically through network functions such as a "clinic centre" in order to benefit from an additional network service. Still, recommendation can be expressed for future work that next generation of VNF Orchestrators shall be able to handle dynamic change request for the deployment of new security functions at run-time.

[7] Defined by the Metro Ethernet Forum in MEF Technical Specification MEF 6.1: Ethernet Services Definitions - Phase 2", April, 2008

7 5G-ENSURE security architecture trials

In this section, we first undergo the mapping of 5G-ENSURE security enablers towards 5G-ENSURE case and deduce the Security controls needed in this context.

7.1 5G-ENSURE enablers towards the security architecture

5G-ENSURE has fostered the design and development of a set of 5G Security enablers focused on a number of key concerns (i.e. AAA, Privacy, Trust, Security Monitoring, Network management and virtualization isolation). In this section we focus on the mapping of these enablers to each of the major building blocks covered by 5G security architecture as now defined. The rationale is here to assess the coverage achieved.

5G-ENSURE Security enablers have been described in D3.6 Open Specifications [d3.6]. From this deliverable, we extracted the mapping of each of the enablers with respect to security domains, security strata and security realms that define the 5G security architecture.

Table 3 gives a synthesis of the mapping of the enablers. From this table, we can see that almost all the domains are covered by the enablers. Exceptions are at the user end for the ME HW and UICC domains which are very specific to the device and chip industry, not represented in the 5G-ENSURE consortium, and the Core Network domain, actually not appearing as is on the domain architecture picture representation since it is composed of the A, H, S and T domains. We can note also a rather good coverage by category or cluster, except for the Network Management and Virtualization Isolation cluster which focuses on the network and not on the user and equipment end.

Regarding the strata, there is also a good coverage of the enablers. The AAA cluster, addressing authentication, authorization and accounting, focuses on the home stratum where user data are managed. Privacy does not address the transport stratum. Trust, Security monitoring and Network management and virtualization isolation split homogeneously over the different strata.

For Security realms, the mapping gives a clear pattern for the AAA enablers mapping the Application, User Equipment and Infrastructure & Virtualization security realms. For other categories, the coverage is well distributed between the different enablers of a category.

We propose also a mapping of the Security enablers towards the Security Control Classes. We note that a focus can be found for each cluster: AAA enablers address Authentication, and ID and Access Management, Privacy enablers address Privacy, Trust enablers address Trust and Assessment, Security Monitoring enablers address Audit. Network Management and Virtualization isolation enablers cover a spread spectrum between Integrity and Availability for the Anti-fingerprint and the Malicious Traffic generator enablers, Audit and Trust assessment for the other enablers of the category. Non-repudiation, Confidentiality and Compliance are not presented as covered by the enablers, also some of them address these properties as a second intention (for example AAA enabler use encipherment to protect the password against an abuse in confidentiality).

Table 3: Mapping of 5G-ENSURE Security enablers towards 5G-ENSURE Security architecture

Category	5G-ENSURE security enablers	Domains														Strata						Security realms						Security Control Classes										
		UE	ME	ME HW	UICC	USIM	IM	A	H	S	CN	IP	T	3P	IP-S	M	Application	Home	Serving	Transport	Access	Management	AN	App	Mgmt	UE	N	I&V	ID & Access Mt	Authentication	Non-repudiation	Confidentiality	Integrity	Availability	Privacy	Audit	Trust & Ass.	Compliance
AAA	Basic AAA enabler		x			x			x	x								x						x		x		x		x								
	Perfect Forward Secrecy		x			x			x	x								x						x		x		x		x								
	Trusted micro-segmentation in 5G networks		x			x			x	x								x						x		x		x		x								
	Internet of things (IoT)		x			x	x		x	x				x	x				x						x		x		x	x	x								
	Non-USIM based authentication		x				x		x	x									x						x		x		x		x								
	vGBA		x			x			x										x						x		x		x		x								
	Bring Your Own Identity									x				x					x						x				x	x	x								
	Group-based authentication		x			x			x	x									x						x		x		x		x								
	Fine-grained Authorization		x			x	x		x					x	x		x		x						x		x			x	x								
	Authorization in Satellite Systems		x			x			x										x						x		x		x		x								
	Authorization and Authentication for RCDs with PD		x				x							x	x		x								x		x		x	x	x								
	Authorization and Authentication for RCDs without		x				x							x	x		x								x		x		x	x	x								
	Federative authentication and identification enabler							x	x					x	x				x					x	x				x	x	x								
	Storage of authentication level							x	x					x	x				x					x	x				x	x	x								
	Usage of authentication level							x	x					x	x				x					x	x				x	x	x								
Privacy	Privacy Enhanced Identity Protection		x			x			x	x						x		x	x			x	x		x	x	x								x			
	Device identifier(s) privacy		x																			x		x		x									x			
	Device-based Anonymization		x													x	x					x		x		x									x			
	Privacy policy analysis		x											x			x							x		x										x		
Trust	Trust Builder															x						x			x			x								x		
	Trust Metric Enabler							x		x				x	x	x			x		x		x	x	x			x								x	x	
	VNF Certification											x				x						x			x			x									x	
	Security Indicator	x																			x		x			x		x									x	
	Reputation based on Root Cause Analysis for SDN								x					x	x	x		x			x	x	x	x	x			x								x		
Security Monitoring	System Security State Repository															x						x						x								x		
	Security Monitor for 5G Micro-Segments							x		x				x	x	x	x		x		x		x	x	x			x								x		
	Satellite Network Monitoring		x					x		x		x								x		x			x		x	x								x		
	Generic Collector Interface							x	x	x		x	x	x	x	x						x	x	x	x		x	x								x		
	PulSAR: Proactive Security Analysis and Remediation							x		x		x	x			x			x	x	x	x	x	x	x		x	x								x		
	Malicious Traffic Generator		x					x	x	x		x	x				x	x	x	x	x		x	x		x	x	x					x					
Netw Mt + Virtualiz. Isolat	Anti-Fingerprinting											x				x				x		x			x			x					x	x				
	Access Control Mechanisms									x		x				x			x			x		x	x			x	x									
	Component-Interaction Audits								x			x		x		x	x		x	x		x		x	x			x	x							x		
	Bootstrapping Trust									x						x			x			x		x				x				x					x	
	Micro Segmentation									x		x				x	x		x			x		x				x	x	x								
	Flow Control: in-network Threat Detection and Mitigation for Critical Functions in Virtu							x	x			x				x		x	x			x		x				x					x					

7.2 5G-ENSURE security architecture practical use case

In this section, we analyse the mapping of an IoT use case on to our security architecture.

IoT is one very promising vertical usage of 5G networks and capabilities. An IoT user group for 5G is smart cities. For example, a smart-grid needs power sensors and control systems to be connected to energy analysing systems. It requires high privacy and availability guarantees. 5G can provide cost-efficient and scalable alternative that provides cities dedicated logical networks (i.e. slices) with required security properties.

The smart city use case involves various actors. Cities collect themselves or sub-contract the collection and the measurement of the data itself. Mobile network operators, infrastructure providers and virtualized infrastructure provider operate different 5G functions to guarantee the required service, security and trust levels.

IoT devices may have different security requirements and capabilities, and also can be operated by different parties. Here, we assume that IoT devices are composed of a sensor, a (e)SIM card, and hardware/software required to communicate via the native 5G radio access technology, and are installed in private locations (e.g., house, office).

Now, we will analyse the smart city use case with regards to our security architecture, and first map it to the Security domains in Figure 11. Starting from the IoT devices, we map them into the UE domain. A sensor itself, as a hardware device, is modelled by a ME HW domain. Let us suppose that the sensor is provided by an electricity meter provider, and that the ME domain is administrated by the city service. A SIM card is modelled by a UICC domain that is provided by a UICC manufacturer and USIM domain administrated by a MNO. Then, the network is composed of several parts: a logical part and an infrastructure part consisting in several IP domains administrated by Infrastructure providers. The logical part is composed of an A domain, an S domain, a T domain, and an H domain and is managed by MNOs. The electricity service of the city is mapped as an external network IPS domain.

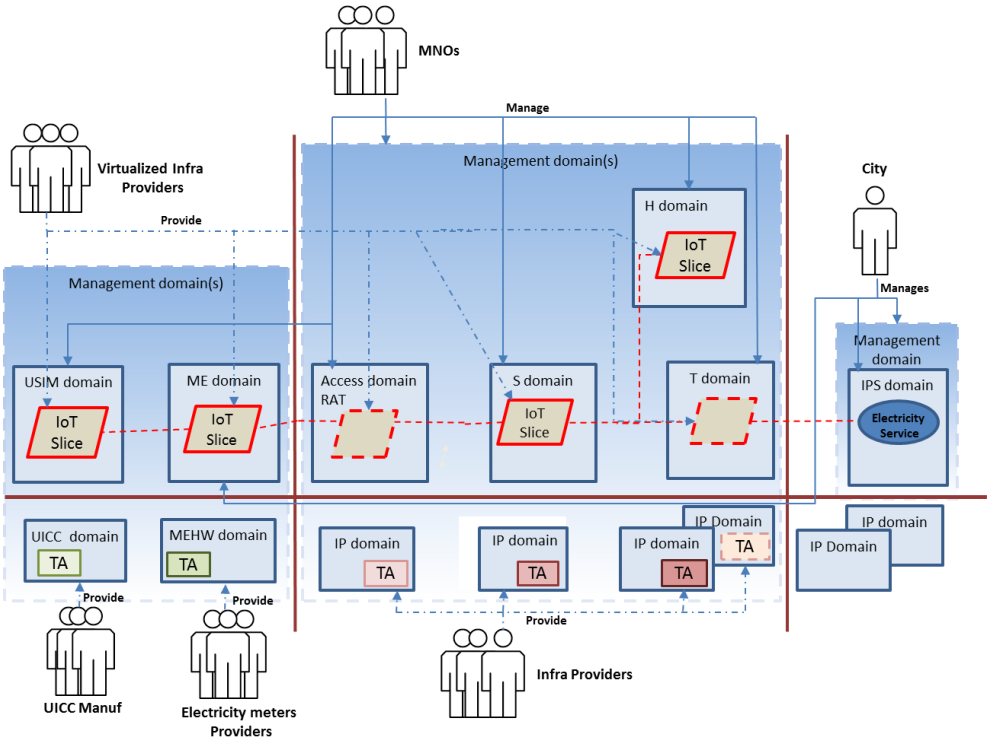

Figure 11: Mapping of the IoT use case to our Security domains

The IoT use cases can be seen as a vertical application to the 5G Architecture. Therefore, it can be mapped as in Figure 12 to the Application strata, even if the use case benefits from all the strata of the architecture.

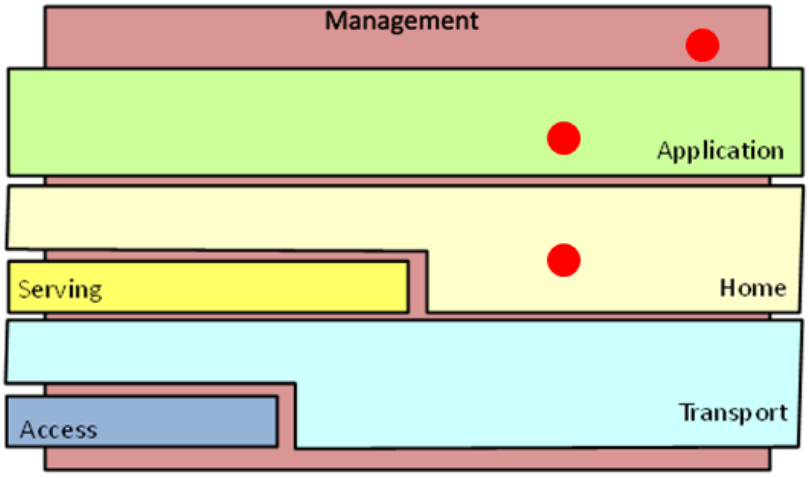

Figure 12: Mapping of the IoT use case to our Security strata

The network authentication and ID management of IoT devices is considered in the home stratum. However, the service authentication and ID management of IoT devices is classified in the application stratum. Finally, the security monitoring and trust computation protocols and functions are part of the management stratum.

Then we come to the stage of analysing the security realms and the security control classes relevant for the use case. For each security realm, Table 4 comments the security control classes needed to implement the

security needs of the use case. It provides IoT specific examples of security controls and enabling technologies. The table illustrates how the architecture enables us to recognize security needs for each realm. By going through all realms and control classes of the architecture, we can more easily identify one-by-one, which controls are needed for realm and control class related security threats. Hence, the architecture provides assurance that relevant control classes have been identified and use case relevant threats are covered completely.

The next step for a deployment would be to search for corresponding enablers to implement the needed security controls, and study how to integrate them in a technical architecture.

Table 4: Mapping security realms to control classes and to control examples that are relevant for the IoT

Security Realm	**Security control classes**	**Security control examples**	**Corresponding 5G-ENSURE enablers**
Access network	Authentication	Authentication and identification can be a challenge for IoT devices: firstly, because resource and energy restricted devices cannot support heavy authentication protocols and, secondly, as synchronously or simultaneously acting IoT devices may cause authentication traffic spikes. Gateways and group authentication protocols can be used to address the challenges.	Basic AAA enabler, Internet of things (IoT), Fine-grained Authorization, Federative authentication and identification enabler
	Identification and access control		
Application	Identification and access control	Meter device specific controls are needed to assure reliability and accuracy of energy measurements. For instance, measurements transmitted using Constrained Application Protocol (CoAP) may be end-to-end secured using datagram transport layer security (DTLS). Operators may provide key management services, optimized for network and applications.	Basic AAA enabler, Internet of things (IoT), Fine-grained Authorization, Federative authentication and identification enabler
	Confidentiality		
	Integrity		
	Non-repudiation	Measurements made by IoT devices may be used for energy billing and hence should be non-repudiable. Application must trust underlying device to provide correct measurements and functionality.	None in 5G-ENSURE project
	Privacy	Measurements may reveal personal information on e.g. residents' habits or movements. Privacy mechanisms, such as aggregation on consumption data, should be therefore utilized. However, to protect network from traffic spikes, each meter should not deliver aggregated data at the same moments of day.	Privacy Enhanced Identity Protection, Device identifier(s) privacy, Device-based Anonymization, Privacy policy analysis
Manage-ment	Auditing	Security monitoring plays an important role in IoT where large amount of potentially vulnerable things is connected. Monitoring, combined e.g. with machine	System Security State Repository, Security Monitor for 5G Micro-

		learning, provides situational awareness and enables detection of on-going attacks. It mitigates threats caused by IoT botnets. Slices increase accuracy of traffic monitoring as they enable monitoring to focus on homogenous IoT specific traffic flows.	Segments, Satellite Network Monitoring, Generic Collector Interface, PulSAR, Malicious Traffic Generator
	Trust and assurance	Monitoring approaches can be combined with trusted hardware based attestation protocols to verify integrity of network and software configuration and to assure that the protection of 5G infrastructure is up-to- date.	Bootstrapping Trust
UE	Trust and assurance	Trust towards IoT devices is based on tamper resistance of UICC and TEE technologies.	None in 5G-ENSURE project
Network	Authentication	Authentication and key agreement protocol (AKA) can be adapted to support different algorithms, some more suitable for power and processing limited devices. The identification can be based on USIM cards that are provisioned to IoT meters by the city. Only authorized nodes - IoT meters deployed by cities -should be allowed to access IoT slices.	Basic AAA enabler, Internet of things (IoT), Fine-grained Authorization, Federative authentication and identification enabler
	Identification and access control		
Infrastruc-ture and virtualiza-tion	Availability	NFV also flexible mechanisms to quarantine disturbing traffic from compromised IoT nodes quickly.	Anti-finger-printing Flow Control: in-network Threat Detection and Mitigation for Critical Functions in Virtual Networks
	Trust and assurance	Trust towards network hardware, and virtual machines on them, can be based e.g. to Trusted Platform Modules (TPM) and secure booting that assures that only operator accepted software is running.	Bootstrapping Trust

8 Existing Work

As mentioned, there is plethora of security architectures for various purposes. We have here chosen to briefly describe and analyse a few selected architectures which are particularly relevant to the work in 5G-ENSURE.

8.1 3GPP

The security architecture, in particular security features and the security requirements of 3G and 4G networks are defined in [ts33.102] and 4G in [ts33.401] respectively. These two architectures address the 2G weaknesses and provide additional security mechanisms to protect 3G/4G services.

The 3G security architecture defines security features and the security requirements, whereas 4G security architecture additionally defines security procedures in the network. However, the set of reasons behind selecting specific security mechanisms and procedures are not discussed in the 3G security architecture. In a separate study [ts33.821], the rationale and track of security decisions in 4G networks are presented by the 3GPP SA3 group.

Both architectures define a generic security model for 3G and 4G mobile networks, however they exclude several factors. For example, while the interfaces between architectural components and their security is defined, end-point (node) security is not considered. Principles together with security objectives are not defined in the architecture documents, however some are discussed in a set of separate documents [ts33.120]. Similarly, 3G and 4G network-specific high-level threats arising from the consideration of security architecture and due to various trade-offs in network performance/availability and regulatory requirements are discussed in a separate technical report [ts33.821].

Definition of trust as an “acceptable level of risk” enables a way of designing secure systems [ros]. In the case of the 3G and 4G security architectures, such a trust level between few network entities is assumed implicitly, and used to derive security protocols and mechanisms. For example, the home environment trusts the serving network by means of service level roaming agreements. In particular, the home environment assumes trust in the serving network to handle subscriber authentication data during AKA protocol in a secure manner.

The 4G architecture extends the trust assumptions made in 3G security as indicated in following Figure 13. The indicated circle demonstrates extended trust between the mobile environment and serving network which is achieved by means of NAS security and key hierarchy mechanisms. However, the 4G security architecture does not define trust levels among network entities explicitly and reasons on why design decisions are at “acceptable level of risk”.

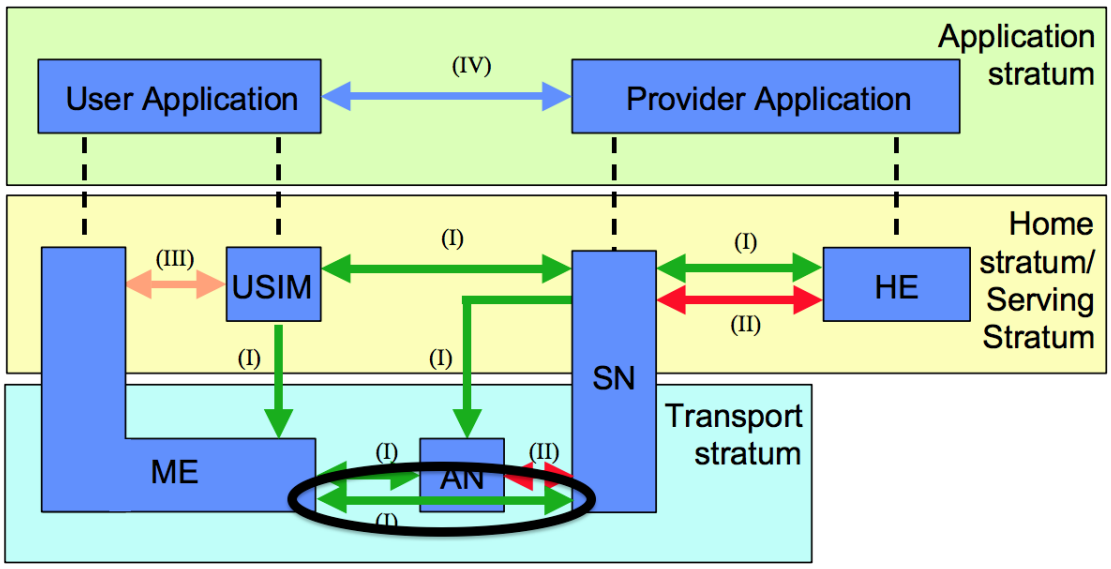

Figure 13: The 4G Security Architecture

Furthermore, implicit trust in user equipment and eNodeB (BTS in 3G) has enabled emerging attacks against both the users and the operator's core network, due to availability of open source tools (2G/3G/4G network software) and low-cost hardware. The research work demonstrates practical impact against commercially available devices [nico] and femtocell-enabled mobile network [ravi]. In this 5G security architecture, we revisit the trust assumption carefully and define trust model of 5G network entities to address potential emerging cyber threats to the infrastructure and subscribers.

8.2 ITU X.805

ITU-T Recommendation X.805 "Security architecture for systems providing end-to-end communications" [x805] has been developed by ITU-T SG 17 (ITU-T Lead Study Group on Telecommunication Security) and was published in October 2003. An overview of the architecture is given in Figure 14. This recommendation defines network security architecture for providing end-to-end network security and the general security-related architectural elements that are necessary for providing end-to end security.

It is based on the concepts of

- Security dimensions (access control, authentication, Non-Repudiation, Data Confidentiality, Communication Security, data integrity, availability, privacy): a security dimension is a set of security measures designed to address a particular aspect of the network security.
- Security Layers (Infrastructure Security Layer, Services Security Layer, Applications Security Layer): they represent a hierarchy of network equipment and facility groupings. 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/Signalling Security Plane): a security plane is a certain type of network activity protected by security dimensions. 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.

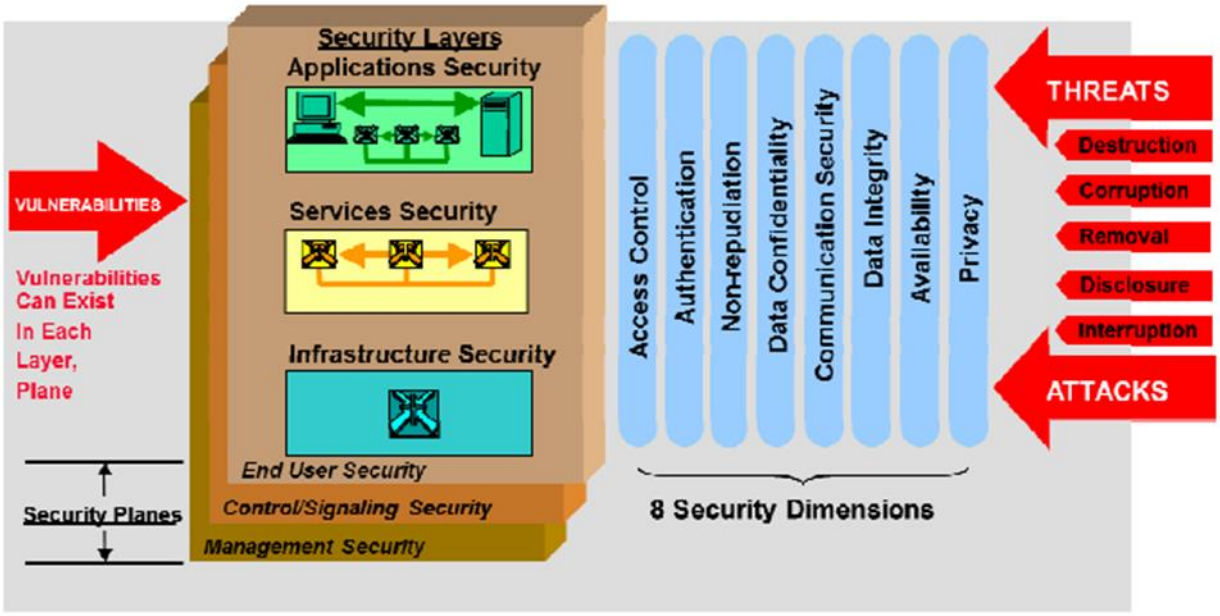

Figure 14: ITU-T X.805 Security Architecture for Systems Providing End-to-End Communications

Then it proposes to apply a security risk methodology to this framework on the basis of ITU-T Recommendation X.800 [x800] which proposes generic threats categories in order to define security objectives and requirements for each cell of the three-dimensional table based on the security layer/security planes/security dimensions presented above. For these reasons, this approach was also taken into consideration in D2.3 [d2.3].

As a comment on ITU X.805 recommendation, it seems that this framework forces the consideration of all possible threats and attacks to provide comprehensive end-to-end network security. Especially, the differentiation between the security layer and the security planes is very meaningful when it comes to define effective end-to-end security at functional level. Nevertheless, the complexity given by this three-dimensional matrix, makes the task quite heavy. Additionally, X.805 does highlight the special importance of (radio) access technology (having specific security issues), nor does it take into account virtualization and thus is further from 5G-ENSURE needs than e.g. the 3GPP architectures.

For this reason, 5G-ENSURE security architecture does not directly build on ITU-T X.805 recommendation, although 5G-ENSURE use case description template uses ITU-T X.805 security dimensions category [d2.3].

8.3 5G-PPP

The European Union funded 5G Public Private Partnership (5G-PPP) is an important initiative where public and private sectors in Europe work together to develop 5G and secure the European leadership. Several projects [5GPPP] have received support to work on areas ranging from physical layer to overall architecture, network management and software networks, to meet the requirements of 5G applications.

In its *View on 5G Architecture* [5GPArch], the Architecture Working Group describes the basis of 5G architecture principles based on the [etsi_mano] with the required features for an Automatic & Cognitive Management and Orchestration at all level of the architecture. An overview of the architecture is given in Figure 15.

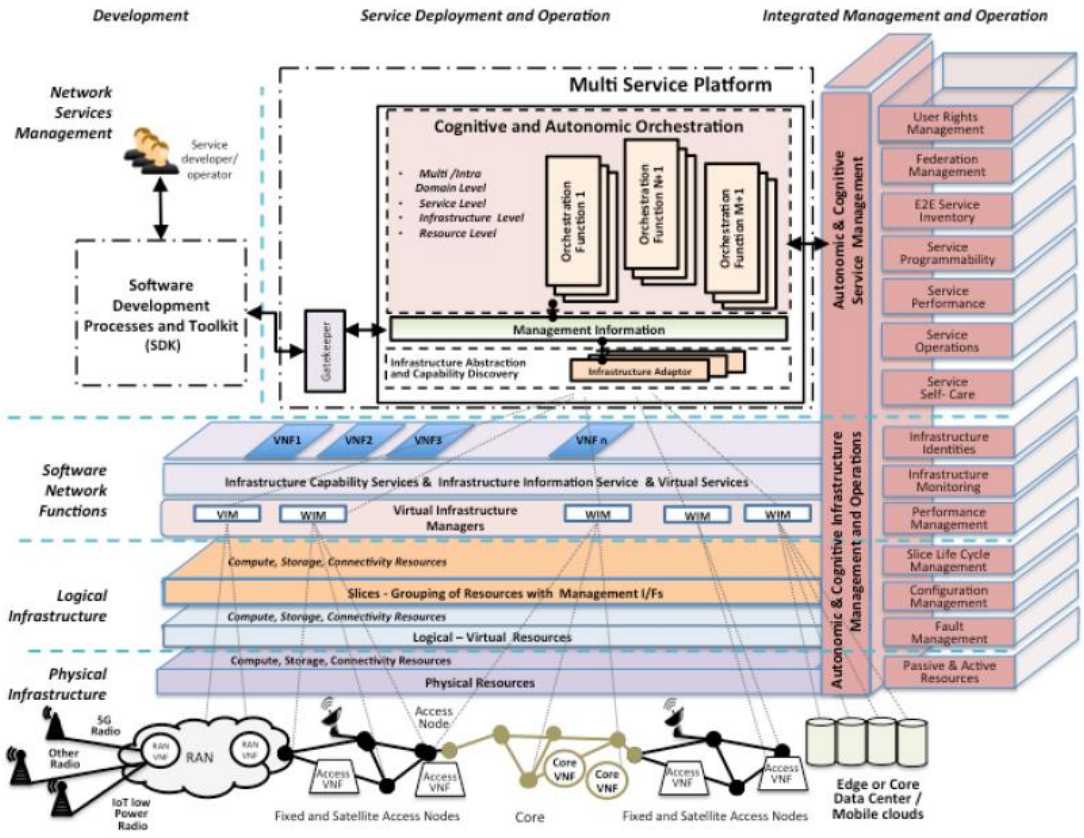

Figure 15: 5G Service & Infrastructure Management and Orchestration Architecture

This architecture serves a multi-tenancy context where the performance requirements of the different verticals served may be diverse and conflicting, see also Figure 16.

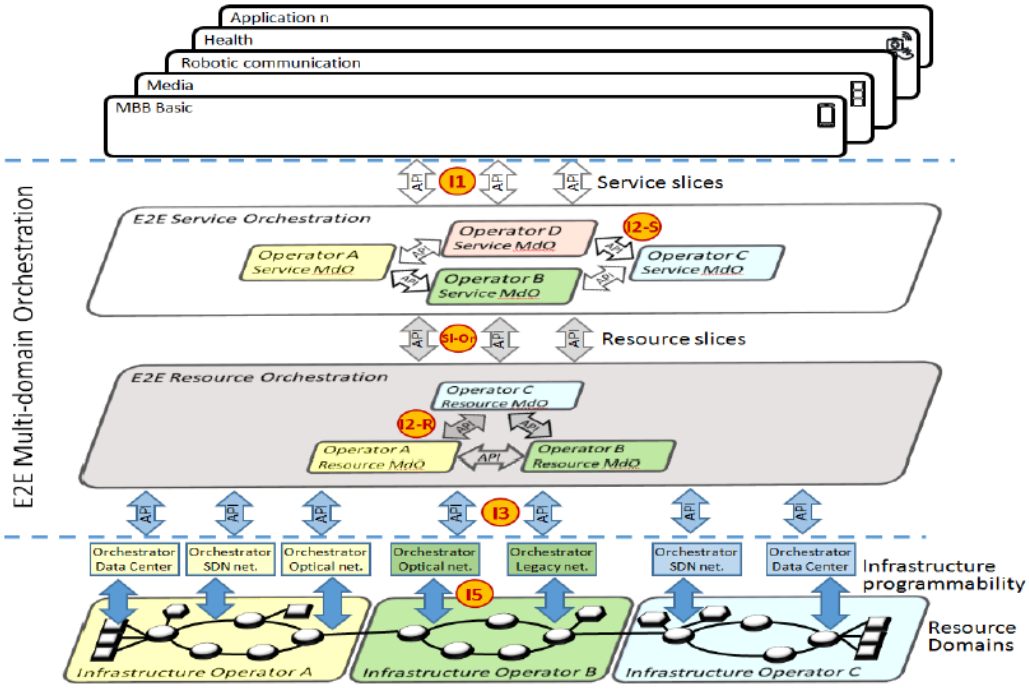

Figure 16 : E2E Multi-Domain Management and Orchestration of different infrastructure domains belonging to different operators

This usage context brings in new threats. From a security point of view, the Architecture Working group states: “The updated security considerations should not only entail new trust models, where mobile infrastructures are shared by multiple virtual mobile telecommunication providers, but also take into account novel technological approaches such as multi-tenancy, network slicing, network virtualization … . Autonomic self-protection capabilities in the 5G network that might defend users against infrastructure attacks (such as a distributed denial-of-service attack), as well as providing self-healing capabilities to the 5G Network, are a key aspect of the network intelligence expected in the novel 5G technologies.”

Further, a whitepaper titled “5G PPP Phase I Security Landscape’” was released by the 5G-PPP security working group in June 2017 [5GPPPSecurity]. This whitepaper provides new major 5G security requirements and risks; in particular, includes 5G-ENSURE security architecture proposed by 5G-ENSURE project.

In 5G-PPP, CHARISMA and 5GNORMA projects focus on security for 5G networks. The CHARISMA proposes an intelligent hierarchical routing and paravirtualized architecture that provides an end-to-end security service chain via virtualized open access physical layer security [charisma]. In particular, project focus is on security aspects to provide a holistic management platform for 5G networks combining cloud, networks slicing, SDN, and NFV technologies. Whereas another 5G-PPP project, 5G NORMA [5GNorma], aims to provide a novel radio multiservice adaptive network architecture for 5G. The project considers potential threats to their novel 5G architecture and evaluates applicability of LTE security concepts to enhance the overall security. In order to guarantee the desired flexibility and dynamics in the allocation of radio network functions, this project introduces a new access stratum security architecture for 5G. In particular security features include basic key hierarchy, support for multi-connectivity, support for multiple radio access technologies, and support for multiple network slices[5GNormaD3].

8.4 NGMN

The Next Generation Mobile Networks (NGMN) alliance goal is to expand and evolve the mobile broadband experience, with a particular focus on 5G networks. The security group, the sub-group of NGMN 5G security architecture group identifies new threats and security issues that may arise with 5G network deployments [ngmn1] [ngmn4]. In particular, this group provides recommendation for network slicing, access network, and 5G low-latency use cases that shall be consider while designing 5G networks.

8.5 IETF and IoT

In the IoT domain, several IETF working groups are acting on related subjects, among which the Authentication and Authorization for Constrained Environments (ACE) WG, the Constrained RESTful Environments (CoRE) WG, and the CBOR Object Signing and Encryption (COSE), leading to the publication of RFCs [RFC7744], [RFC7252].

New Birds of a Feather meetings (IETF Pre-WG Efforts) initiatives such as netslicing and 5G IP [5gIP] are tightly bound to 5G as the attendance of IETF chair at 3GPP 5G meetings shows it.

8.6 OMA

The Open Mobile Alliance (OMA) specified the LightweightM2M protocol [LWM2M] in the domain of IoT, which is relevant to 5G security.

9 Summary and Conclusions

We have presented the 5G-ENSURE security architecture for 5G. This 5G Security Architecture is based upon the already well-established architectures from 3GPP (TS23.101. 33.102 and 33.401) with extensions to cover 5G networks. With these extensions, the presented security architecture captures all technical characteristics of 5G related to softwarization, virtualization, multi-access, etc, as well as business model specific aspects related to 5G (security) use cases studied such as interworking with an external vertical industry's AAA functions. The presented 5G security architecture models the network and its security functionality in terms of domains, strata, security realms and security control classes. The security architecture design is based on security objectives related to the architecture itself. One of the major objectives is to have an extensible and flexible architecture which we see as being accomplished through the creation of new domains, strata, security realms and security control classes that can be defined as required to capture new network architectures, services and functions.

The 5G security architecture defined comes together with a "methodology" to get it instantiated in the context of 5G systems at hands, see [Chapter 4.6]. As shown this methodology, equipped with some tooling (e.g. to model trust), makes the proposed 5G security architecture actionable. Indeed, this methodology enables the instantiation of the 5G security architecture to meet security objectives of the (5G) system considered by engaging proper security controls either generic or specific. The latter being determined via the enactment of a TVRA resulting in a risk treatment plan.

The security architecture groups security objectives (or risks and threats) according to the defined security realms because the strata and domains in a security realm would be exposed to the same threat and risk environment. The security objectives (or risks and threats) per security realm would then be a structured input to the required TVRA. The same structure can then be used for defining the required security controls. The result would then be a logical structure for mapping required controls onto the network architecture. Working in this way would make it a relatively straightforward task to review the risk treatment plan for completeness, i.e. that all risks that should be covered are addressed.

The security architecture has been shown to be relevant and useful and fulfil the objectives for its design. A number of examples, notably the 5G logical architecture (Chapter 4.2.6) has been mapped onto the domains of the security architecture. Furthermore, the 5G-ENSURE enablers, see [d3.6], have been mapped on the security architecture, see Table 3 in Chapter 7. To show the applicability of the security architecture an IoT use case, see Chapter 7 , has also been analysed.

We have also studied the design principles and associated security concepts (Chapter 6), where we make recommendations regarding the design phases and certain aspects of the implementation. We also report on the lessons learned from the development of our enablers. One key notable difference with 5G system compared to earlier generations of mobile networks is their significantly increased reliance upon software based systems which put an emphasis on reliability and testing of all these interconnected software systems.

References

[5gIP] D. von Hugo, B. Sarikaya, T. Herbert, K. Satish, R. Schott, S. Seo, 5G IP Access and Session Management Protocols - draft-xyx-5gip-ps-01, IETF Internet-Draft, May 2017, https://tools.ietf.org/html/draft-xyx-5gip-ps-01

[5GNorma] 5G Novel Radio Multiservice adaptive network Architecture, https://5g-ppp.eu/5g-norma/

[5GNormaD3] 5G NORMA network architecture https://5gnorma.5g-ppp.eu/wp-content/uploads/2017/03/5g_norma_d3-2.pdf

[5GPArch] 5G PPP Architecture Working Group, View on 5G Architecture, Version 1.0, July 2016

[5GPPP] 5G PPP Phase I Projects - https://5g-ppp.eu/5g-ppp-phase-1-projects/

[5GPPPArchWP] 5G PPP 5G Architecture White Paper 2- Summer 2017_For Public Consultation. Available at https://5g-ppp.eu/wp-content/uploads/2017/07/5G-PPP-5G-Architecture-White-Paper-2-Summer-2017_For-Public-Consultation.pdf

[5GPPPSecurity] 5G PPP Phase1, Security Landscape, https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

[bt] BT Group plc, Deutsche Telekom, Ericsson, Hutchison Whampoa Europe, Inmarsat plc, Nokia, Orange, Proximus SA/NV, Royal KPN N.V., SES, Tele2 AB, Telecom Italia S.p.A., Telefonica, Telekom Austria Group, Telenor Group, Telia Company, Vodafone Group, «5G Manifesto for timely deployment of 5G in Europe,» 7th July 2016. Available: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=16579

[cc] Common Criteria, available at https://www.commoncriteriaportal.org/

[charisma] CHARISMA Project, http://www.charisma5g.eu/index.php/overview/

[d2.1] 5G-ENSURE, “Deliverable D2.1 Use Cases,” 2016. Available at: http://5gensure.eu/deliverables

[d2.3] 5G-ENSURE, “Deliverable D2.3 Risk Assessment, Mitigation and Requirements (draft)”, 2016. Available at: http://5gensure.eu/deliverables . Available: https://www.ericsson.com/res/docs/whitepapers/wp-5g.pdf

[d2.4] 5G-ENSURE, “Deliverable 2.4 Security Architecture (draft)” 2016. Available at: http://5gensure.eu/deliverables

[d2.5] 5G-ENSURE, “Deliverable D2.5 Trust model (final)”, 2017. Available at: http://5gensure.eu/deliverables

[d2.6] 5G-ENSURE, “Deliverable D2.6 Risk Assessment, Mitigation and Requirements (final)”, 2017. Available at: http://5gensure.eu/deliverables

[d3.2] 5G-ENSURE, “Deliverable D3.2 5G-PPP security enablers open specifications (v1.0)” 2016. Available at: http://5gensure.eu/deliverables

[d3.6] 5G-ENSURE, “Deliverable D3.6 5G-PPP security enablers open specifications (v2.0)”, Available at http://5gensure.eu/deliverables

[e860] ITU-T E860 Framework of a service level agreement (06/2002), Available: https://www.itu.int/rec/

[ericsson] Ericsson, “5G radio Access,” april 2016. [En ligne]

[etsi_mano] ETSI, “ETSI GS NFV-MAN 001 V1.1.1 (2014-12), Network Functions Virtualisation (NFV); Management and Orchestration”

[etsi_nfv] ETSI, “ETSI GS NFV-SEC 003, Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance”

[etsi-sw-2017] ETSI Security Week 2017, http://www.etsi.org/etsi-security-week-2017

[huawei] Huawei PSIRT, Several Vulnerabilities in Huawei Honor Routers. Link - http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160607-01-honorrouter-en, last visited 15 Sept 2016

[iso27001] ISO/IEC 27001:2013. Information technology – security techniques – information security management systems – requirements. https://www.iso.org/standard/54534.html, 2013.

[LWM2M] OMA, Lightweight Machine to Machine Technical Specification, http://openmobilealliance.org/iot/lightweight-m2m-lwm2m

[ngmn1] NGMN Alliance, 5G security recommendations Package #2: Network Slicing, https://www.ngmn.org/uploads/media/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf

[ngmn4] NGMN Alliance, 5G security recommendations Package #3: Mobile edge computing, low latency, consistent user experience. https://www.ngmn.org/uploads/media/161028_NGMN-5G_Security_MEC_ConsistentUExp_v1.3_final.pdf

[nico] Nico Golde, “On the Impact of Modiied Cellular Radio Equipment”, TU Berlin, PhD Thesis.

[nist] NIST Special Publication SP 800-53. Assessing security and privacy controls in federal information systems and organizations. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf, 2014.

[nist-sec] Barbara Guttman and Edward A. Roback. 1995. SP 800-12. an Introduction to Computer Security: The NIST Handbook. Technical Report. NIST, Gaithersburg, MD, United States.

[p806] EURESCOM P806-GI project, Deliverable 1

[ravi] Ravishankar Borgaonkar, Security Analysis of Femtocell-Enabled Cellular Network Architecture, TU Berlin, PhD thesis

[RFC7252] Z. Shelby, K. Hartke, and C. Bormann. The Constrained Application Protocol (CoAP). RFC 7252 (Proposed Standard), June 2014. Updated by RFC 7959[LWM2M]

[RFC7744] L. Seitz, S. Gerdes, G. Selander, M. Mani, and S. Kumar. Use Cases for Authentication and Authorization in Constrained Environments, RFC 7744 (Informational), Jan. 2016.

[ros] Bill Roscoe et al, “Research directions for trust and security in human-centric computing

[tosca1] TOSCA Simple Profile in YAML Version 1.0, Committee Specification 01, 12 June 2016.

[tosca2] TOSCA Simple Profile for Network Functions Virtualization (NFV) Version 1.0, Committee Specification Draft 03, 17 March 2016

[tr22.891] 3GPP, “Study on New Services and Markets Technology Enablers (TR 22.891)”

[tr33.899] 3GPP, “Study on the security aspects of the next generation system (TR33.899)”

[ts23.101] 3GPP, “General Universal Mobile Telecommunications System (UMTS) architecture (Release 13)”, (TS 23.101).

[ts23.501] 3GPP, “System Architecture for the 5G System (Release 15”)

[ts33.102] 3GPP, "Technical Specification Group Services and System Aspects; 3G Security; Security architecture" (TS 33.102)

[ts33.120] 3GPP, “Security Objectives and Principles” (TS 33.120)

[ts33.401] 3GPP, "Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture" (TS 33.401)

[ts33.821] 3GPP, “Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE)” (TR 33.821)

[x800] ITU-T Recommendation X.800, Security architecture for Open Systems Interconnection for CCITT applications. Available at https://www.itu.int/rec/T-REC-X.800-199103-I/en

[x805] ITU-T Recommendation X.805 “Security architecture for systems providing end-to-end communications”. Available at https://www.itu.int/rec/T-REC-X.805-200310-I/en

A Annex: Mapping of security objectives versus security enablers

Table 5: Mapping of security objectives versus security

Category		AAA							Privacy				Trust					Security Monitoring						Netw Mt + Virtualiz. Isolation					
			Internet of things (IoT)																										
5G-ENSURE security enablers		Basic AAA enabler	Non-USIM based authentication	vGBA	Bring Your Own Identity	Group-based authentication	Fine-grained Authorization	Federative authentication and identification enabler	Privacy Enhanced Identity Protection	Device identifier(s) privacy	Device-based Anonymization	Privacy policy analysis	Trust Builder	Trust Metric Enabler	VNF Certification	Security Indicator	Reputation based on Root Cause Analysis for SDN	System Security State Repository	Security Monitor for 5G Micro Segments	Satellite Network Monitoring	Generic Collector Interface	PullSAR: Proactive Security Analysis and Remediation	Malicious Traffic Generator	Anti-Fingerprinting	Access Control Mechanisms	Component-Interaction Audits	Bootstrapping Trust	Micro Segmentation	Flow Control: in-network Threat Detection and ...
Objectives																													
Architecture	O1.1																												
	O1.2					x							x							x		x							
	O1.3												x			x				x									
	O1.4												x			x				x									
	O1.5												x																
	O1.6												x									x							
	O1.7		x										x																
	O1.8																												
	O1.9							x		x						x				x									
	O1.10																												
	O1.11						x		x	x	x				x												x	x	
New business	O2.1								x	x	x		x																
	O2.2							x																					
Legacy System	O2.3	x						x	x	x	x	x				x													
	O2.4								x	x	x	x	x			x													
Regulatory	O2.5								x	x	x	x																	
Access network	O3.1								x	x				x		x		x		x									x
	O3.2																												
	O3.3						x			x						x													
	O3.4								x							x													
	O3.5																												
	O3.6																												
Management	O4.1															x									x				
	O4.2							x					x			x	x					x				x	x		
	O4.3															x									x	x	x		
	O4.4							x	x																				
	O4.5					x		x																					
	O4.6																	x	x	x	x	x							x
	O4.7							x												x	x								
	O4.8	x				x			x																				
	O4.9							x		x	x															x		x	
User Equipment	O5.1																												
	O5.2		x	x	x	x	x			x																			
	O5.3		x	x			x																						
	O5.4				x		x		x		x																		
Network	O6.1										x			x			x			x		x	x	x					x
	O6.2																			x			x						
	O6.3								x											x		x	x	x					
	O6.4																						x						
	O6.5																										x		
Infrastructure & Virtualization	O7.1		x																						x			x	
	O7.2				x										x	x			x							x			
	O7.3	x	x		x								x			x		x									x		
	O7.4													x															x
	O7.5																											x	
	O7.6														x													x	x
	O7.7																												