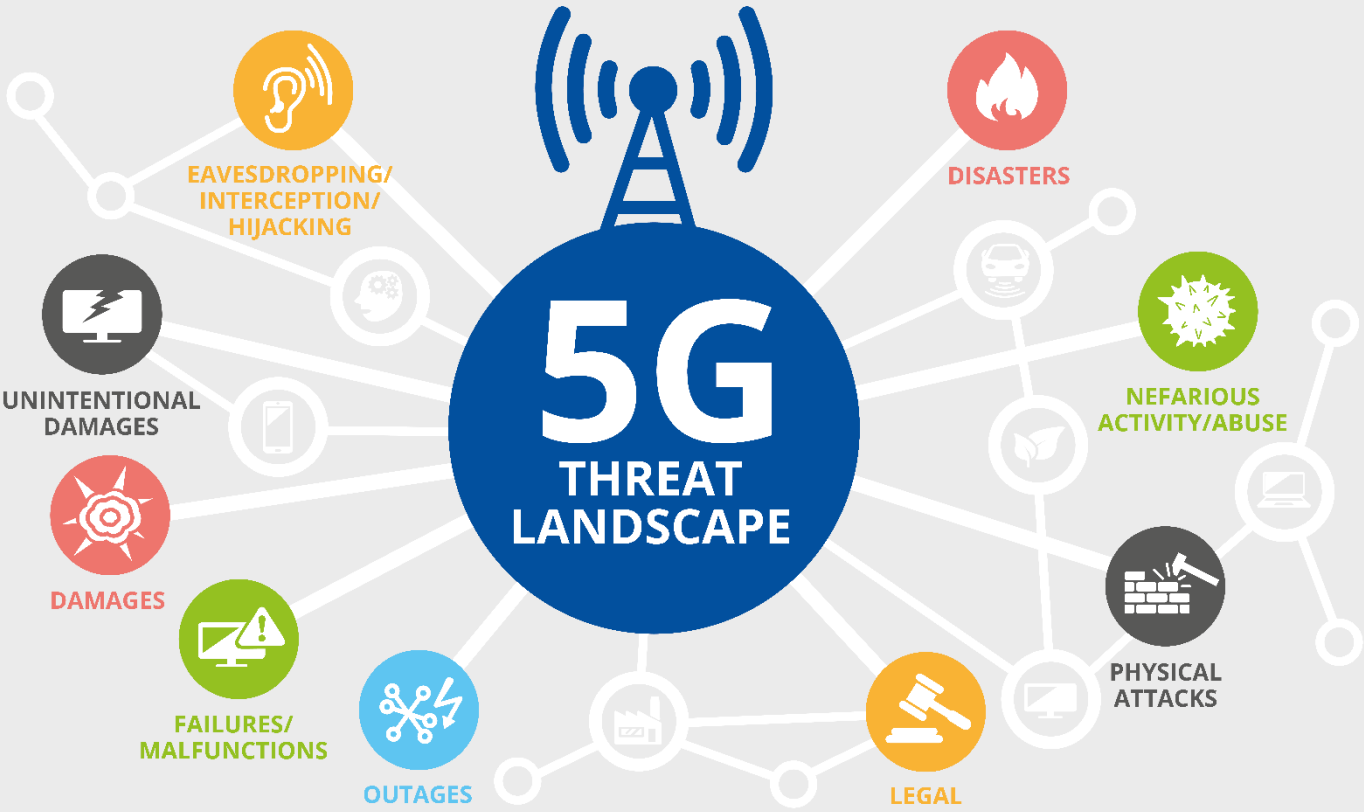
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



ENISA THREAT LANDSCAPE FOR 5G NETWORKS

Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)

DECEMBER 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

EDITORS
Marco Barros Lourenço, Louis Marinos, Lampros Patseas - EU Agency for Cybersecurity

CONTACT
For contacting the authors please use enisa.threat.information@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

ACKNOWLEDGEMENTS
We would like to thank the ENISA contractor Andrei Hohan (ENERSEC), Adrian Anghel (ENERSEC) for the desk-top analysis of open-source material and all members of the ENISA ad-hoc 5G Expert Group, acting on an ad personam basis: Ioannis Askoxylakis, Pascal Bisson, Jon France, Patrik Palm and Jean-Philippe Wary, for supporting the ENISA team in information collection, knowledge transfer in the subject matter.

LEGAL NOTICE
Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time. Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN: 978-92-9204-445-9 - DOI: 10.2824/802229

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

ACRONYMS	DESCRIPTION
3GPP	3rd Generation Partnership Project
3GPP TS	3GPP Technical Specification
3GPP TR	3GPP Technical Report
5GC	5G Core
5G-PPP	5G Infrastructure Public Private Partnership
AAA	Authentication, Authorisation and Accounting
AF	Application function
AKA	Authentication and key agreement
AMF	Access and mobility management function
API	Application programming interface
ARLC	Air radio link control
ARP	Address resolution protocol
ARPF	Authentication credential repository and processing function
AS	Access stratum
AUSF	Authentication server function
CAPIF	Common API Framework
CGI	Common Gateway Interface
CN	Core network
COTS	Commercial of the shelf
CSA	Cloud Security Alliance
CSCF	Call / Session Control Function
CSMF	Communication service management function
CSP	Communication Service Provider
CTI	Cyber Threat Intelligence
CU	Control unit (RAN)
DC	Data Centre
DCSP	Data Centre Providers
DDoS	Distributed Denial of Service
DN	Data network
DNS	Domain Name System
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
DU	Distributed unit (RAN)
E2E	End-to-end
EM	Element management
EU	European Union
eMBB	Enhanced mobile broadband
eNB	E-UTRAN Node B, also known as Evolved Node B
ECCG	European Consumer Consultative Group
ENISA	European Union Agency for Network and Information Security
EPC	Evolved Packet Core
ESP	Encapsulating Security Payload
eTOM	enhanced Telecom Operation Map

ACRONYMS	DESCRIPTION
ETSI	European Telecommunications Standards Institute
FOSS	Free and Open Source Software
gNB	Next generation Node B
GMLC	Gateway Mobile Location Centre
GNP	Generic Network Product
GSMA	GSM Association
GTP	GPRS Tunnelling Protocol
GTP-C	GPRS Tunnelling Protocol Control
GTP-U	GPRS Tunnelling Protocol User
HBRT	Hardware-Based Root of Trust
HTTP	Hypertext Transfer Protocol
IAB	Integrated Access and Backhaul
IE	Information Element
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IKEv2	Internet Key Exchange Protocol Version 2
IMSI	International Mobile Subscriber Identity
IoT	Internet of things
ITU	International Telecommunications Unit
IP	Internet protocol
IPsec	IP Security
IPX	IP Exchange Service
ISAC	Information sharing and analysis centres
ISF	NFVI-based Security Function
ISO	International standards organisation
ITU	International Telecommunication Union
IXP	Internet Exchange Point
JSON	JavaScript Object Notation
JWS	JSON Web Signature
KPI	Key Performance Indicators
LCM	Life Cycle Management
LEA	Law Enforcement Agency
LI	Lawful Interception
LMF	Localisation Management Function
LTE	Long-Term Evolution
M2M	Machine to Machine
MAC	Media access control
MANO	Management and orchestration
MEC	Multi-access edge computing
MIMO	*Multi-input multi-output*
MME	*Mobility Management Entity*
mMTC	*massive Machine-Type Communication*
MNO	Mobile network operator
NAS	Non access stratum
NCA	National Certification Authorities
NCSC	National cybersecurity coordinator/agency/centre
NEF	Network exposure function
NESAS	Network Equipment Security Assurance Scheme
NF	Network function
NFVI	Network function virtualisation infrastructure

ACRONYMS	DESCRIPTION
ng-eNB.	Next generation - evolved Node B
NG RAN	Next generation Radio Access Network
NIS Directive	The Directive on security of network and information systems
NOP	Network operator
NR	New radio
NRA	National Regulator
NRF	Network repository function
NS	Network slice
NSA	Non-standalone
NSI	Network slice instance
NSM	NFV Security Manager
NSMF	Network slice management function
NSSAAF	Network Slice Specific Authentication and Authorisation Function
NSSAI	Network Slice Selection Assistance Information
NSSF	Network slice selection function
NSSI	Network Slice Subnet Instance
NSSMF	Network slice subnet management function
NSST	Network Slice Subnet Template
NTC	National 5G test centres
OAM	Operation, Administration, and Management
O&M	Operations & Maintenance
OS	Operating system
OSS/BSS	Operations Support System/Business Support System
PCF	Policy control function
PDCP	Packet data conversion protocol
PDU	Protocol data unit
PLMN	Public Land Mobile Network
PNF	Physical Network Function
PSF	Physical Security Function
QoS	Quality of service
RACS	Radio Capabilities Signalling
RAT	Radio access technology
RES*	Response (authentication response)
RFC	Request for Comments
RRC	Radio Resource Control
RU	Radio Unit
SA	Security architecture
SaaS	Software as a Service
SBA	Service-based architecture
SBI	Service-based interface
SC	Service customers
SCAS	3GPP Security Assurance Specifications
SCP	Service Communication Proxy
SDAP	Service data adaptation protocol
SDN	Software defined network
SEAF	Security anchor functionality
SECAM	3GPP *Security Assurance* Methodology
SEPP	Security edge protection proxy
SFTP	Secure File Transfer Protocol
SGW	Serving gateway
SIDF	Subscription identifier de-concealing function

ACRONYMS	DESCRIPTION
SLA	Service level agreement
SMC	Security Mode Command
SMF	Session management function
SMS	Short message service
SMSF	SMS function
SP	Service providers
SSA	NFV security services agent
SSI	Server Side Includes
SSH	Secure Shell
SSP	NFV security services provider
SUCI	Subscription concealed identifier
SUPI	Subscription Permanent Identifier
TCP	Transmission Control Protocol
TEID	Tunnel Endpoint Identifier
TLS	Transport Layer Security
TPM	Trusted platform module
TSN	Time Sensitive Networking
UCMF	UE radio Capability Management Function
UICC	Universal Integrated Circuit Card
UDM	Unified data management
UDR	Unified data repository
UDSF	Unstructured data storage function
UE	User equipment
UP	User Plane
UPF	User plane function
URLLC	Ultra-reliable low-latency communication
USIM	Universal subscriber identity module
V2V	Vehicle to vehicle protocol
V2X	Vehicle to everything protocol
VISP	Virtualisation infrastructure service providers
VIM	Virtualised infrastructure manager
VM	Virtual machine
VNF	Virtualised Network Function
VNFD	VNF descriptor
VNFM	VNF manager
VNFI	VNF Infrastructure
VSF	Virtual Security Function

1. INTRODUCTION

This report is an update of the ENISA 5G Threat Landscape, published in its first edition in 2019[1]. This document is a major update of the previous edition. It encompasses all novelties introduced, it captures developments in the 5G architecture and it summarizes information found in standardisation documents related to 5G. Moreover, the vulnerability and threat assessments found in this document introduce a significant advancement to the previous edition, by providing more comprehensive information about the exposure of assets of the updated 5G architecture.

Beyond these changes, some additional elements have been taken into account. Firstly, implementation/migration options of a gradual migration to 5G from 4G have been taken into account. Secondly, security issues of operational processes have been considered. These two changes enlarge the scope of the assessment and include important parts for the enhancement of operational security.

For all these elements, this report provides a vulnerability analysis, indicating how these vulnerabilities can be exploited through cyberthreats and how this exploitation can be mitigated through security controls. The assessed vulnerabilities are consolidated from various sources, including main 5G standardisation documents and telecommunication best practices (3GPP, ITU, ETSI, ISO, NIST and GSMA). A consolidation and mapping of cyberthreats used in these standards has also been performed. Clearly, the complexity of 5G infrastructure and the dependencies of assets, controls and threats is reflected in the complexity of the produced information. ENISA would like to develop a tool-based version of this information, so that users of the material can better navigate this complex information in a more efficient way than the static, highly interlinked tables presented in this report. This task will be accounted for in the near future.

The performed assessments in this report are based on specifications of 5G infrastructure, thus potentially having a certain “distance” from actual implementations. Moreover, assessed vulnerabilities have been extrapolated from experiences of weaknesses of technical implementations of similar non-5G components. As such, they comprise rather hypothetical assumptions that are to be validated on the basis of implementations. ENISA states in this document the importance of bridging the gap between functional specifications and implemented functions. As 5G implementation are proceeding, it is important to develop ways to check the compliance of implementations towards the specified content and feedback information to the specification efforts. Initially, the creation of implementation guidelines may be a useful tool to assess the quality of implementations. In addition, security assurance methods may be a good way to support developers and/or entities that will test the compliance of implemented 5G functions.

A good method to overcome these limitations and at the same to further advance the quality of this and other relevant material (ENISA, European Commission, Member States, 3GPP, BEREC, etc.) is to use it within detailed 5G threat/risk assessments in a coordinated manner. Besides validation of the produced information, such actions will contribute towards a more secure 5G infrastructure and have as consequence the creation of a competitive advantage of European stakeholders in the area of 5G. At the same time, it will increase efficiency of used resources by avoiding duplication of efforts.

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks, accessed October 2020.

The authoring of this report has been performed exclusively by ENISA. It is based on Open Source Intelligence (OSINT) collection of publicly available information. Following a desk-top analysis of this material by an external contractor, an update of the 5G architecture has been performed by ENISA, vulnerabilities have been collected and consolidated and threat exposure has been assessed. Mitigation controls found in publicly available documents have been associated to the identified exposure, leading to a reduction of attack surface. An ad-hock expert group consisting of 5G experts has contributed on an ad-personam basis and has supported the work of ENISA. Their contributions were towards information collection and knowledge transfer in the subject matter. Their contributions has been considered and compiled by ENISA using it as an input.

For the time being, the material presented in this report aims at supporting various stakeholders understanding the relevant vulnerabilities and cyberthreats resulting to an exposure of 5G assets by exploiting the vulnerabilities. When requested, ENISA is in the position to support stakeholders 'drilling down' the analysis further, by including granular details from the components in focus, and examine the relevance of the assessed cyberthreats and the efficiency of developed security measures.

To better understand the cyber-threats affecting 5G Networks, it is essential to know the vulnerabilities and weaknesses of assets, assessing thus their attack surface and how it can be exploited by malicious actors.

1.1 POLICY CONTEXT

In January 2020, the European Commission has issued a communication calling Member States to take steps to implement the set of measures recommended in the 5G toolbox[2,3]. In June 2020, a "*Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*[7]" has been published NIS Cooperation Group with the objective to provide an overview of the state of play of the ongoing toolbox implementation process by Member States as of June 2020.

The present report contributes to the implementation of 5G toolbox measures (SMs, TMs) and supporting actions (SAs). Its main contribution is supporting action 9 (SA09), stating "*Consider the use of existing cooperation, coordination and information sharing mechanisms, including actions and support by ENISA, notably through regular threat assessments*". Moreover, by providing all details about vulnerabilities, threats, security requirements and mitigation controls, this document builds the basis for performing technical risk assessments for various sub-systems and components of the 5G architecture, by delivering input to identify the main technical "*risk factors*" for 5G.

Since the adoption of the EU 5G Toolbox in January 2020 and the publication of Member States progress report of the implementation June 2020[4], Member States had paid increasing attention to the implementation of SM05 and SM06. The purpose of SM05 and SM06 is to ensure resilience through diversity while addressing risk R4 at individual MNO level and national level. However it is essential to recognize that the updated ENISA 5G Threat Landscape report has not been revised to the extent that it can provide Member States with guidance on how to implement SM05 and SM06. This is due to the fact that this report does not specify all relevant assets in the 5G ecosystem supply chain (devices, cloud and network assets) and objective criteria for key stakeholders to assess resilience and diversity in the context of SM06. Furthermore, the current report does not provide a set of common mitigation methods to proportionally apply across the 5G ecosystem and key stakeholders, at national (SM06 such as issues of number of MNO, network sharing) or at individual network level (SM05). Consequently, it is not possible from this report to make conclusions about how to consistently and proportionally implement mitigations across EU. Within this report, supporting actions SA03

[2] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission, accessed October 2020.
[3] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468, accessed October 2020.
[4] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1378, accessed November 2020.

and SA04 are extensively covered (by numerous contributing to TM01, and TM02, as indicated in the mapping found in the vulnerability assessment).

Moreover, in the new ENISA regulation, the need to analyse current and emerging risks is expressed. In line with this role, ENISA regulation stipulates that: "*the Agency should, in cooperation with Member States and, as appropriate, with statistical bodies and others, collect relevant information*"[5]. More specifically, it is stated that it should "*enable effective responses to current and emerging network and information security risks and threats*"[6].

Therefore, the ENISA 5G Threat Landscape aims at contributing to the EU Cybersecurity Strategy and more specifically, to ongoing policy initiatives related with the security of networks and information systems; it streamlines and consolidates available information on cyber-threats and their evolution, thus supporting EU and national risk assessment activities.

1.2 SCOPE AND METHODOLOGY

Unlike the conditions of previous year regarding the state-of-play of 5G developments, in 2020 several national, European and international developments have led to a clearer picture of 5G infrastructure developments at various levels. The 5G specification has done significant progress, implementation options and migration paths from 4G to 5G have been better clarified, relevant operational processes for 5G infrastructure have been developed and taken up and specialized 5G functions for verticals have been specified. Moreover, at the EU level, a 5G toolbox[7] has been developed and pilots towards 5G certification schemes are envisaged, in preparation of potential requests to ENISA issued by the ECCG in the future.

This situation gives a far better visibility on the details of 5G infrastructures and is a better starting point for updating the ENISA 5G Threat Landscape. Having regard to these developments, the objectives, working methods and scope of this report are as follows:

- The material collected and processed within this report consists of open source resources. It covers mainly the state-of-the art of the 5G specification work, white papers and good practices. No concrete implementations of 5G functions from vendors, operators, etc. have been considered or analysed for the purpose of this report.

- The threat and vulnerability analysis performed is based on the extrapolation of existing threats and vulnerabilities found in collected material. In this respect, vulnerabilities referred in various processed documents have been "reverse-engineered" based on their relevance to various components/assets; subsequently, they have been grouped under the various zoom-ins and reflect the assessed technical and operational weaknesses, as mentioned in the various standards/good practices. It has to be noted that this is a pure desk-top exercise based on assumed vulnerabilities and threats and is not funded by real incidents. Equivalently, threat actors assumed in this report are rather hypothetical, as no known attacks to such infrastructure do yet exist. For this reason, 5G attack vectors have not been taken into account in this work.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN, accessed November 2020.
[6] https://www.enisa.europa.eu/publications/ed-speeches/towards-a-new-role-and-mandate-for-enisa-and-ecsm, accessed October 2020.
[7] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures, accessed October 2020.

- The comprehensive architecture of 5G developed in the previous threat landscape report[8] has been updated to include novelties of the 3GPP specification. This work has taken into account all details that have been available in the 5G specification work.

- Implementation options – migration paths from 4G to 5G infrastructures have been covered.

- A process map has been developed showing the contribution of operational, life-cycle and security assurance processes to the overall security of 5G infrastructures.

- A detailed technical and operational vulnerability analysis has been performed for the components of the 5G architecture. This analysis takes into account the threats exploiting those vulnerabilities and the controls reducing exposure to these threats, as defined by international organisations (3GPP, ETSI, GSMA, ISO, ITU, NIST).

- Except from generic functions developed for verticals by 3GPP, no information about verticals per se (e.g. Transportation, eHealth, Industrial Internet-of-things (IIoT), Smart Environments, etc.) have been covered in this report. This is due to potential complexity of those environments and the unavailability of information due to their early specification, implementation and deployment stages of 5G verticals.

- Detailed information and security requirements for various functions and interfaces are included in this report, mainly via the annexes detailing the assessed vulnerabilities. They cover security requirements, mitigation controls, involved stakeholders and references to related specifications and the EU toolbox measures. Moreover, the threats used in various reports have been consolidated by means of the threat taxonomy delivered in this report.

- The scope of this report is in line with work developed by ENISA, in particular, the 5G Threat Landscape in its 2019 edition[8], and it also coherent to ENISA deliverables in the area of 5G Standardisation.

- The development of this report followed a ‘best-effort’ approach. The collected information is not exhaustive but representative of the matters covered.

- To collect relevant technical material and available 5G knowledge, ENISA has maintained an ad hoc expert group consisting of skilled individuals in the area of 5G. The selection of experts has been made based on technical experience of the selected individuals, acting ad personam. A member of the team is an active member (co-chair) of the 3GPP security sub-group and has acted as an interface between ENISA and 3GPP. The selection has aimed at covering detailed technical 5G knowledge skills from the most representative stakeholder types that are currently engaged in 5G activities.

- The content of this report was restricted to components/matters found in relevant open-source material covering the entire specification, security requirements and research results related to 5G network functions (NFs). The presented material has been put together by ENISA.

[8] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks, accessed October 2020.

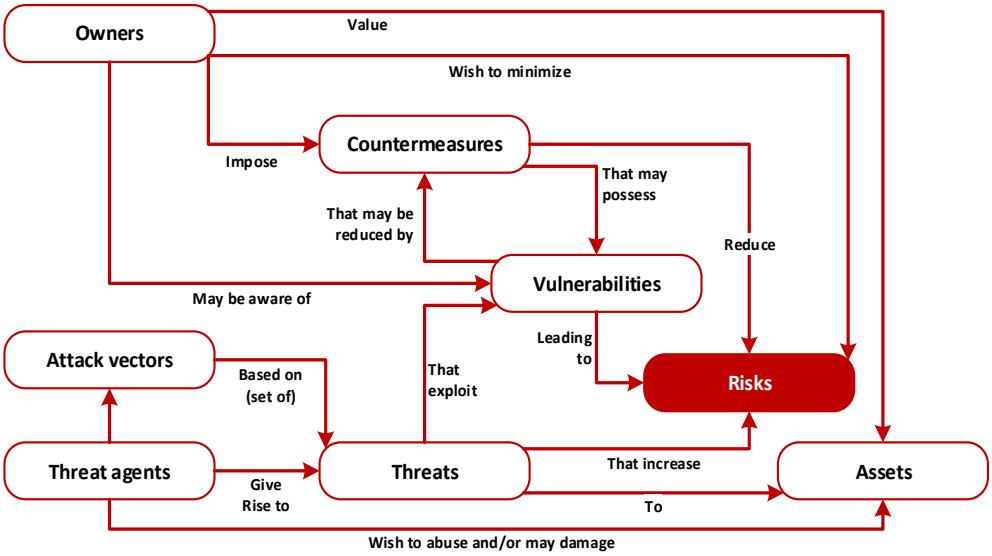
- Issues regarding Law Enforcement Agencies (LEA) and Lawful Interception (LI) have not been covered in this document, apart from a reference in the threat taxonomy and few references found in 3GPP specifications, both kept for the shake of completeness.

- This report addresses in detail all technical aspects of 5G networks and related threats emerging from the collected material (e.g. 3GPP specification, standards, good-practices). It does not cover non-technical threats (i.e. geopolitical), such as threats leading to regulatory risks or risks of interference from third countries through the supply chain.

The method adopted for this study is in line with the methodology developed by ENISA for the preparation of its annual Cyberthreat Landscape. According to this methodology, the process requires an initial identification of relevant assets within the architecture before performing a vulnerability and a threat assessment, which evaluates the different levels of asset exposure. Finally, by assigning security controls to the exploitable vulnerabilities, it reduces the threat surface of relevant assets.

The elements of cyberthreats and the relationship to risks are graphically depicted inFigure 1. The report describes the different relationships between assets, threats and threat agents. In future versions of this report, we will cover vulnerabilities and countermeasures (mitigation measures/security controls).

Figure 1: Methodology adopted based on ISO 27005



Threats play a central role in a risk assessment, especially when considering the different components of risks. The ISO 27005, a widely adopted risk management standard, defines that risks emerge when: “Threats abuse vulnerabilities of assets to generate harm for the organisation”[9].

Following this methodology, we have identified assets, threats and threat agents. These constitute the core of the 5G Threat Landscape presented in this report. Furthermore, the identification and analysis of assets and cyber-threats are based on the study of specifications, white papers and literature, without attempting any interpretation/evaluation of the assumptions stated in these reports. It has to be noted, that the logical relationship between Threat Agents

[9] https://www.iso.org/standard/75281.html, accessed October 2020.

and Attack Vectors has not been implemented in this document for the reasons: a) the threat agent profiles are still very rudimentary and b) attack vectors in the area of 5G are unknown, while any assumptions on attack vectors based on specified functions (3GPP) would be premature.

1.3 TARGET AUDIENCE

Main purpose of this report is to provide knowledge and information on 5G cybersecurity issues to the relevant community. This information may be useful to a variety of target groups:

- *Non-technical stakeholders such as* policy-makers, *regulators, law enforcement*: this target group may find this report useful to understand the current state of specification work, the overall architecture of 5G, the emerging vulnerabilities and threats and respective mitigation practices and measures. For example, the threat landscape identified in this report may support policy actions in the areas of 5G networks, SDN, NFV, cybersecurity, critical infrastructure protection, and other sectors/verticals that plan to use the 5G Network.
- *Experts working in the telecommunication sector, such as operators, vendors, and service providers*: this target group may find this report useful to carry out detailed threat analyses and risk assessments in accordance with their particular needs and mandate (e.g., protect a specific number of components based on asset impact analysis, respond to specific vulnerabilities with customized mitigation measures among others).
- *Businesses, consultants, product developers*: this target group can draw valuable conclusions from the developed analysis and material for their offerings (products, services). This can have the form of demonstrating how vulnerabilities have been eliminated by using developed defences, use of the material within customer projects, or use the material as a benchmark for defining cybersecurity protection policies for such infrastructures (e.g. for the development of verticals). Moreover, the developed material can be used in developing security audits for 5G infrastructures.
- *Experts in research and innovation*: the presented material provides a detailed view on security issues of 5G. This target group may use this material as basis for gap analysis, as material to evaluate the impact of research and as source for innovation actions with regard to the further development and implementation. Finally, this target group may use this material as a useful resource for numerous academic activities, such as teaching, research, support of scholars, etc.

Beyond these main target groups, some individual parts of the information provided in this report may be useful to a further number of target groups. For example, the assessed vulnerabilities – as a consolidation from various sources - may be a valuable resource for standardisation work in order to check the completeness of already performed assessments. Moreover, the provided material may be used within risk assessment within certification activities, providing information about the threat exposure, as well threat actor motives and objectives. Finally, both the 5G asset inventory and the 5G threat taxonomy can be used as-is or further developed by any stakeholders in performing their own vulnerability, threat and risk assessments.

1.4 STRUCTURE OF THE REPORT

This report presents the results of the performed vulnerability and threat assessment work in the following manner

- **Chapter 2** presents the stakeholders having a role in all phases of 5G implementation, covering specification, development, deployment, operation and supervision of the 5G infrastructure. They constitute an essential part of the 5G ecosystem. The identified, stakeholders carry the main responsibility for the implementation and management of cybersecurity controls, thus being responsible for mitigating the threats identified in this report.
- **Chapter 3** presents the architectural framework of 5G technology by offering a generic architecture. By means of 'Zoom-ins' it provides details of various components, including introduced novelties and an overview of security considerations. These details will contribute to the process of identifying the critical assets of the technology.
- **Chapter 4** presents the results of the vulnerability assessment of for each zoom-in. It presents vulnerability groups affecting the assets of each particular zoom-in. It provides an overview of the detailed vulnerabilities presented in the annexes (Annexes C-M) of this report. While this chapter provides an overview of vulnerability groups per zoom-in, the detailed information embraces detailed vulnerabilities, associated with threats, mitigation controls and references to corresponding collected material,
- **Chapter 5** presents the 5G asset inventory. It consists of a collection of important assets drawn for the components presented in the zoom-ins in the form of a mind map available in Annex A. The assets inventory contains assets whose vulnerabilities have been assessed in the previous chapter.
- **Chapter 6** presents an overview of the assessed cyber-threats. Interrelated threats have been grouped to form a taxonomy that is presented as a detailed mind map in Annex B.
- **Chapter 7** provides information on threat agents. It is a first approach towards the assessment of potential motives emerging from the abuse/misuse of 5G assets.
- **Chapter 8** provides recommendations and conclusions drawn from the threat analysis.

The detailed vulnerabilities, emerging security requirements, corresponding threat groups exploring them, and mitigation controls are presented in the Annexes. The material used in the analysis produced for this report, which is referenced in footnotes through URLs, was last accessed on the day of publication of this study. The referenced material will help interested readers to dive into further detail in the complexity of the 5G infrastructure when needed.

2. 5G STAKEHOLDERS

2.1 STAKEHOLDERS MAPPING

The stakeholders of the 5G ecosystem have not considerably changed since the previous edition of the 5G Threat Landscape. However, by going into some additional details, one could amend the list of stakeholders to include some additional ones that will have a role in the 5G ecosystem, firstly due to the inclusion of processes in the scope, and secondly by reaching a degree of detail that may potentially motivate other stakeholders to take action in 5G.

Stakeholders will play different roles in the 5G ecosystem. Among other things, these entities will be responsible for assuring the security of the network at different levels and in separate layers. According to the 5G-PPP White Paper on the architecture,[10] the list of stakeholder roles in the 5G ecosystem is the following:

- *Service customers (SC)*;
- *Service providers (SP)*;
- *Mobile Network Operators (MNO) also known as Network Operators (NOP)*;
- *Virtualisation Infrastructure Service Providers (VISP)* and
- *Data Centre Providers (DCSP)*.

In the meantime, 5GPPP has issued a very comprehensive and detailed collection of 5G stakeholders. The graph can be found here[11]. The provided stakeholder groups and the detail list of organisation types provide the full picture of entities engaging in the 5G ecosystem, including private, governmental and international organisations.

The major stakeholder roles remained the same as in the previous 5G Threat Landscape edition. These were:

- *Network infrastructure providers*;
- *National Regulators (NRAs)*;
- *Information sharing and analysis centres (ISACs)*;
- *National cybersecurity coordinators/agencies/centres (NCSCs)*;
- *National 5G Test Centres (NTCs)*;
- *National Certification Authorities (NCAs)* and
- *Competent EU institutions, European Commission Services, Agencies, Bodies, Committees and Groups (including NIS-CG, ECCG, ECSO, ENISA and BEREC)*.

Interested readers that would like to revisit the role of the above stakeholders in the 5G ecosystem, may revisit the previous 5G Threat Landscape edition[8].

Some additional roles encountered in the collected material are worth mentioning at this point. The importance of these roles has emerged through a better understanding of 5G implementation and roll-out details on the one hand, but also from additional operational and organisational needs w.r.t. 5G in shorter and longer term. These roles are:

- *International standardisation bodies* holding an obvious role in the development of open, publicly available and traceable 5G standards;

[10] https://5g-ppp.eu/wp-content/uploads/2020/02/5G-PPP-5G-Architecture-White-Paper_final.pdf, accessed October 2020.
[11] https://5g-ppp.eu/revised-5g-ppp-stakeholders-picture-and-glossary/, accessed October 2020.

- *Accreditation bodies* will be active in the assurance of security capabilities/requirements of accredited entities (e.g. 5G test-labs, auditors, skills, etc.);
- *Accredited 5G labs* taking over testing and certification of 5G related components;
- *Telco/5G related professional organisations/associations* developing good practices for 5G cybersecurity policies at technical and organisational level;
- *Audit organizations* developing audit-guidelines for 5G infrastructures, services and operation;
- *Research organisations* contributing to R&D tasks related with all kinds of innovation actions in the areas related to 5G, including verticals and
- *Open source organisations* providing technological support and guidance in the development of 5G functions and services.

When assuming these roles, the entities mentioned above should have different levels of concern regarding 5G assets, among other things carrying responsibility for the risk mitigation pertinent to the assets of concern. Although all above stakeholders do play a role in the 5G ecosystem, their engagement emerges on a rather ad-hoc manner in current 5G activities. When a more systematic description of activity-engagement is available, a more systematic role mapping will be beneficial for a clearer assignment of responsibilities and a better coordination of their actions.

3. 5G NETWORK DESIGN AND ARCHITECTURE

This chapter is an update of the 5G Architecture of the 2019 5G Threat Landscape report[12]. Main source of the changes of the 5G architecture is progress made in the 3GPP specification work as it is documented in the recent version (3GPP Release 16).

Just as in the 2019's landscape, this chapter consists of a generic 5G architecture and provides the details of individual key components by means of 'Zoom-ins', allowing further detailing of their functionality and purpose. By doing so - besides the generic 5G architecture depicted - a number of detailed views of particular components is being presented, namely: Core Network, Management and Network Orchestrator (MANO), Radio Access Network (RAN), Network Function Virtualisation (NFV), Software Defined Network (SDN), Multi-access Edge Computing (MEC), User Equipment (UE), Security Architecture (SA) and 5G Physical Infrastructure components. These zoom-ins have been adopted from the previous version of the 5G Threat Landscape and have been updated according to the progress of the specification work.

In this year's version, some additional zoom-ins have been developed, in particular a zoom-in dedicated to implementation options and a zoom-in on processes. These zoom-ins capture some additional elements adopted/developed during 2020 that capture i) the migration options of 5G infrastructure and ii) a process map with the relevant processes for the procurement, development and maintenance of 5G infrastructure. In contrast to the rest of the presented zoom-ins, the process map consists solely of various processes. We have included this zoom-in in the 5G architecture in order to ensure a unified way of addressing vulnerabilities and threats for pertinent to matters related to processes.

An additional element introduced for each zoom-in are two sections, one describing the novelties established in 2020, and a second presenting security considerations related to components of each zoom-in. While the former provides a summary of the performed changes, the latter establishes a "bridge" to the vulnerabilities chapter (see chapter 4).

Not all components of 5G architecture have undergone changes. For the sake of completeness, however, unchanged components of the previous 5G Threat Landscape version are repeated in this document. They are amended with the introduced changes (marked with blue text). This redundancy has been introduced in order to make the presented content self-contained and facilitate reading.

Just as in the 5G Threat Landscape of 2019, in order to deal with complexity both at the level of the generic 5G architecture and individual zoom-ins, the details of the various interfaces and protocols have not been considered. A short description of the purpose and functionality is provided in a separate table for each individual component. A generic 5G architecture and the corresponding zoom-ins facilitate the identification of assets presented in chapter 5.

[12] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks, accessed October 2020.

3.1 5G USE CASES

The 5G architecture supports the various use-cases of this infrastructure, as these have been envisaged in the 3GPP specification. An understanding of these use-cases provides the context of use for various supported functions and architectural decisions met within the 3GPP group.

The new release 16 introduces new concepts and changes to the technical specifications of 5G mobile networks. The work of the various 3GPP working groups resulted in the completion of the 5G NR specifications for standalone (SA) mode. An important feature of this release is to leverage the LTE core network to support the expansion of the 5G Network. The release 16 is all about incrementing enhancements for mobile broadband in various requirements such as coverage, latency, capacity, mobility, power, reliability, ease of deployment, among others. Another core improvement with release 16 is the support to new use cases.

This has led to an enrichment of use-cases. While the previous edition of the 5G specification envisaged the use cases: i) Enhanced mobile broadband (eMBB), ii) Ultra-reliable low latency communication (URLLC) and iii) Machine Type Communications (MTC), the current version enlarges significantly the scope by taking into account some verticals. The table below provides an overview of those verticals.

Table 1: 5G Deployment Scenarios

Deployment Scenarios
Intelligent transportation systems (ITS) and vehicle-to-anything (V2X) communications
One example of a mission-critical use case is the transport system. The use of the 5G Network to enhance automotive safety is another focus area of release 16. It includes several enhancements in support to cellular-vehicle-to-everything (C-V2X) communications and intelligent transportation systems (ITS). The improvements in C-V2X specification include vehicle-to-vehicle (V2V), vehicle-to-pedestrian (V2P), and vehicle-to-infrastructure (V2I) communications. These are all required to increase transport safety in the current environment but also in the future implementation of autonomous driving. Intelligent transportation systems are another major vertical focus area in release 16. This vertical area will provide a wide range of transport and traffic-management use cases to the network.[13]
Industrial Internet of Things (IIoT) and ultra-reliable low latency communication (URLLC)
The IIOT is also a major vertical focus area of release 16. The introduction of 5G NR into IIoT use cases will enable the research and innovation of a future wirelessly connected and reconfigurable factory. It creates an opportunity to introduce IIoT to support factory automation, electrical power distribution and transportation. It introduces important enhancements in network latency and reliability. The support for time-sensitive networking (TSN) is also included in this release, where very accurate time synchronization is essential in factory automation use IIoT.
Integrated access and backhaul (IAB)
To expand 5G NR mmWave network coverage the cost of new fibre optics backhaul installations is typically high and a major challenge when deploying additional base stations. Release 16 eliminates the need for this wired backhaul, since it introduces integrated access allowing a base station to provide both wireless access for devices and wireless backhaul connectivity.
NR-Based access to unlicensed spectrum (NR-U)
Release 16 allows 5G Networks to operate in unlicensed spectrum that is the largest available. The existing global 5 GHz and 6 GHz unlicensed band is used by Wi-Fi and LTE LAA and is attractive use case for increasing data rates and capacity to the network. The specifications define two operation modes: NR-U with an anchor in licensed-assisted (shared spectrum) and standalone NR-U with only unlicensed spectrum.

[13] https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-nr-evolution, accessed October 2020.

Besides these verticals, the new specification adds more than 20 standard technological features, including a series of improvements for enhanced mobile broadband (eMBB) and further vertical applications. These eMBB improvements cover Massive MIMO, cell interruption-free handover, and remote interference suppression. Moreover, introduced additional improvements may be considered as enablers that will enhance the efficiency of 5G for a series of further applications. The table below provides a summary of those improvements/features.

Table 2: Additional 5G enabling features for all verticals

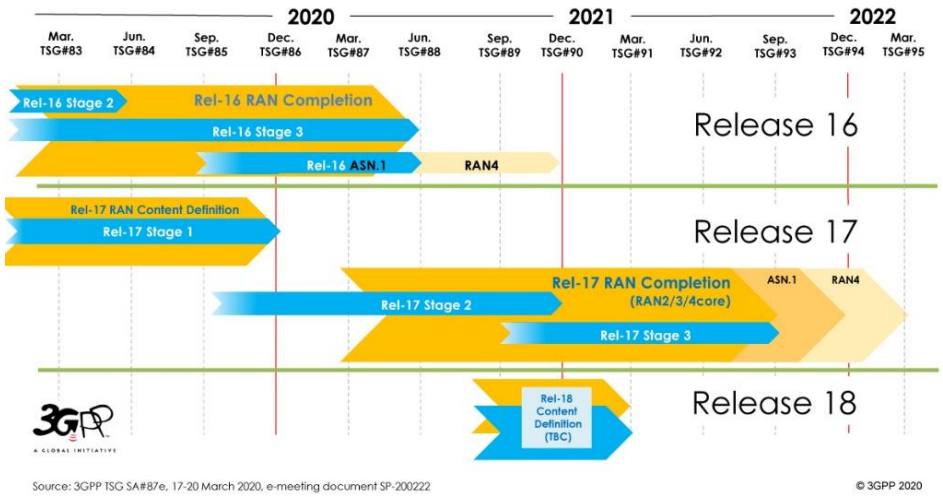
5G EFFICIENCY
Important enhancements in release 16 features can be found in the areas of multiple-input, multiple-output (MIMO) and beamforming enhancements, dynamic spectrum sharing (DSS), dual connectivity (DC) and carrier aggregation (CA), positioning and user equipment (UE) power saving. The most relevant 5G efficiency improvements are as follows:
Interference mitigation
Release 16 introduces Remote Interference Mitigation (RIM) and Cross-Link Interference (CLI) features. Base stations can communicate and coordinate (Via reference signals (RIM-RS) over-the-air or in combination with backhaul signalling) mitigation of base station TDD DL-to-UL ducting interferences (to indicate the presence of interference and whether enough mitigation is in place). With CLI, devices can measure and report inter-/intra-cell interferences (Inter-cell: when devices have semi-static TDD scheduling, Intra-cell: when devices support dynamic TDD) caused by neighbouring devices with different TDD configurations.
MIMO Performance
Release 16 introduces MIMO enhancements including: • enhanced beam handling; • channel-state information (CSI) feedback; • support for transmission to a single UE from multiple transmission points (multi-TRP) • full-power transmission from multiple UE antennas in the uplink (UL). Some of these enhancements are meant to increase the throughput of the network, reduce overhead, and/or provide additional robustness.
High-precision positioning
With an increase in the number of use cases and applications requiring accurate outdoor and indoor positioning, release 16 introduces various DL-based and UL-based positioning methods, to meet the accuracy requirements for different use cases. The way it is operated, the network location server collects and distributes information related to positioning of the user device (UE capabilities, assistance data, measurements, position estimates, etc.) to the other entities involved in the positioning procedures. Single and multi-cell positioning also brings precision geolocation in support of ITS/V2X communications and IIoT applications (see use cases).
Power consumption
Another important aspect of release 16 is to further reduce device power consumption in user devices. For example, the use of a wakeup signal (WUS), a low-power control channel to indicate activity or lack thereof in the corresponding DRX (discontinuous reception) monitoring period. Others examples include optimized low-power settings, efficient power controls, and overhead reduction, and more efficient power control mechanisms. Smart new power-saving features help improve device battery autonomy even in high-use applications[14].
Dual connectivity and carrier aggregation (CA/DC)
Release 16 also reduces latency for CA/DC setup and activation to achieving higher data rates. In this case, connectivity can be resumed after periods of inactivity. Furthermore, release 16 also introduces a triggering of CSI reference signal transmissions in case of the aggregation of carriers with different numerology.

[14] https://www.qualcomm.com/news/onq/2020/07/07/propelling-5g-forward-closer-look-3gpp-release-16?, accessed October 2020.

Mobility enhancements
Reduced interruption time 0ms handover enabled by dual active protocol stack with concurrent source/target cell transmissions/reception. Improved mobility robustness Device-driven conditional handover for single and dual connectivity, and fast handover failure recovery. • Sub-7 GHz and mmWave; • Both inter- and intra-frequency handovers; • Beneficial to high-mobility use cases (e.g., train, aerial).
Enhanced ultra-reliable, low-latency communication (eURLLC)
An important Work Item in Release 16 was aimed at enhancing support for ultra-high reliability and low-latency communications. The main features introduced by this work item include enhancements in the 5G Core network mechanisms, physical layer enhancements for 5G New Radio and support of New Radio Industrial Internet of Things Mechanisms to increase reliability include a redundant transmission mechanism, enhanced QoS monitoring and RAN support for higher layer multi-connectivity[15]. Mechanisms to reduce latency and to guarantee session continuity were also introduced in the 5G Core functions and supported by enhancements in the physical layer specification of the 5G New Radio. Finally, enhancements aimed specifically at industrial IoT scenarios include accurate reference timing delivery, scheduling enhancements and improved handling of Time Sensitive Communication data.
Self-Organised Network (SON)
Release 16 enhances SON with the concept of mobility robust optimization (MRO), mobility load balancing (MLB), and RACH optimization. Specifying device reporting needed to enhance network configurations and inter-node information exchange (e.g., enhancements to interfaces like N2, and Xn).

Concluding this section, we would like to present the planned evolution of 5G 3GPP specification. 5G specifications are in continuous development by the 3rd Generation Partnership Project (3GPP). Since last year's report, the current 5G specification is Release 16, which reached specification freeze in July 2020, with items related to Radio Access Network due for finalisation in December 2020. The timeline of specification development is presented below[16]:

Figure 2: Timeline of 3GPP specification versions



It is considered as meaningful to plan prospective versions of the 5G Threat Landscape in order to accommodate updates introduced by newer versions of the specification (e.g. end of 2021, covering Release 17 Stage One, and end 2022 covering Release 17 Stage Two).

[15] 3GPP TR 21.916 V0.5.0 (2020-07) Technical Report 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Release 16 Description; Summary of Rel-16 Work Items (Release 16) - https://www.3gpp.org/ftp/Specs/archive/21_series/21.916, accessed October 2020.
[16] https://www.3gpp.org/release-16, accessed October 2020.

3.2 GENERIC 5G ARCHITECTURE

In this section, we present the evolvement of the 5G architecture as resulted from the specification updates of 3GPP Release 16[27]. Within this chapter, the complete architecture is being presented, whereas novelties are marked through blue coloured text in the tables detailing the zoom-in components. Updates have been implemented either at the level of descriptions, or as new components introduced by the 3GPP specification Release 16. At the level of zoom-ins, a special section describes in more details the rational and functions behind the introduced novelties. A further section describes the security considerations relating to each zoom-in.

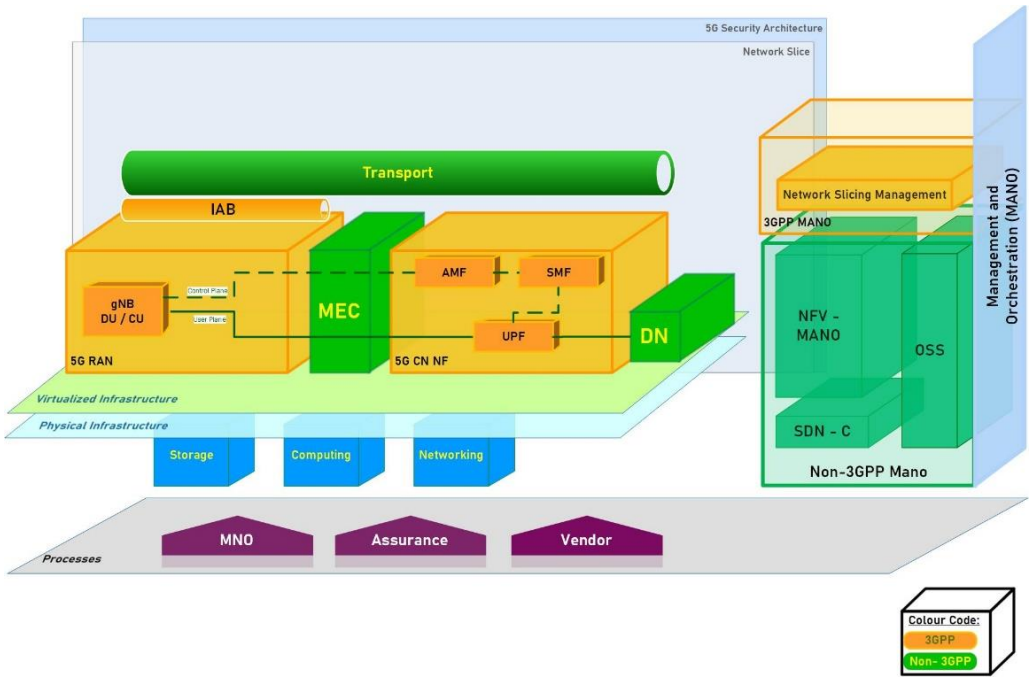
Just as in the previous version of the 5G TL, the generic 5G architecture is presented through its main components depicted as labelled boxes. These boxes have been arranged based on layers, depicting their functional role in the 5G architecture (i.e. virtualisation layer and physical infrastructure layer). This architecture aims at providing an overview of the main groups of foreseen 5G functionality and is a consolidation of components/functions found in the analysed material (e.g. 14, 19, 24, 25, 26, 27, 28).

Specifically in 5G, the architecture was designed in a way that connectivity and services can be supported, enabling techniques such as Network Function Virtualisation (NFV), Network Slicing (NS) and Software Defined Networking (SDN), Slicing, etc. This service-based architecture meets multiple functional and performance requirements built upon new use cases.

The generic 5G architecture presents an overview of the various components that are further detailed and depicted through specific 'Zoom-ins' in forthcoming sections. It is worth mentioning that for the Transport and OSS components, no 'Zoom-in' was developed. However, they have been included in the generic 5G architecture for consistency reasons, and relations with OSS are detailed in the corresponding zoom-ins for NVF and Network Slicing Management.

Also, as an evolution from the first version of the architecture, in this version relevant processes are taken into account, as MNO, Vendor and Assurance processes are consequential for the overall security of the 5G Network. The 5G generic or high-level technical architecture is depicted in the following figure.

Figure 3: Generic 5G Architecture

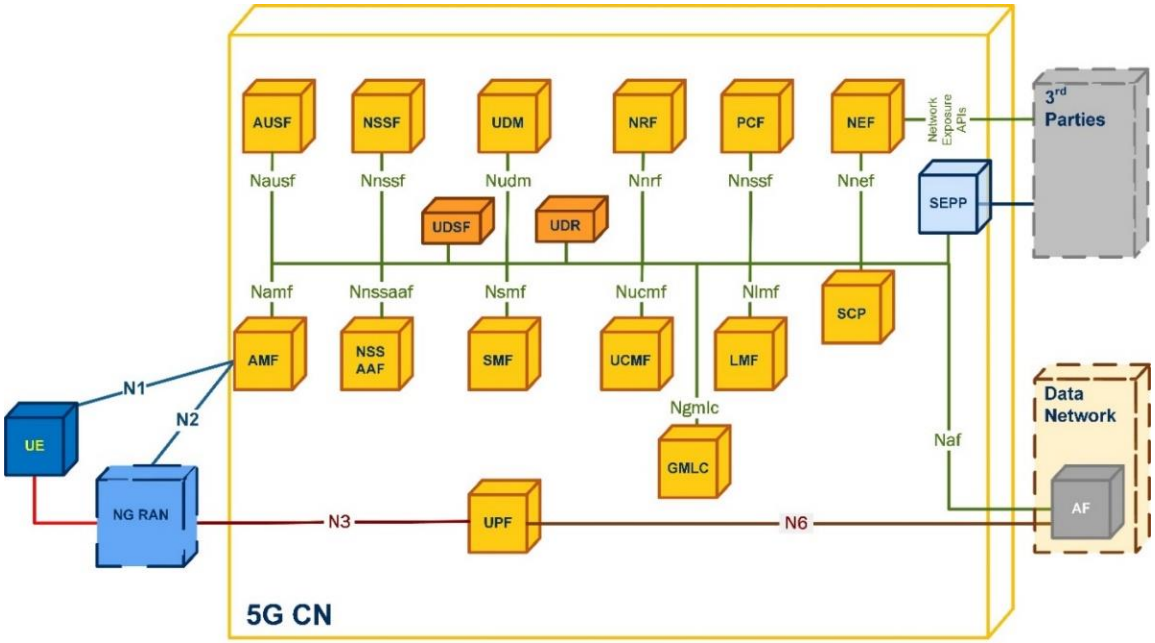


3.3 CORE NETWORK ARCHITECTURE (ZOOM-IN)

One of the most important innovations in the 5G architecture is the complete virtualisation of the Core network. As an example, the 'softwarisation' of network functions will enable easier portability and higher flexibility of networking systems and services (Control-User Plane Separation, CUPS). The Software Defined Network (SDN) abstracts low-level network functionalities to simplify network management. Network Function Virtualisation (NFV) provides the enabling technology for placing various network functions in different network components on the basis of performance needs/requirements; and eliminates the need for function-or service-specific hardware. SDN and NFV, complementing each other, improve the network elasticity, simplify network control and management, break the barrier of vendor-specific or proprietary solutions, and are thus considered as highly important for future networks. These novel network technologies and concepts that rely heavily on 'softwarisation' and virtualisation of network functions will introduce new and complex threats. The core network is the central part of the 5G infrastructure and enables all functions related to multi-access technologies. Its main purpose is to deliver services over all kinds of networks (wireless, fixed, converged) .

All in all, in the new specification Core Network has been amended with some new functions and few components, while the overall structure remained almost unchanged. The majority of added functions are related to localization issues and implementation of location services. In the figure presented below, these new functions have been added. At the same time, slicing has been omitted in the Core Network zoom-in, as it is included in a specialized zoom-in later in this chapter. The Core network has been defined by 3GPP and its structure is as follows:

Figure 4: Core network architecture Zoom-in



The description of the elements of 5G Core network are as follows:

Element	Short description
Access and Mobility Management function (AMF)	(As defined in 3GPP TS23.501 Section 6.2.1[17]) AMF may include the following functionalities: ▪ Termination of RAN CP interface; ▪ Termination of NAS, NAS ciphering and integrity protection; ▪ Registration management; ▪ Connection management; ▪ Reachability management; ▪ Mobility Management;Provide transport for SM messages between UE and SMF; ▪ Transparent proxy for routing SM messages; ▪ Access Authentication; ▪ Access Authorisation. ▪ Provide transport for SMS messages between UE and SMSF; ▪ Security Anchor Functionality; ▪ Location Services management for regulatory services; ▪ Provide transport for Location Services messages between UE and LMF as well as between RAN and LMF; ▪ EPS Bearer ID allocation for interworking with EPS; UE mobility event notification; ▪ Support for Control / User Plane Cellular IoT (CIoT) optimisation; ▪ Support for Network Slice Specific Authentication and Authorisation.
Session Management function (SMF)	(As defined in 3GPP TS23.501 section 6.2.2) SMF may include the following functionalities: ▪ Session Management; UE IP address allocation & management (DHCPv4 and v6 (server and client) functions); ▪ Respond to Address Resolution Protocol (ARP) requests and / or IPv6 Neighbour Solicitation requests; ▪ Selection and control of UP function, including controlling the UPF to proxy ARP or IPv6 Neighbour Discovery; ▪ Selection and control of UP function; ▪ Configures traffic steering at UPF to route traffic to proper destination; ▪ Termination of interfaces towards Policy control functions;Charging data collection and support of charging interfaces; ▪ Control and coordination of charging data collection at UPF; ▪ Termination of Session Management parts of NAS messages; ▪ Downlink Data Notification; ▪ Determine Session and Service Continuity mode of a session. ▪ Support for Control Plane CIoT Optimisation ▪ Support of header compression; ▪ Provisioning of external parameters (Expected UE Behaviour parameters or Network Configuration parameters); ▪ Support Proxy-CSCF discovery for IP Multimedia Subsystem (IMS) services; ▪ Roaming functionality; ▪ Handle local enforcement to apply QoS SLAs (VPLMN); ▪ Charging data collection and charging interface (VPLMN); ▪ Lawful intercept (in VPLMN for SM events and interface to LI System); ▪ Support for interaction with external DN for transport of signalling for PDU Session authentication/authorisation by external DN; ▪ Instructs UPF and NG-RAN to perform redundant transmission on N3/N9 interfaces. (NOTE: Not all of the functionalities are required to be supported in an instance of a Network Slice. In addition to the functionalities of the SMF described above, the SMF may include policy related functionalities as described in clause 6.2.2 in TS 23.503[18])

[17] 3GPP TS 23.501 V16.6.0 (2020-09) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2 (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip ,accessed October 2020.
[18] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3334, accessed October 2020.

User plane function (UPF)	UPF supports: ▪ Packet routing & forwarding; ▪ Packet inspection; ▪ QoS handling; ▪ Lawful intercept (UP collection); ▪ Traffic usage reporting; ▪ It acts as external PDU session point of interconnect to Data Network (DN); ▪ Is an anchor point for intra- & inter-RAT mobility; ▪ Functionality to respond to Address Resolution Protocol (ARP) requests and / or IPv6 Neighbour Solicitation requests based on local cache information for the Ethernet PDUs; ▪ Time sensitive Networking (TSN) Translator functionality; ▪ High latency communication, see clause; ▪ Access Traffic Steering, Switching and Splitting (ATSSS) functionality to steer the Multi Access PDU Session traffic; ▪ Inter PLMN UP Security (IPUPS) functionality.
Policy Control Function (PCF)	PCF supports: ▪ Unified policy framework; ▪ Policy rules to CP functions and ▪ Access subscription information for policy decisions in UDR.
Network Exposure Function (NEF)	NEF supports: ▪ Exposure of capabilities and events; ▪ Secure provision of information from external application to 3GPP network; ▪ Translation of internal/external information; ▪ NEF may also support a 5GLAN Group Management Function: The 5GLAN Group Management Function in the NEF may store the 5GLAN group information in the UDR via UDM as described in TS 23.502[19]; ▪ Exposure of analytics; ▪ Support of Non-IP Data Delivery; ▪ When UE is capable of switching between EPC and 5GC, an SCEF+NEF is used for service exposure.
Network Repository Function (NRF)	NRF supports service discovery function and maintains NF profile and available NF instances. ▪ Supports Proxy-CSCF discovery for IP Multimedia Subsystem (IMS) services; ▪ Supports Service Communication Proxy (SCP) discovery, and maintains SCP profile of available SCP instances; ▪ Notifies about registered/updated/ deregistered NF and SCP instances, and maintains the health status of NFs and SCP.
Unified Data Management (UDM)	UDM supports: ▪ Generation of Authentication and Key Agreement (AKA) credentials; ▪ User identification handling; ▪ Access authorisation; ▪ Subscription management; ▪ 5GLAN group management handling; ▪ Support of external parameter provisioning.
Authentication Server Function (AUSF)	AUF supports authentication for 3GPP access and untrusted non-3GPP access.
Application Function (AF)	AF interacts with the Core network in order to provide services, for example to support the following: ▪ Application influence on traffic routing; ▪ Accessing Network Exposure Function; ▪ Interacting with the Policy framework for policy control. ▪ Interactions of the IP Multimedia Subsystem (IMS) with the 5G Core

[19] 3GPP TS 23.502 V16.6.0 (2020-09) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS); Stage 2 (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.

Unified Data Repository (UDR)	UDR supports the following functionality: ▪ Storage and retrieval of subscription data by the UDM; ▪ Storage and retrieval of policy data by the PCF; ▪ Storage and retrieval of structured data for exposure; ▪ Application data (including Packet Flow Descriptions (PFDs) for application detection; ▪ AF request information for multiple UEs), by the NEF. (See also 3GPP TS23.501 section 6.2.11) ▪ Storage and retrieval of NF Group ID corresponding to subscriber identifier (e.g. IMPI, IMPU, SUPI);
Unstructured Data Storage Function (UDSF)	The UDSF is an optional function that supports Storage and retrieval of information as unstructured data by any NF.
Network Slice Selection Function (NSSF)	The NSSF offers services to the AMF and NSSF in a different PLMN via the Nnssf service based interface (see 3GPP TS 23.501and 3GPP TS 23.502).
Gateway Mobile Location Centre (GMLC)[20]	The GMLC contains functionality required to support Location Services (LCS). In one PLMN, there may be more than one GMLC. A GMLC is the first node an external LCS client accesses in a PLMN. AFs and NFs may access GMLC directly or via NEF. After performing authorisation of an external LCS Client or AF and verifying target UE privacy, a GMLC forwards a location request to either a serving AMF or to a GMLC in another PLMN in the case of a roaming UE.
Localisation Management Function (LMF)	The LMF manages the overall co-ordination and scheduling of resources required for the location of a UE that is registered with or accessing 5GCN. It also calculates or verifies a final location and any velocity estimate and may estimate the achieved accuracy. The LMF receives location requests for a target UE from the serving AMF using the Nlmf interface. The LMF interacts with the UE in order to exchange location information applicable to UE assisted and UE based position methods and interacts with the NG-RAN, N3IWF or TNAN in order to obtain location information.
Service Communication Proxy (SCP)	An NF service is one type of capability exposed by an NF (NF Service Producer) to other authorized NF (NF Service Consumer) through a service-based interface NF services may communicate directly, or indirectly via an SCP. As defined in 3GPP TS 23.501, Clause 6.2.19, the Service Communication Proxy (SCP) includes one or more of the following functionalities: ▪ Indirect Communication; ▪ Delegated Discovery; ▪ Message forwarding and routing to destination NF/NF service; ▪ Message forwarding and routing to a next hop SCP; ▪ Communication security (e.g. authorisation of the NF Service Consumer to access the NF Service Producer API), load balancing, monitoring, overload control, etc.
UE radio Capability Management Function (UCMF)	The UCMF is used for storage of dictionary entries corresponding to either PLMN-assigned or Manufacturer-assigned UE Radio Capability IDs. An AMF may subscribe with the UCMF to obtain from the UCMF new values of UE Radio Capability ID that the UCMF assigns for the purpose of caching them locally.
Network Slice Specific Authentication and Authorisation Function (NSSAAF)	The Network Slice Specific Authentication and Authorisation Function (NSSAAF) offers support for Network Slice-Specific Authentication and Authorisation as specified in TS 23.502 with an Authentication, Authorisation and Access Server (AAA-S).
Nausf, Nnrf, Nudm, Nnef, Namf, Nmssf, Nsmf, Npcf, Naf, Nlmf, Ngmlc, Nssaaf, Nucmf	These are service-based interfaces exhibited by 5G Core Control-plane functions.
N1	Reference point between the UE and the AMF.
N2	Reference point between the RAN and the AMF.
N3	Reference point between the RAN and the UPF.
N6	Reference point between the UPF and a Data Network.

[20] 3GPP TS 23.273 V16.4.0 (2020-07) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 5G System (5GS) Location Services (LCS); Stage 2 (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.

3.3.1 ELEMENTS OF NOVELTY IN RELEASE 16

The new features and enhancements brought by release 16 of the GPP specification, presented in the section Generic Architecture are reflected in updates and additions to the 5G Core functions, as highlighted in the detailed table above. The most important enhancements and their impact on the 5G Core are presented below:

New functions are added to the 5G Core toolset, to support Network-Slice Specific Authentication (NSSAAF), Location Services (GMLC), and enhancements to existing functions' specification support use-cases such as cellular IoT Support, Ultra-reliable low latency architecture, 5G LAN services, Time Sensitive Networking for Industrial IoT, Vehicle to everything.

A significant enhancement for the Service Based Architecture is the enablement of indirect communication and delegated discovery through the Service Communication Proxy. This increases flexibility, allowing communication between Network Functions via Network Repository Function (NRF) and Service Communication Proxy (SCP).

Enhancements in the network analytics exposure features is an important enabler for Network Automation in the 5G system.

Another feature provided is Radio Capabilities Signalling (RACS) Optimization via optimized signalling of UE Radio capabilities by introducing mapping of RACS ID to UE Radio Capability in the network. The mapping between RACS ID to UE Radio capabilities will be stored in the new Network Function UE (radio) Capability Management Function (UCMF) and cached in the AMF and gNB.

The network slicing function is improved beyond network-slice specific authentication with enhanced SMF/AMF topologies and with interworking support with the Evolved Packet System, in view of the Non Standalone (NSA) deployments.

3.3.2 SECURITY CONSIDERATIONS

The specification of 5G Core network functions were developed as to close known vulnerabilities in existing network. The effort is ongoing; for instance, the most recent version of the 5G architecture specification[21] further enhances the closing of a known User Plane Integrity Protection vulnerability, by adding new requirements for the UE to support User Plane Integrity Protection at full-rate. . The full set of security mechanisms in the 5G system is presented in the Security Architecture section.

However, the 5G core functions rely on an underlying infrastructure of hardware, software and processes that come with their security threats and vulnerabilities. In the NFV and SDN zoom-ins we will address the relevant security considerations related to virtualisation, softwarisation and associated management and orchestration mechanisms. In the Processes map section, we discuss the relevant security considerations.

Apart from these, the following general security considerations apply:

Service-based architecture

The 5G Core functions is meant to be largely composed of applications running on general-purpose hardware that communicate through application programming interfaces (APIs). The

[21] 3GPP TS 23.501 V16.6.0 (2020-09) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2 (Release 16), https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-g60.zip, accessed October 2020.

integrity of the software, especially from open-source locations and the overall software supply chain, is an area of vulnerability. As services can be created, destroyed, and communicate with each other dynamically, systems must be properly authenticated and communications protected in order to prevent unauthorized execution of functions or access to data[22].

Affected components: Service-based interfaces

Failure to meet General Security Assurance Requirements

The security assured by the 5G Core functions and the security of the 5G Core itself is built upon the permanent update of Security Assurance Requirements for critical network components such as UDM, AUSF, SEPP, NRF, NEF, SMF, AMF and UPF.

However, a security update gap between new security requirements and deployment of updated versions of network functions in operational systems will unavoidably exist. There are two major factors in reducing this gap: a) vendors' responsiveness in issuing and validating new versions of the network functions that address the updated requirements, and b) timeliness and effectiveness of MNO processes to update operational systems to recently released and SCAS-evaluated versions.

Affected components: UDM, AUSF, SEPP, NRF, NEF, SMF, AMF, UPF.

IP Based Protocol stack

5GC moves to an IP based protocol stack, allowing interoperability with a wider number of services and technologies in the future. The following protocols, schemas and processes will be adopted in 5GC:

- HTTP/2 and JSON as application layer and serialization protocols, replacing Diameter over the S6a reference point
- TLS as an additional layer of protection providing encrypted communication between all network functions (NF) inside a public land mobile network (PLMN)
- TCP as the transport layer protocol
- RESTful framework with OpenAPI 3.0.3 as the Interface Definition Language (IDL).

As these protocols are used in the wider IT industry it will likely lead to a shorter vulnerability to exploitation timeline, and higher impact of vulnerabilities within these protocols. Vulnerability reporting schemes will have to manage the increased scope of these protocols. Once located the time to patch for vulnerabilities should be short.

Affected components: All functions

3.4 NETWORK SLICING (NS) (ZOOM-IN)

One of 5G's key features will be the opportunity for network slicing23: enables the flexible and efficient creation of specialized end-to-end logical networks on top of shared network infrastructure. Network slicing belongs to the category of virtualization networking paradigm, together with Software-Defined Networking (SDN) and Network Function Virtualization (NFV).

[22] Security considerations for the 5G era, 5G Americas, July 2020, https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf accessed October 2020.
[23] https://www.sdxcentral.com/5g/definitions/5g-network-slicing/, accessed October 2020.

Network slicing can take advantage of SDN and NFV, but it can be seen as an independent technology24.

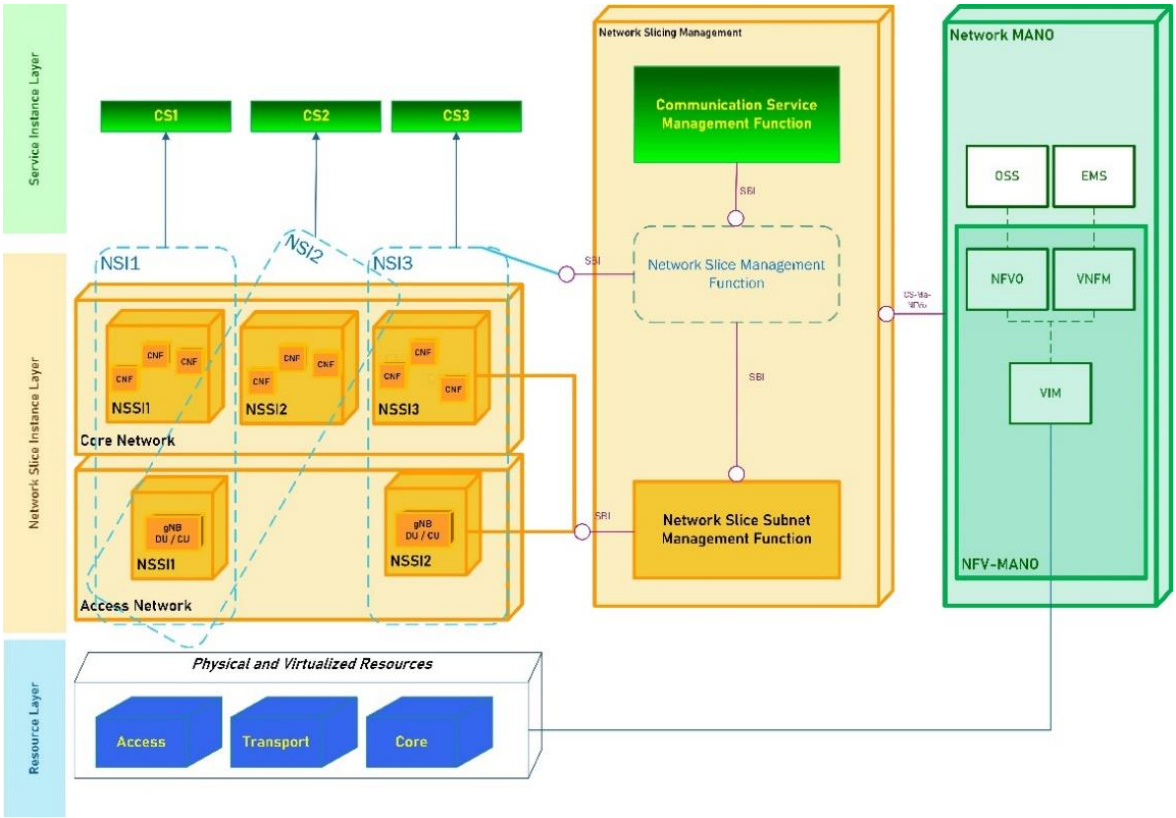
5G system is expected to be able to provide optimized support for a variety of different communication services, different traffic loads, and different end user communities[25]. A clear benefit of 5G network slicing for operators will be the ability to tailor the functionalities and allocation of network resources to specific customers and particular market segments.

In this update of the 5G architecture, we include in this zoom-in all interrelated slicing functions that are located within the scope of other zoom-ins. This decision has been made in order to have in a single picture all relevant slicing components and functions, providing thus an integrated view.

Communication between autonomous cars, for instance, requires minimal latency (the lag time it takes for a signal to travel), but not necessarily high throughput (the amount of data a network can process per second) while a use-case such as augmented reality will require more bandwidth.

Network Slicing components are presented in relation to the impacted elements of the network architecture, as depicted in the various 'Zoom-ins'. This cross-reference/mapping is an alternative means for describing slice functions of 5G. The dependency of slices with the various components of the 5G generic architecture is shown in the figure below:

Figure 5: Network slicing architecture Zoom-in



[24] R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in IEEE Access, vol. 8, pp. 99999-100009, 2020, doi: 10.1109/ACCESS.2020.2997702, accessed October 2020.
[25] 3GPP TS 28.530 V16.2.0 (2020-07) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Management and orchestration; Concepts, use cases and requirements (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.

The elements of the 3GPP Slicing Management System are as follows:

Element	Short description
Service Instance Layer (Communication Services)	The Service Instance Layer represents the services (end-user service or business services) which are to be supported. Each Communication Service is represented by a Service Instance. Typically services can be provided by the network operator or by 3rd parties. In line with this, a Service Instance can either represent an operator service or a 3rd party provided service.[26].
Communication Service Management Function (CSMF)	This function is responsible for translating the communication service related requirement to network slice related requirements. The CSMF communicates with the Network Slice Management Function (NSMF).
Network Slice Management Function (NSMF)	This function is responsible for the management (including lifecycle) of NSIs. It derives network slice subnet related requirements from the network slice related requirements. NSMF communicates with the NSSMF and the CSMF.
Network Slice Subnet Management Function (NSSMF)	This function is responsible for management and orchestration of Network Slice Subnet Instances.
Network Slice Instance (NSI)	The Network Slice is a logical network that provides specific network capabilities and network characteristics. The Network Slice Instance is a representation of a set of network functions and the associated resources (e.g. compute, storage and networking resources) supporting network slice.[27].
Network Slice Subnet Instance (NSSI)	The network slice subnet represents a group of network functions (including their corresponding resources) that form part or complete constituents of a network slice. The grouping of the network functions allows the management of each group of network functions to be conducted independently of the network slice.
Network Functions (NF) ***Core Network Functions (CNF)*** ***Access Network Functions (gNB)***	A network slice instance (NSI) contains Network Functions, including the Core Network Control Plane and User Plane Network Functions in the Home Network and the Access Functions in the serving network[28]. Release 16 of the 3GPP specification includes improved interworking with the LTE Evolved Packet Core (EPC).
NFV MANO	NFV MANO includes NFV Orchestrator (NFVO), VNF manager (VNFM) and Virtualised infrastructure manager (VIM).
Element Management System (EMS)	The Element Management is responsible for FCAPS management of network functions used in the network slice instance.
Operations Support System (OSS)	OSS functions provide management and orchestration of systems including legacy ones and may have full end-to-end visibility of services provided by legacy network functions in an operator's network.
Resources layer	Network functions will run as software components on top of hardware infrastructure. Virtualization enables an elastic, automated environment where network, compute and storage services can expand, or contract as needed. Many resources can now be hosted as software services and dynamically instantiated in different network segments.
Management Functions Service Based Interface (SBI)	The management of the 3GPP network is provided by management services. Management Services offer their services via standardized service interfaces composed of individually specified components.
Os-Ma-nfvo	The Os-Ma-nfvo reference point can be used for the interaction between 3GPP slicing related management functions and NFV-MANO. To properly interface with NFV-MANO, the NSMF and/or NSSMF consume the NFV MANO interface, exposed in the Os-Ma-nfvo , Ve-Vnfm-em and Ve-Vnfm-vnf reference points (last two not displayed in the Figure due to graphical limitations).

[26] 3GPP TR 23.799 V14.0.0 (2016-12) Technical Report 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Architecture for Next Generation System (Release 14), accessed October 2020.
[27] 3GPP TS 23.501 V16.5.1 (2020-08), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2 (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.
[28] 3GPP TS 23.501 V16.5.1 (2020-08), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2 (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.

3.4.1 ELEMENTS OF NOVELTY

In release 16 of the 3GPP specification, the network slicing function is improved with the following features:

- Enhancement of interworking between LTE Evolved Packet Core (EPC) and 5G Core to manage mobility of User Equipment and its allocated Network Slice between networks
- A newly introduced Network Slice Specific Authentication and Authorisation (NSSAA) mechanism that enables separate authentication and authorisation per Network Slice. The trigger of NSSAA is based on subscription information from UDM and operator policy and may be performed when UE indicates support for the feature.[29]

3.4.2 SECURITY CONSIDERATIONS

Security-as-a-Service

Network slices are used to deploy services at the multi-access edge across a distributed cloud infrastructure. Network slices can be configured based upon the service-type (eMBB, mMTC, URLLC), customer, and application to provide the required latency, bandwidth, QoS, and security. While slices provide inherent security through segmentation, slices can also be used to provide additional security protection and security services specific to the use case and customer requirements.

However, although realisation of Security-as-a-Service (SECaaS) offerings is feasible technically, it would rest ultimately with the Mobile Network Operator (MNO) to include such services in the offer, depending on its service strategy, market context, and in relation to vertical use-cases.

Related component(s): Communication Services

End-to-end security

Network slices are end-to-end logical networks, so it is natural to aim for end-to-end security. The concept of end-to end security is closely connected to the concepts of isolation and orchestration. Moreover, it is dependent on the business model and on the associated trust model.[30]

Release 16 introduces the mechanism of Network Slice Specific Authorisation Identifier that enables network-slice-specific authentication and authorisation mechanisms to complement network-side authentication mechanisms.

Related component(s): Network Slice Instance

Resource isolation

One of key expectations of network slicing is resources isolation. Each slice may be perceived as isolated set of resources configured through the network environment and providing defined set of functions. Level and strength of isolation may vary depending on requirements and usage scenarios for slicing.[31]

[29] 3GPP TR 21.916 V0.5.0 (2020-07) 3rd Generation Partnership Project; Technical Specification Group Services and ystem Aspects; Release 16 Description; Summary of Rel-16 Work Items, (Release 16), https://www.3gpp.org/ftp/Specs/archive/21_series/21.916/, accessed October 2020.
[30] R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in IEEE Access, vol. 8, pp. 99999-100009, 2020, doi: 10.1109/ACCESS.2020.2997702, accessed October 2020.
[31] Z. Kotulski et al., "On end-to-end approach for slice isolation in 5G networks. Fundamental challenges," 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, 2017, pp. 783-792, doi: 10.15439/2017F228, accessed October 2020.

The isolation of the slices can be considered in at least four areas:

- Isolation of traffic: the network slices should ensure that data flow of one slice does not move to another.
- Isolation of bandwidth: slices should not utilize any bandwidth assigned to other slices.
- Isolation of processing: while all virtual slices use the same physical resources, independent processing of packets is required.
- Isolation of storage: data related to a slice should be stored separately from data used by another slice[32]

Related component(s): Network Slice Instance, Shared Resources

Secure Management and Orchestration

The architecture of the network slice MANO is challenging from a business model perspective because of the variety of scenarios with different actors, multi-domain environments, and several layers of imbricated tenants, which can play different roles and have different rights. Technically, this means high complexity and flexibility, which bring in higher security risks. 3GPP defines requirements for management services' security that include use of secure communication protocols for protection of interactions at the management service interfaces and authorisation of management service requests[33], but it is to be noted the most recent 3GPP specifications are yet to be implemented.

Another relevant issue is management of network-slice-specific log information to support post-incident analysis. Such information may include proof of transit, remote attestation, as well as data to support root cause analysis.

Related component(s): NSMF, NFV-MANO, Os-Ma-NFVO, SBI

Trust Model

In 5G three role models are envisaged for stakeholders.

1) The MNO owns and manages both the access and core network.
2) An MNO owns and manages the core network, the access network is shared among multiple operators (i.e., RAN sharing).
3) Only part of the network is owned and/or managed by the MNO, with other parts being owned and/or managed by a 3rd party.

The 3GPP appropriate APIs and management functions are needed to support this extended 3rd party access and control of capabilities provided by the MNO, and to do so in a secure manner. The 3rd party has increasing control over the network capabilities that support its service. However, this control is limited to what is allowed by the MNO through the provided APIs.[34]

Related component(s): SBIs, Os-Ma-nfvo

[32] Gutz, A Story, C Schlesinger, N Foster, inProc.1st Workshop on Hot Topicsin Software Defined Networks. Splendid isolation: a slice abstraction for software-defined networks, (2012), pp. 79–84.https://doi.org/10.1145/2X00000.342441.2342458, accessed October 2020.
[33] 3GPP TS 33.501 V16.3.0 (2020-07), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system, https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/, accessed October 2020.
[34] 3GPP TR 22.830 V16.1.0 (2018-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on Business Role Models for Network Slicing (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.

3.5 MANAGEMENT AND NETWORK ORCHESTRATOR (MANO) (ZOOM-IN)

Management and Network Orchestration (MANO) is not further maintained in the current version of the 5G architecture as a stand-alone zoom in. Rather, it has been integrated with the NFV zoom in. This is because the functions used for are covered completely in the NFV zoom-in (see section **Error! Reference source not found.**).

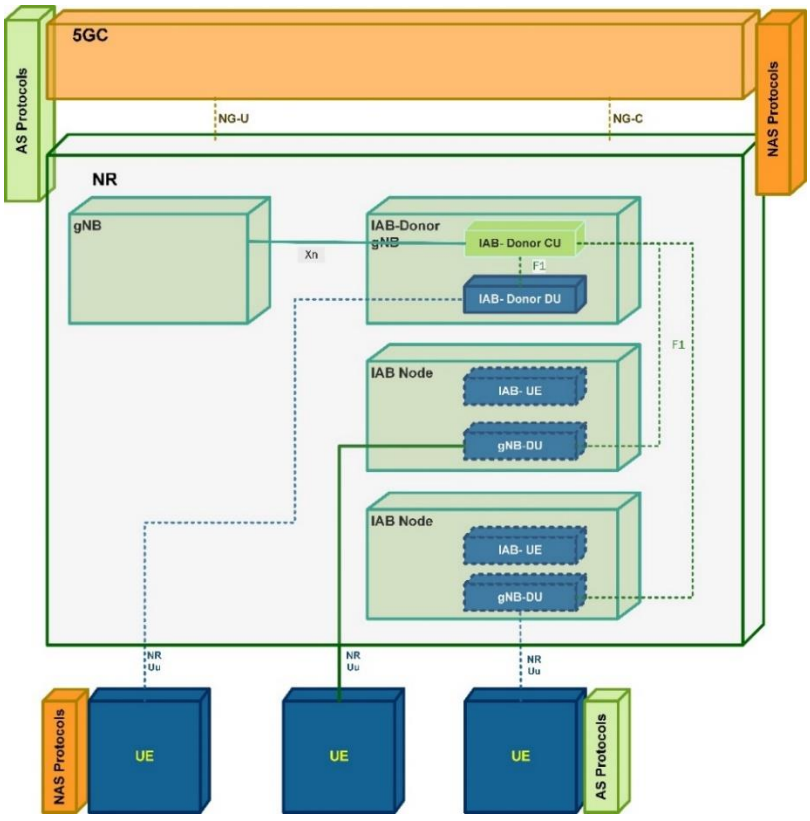
3.6 RADIO ACCESS NETWORK (RAN) (ZOOM-IN)

5G New Radio (NR) is the standard the 5G wireless air interface. 5G New Radio is set to deliver faster and more responsive mobile broadband services and to extend mobile technology to connect and support a multitude of new industries.

The baseline architecture described by 5G-PPP referring 3GPP Release 16 specifications on NG-RAN identifies as a main innovation the split of the F1 interface into Centralized Unit (CU) and Distributed Unit (DU), with a Service Data Adaptation Protocol (SDAP). The SDAP architecture includes a Packet Data Conversion Protocol (PDCP) located in the CU and an Air Radio Link Control (ARLC) located in the DU. Release 16 adds integrated access and backhaul (IAB) to the 5G toolkit. IAB allows base stations to provide both wireless access for devices and wireless backhaul connectivity, which can replace temporarily or permanently wired backhauls.

Another key aspect of the NG-RAN is the ability to provide small-cell coverage to multiple operators "as-a-service" in two-tier architecture. These tiers are in support of the previously mentioned 5G use cases providing low latency services and high processing power. The structure of the RAN architecture is depicted in the following figure[35]:

Figure 6: RAN architecture Zoom-in



[35] 3GPP TS 38.401 V16.2.0 (2020-07), Technical Specification 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NG-RAN; Architecture description (Release 16), https://www.3gpp.org/ftp/Specs/archive/38_series/38.401/, accessed October 2020.

The elements of the RAN architecture are as follows:

Element	Short description
User Equipment (UE)	Allows a user access to network services. The User Equipment is subdivided into the UICC domain and the ME (Mobile Equipment) Domain. The ME Domain can further be subdivided into one or more Mobile Termination (MT) and Terminal Equipment (TE) components showing the connectivity between multiple functional groups.
gNB	Next generation Node/Base Station is a node providing NR user plane and control plane protocol terminations towards the UE, and connected via the NG interface to the 5GC.
gNB Distributed Unit (gNB-DU)	gNB-DUa logical node hosting RLC, MAC and PHY layers of the gNB or en-gNB, and its operation is partly controlled by gNB-CU. One gNB-DU supports one or multiple cells. One cell is supported by only one gNB-DU. The gNB-DU terminates the F1 interface connected with the gNB-CU.
gNB Central Unit (gNB-CU)	gNB-Central Unit (CU) is a logical node hosting RRC, SDAP and PDCP protocols of the gNB or RRC and PDCP protocols of the en-gNB that controls the operation of one or more gNB-DUs. The gNB-CU terminates the F1 interface connected with the gNB-DU.
Xn	Xn is a network interface between NG-RAN nodes; 3GPP TS 38.420[36] specifies Xn interface general aspects and principles.
NG interface	The gNBs are connected by means of the NG interfaces to the 5G Core, more specifically to the AMF (Access and Mobility Management Function) by means of the NG-C interface and to the UPF (User Plane Function) by means of the NG-U interface.
NR Uu	The New Radio Unified Air Interface (NR-Uu) is the radio interface between the mobile and the radio access network.
IAB Donor	gNB that provides network access to UEs via a network of backhaul and access links[37].
IAB Node	RAN node that supports New Radio access links to UEs and New Radio backhaul links to parent nodes and child nodes. The IAB-node does not support backhauling via LTE.
Non Access Stratum (NAS)	NAS is a functional layer in the protocol stack between UE and Core Network. (NAS) protocol for 5G System (defined in 3GPP TS 24.501).
Access Stratum (AS)	AS is a functional layer in the protocol stack between UE and RAN responsible for transporting data over the wireless connection and managing radio resources.
F1	The F1 interface provides means for interconnecting a gNB-CU and a gNB-DU of a gNB within an NG-RAN, or for interconnecting a gNB-CU and a gNB-DU of an en-gNB within an E-UTRAN. It facilitates that a gNB-CU and a gNB-DU supplied by different manufacturers can work seamlessly[38].

3.6.1 ELEMENTS OF NOVELTY

While a significant part of the Release 16 enhancements involve the 5G-RAN to a certain extent, the following enhancements brought by Release 16 of the 3GPP specification are directly relevant for the 5G-RAN:

[36] 3GPP TS 38.420 V16.0.0 (2020-07), Technical Specification, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NG-RAN; Xn general aspects and principles (Release 16), https://www.3gpp.org/ftp/Specs/archive/38_series/38.420, accessed October 2020.
37 3GPP TS 38.300 V16.2.0 (2020-07), Technical Specification, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description; Stage 2 (Release 16), https://www.3gpp.org/ftp/Specs/archive/38_series/38.300/ , accessed October 2020
[38] 3GPP TS 38.470 V16.2.0 (2020-07) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NG-RAN; F1 general aspects and principles (Release 16), https://www.3gpp.org/ftp/Specs/archive/38_series/38.470, accessed October 2020.

Integrated access and backhaul (IAB)

One of the major 5G challenges for operators looking to expand network coverage is the cost of deploying base stations. The limited range of mmWave signals for fiber-optics backhaul installations to service these base stations can make mmWave deployment cost intensive. IAB addresses directly this issue. IAB base stations provide both wireless access for devices and wireless backhaul connectivity, thus eliminating the need for wired backhauls. Operators may resort to these capabilities to speed up densification, and install fiber to increase backhaul capacity at a later time, as demand increases.

Multiple-input and multiple-output (MIMO) enhancements

MIMO multiplies a radio link's capacity by using multiple transmission and multiple receiving antennas. Multi-user multiple-input and multiple-output (MU-MIMO) enhancements include support for multiple transmission and reception points (multi-TRP) and improved multi-beam management for enhanced link reliability. Improvements also aim at reducing peak-to-average power ratio, and improved coverage at the network's edge.

Simplified Random Access Procedure

Release 16 introduces a simplified random access procedure. This reduces the number of interactions between the UE and network during the connection setup and connection resume, thereby enabling a lower control plane latency. In case of connected mode, a small amount of data can be sent via 2-step RACH procedure thus also enabling a lower latency for UL UP data for connected mode UEs.

Private network support for NG-RAN

The second Release 16 project aimed at expanding 5G's reach beyond traditional public mobile networks involves improved support in the system architecture for private networks. Private networks utilize dedicated base stations that are independently managed, implement customized security and privacy controls, and deliver optimizations for local applications, such as low latency or data flow control. Private networks are directly aimed at new use cases such as industrial IoT.

UE Power Saving

UE battery life is an important aspect of the user's experience. The study of the Rel-16 UE power saving had shown substantial power saving gain comparing to considered Rel-15 NR features. The work item of UE power saving in NR includes the power saving techniques, such as DRX adaptation, cross-slot scheduling, and maximum MIMO layer adaptation in CONNECTED state, fast transition out of CONNECTED state, and reduced RRM (Radio Resource Management) measurements in idle/inactive states[39].

NR-Based Access to Unlicensed spectrum

To expand 5G's reach, 3GPP completed two projects in Release 16 that are key for new vertical use cases. One of them is 5G NR-U, that allows 5G to operate in unlicensed spectrum. It defines two operation modes, anchored NR-U requiring an anchor in licensed or shared spectrum and standalone NR-U that utilizes only unlicensed spectrum.

[39] 3GPP TR 21.916 V0.5.0 (2020-07) Technical Report 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Release 16 Description; Summary of Rel-16 Work Items (Release 16),https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip , accessed October 2020.

Time sensitive networking (TSN)

As part of the effort for 5G to support new Industry 4.0 use cases such as factory automation, 5G RAN Release 16 added support for TSN integration that can ensure time-deterministic delivery of data packets.

Precision geolocation

3GPP support location service features, to allow new and innovative location-based services to be developed. 5G specifications make possible to identify and report the current location of the user's terminal and to make the information available to the user, ME, network operator, service provider, value added service providers and for PLMN internal operations40 Enhancements in high-precision positioning brought by 5G NR Release 16, meet accuracy targets of 3 meters indoors and 10 meters outdoors.

3.6.2 SECURITY CONSIDERATIONS

In recent years, a large body of literature has revealed numerous security and privacy issues in 4G mobile networks. Most of the published attacks at the 4G RAN layer involve Rogue Base Stations (RBSs) or IMSI catchers to target individual user(s) during the UE's initial attach procedure to the network or paging attacks using the IMSI paging feature. In such attacks, the information obtained on IMSIs may be used later for other types of attacks[41].

5G NR technologies address and close known IMSI threats, but new functionalities in the Release 16 also bring security considerations that are subject to open studies:

Security of Ultra-Reliable Low-Latency Communication (URLLC)

URLLC needs to support both high reliability and low latency. In order to ensure the high reliability, redundant transmission in 5GS is supported on multiple user plane data paths. Accordingly, the applicable security mechanisms for supporting redundant transmission cover all aspect of the communication, including PDU session establishment, handover etc. As for the low latency aspect, the other important requirements for URLLC include QoS Monitoring to assist URLLC service and optimization for handover procedure. The security considerations in this case are covered as well. Additional security aspects are related to control plane and user plane optimizations for ensuring the high reliability and reducing latency[42].

Related components: gNB, interfaces: Uu, F1, Xn

Security of NR Integrated Access and Backhaul

A study is underway at 3GPP to identify potential security threats and vulnerabilities that are applicable to the new IAB architecture[43]. Key security issues include Topology Discovery and Masquerading, IAB Node Authentication to prevent connection of false IAB-node and manipulation of Radio Link Failure recovery and security of F1 interface.

[40] 3GPP TS 22.071 V16.0.0 (2020-07) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Location Services (LCS); Service description; Stage 1 (Release 16) https://www.3gpp.org/ftp/Specs/archive/22_series/22.071, accessed October 2020.
[41] Rupprecht, David & Dabrowski, Adrian & Holz, Thorsten & Weippl, Edgar & Pöpper, Christina. (2017). On Security Research Towards Future Mobile Network Generations. IEEE Communications Surveys & Tutorials. PP. 10.1109/COMST.2018.2820728, accessed October 2020
[42] 3GPP TR 33.825 V16.0.1 (2019-10) Technical Report 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security of Ultra-Reliable Low-Latency Communication (URLLC) for the 5G System (5GS) (Release 16) https://www.3gpp.org/ftp/Specs/archive/33_series/33.825 , accessed October 2020
[43] 3GPP TR 33.824 V0.6.0 (2019-11) Technical Report 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Security for NR Integrated Access and Backhaul; (Release 16) https://www.3gpp.org/ftp/Specs/archive/33_series/33.824, accessed October 2020.

Related components: IAB Donor, IAB UE, F1 interface

Vulnerability to Radio Jamming Attacks

As any wireless cellular networks, 5G networks are built upon open sharing in which the communication medium is the free frequency space making them prone to interference. This weakness can be used by some adversary nodes to cause intentional interference and hinder legitimate user's communication over specific wireless channels. 5G improves resilience against jamming attacks over the 4G LTE, but remains vulnerable to customised attacks. Massive MIMO deployment may be vulnerable to jamming attacks[44]. Jamming attacks are a special concern for mission-critical applications.

Related components: Uu

Failure to meet General Security Assurance Requirements

Security of 5G RAN is built upon the permanent update of Security Assurance Requirements for critical network components such as gNB.

However, a security update gap between new security requirements and deployment of updated versions of network functions in operational systems will unavoidably exist. There are two major factors in reducing this gap: a) vendors' responsiveness in issuing and validating new versions of the network functions that address the updated requirements, and b) timeliness and effectiveness of MNO processes to update operational systems to recently released and SCAS-evaluated versions.

Affected components: gNB

3.7 NETWORK FUNCTION VIRTUALISATION (NFV) – MANO (ZOOM-IN)

NFV introduces a new concept for service providers to accelerate the deployment of new network services in support of their revenue and growth plans. It translates to the use of standard IT virtualisation technologies applied to the deployment of Network Functions, aiming at a faster provision of new network services. With this, several providers formed the NFV ISG under the European Telecommunications Standards Institute (ETSI). The foundation of NFV's basic requirements and architecture resulted from the work produced by ETSI NFV ISG [45][46].

Although 5G networks will be very different compared to its predecessors in some regards (e.g. through the use of virtualisation and support for diverse and critical non-telecom-oriented services), they still share similarities and will reuse and extend existing concepts that have proved successful and are widely adopted.

The NFV has a tight interaction with Virtual Network Functions (VNF), MANO and OSS/BSS and security management components. The NFV 'Zoom-in' presented in Figure 7 refers to all relevant Core Network and Access Network Functions, as defined by the 3GPP specification and outlined in their respective zoom-ins.

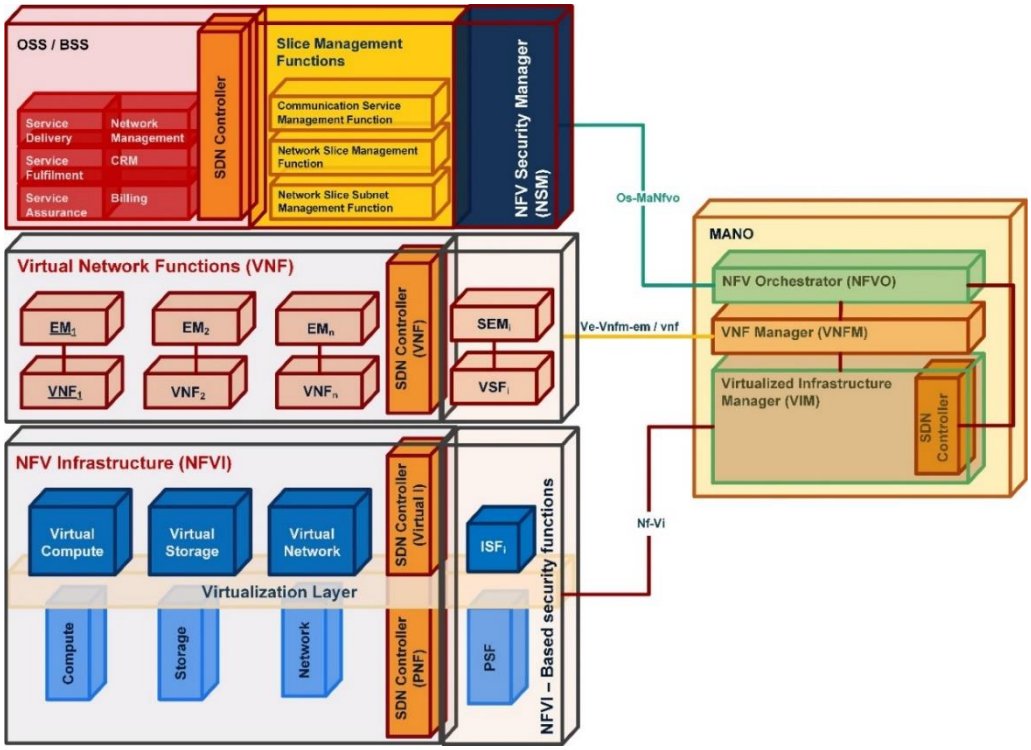
The structure of NFV has remained almost unchanged. The updates of NFV introduced, constitute an evolution of previous specifications and concentrate mainly in the adaptation of functions virtualization to various requirements dictated by the needs of various components. At

[44] Y. Arjoune and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2020, pp. 1010-1015, doi: 10.1109/CCWC47524.2020.9031175, accessed October 2020.
[45] https://www.etsi.org/technologies/nfv, accessed October 2020.
[46] https://www.sdxcentral.com/networking/nfv, accessed October 2020.

the same time, they contain provisions to adapt NFV to recent cloud, software, and virtualization techniques, novel management architectural styles and operationalization aspects.

Also, the 3GPP Network Slicing Management system consumes management interfaces provided by NFV MANO for purposes such as Network Slice Lifecycle Management (LCM), Virtual Network Function LCM, Performance, Fault and Configuration Management. The structure of NFV architecture and its interfaces to related components is shown in the following figure.

Figure 7: NFV architecture Zoom-in



The elements of the NFV architecture are as follows:

Element	Short description
Operations Support System/Business Support System (OSS/BSS)	OSS/BSS functions provide management and orchestration of systems including legacy ones and may have full end-to-end visibility of services provided by legacy network functions in an operator's network. Processes covered by OSS/BSS include: Network Management, Service delivery / fulfilment / assurance, Customer Relationship management and Billing.
Virtualised Network Function (VNF)	A VNF is a virtualisation of a network function in a legacy non-virtualised network. ETSI GS NFV 001 provides a list of use cases and examples of target network functions (NFs) for virtualisation. Functional behaviour and state of a NF are largely independent of whether the NF is virtualised or not. The functional behaviour and the external operational interfaces of a Physical Network Function (PNF) and a VNF are expected to be the same. All Core and Access Network functions in the 5G system are potential subjects of virtualisation, in certain implementation scenarios.
Element Management (EM)	The Element Management is responsible for: • Configuration for the network functions provided by the VNF. • Fault management for the network functions provided by the VNF. • Accounting for the usage of VNF functions. • Collecting performance measurement results for the functions provided by the VNF. • Security management for the VNF functions.

Element	Short description
NFV Infrastructure (NFVI)	The NFV Infrastructure is the totality of all hardware and software components which build up the environment in which VNFs are deployed, managed and executed. The NFV Infrastructure can span across several locations, i.e. places where NFVI-PoPs are operated. The network providing connectivity between these locations is regarded to be part of the NFV Infrastructure. From the VNF's perspective, the virtualisation layer and the hardware resources look like a single entity providing the VNF with desired virtualised resources.
Hardware Resources	In NFV, the physical hardware resources include computing, storage and network that provide processing, storage and connectivity to VNFs through the virtualisation layer (e.g. hypervisor). Computing hardware is assumed to be COTS as opposed to purpose-built hardware. Storage resources can be differentiated between shared network attached storage (NAS) and storage that resides on the server itself. Computing and storage resources are commonly pooled. Network resources are comprised of switching functions, e.g. routers, and wired or wireless links.
Virtualisation Layer and Virtualised Resources	The virtualisation layer abstracts the hardware resources and decouples the VNF software from the underlying hardware, thus ensuring a hardware independent lifecycle for the VNFs. In short, the virtualisation layer is responsible for: •Abstracting and logically partitioning physical resources, commonly as a hardware abstraction layer. •Enabling the software that implements the VNF to use the underlying virtualised infrastructure. •Providing virtualised resources to the VNF, so that the latter can be executed.
Virtualised Infrastructure Manager	From NFV's point of view, virtualised infrastructure management comprises the functionalities that are used to control and manage the interaction of a VNF with computing, storage and network resources under its authority, as well as their virtualisation. According to the list of hardware resources specified in the architecture, the Virtualised Infrastructure Manager performs resource and operations management.Multiple Virtualised Infrastructure Manager instances may be deployed.
NFV Orchestrator	The NFV Orchestrator is in charge of the orchestration and management of NFV infrastructure and software resources, and realizing network services on NFVI.
VNF Manager	VNF Manager is responsible for VNF lifecycle management (e.g. instantiation, update, query, scaling, and termination). Multiple VNF Managers may be deployed; a VNF Manager may be deployed for each VNF, or a VNF Manager may serve multiple VNFs.
Os-Ma-nfvo	This reference point is used for exchanges between OSS/BSS and NFV Orchestrator, and supports the following: • Network Service Descriptor and VNF package management; • Network Service instance lifecycle management; • VNF lifecycle management; • Policy management and/or enforcement for Network Service instances, VNF instances and NFVI resources; • Querying relevant Network Service instance and VNF instance information from the OSS/BSS; • Forwarding of events, accounting and usage records and performance measurement results regarding Network Service instances, VNF instances, and NFVI resources to OSS/BSS, as well as and information about the associations between those instances and NFVI resources.
Ve-Vnfm-em	This reference point is used for exchanges between EM and VNF Manager, and supports the following: VNF instantiation / VNF instance query / VNF instance update / VNF instance scaling out-in, and up-down / VNF instance termination / Forwarding of configuration and events from the EM to the VNFM / Forwarding of configuration and events regarding the VNF from the VNFM to the EM. NOTE: This reference point is only used if the EM is aware of virtualisation.
Ve-Vnfm-vnf	This reference point is used for exchanges between VNF and VNF Manager, and supports the following: VNF instantiation / VNF instance query / VNF instance update / VNF instance scaling out-in, and up-down / VNF instance termination / Forwarding of configuration and

Element	Short description
	events from the VNF to the VNFM / Forwarding of configuration and events regarding VNF, from the VNFM to the VNF / Verification that the VNF is still alive/functional.
NFVI - Virtualised Infrastructure Manager (Nf-Vi)	This reference point is used for: Specific assignment of virtualised resources in response to resource allocation requests / Forwarding of virtualised resources state information / Hardware resource configuration and state information (e.g. events) exchange.
NFV Security Manager (NSM)	NSM is the logical functional block for overall security management, e.g. on the behalf of network services. In cooperation with MANO blocks dedicated to managing the virtualised network, the policy driven NSM is specialized to manage the security on a network service over its entire lifecycle. It covers the following functionalities: • Security Policy Planning designs and optimizes security policies for specific targets of protection (e.g. network services); • Security Policy Enforcement & Validation automates the deployment and supports lifecycle management of security functions as defined in the design phase, then configure security policies on the security functions. In addition, during lifetime of a network service, the validation and re-configuration/remediation of associated security policies is supported, also in automated manner; • NFVI Security Manager (ISM) – see below.
NFVI Security Manager (ISM)	NFVI Security Manager is the logical function dedicated to security management in NFVI layer. It builds and manages the security in NFVI to support NSM requests for managing security of network services in higher layer.
Security Element Manager (SEM)	SEM refers to Element Manager managing Security Functions.
Virtual Security Function (VSF)	This element is a special type of VNF running on top of NFVI with tailored security functionality (e.g. firewall, IDS/IPS, virtualised security monitoring functions like vFEP, vTap). VSFs are mainly required to protect the other VNFs, which constitute a network service. VSF is managed by either dedicated VNFM or generic VNFM with respect to its lifecycle.
NFVI-based Security Function (ISF)	This element is a security function provided by the NFV Infrastructure. It includes virtualised security appliances or software security features (e.g. hypervisor-based firewalls) and hardware-based security appliances/modules/features (e.g. Hardware Security Modules, Crypto Accelerators, or Trusted Platform Modules).
Physical Security Function (PSF)	This element is a conventionally realized security function in the physical part of the hybrid network. Even if a telco network is virtualised, additional PSFs are still needed, for instance to protect the NFV infrastructure (and inherently, the Network Services running on top) as a whole. PSF is part of the non-virtualised traditional network and not maintained by the NFVI provider, hence it is managed by the SEM instead of the VIM.
NFVI - Virtualised Infrastructure Manager (NF-Vi)	This reference point is used for: specific assignment of virtualised resources in response to resource allocation requests / Forwarding of virtualised resources state information / Hardware resource configuration and state information (e.g. events) exchange.

3.7.1 ELEMENTS OF NOVELTY (RELEASE 4)

The ETSI Industry Specification Group for Network Functions Virtualisation (NFV) has started working in 2019 on its next specification release, known as Release 4. Release 4 addresses several issues in the following technical areas: the evolution of the NFV framework to support the most recent cloud, software, and virtualization techniques; novel management architectural styles and operationalization aspects, leveraging virtualization characteristics to simplify deployments; and increased support for automation.[47]

[47] https://www.etsi.org/newsroom/press-releases/1652-2019-10-etsi-nfv-release-4-empowers-orchestration-and-cloud-enabled-deployments, accessed October 2020

Key areas of focus for the NFV Release 4 include[48]:

- NFVI evolution, focusing on enhancements to support lightweight virtualization technologies such as OS containers, optimizing NFV Infrastructure (NFVI) abstraction for reducing the coupling of VNFs to infrastructure
- Enhancing NFV automation and capabilities, covering aspects such as: improving life-cycle management and orchestration, the simplification of VNF and NS management aspects leveraging virtualization, and handling advances in autonomous networking
- Evolving the NFV-MANO (Management and Orchestration) framework, focusing primarily on optimizing internal NFV-MANO capability exposure and usage, and on enhanced reliability and availability
- Accompanying operationalization aspects which include: the simplification of NFV to ease development and deployment of sustainable NFV based solutions, verification and certification procedures and mechanisms, and operationalization, integration and use of NFV with other management and network frameworks
- In addition to the above technical areas, several security hardening aspects of NFV and other small specific technical enhancements necessary to maximize the impact of virtualization and future NFV deployments are also expected to be part of the work programme

The "Release 4 Definition" lists all the new features proposed for the Release 4. Among other features that had not been fully completed in the previous Release and have been carried over into Release 4, the list of new features includes:

- Network connectivity integration and operational for NFV
- NFV-MANO automation and autonomous networks
- NFV enhancements for 5G
- Multi-tenancy enhancements for NFV-MANO
- Service-based architecture (SBA) for NFV-MANO
- VNF generic management functions, and
- Continuous VNF integration

However, the current network architecture of the operators differs in critical points from the envisioned ETSI NFV architecture. Even if NFV technologies have proven successful technologies in the IT industry, some adaption is needed to accommodate the special needs of the telecommunications industry. Currently, traditional network functions are coupled with underlying dedicated hardware, which are vendor proprietary. Network virtualization migration from traditional network functions to the ETSI NFV architecture involves restructuring infrastructure, service functions, and operation and maintenance (O&M)[49].

Further consideration is needed for allocation of resources for critical infrastructure services. Sharing of such resources may not be allowed by national regulators for considerations of availability, response time and confidentiality.

Similarly, NFV functions part of Release 4, such as Multi-tenancy enhancements for NFV-MANO or Continuous VNF integration, will face adoption hurdles because of national certification and authorisation schemes.

[48] NFV Release 4 Definition v0.2.0 (2020-07) https://docbox.etsi.org/ISG/NFV/Open/Other/ReleaseDocumentation/NFV(20)000160_NFV_Release_4_Definition_v0_2_0.pdf, accessed October 2020.
[49] https://www.gsma.com/futurenetworks/5g/migration-from-physical-to-virtual-network-functions-best-practices-and-lessons-learned/, accessed October 2020.

3.7.2 SECURITY CONSIDERATIONS

Virtualization

NFV benefits from the inherent security protection brought by the virtualization layer[50]. The security threats associated with VNFs are the combination of the security threats on physical networking and on virtualization technologies. VNFs run over virtual resources such as VMs and cross-contamination for shared hardware resources is possible, in particular MNO should carefully investigate risks to operate VNF categorized as critical with others VNF on the same physical resources. Virtualization brings with it some new attack surface with known vulnerabilities in virtualization environments. If hypervisor is compromised, other vulnerabilities can arise exponentially. There are potential security issues associated with NFVI, considering some potential attack scenarios such as VM escape attack, attack on hypervisor management interface, denial of service (DoS), DNS amplification attack.

A 3GPP Study[51] considers the consequences of virtualisation on 3GPP architectures, in order to identify threats and subsequent security requirements. To adequate security in virtualised deployments, the underlying infrastructure needs to provide minimum security capabilities in a standardised form which can be requested and or consumed at the 3GPP layer.

Related component(s): VIM, Virtualisation Layer, NFVI

Management Interfaces / APIs

One of the security challenges is to define the standard interface in the ETSI NFV architecture. New APIs introduce new threat vectors. Standardisation of interfaces will address security from design phase. Management Interfaces / APIs must have safeguards in place to avoid being manipulated in unintended ways to cause disruption. Security challenges are related to Web/API vulnerabilities, Account compromise, Privileged User Access, Unauthorized access, Unauthorized data/packet, Inspection / Modification of data, compromise of MANO components. Improper enforcement of security policies, or improper updating policy rules and data access procedures, allowing attackers to gain access to the NFV MANO module and further perform unauthorized control for all operations.

Related component(s): Os-Ma-nfvo, Ve-Vnfm-em, Ve-Vnfm-vnf

Localisation of functions

Attacks aiming to place and migrate workload outside the legal boundaries were not possible using traditional infrastructure. Using NFV, violation of regulatory policies and laws becomes possible by moving one VNF from a legal location to another illegal location, because there is no mechanism to enforce geo-restrictions.

Related component(s): NFVO, VNFM, VIM

[50] Security Considerations for the 5G Era – July 2020 https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf, accessed October 2020.
[51] 3GPP TR 33.848 V0.5.0 (2019-11) Technical Report 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Aspects; Study on Security Impacts of Virtualisation (Release 16), accessed October 2020.

3.8 SOFTWARE DEFINED NETWORK (SDN) (ZOOM-IN)

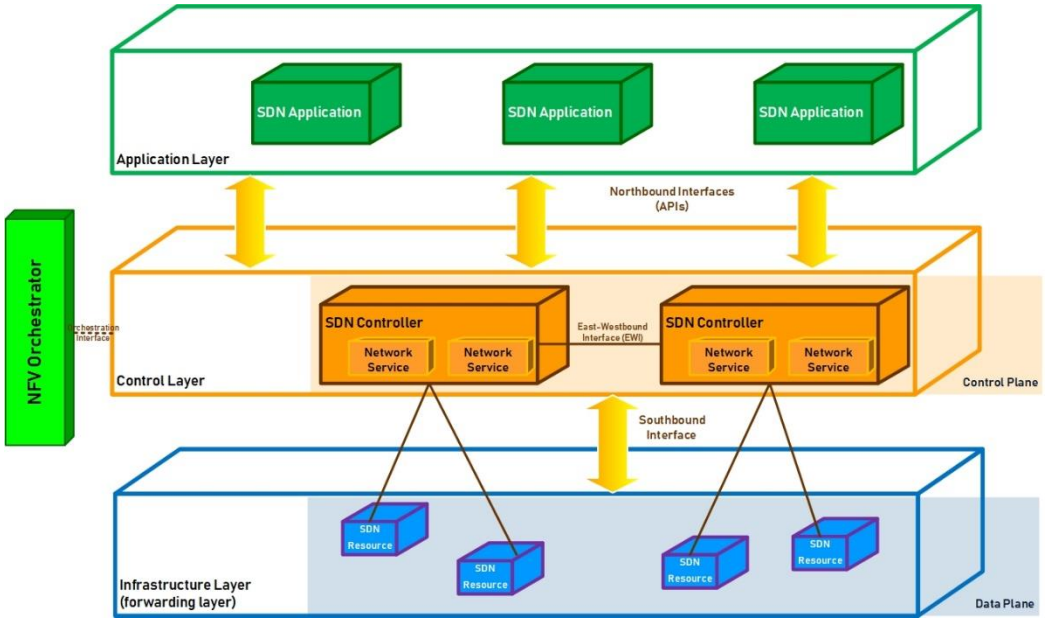
5G will be driven by the influence of software on network functions, known as software defined network (SDN) and network function virtualisation (NFV). The key concept that underpins SDNs is the logical centralisation of network control functions by decoupling the control and packet-forwarding functionality of the network. While SDN separates the control and forwarding planes, NFV primarily focuses on optimizing the network services themselves. NFV complements this vision through the virtualisation of these functionalities based on recent advances in general server and enterprise IT virtualisation. In this document, the provisions regarding SDN threats are the ones described in the ENISA Thematic Landscape SDN/5G[52].

As previously mentioned, the fundamental concept of SDN relies on decoupling of the control and packet forwarding functionality of the network. In classic networks, these two functionalities were the responsibility of the forwarding devices of the network. In SDN, these two functionalities have been separated into two functionality planes: the control plane and the data plane. The separation of these two functionality planes in SDNs has two significant consequences:

a) it reduces the difficulty in the configuration and alteration of the control functions of the network, as this functionality has no longer the responsibility of the forwarding devices of the network that tend to have proprietary implementations (e.g., operating systems), and
b) it enables the implementation of more consistent control policies through fewer and uniformly accessible controllers.

The typical SDN architecture, as described by the Open Networking Foundation[53], is shown in the following figure.

Figure 7: SDN architecture Zoom-in



[52] ENISA Threat Landscape and Good Practice Guide for Software Defined Networks/5G https://www.enisa.europa.eu/publications/sdn-threat-landscape/at_download/fullReport, accessed October 2020.

The elements of the SDN architecture are as follows:

Element	Short description
SDN controller	SDN Controller: The SDN Controller is a logically centralized entity in charge of: • Translating the requirements from the SDN Application layer down to the SDN Resources and • Providing the SDN Applications with an abstract view of the network (which may include statistics and events). SDN controller is the "brain" of SDN network. An SDN controller manages flow control to the switches/routers 'below' (via southbound APIs) and the applications and business logic 'above' (via northbound APIs) to deploy intelligent networks[54].
SDN Application	SDN Applications are programs that explicitly, directly, and programmatically communicate their network requirements and desired network behaviour to the SDN Controller. Multiple case scenarios might be envisioned, for the position of the SDN applications in the NFV architectural framework, such as: • The network hardware might be a physical appliance talking to an SDN controller, or a complete solution including multiple SDN components, such as SDN controller + SDN application for instance; • The VIM might be an application interfacing with an SDN controller in the NFVI - for instance OpenStack Neutron as a VIM interfacing with an SDN controller in the NFVI; • The SDN application might be a VNF talking to an SDN controller, being virtualised or not. For instance, a PCRF VNF might talk to an SDN controller for some policy management for traffic steering; • The SDN application might be an element manager interfacing with an SDN controller to collect some metrics or configure some parameters; • The SDN application might be an application interfacing with an SDN controller for instance in the OSS-BSS for tenant SDN service definitions.
SDN resources	Multiple scenarios might be envisaged for the actual location of SDN resources: • physical switch or router; • virtual switch or router; • e-switch, software based SDN enabled switch in a server NIC; • switch or router as a Virtual network function (VNF).
Northbound Interface	SDN Northbound Interfaces are interfaces between SDN Applications and SDN Controllers and typically provide abstract network views and enable direct expression of network behaviour and requirements. This may occur at any level of abstraction (latitude) and across different sets of functionalities (longitude). One value of SDN lies in the expectation that these interfaces are implemented in an open, vendor-neutral and interoperable way[55].
Southbound Interface	The SDN Southbound Interface is the interface defined between an SDN Controller and an SDN Data-path, which provides at least: • programmatic control of all forwarding operations; • capabilities advertisement; • statistics reporting, and • event notification. One value of SDN lies in the expectation that the Southbound Interface is implemented in an open, vendor-neutral and interoperable way.
Eastbound-Westbound Interface	This interface is implemented by the different controllers of the SDN and is used to facilitate communications between them (Controller – Controller interface).
Control Plane (CP)	The plane responsible for the control functionality of the network. Part of the network that is assigned to control one or more SDN resources. CP instructs network devices how to treat and forward packets. The Control Plane (CP) communicates with Data Plane (DP) of devices using a control plane Southbound Interface (SBI).
Data Plane (DP) or Forwarding Plane (FP)	The plane responsible for the data forwarding functionality of the network. The functionality of this plane is realized through a set of physical network devices (network elements).

[54] https://www.sdxcentral.com/networking/sdn/definitions/what-is-sdn-controller/, accessed October 2020.
[55] SDN Architecture Overview https://www.opennetworking.org/wp-content/uploads/2013/02/SDN-architecture-overview-1.0.pdf, accessed October 2020.

3.8.1 ELEMENTS OF NOVELTY

Software-defined network (SDN) radically changes the network architecture by decoupling the network logic from the underlying forwarding devices. This architectural change rejuvenates the network-layer granting centralized management and programmability of the networks. From a security perspective, SDN separates security concerns into control and data plane, and this architectural re-composition brings up exciting opportunities and challenges. The overall perception is that SDN capabilities will ultimately result in improved security. However, in its raw form, SDN could potentially make networks more vulnerable to attacks and harder to protect. Although nothing comes without risks or trade-offs, when it comes to security and SDN clearly the security benefits of SDN outweigh security risks[56].

3.8.2 SECURITY CONSIDERATIONS

Control Plane

SDN provides a logically centralized control plane to the network. The controller of the network maintains a global view of the network and programs forwarding devices as per the policies defined at the application layer. While initially controllers were developed as single devices, recently there has been a shift of trend to distributed controllers with the goal of adjusting to scalability and reliability requirements of real-world scenarios. In this case, each set of forwarding devices is assigned to a specific instance of controllers and the controllers, follow a Master/Slave deployment model.

Control Plane attack refers to the case where an attacker may deduce the forwarding policy of the network just by analysing the performance metrics of a forwarding device. For example, an input buffer may be used to identify rules, and by analysing the packet processing times, an attacker could identify the forwarding policy.

Related component(s): Control Plane, SDN controller

Data Plane

The data plane is composed of networking equipment such as switches and routers specialized in packet forwarding.

However, unlike traditional networks, these are just simple forwarding elements with no embedded intelligence to take autonomous decisions. These devices communicate through standard OpenFlow interfaces with the controller - which ensures configuration and communication compatibility and interoperability among different devices.

A Protocol Attack refers to attacks targeting the data plane of an SDN by exploiting network protocol vulnerabilities in the forwarding devices .

A Device Attack refers to all those attacks, where the adversary aims to exploit software or hardware vulnerabilities of an SDN-capable switch to compromise SDN's data plane. In this case, an attacker may target software bugs (e.g., firmware attacks) or hardware features (e.g., TCAM memory) of a forwarding device.

Related component(s): Data Plane, SDN resources

[56] The Security Benefits Behind the Software Defined Network https://businessinsights.bitdefender.com/security-benefits-software-defined-network, accessed October 2020.

Programmable Interfaces (APIs)/ SDN Programming languages

There the attacks against the Southbound API of an SDN include: Interaction, Eavesdrop, Availability and TCP-attacks. While with an Eavesdrop Attack, the attacker aims to learn about information exchanged between the control and data plane as part of a larger attack plot, in an Manipulation Attack the attacker's goal is to corrupt the network behaviour by modifying the messages being exchanged. The Availability Attack refers to Denial of Service (DoS) attacks, where the Southbound API is flooded with requests causing the network policy implementation to fail. Attackers can infer flow rules in SDN from probing packets by evaluating the delay time from probing packets and classifying them into classes. Knowing the reactive rules, attackers can launch DoS attacks by sending numerous rule-matched packets which trigger packet-in packets to overburden the controller.

Similar to SDN's Southbound API, the Northbound API is susceptible to Interception, Eavesdrop and Availability.

Attacks. While the nature of both attacks is similar, there are a few key differences:

- An attacker targeting the Northbound API requires higher-level of access to the system and is potentially sitting on the application plane. There may be cases that the applications do not run on the same device and in that case the attack complexity may be reduced as to Southbound API.
- The impacts of a compromised Northbound API are potentially larger given that information exchanged between the control and application plane affect network-wide policies. Unlike Southbound API, where OpenFlow is adopted as the standard, the Northbound API lacks any standardization. Specifically, each controller has different specifications for the Northbound API, and this leads to insecure developments[57].

Another issue that needs to be looked at is the potential exposure caused by SDN programming languages (e.g. P4 Programming Protocol-independent Packet Processors), used to dynamically reconfigure the network. The use of these extremely dynamic and event-based languages increases the attack surface. Although these languages have not been considered in the current document, it is proposed to perform a detailed analysis of their misuse potential in prospective, more detailed threat assessments.

Related component(s): Northbound Interfaces, Southbound Interfaces, Eastbound-Westbound Interface

Virtualization

There are threats related to the underlying IT infrastructure used for virtualising network operations, like: Virtualised host abuse, Data-Centre threats, Network Virtualization bypassing.

Related component(s): Control Plane, Data Plane

3.9 MULTI-ACCESS EDGE COMPUTING (MEC) (ZOOM-IN)

Multi-access Edge Computing (MEC) stands for the provision of cloud computing capabilities at the edge of the network, that is, for high bandwidth, low latency end-user applications. MEC is located in the logical vicinity of base stations through authorised third parties willing to offer processing and storage capabilities to subscribers of the 5G network. MEC is a novel approach

[57] Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions https://arxiv.org/pdf/1804.00262.pdf, accessed October 2020.

in the 5G ecosystem that enhances mobile user experience by covering services that, in previous generations, were using the run-time of end-user devices.

MEC provides a new ecosystem and value chain. Operators can open their Radio Access Network (RAN) edge to authorized third-parties, allowing them to flexibly and rapidly deploy innovative applications and services towards mobile subscribers, enterprises and vertical segments.

Multi-access Edge Computing will enable new vertical business segments and services for consumers and enterprise customers. Use cases include:

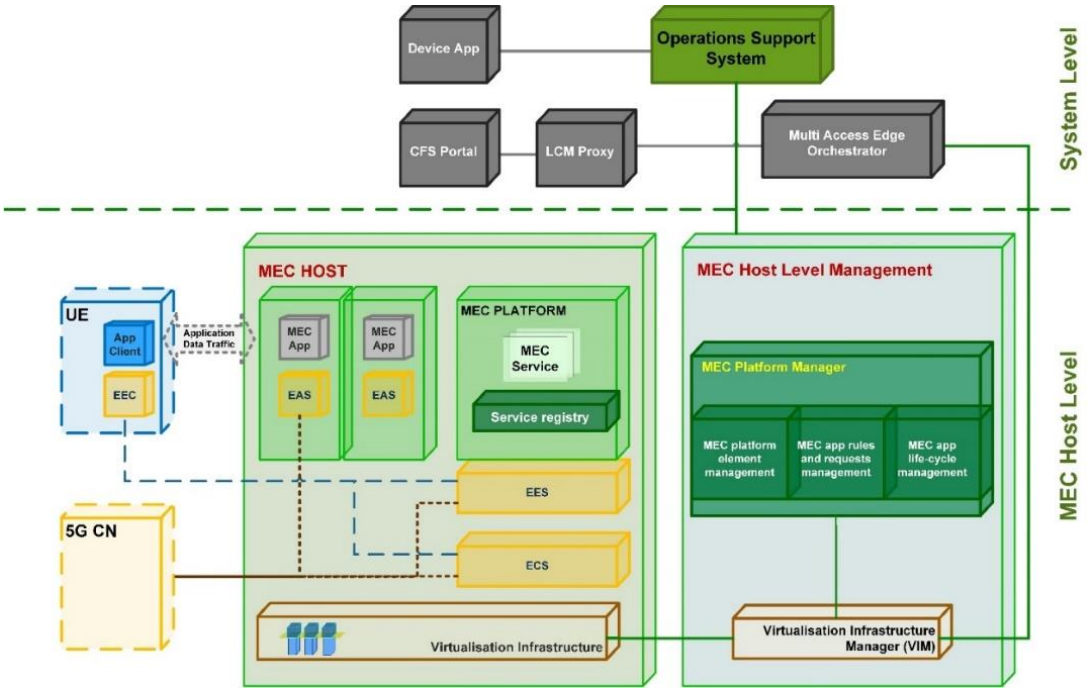
- video analytics;
- location services;
- Internet-of-Things (IoT);
- augmented reality;
- optimized local content distribution and
- data caching.

It is expected that MEC is going to emerge following the evolution of application services and verticals and will be one of the main drivers for a wider coverage and penetration of 5G Networks.

Besides offering these services, MEC takes an important role in the 5G infrastructure. It possesses orchestration functions, interacts with the 5G policy component and supports lifecycle matters of the offered applications.

By deploying various services and caching content at the network edge, Mobile core networks are alleviated of further congestion and can efficiently serve local purposes. The structure of MEC and its elements is shown in the figure below:

Figure 8: MEC architecture Zoom-in



The elements of MEC are as follows:

Element	Short description
Customer facing service (CFS) portal	The customer facing service portal allows operators' third-party customers (e.g. commercial enterprises) to select and order a set of MEC applications that meet their particular needs, and to receive back service level information from the provisioned applications.
Device application	Device applications as defined in the present document are applications in the device (e.g. UE, laptop with internet connectivity) that have the capability to interact with the MEC system via a user application lifecycle management proxy.
Application Client(s)	Application Client is the application resident in the UE performing the client function.
Edge Enabler Client (EEC)	Edge Enabler Client (EEC) provides supporting functions needed for Application Client(s). Functionalities of Edge Enabler Client are: • retrieval and provisioning of configuration information to enable the exchange of Application Data Traffic with the EAS; • discovery of EAS available in the Edge Data Network.
Edge Configuration Server (ECS)	Edge Configuration Server (ECS) provides supporting functions needed for the Edge Enabler Client to connect with an EES. Functionalities of ECS are: • Provisioning of Edge configuration information to the Edge Enabler Client. The Edge configuration information includes the following: o the information for the EEC to connect to the EES (e.g. service area information applicable to LADN); and o the information for establishing a connection with EES (such as URI).
User application lifecycle management (LCM) proxy	The user application lifecycle management proxy allows device applications to request on-boarding, instantiation, termination of user applications and when supported, relocation of user applications in and out of the MEC system. It also allows informing the device applications about the state of the user applications. The user application lifecycle management proxy authorizes requests from device applications in the device and interacts with the OSS and the multi-access edge orchestrator for further processing of these requests.
Multi-access edge orchestrator	The multi-access edge orchestrator is the core functionality in MEC system level management, responsible for the following functions: maintaining an overall view of the MEC system; on-boarding of application packages; selecting appropriate MEC host(s) for application instantiation; triggering application instantiation and termination; triggering application relocation as needed when supported.
MEC host	MEC host is an entity that contains a MEC platform and a virtualisation infrastructure which provides compute, storage, and network resources, for the purpose of running MEC applications.
Virtualisation infrastructure	It provides compute, storage, and network resources for the MEC applications. The virtualisation infrastructure includes a data plane that executes the traffic rules received by the MEC platform, and routes the traffic among applications, services, DNS server/proxy, 3GPP network, other access networks, local networks and external networks.
MEC platform	It is the collection of essential functionalities required to run MEC applications on a particular virtualisation infrastructure and enable them to provide and consume MEC services. The MEC platform can also provide services.

Element	Short description
Edge Enabler Server (EES)	Edge Enabler Server (EES) provides supporting functions needed for EAS and EEC. Functionalities of EES are: • provisioning of configuration information to EEC, enabling exchange of application data traffic with the EAS; • supporting the functionalities of API invoker and API exposing function58 as specified in 3GPP TS 23.222; • interacting with 3GPP Core Network for accessing the capabilities of network functions either directly (e.g. via PCF) or indirectly (e.g. via SCEF/NEF/SCEF+NEF); • support the functionalities of application context transfer; • supports external exposure of 3GPP network capabilities to the EAS over EES interface.
MEC applications	MEC applications are instantiated on the virtualisation infrastructure of the MEC host, based on configuration or requests validated by the MEC management.
Edge Application Server (EAS)	Edge Application Server (EAS) is the application server resident in the Edge Data Network, performing the server functions. The Edge Application Server may consume the 3GPP Core Network capabilities: invoke 3GPP Core Network function APIs directly, invoke 3GPP Core Network capabilities through the EES or invoke the 3GPP Core Network capability through the capability exposure functions (i.e. SCEF or NEF).
MEC service	It is a service provided via the MEC platform either by the MEC platform itself or by a MEC application.
Service registry	In MEC, the services produced by the MEC applications are registered in the service registry of the MEC platform – as opposed to the network functions and the services they produce which are registered in the Network Resource Function (NRF).
Application Data Traffic	Data traffic between the application installed on the User Equipment (UE) and the application server (EAS / MEC App).
MEC host level management	It handles the management of the MEC specific functionality of a particular MEC host and the applications running on it. Is comprised of the MEC platform manager and the virtualisation infrastructure manager.
MEC platform manager	The MEC platform manager is responsible for the following functions: • Managing the life cycle of applications including informing the multi-access edge orchestrator of relevant application related events; • Providing element management functions to the MEC platform and • Managing the application rules and requirements. The MEC platform manager also receives virtualised resources fault reports and performance measurements from the virtualisation infrastructure manager for further processing.
Virtualisation infrastructure manager	The functionality provided by the virtualisation infrastructure manager in this 'Zoom-in' overlaps generally with the functionality provided by the VIM described in the NFV 'Zoom-in'.

3.9.1 ELEMENTS OF NOVELTY

ETSI ISG MEC and 3GPP have both worked on their own architectures for edge computing within the boundaries of their different scopes. Their common purpose is to create an open and standardized IT service environment for hosting and supporting third-party applications in edge environments. Synergized Mobile Edge Cloud Architecture[59] provides common practices to

[58] 3GPP TS 23.222 – Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.
[59] ETSI White Paper #36 - Harmonizing standards for edge computing - A synergized architecture leveraging ETSI ISG MEC and 3GPP specifications, 1st edition – July 2020, accessed October 2020.

developers such that they can create a single application software module running on common edge environments.

At the heart of the ETSI ISG MEC and 3GPP SA6 architectures lie the MEC Platform/Edge Enabler Server and the MEC Applications/Edge Application Servers respectively. There is a great degree of synergy in the two architectures on these aspects, and in the information carried between these functional entities. ETSI GR MEC 031 will provide solution proposals and recommendations for MEC integration into 3GPP 5G system. On the other hand, 3GPP TS 23.558 Architecture for enabling Edge Applications (Release 17) provides application layer architecture and related procedures for enabling edge applications over 3GPP networks.

3.9.2 SECURITY CONSIDERATIONS

Virtualization and containerization

Cloud computing will leverage on multiple virtualized systems in order to optimize available resources and deliver on its proposed benefits. Cloud native MEC provides inherent security protection due to the isolation and containerization.

- Each container performs a dedicated function, enhancing behaviour profiling and anomaly detection.
- Isolation of containers prevents spread of malware and viruses.
- Decomposed software provides efficient software version updates and security patches.
- Compute services in cloud-native applications are designed to be ephemeral, reducing the attack surface.
- Resiliency is gained with increased speed to start a container and horizontal scale to dynamically respond to threats.
- Segmentation with network slicing separates traffic and isolates compute resources.

However, cloud native MEC architecture is exposed to a number of threats[60]:

- The uses of open source code, more interfaces, and new APIs introduce new threat vectors.
- Shared hardware resources can result in cross-contamination.
- Vulnerabilities in the shared host platform, Container-as-a-Service (CaaS) and Platform-as-a-Service (PaaS) can impact the container security.
- Containers requiring elevated privileges can cause security risk to both host as well as other tenant containers.
- Dependency upon central orchestration introduces a new threat vector.
- High data volume and sessions increase risk from an attack.
- Applications running in a micro-service architecture are as vulnerable to the same attacks as traditional applications.

Related component(s): Virtualisation infrastructure, MEC host, MEC applications

Physical security

Improper physical and environmental security of edge computing facilities can lead to destruction of edge computing facilities, unauthorised access at system level as an entry point to all hosted resources, theft of data on local storage.

[60] Security Considerations for the 5G Era – July 2020 https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf, accessed October 2020.

Edge computing facilities are, by their nature, seated in locations distributed geographically and this makes the physical security measures lower than a centralized Data Centre.

Related component(s): MEC Host

Application-Programming Interfaces (APIs)

Edge Applications facilitate communication between application clients and applications deployed at the edge. The architecture enables the CAPIF (Common API Framework) to be leveraged as a standardized means of providing and accessing APIs in the Edge Cloud. The main purpose of CAPIF is to have a unified north bound API framework across several 3GPP functions.

Application Programming Interface (API) Security is the design, processes, and systems that keep a web-based API responding to requests, securely processing data and functioning as intended. Like any software, APIs can be compromised and data can be stolen. Since APIs serve as conduits that reveal applications for third-party integration, they are susceptible to attacks.

Related component(s): 3GPP SA6 interfaces, ETSI MEC interfaces

Regulatory issues

In European countries there is specific legislation on the implementation of the NIS directive[61] The goal is to protect critical infrastructure that ensure national security. A critical service should be operated in an area with a security level compatible to this criticality.

If an operator operates in a MEC environment a regulated critical service, it will have to demonstrate that its environment is compatible with the regulation imposed by the critical service in the particular country of operation. Physical and logical resources should not be shared with components which have not the same criticality. This constraint requires the right level of isolation around the service to prevent regulation pollution to its own components and infrastructures. A simple solution can be the complete segregation of physical resources between the operator's MEC functions and the 3rd party ones.

Related component(s): Virtualisation infrastructure, MEC host, MEC Platform.

3.10 SECURITY ARCHITECTURE (SA) (ZOOM-IN)

The 5G security architecture consists of various network functions (NF) and components that are responsible for securing end-to-end communications, providing authentication functions and various other security functions. The 5G security architecture consists of components that are part of various other architectures (“Zoom-ins” in terms of this report), acting thus in a horizontal manner across all other architectures. In particular, security functions are securing the access of users within the radio access network (RAN), they cover security functions in the core network and perimeter entities (edge computing) and they provide security functions in the Network Function Virtualization. Finally, a set of elements is covering security management functions, audit and analytics.

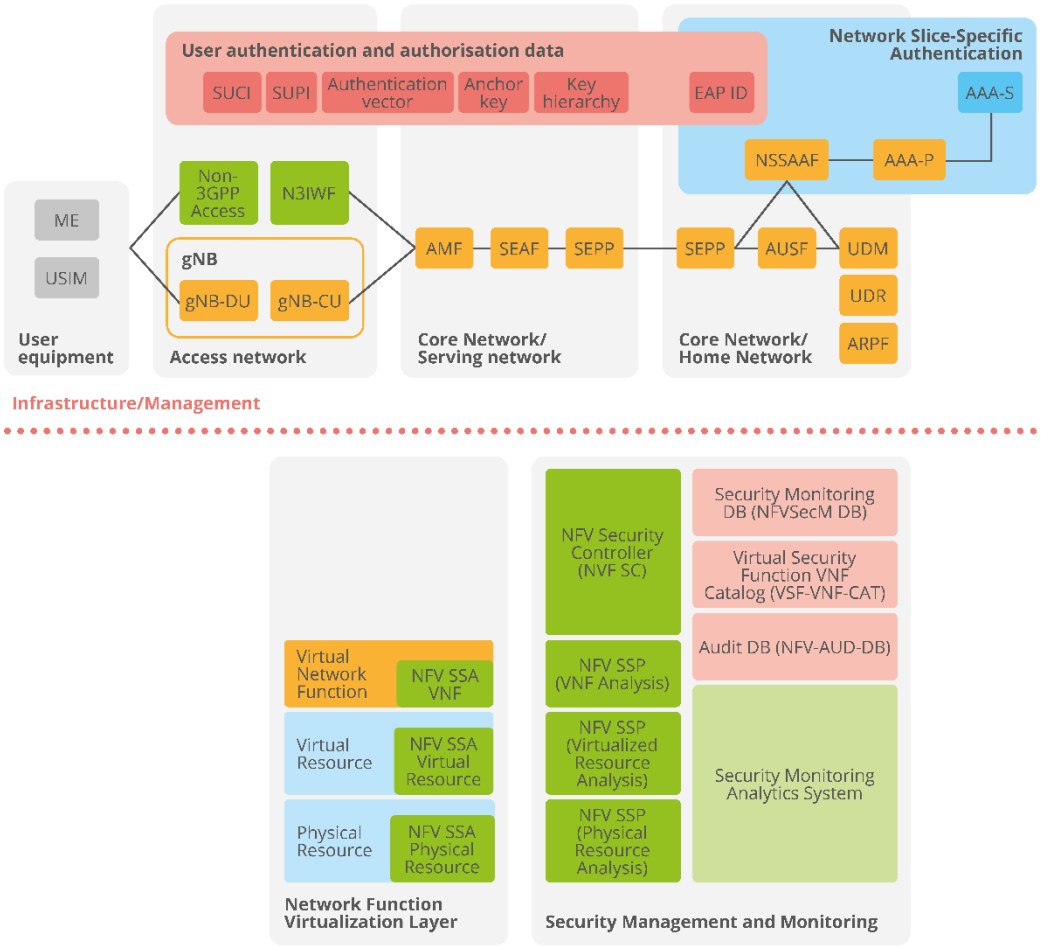
The 5G security architecture is defined in 3GPP technical specification[62] as spanning complementary different domains.

[61] The Directive on security of network and information systems (NIS Directive) https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, accessed October 2020.
[62] 3GPP TS 33.501 V16.4.0 (2020-09) Security architecture and procedures for 5G system (Release 16) https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.

- Network access security (I): the set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and Non-3GPP access, and in particularly, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from SN to AN for the access security.
- Network domain security (II): the set of security features that enable network nodes to securely exchange signalling data and user plane data.
- User domain security (III): the set of security features that secure the user access to mobile equipment.
- Application domain security (IV): the set of security features that enable applications in the user domain and in the provider domain to exchange messages securely. Application domain security is not in the scope of the present analysis.
- SBA domain security (V): the set of security features that enables network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains. Such features include network function registration, discovery, and authorisation security aspects, as well as the protection for the service-based interfaces.
- Visibility and configurability of security (VI): the set of features that enable the user to be informed whether a security feature is in operation or not.

The detailed structure of the 5G security architecture is shown in the following figure.

Figure 9: 5G Security architecture Zoom-in



The elements of the 5G security architecture are as follows:

Element	Short description
Mobile Equipment (ME)	ME stands for all kinds of mobile equipment that can be connected to the 5G network. ME can be sensors, IoT components, connected autonomous systems, eHealth devices, etc.
Universal Subscriber Identity Module (USIM)	USIM is the SIM card of 5G.It is a platform for securing access and communication in 5G. It is the only security module mentioned in 3GPP specification.
5G Node Base Station Central Unit (gNB-CU)	Some security requirements for gNB-CU have been formulated by 3GPPP. Though not a security element per se, these requirements increase the security properties of gNB and – when implemented - are considered to be relevant to the security architecture.
Non-3GPP Access Network	Security for non-3GPP access to the 5G Core network is achieved by a procedure using IKEv2 as defined in RFC 7296 to set up one or more IPsec ESP security associations. The role of IKE initiator (or client) is taken by the UE, and the role of IKE responder (or server) is taken by the N3IW.
Non-3GPP access Inter-Working Function (N3IWF)	This Network Function is responsible for interworking between untrusted non-3GPP networks and the 5G Core. As such, the N3IWF supports both N2 and N3 based connectivity to the core, whilst supporting IPsec connectivity towards the device.
Access and Mobility Management Function (AMF)	The Core Access and Mobility Management Function is part of the 3GPP 5G Architecture. Its primary tasks include registration Management, Connection Management, Reachability Management, Mobility Management and various function relating to security and access management and authorisation.
Security Anchor Function (SEAF)	The *SEAF* will create for the primary authentication a unified *anchor* key KSEAF (common for all accesses) that can be used by the UE and the serving network to protect the subsequent communication[63].
Authentication server function (AUSF)	The Authentication server function (AUSF) shall handle authentication requests for both, 3GPP access and non-3GPP access. The AUSF shall provide SUPI to the VPLMN (Core Network / Serving Network) only after authentication confirmation if authentication request with SUCI was sent by VPLMN. The AUSF shall inform the UDM that a successful or unsuccessful authentication of a subscriber has occurred.
Authentication credential Repository and Processing Function (ARPF)	ARPF selects an authentication method based on subscriber identity and configured policy and computes the authentication data and keying materials
User Data Management (UDM) Function	Unified data management (UDM) manages network user data in a single, centralized element. UDM is similar to the 4G network's home subscriber service (HSS) but is cloud-native and designed for 5G specifically. The SIDF is responsible for de-concealment of the Subscription Concealed Identifier (SUCI) and shall fulfil the following requirements: • The SIDF shall be a service offered by UDM; • The SIDF shall resolve the SUPI from the SUCI based on the protection scheme used to generate the SUCI.
Unstructured Data Repository (UDR)	Repository for management of unstructured data, designed to manage massive and various types of unstructured data including text, image, audio and video.
Security Edge Protection Proxy (SEPP)	The 5G System architecture introduces a Security Edge Protection Proxy (SEPP) as the entity sitting at the perimeter of the mobile network. The SEPP shall act as a non-transparent proxy node.

63 https://www.researchgate.net/profile/Andreas_Kunz2/publication/319527681_Overview_of_5G_security_in_3GPP/links/59b116d80f7e9b37434a8248/Overview-of-5G-security-in-3GPP.pdf, accessed October 2020.

Element	Short description
Network Slice Specific Authentication and Authorisation Function (NSSAAF)	The Network Slice Specific Authentication and Authorisation Function (NSSAAF) supports the following functionality: • Support for Network Slice-Specific Authentication and Authorisation as specified in TS 23.502 64with a AAA Server (AAA-S).
AAA-S	In the optional-to-use Network slice-specific authentication and authorisation, an AAA server (AAA-S) may be owned by an external 3rd party enterprise.
AAA-P	In the above-mentioned scenario, if the AAA-S belongs to a third party, the NSSAAF may contact the AAA-S via an AAA proxy. The NSSAA Function and the AAA-P may be co-located.
EAP-ID	Network slice-specific authentication and authorisation uses a User ID and credentials, different from the 3GPP subscription credentials (e.g. SUPI and credentials used for PLMN access) and takes place after the primary authentication[65].
NFV Security Services Agent (SSA)	The NFV SSA exists in both the NFVI domain and in VNF domain. NFV SSA in VNF domain may exist as a separate VSF, or within a VNF. The NFV SSA is responsible for securely receiving the Security Monitoring policy and implementing the same.
NFV Security Controller (SC)	The NFV SC may interface with other security systems (e.g. Security Analytics), security databases and other policy engines. The NFV SC orchestrates system wide security policies. The NFV SC acts as a trusted 3rd party that resides independently. An NFV SC manages NFV SSAs (like VSFs) to keep them in a consistent state according to the policy specified. SC also facilitates secure bootstrapping of SSAs (like VSFs), managing instances of SSAs, secure pairing up with SSA's VNFMs and EMs, personalize the SSAs, policy management, integrity assertion, credential management, facilitate clustering of multiple SSAs into a distributed appliance, monitoring of SSAs for failure and remediation.
NFV Security Services Provider (SSP)	The NFV SSP is comprised within the VIM and VNFM, and is responsible for security monitoring policy orchestration received from the Security Controller (NFV SC) and interacting with the various VIM/VNFM components to implement the policy across various systems comprising the NFVI/VNF. Furthermore, NFV SSP is also responsible for receiving the telemetry data from various NFV SSAs, and optionally making some analysis based on this data.
NFV Security Monitoring Database	The NFV SecM-DB is a secure database consisting of security data used for deploying NFV system wide Security Monitoring. This includes Security Monitoring policy and configurations, security credentials for facilitating secure communications between the various Security Monitoring components, and credentials for secure storage of telemetry, including tenant-specific security policies.
SA/VSF Catalogue Database (VSF-NVNF-CAT)	The NFV VSF-VNF-CAT is a repository for Security Services Agents like the Virtual Security Functions (VSF) VNFs. The catalogue has capability to add and remove SSAs (VSF) packages and/or images, and also includes a VSF VNFD (VNF Descriptor) containing meta data and information about that VSF VNF. Once the SSA (VSF) package or instance is added to the catalogue, it becomes available for orchestration.
Audit DB	The NFV AUD-DB is a secure database consisting of security audit information.
Security Monitoring Analytics System	The Security Monitoring Analytics system securely receives Security Monitoring telemetry from across the NFV systems, including the MANO and all the NFVIs that may be geographically distributed. The analytics system applies advanced machine learning techniques on the telemetry to perform advanced detection of security anomalies and emerging threats in the system. This system also can trigger remediation actions through the NFV SC.

[64] 3GPP TS 23.502 V16.5.1 (2020-08) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS); Stage 2 (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.
[65] 3GPP TS 33.501 V16.3.0 (2020-07) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.

Element	Short description
Subscription Concealed Identifier (SUCI)	A one-time use subscription identifier, which contains the Scheme-Output, and additional non-concealed information needed for home network routing and protection scheme usage.
Subscription Permanent Identifier (SUPI)	In 5G, all subscribers will be allocated a globally unique 5G SUPI. Example SUPI formats include the IMSI and NAI (Network Access Identifier)
Authentication Vector	A vector consisting of RAND, authentication Token (AUTN) and Hash eXpected RESponse (HXRES).
Anchor Key	The security key KSEAF provided during authentication and used for derivation of subsequent security keys.
Key Hierarchy	Hierarchy of cryptographic key derived from Anchor Key, (as defined in ETSI TS 133 501[66] section 6.2.). It includes the following keys: KAUSF, KSEAF, KAMF, KNASint, KNASenc, KN3IWF, KgNB, KRRCint, KRRCenc, KUPint and KUPenc.

3.10.1 ELEMENTS OF NOVELTY

While many new features in Release 16 contribute to increased security, the relevant addition at the level of Security Functions is the enhanced support for Network Slice-Specific Authentication and Authorisation. The feature allows the use of a User Identifier independent of existing identifiers relating to a 3GPP subscription or UE, for Network Slice-Specific Authentication and Authorisation. For such Network Slice Specific Identifiers, the AMF invokes an EAP-based Network Slice-Specific authentication procedure in which the AUSF exchanges AAA protocol messages with a potentially external AAA Server (AAA-S) via an optional AAA Proxy (AAA-P) to authenticate and authorize a UE for the network slice. Depending on the result of the procedure a UE is either authorized for a network slice, re-allocated to a different one or deregistered.[67].

Other relevant security aspects of enhancing the 5G system include:

- Security for enhanced Service Based Architecture
- Security for User Plane Gateway Function for Inter-PLMN Security
- Security aspects of Enhanced Network Slicing
- Security for NR Integrated Access and Backhaul
- Security aspects of Service Enabler Architecture Layer for Verticals
- Security of evolution of Cellular IoT security for the 5G System
- 3GPP profiles for cryptographic algorithms and security protocols

Last but not least, Release 16 of 5G specifications include updated versions of the 5G Security Assurance Specifications (SCAS). SCAS provide an extensive description of the security requirements (including test cases) to demonstrate compliance of the network product with the security requirements defined by 3GPP. SCAS are continuously developed to embed solutions to disclosed vulnerabilities and ensure the security of 5G system's critical components, and of the 5G system as a whole.

[66] https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.01.00_60/ts_133501v150100p.pdf, accessed October 2020

[67] 3GPP TR 21.916 V0.5.0 (2020-07) Technical Report 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Release 16 Description; Summary of Rel-16 Work Items (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.

The following SCAS requirements have been updated to reflect changes proposed by Release 16:

TS 33.512 - Access and Mobility management Function (AMF)

TS 33.514 - Unified Data Management (UDM)

TS 33.515 - Session Management Function (SMF)

TS 33.516 - Authentication Server Function (AUSF)

TS 33.517 - Security Edge Protection Proxy (SEPP)

TS 33.520 - Non-3GPP Inter-Working Function (N3IWF)

3.10.2 SECURITY CONSIDERATIONS

No security considerations have been developed for this zoom-in. This is due to the fact that all security consideration covered in the rest of the zoom-ins constitute the entire set of security considerations, underlying thus its horizontal nature of security. Hence, it is considered that they cover this topic in an exhaustive manner and there is no need to be repeated in this section.

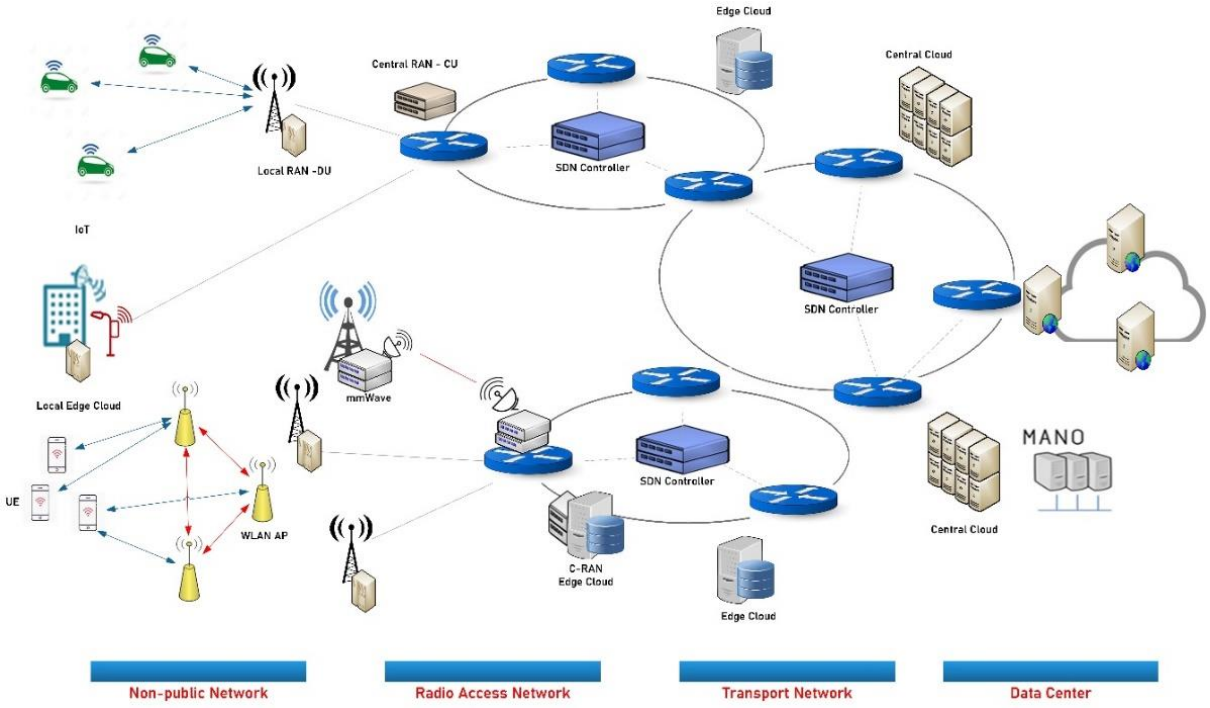
3.11 5G PHYSICAL INFRASTRUCTURE (ZOOM-IN)

One of the most relevant aspects in the transition from previous generations of mobile telecommunications into 5G is the fact that part of the network functions, previously performed by physical appliances, are now executed by software that virtualizes the functionality of physical components. Additionally, some of these physical components were mostly proprietary and incompatible with other solutions but with 5G, the network software can run in any commercial-of-the-shelf (COTS) hardware, allowing the operators to have more independence from manufacturers and share physical infrastructures among various tenants and applications.

This significant change will allow great scalability, quicker deployments, cost efficiency and integration between different components of the network. On the other hand, the virtualisation of physical infrastructure components increases significantly the impact of failures: a shared physical component will serve multiple functions (e.g. virtual functions, slicing, user equipment functions, etc.), playing thus a significant role in the service provisioning chain.

Nonetheless, the physical 5G architecture is going to remain exposed to more generic threats that are pertinent to physical components, such as damage/theft, sabotage, natural disasters, outages, failures and malfunctions, just to name the most important ones. While in previous mobile networks such failures had a more “restricted” influence in service provisioning, with the 5G virtualisation failures of physical components may have an amplified impact, typical to shared resources. This fact increases the criticality of 5G physical infrastructure components, as multiple services are going to depend on them. The 5G physical infrastructure is depicted in the following the figure.

Figure 10: 5G physical infrastructure Zoom-in



3.11.1 ELEMENTS OF NOVELTY

While 5G Release 16 does not bring any novelties to the physical infrastructure per se, a series of enhancements referred to in other sections of the document will impact the physical infrastructure and associated security considerations:

- Integrated Access and Backhaul, eliminates the need for wired backhaul connection, allowing a speedier densification of the wireless network.
- Improved support for non-public networks (NPN) will lead to an increase in deployment scenarios that involve private networks that utilize dedicated small cell base stations) that are independently managed to deliver locally-optimized applications. Further detail is given in section the 5G RAN zoom-in (see section **Error! Reference source not f ound.**).

3.11.2 SECURITY CONSIDERATIONS

Impact of virtualisation

Software Defined Networking (SDN) and Network Function Virtualization (NFV) allow disconnection of software execution from specific physical hardware and provide for better resilience and latency. SDN offers flexibility how to configure the routing paths between dynamically configured virtualized network functions.

It should be noted, that container technology generates a bigger attack surface against systems (e.g. via supported APIs, and through intrinsically less security functions, by being a technology at initial maturity levels). However, softwarisation and virtualization of functions may increase availability and integrity requirements for shared physical resources, some of them placed in remote locations. Physical security controls for such resources should be commensurate with their respective importance.

Affected components: Central DC, Local DC

General Physical security considerations

Physical security considerations valid for previous generations of mobile networks still apply. They focus around two general objectives: ensuring appropriate environmental conditions for equipment operations and protection of perimeters hosting sensitive assets.

Special consideration must be given to equipment located in third party premises or otherwise remote facilities rooms. These should be protected using a risk-calibrated set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters. Failure to do so may lead to unauthorised access, destruction of assets and impairment of operations.

Related components: Local DC, gNB-DU, gNB-CU

Threats to edge cloud computing resources

The deployment of Edge Cloud computing resources at the edge of the network, in data centres or data rooms with significantly less physical control and protection than the central data centres expose important computing resources to physical security threats, which can lead to service compromise or even an access path to central resources.

Affected components: Edge DC

Vulnerability of air interface to jamming attacks

As any wireless cellular networks, 5G networks are built upon open sharing over specific frequencies, making them prone to interference. This weakness can be used by some adversary nodes/equipment to cause intentional interference and hinder legitimate user's communication over the spectrum of wireless channels dedicated to this technology. 5G improves resilience against jamming attacks over the 4G LTE, but remains vulnerable to customised attacks[68]. Jamming attacks are a particular concern for mission-critical applications.

Related components: Base stations

3.12 IMPLEMENTATION OPTIONS / MIGRATION PATHS ZOOM IN

5G can be deployed in different deployment options, where SA (standalone) options consist of only one generation of radio access technology and NSA options consist of two generations of radio access technologies (4G LTE and 5G). The early deployments will be adopting either non-standalone option 3 or standalone option 2 as the standardisation of these two options have already been completed[69].

Non-standalone option 3 is where radio access network is composed of eNBs (eNode Bs) as the master node and gNBs (gNode Bs) as the secondary node. The radio access network is connected to EPC (Evolved Packet Core). The NSA option 3, as it leverages existing 4G deployment, can be brought to market quickly with minor modification to the 4G network. This option also supports legacy 4G devices and the 5G devices only need to support NR (New Radio) protocols so device can also be developed quickly.

On the other hand, NSA option 3 does not introduce 5GC and therefore may not be optimised for new 5G use cases beyond mobile broadband. In addition, depending on how 5G devices are

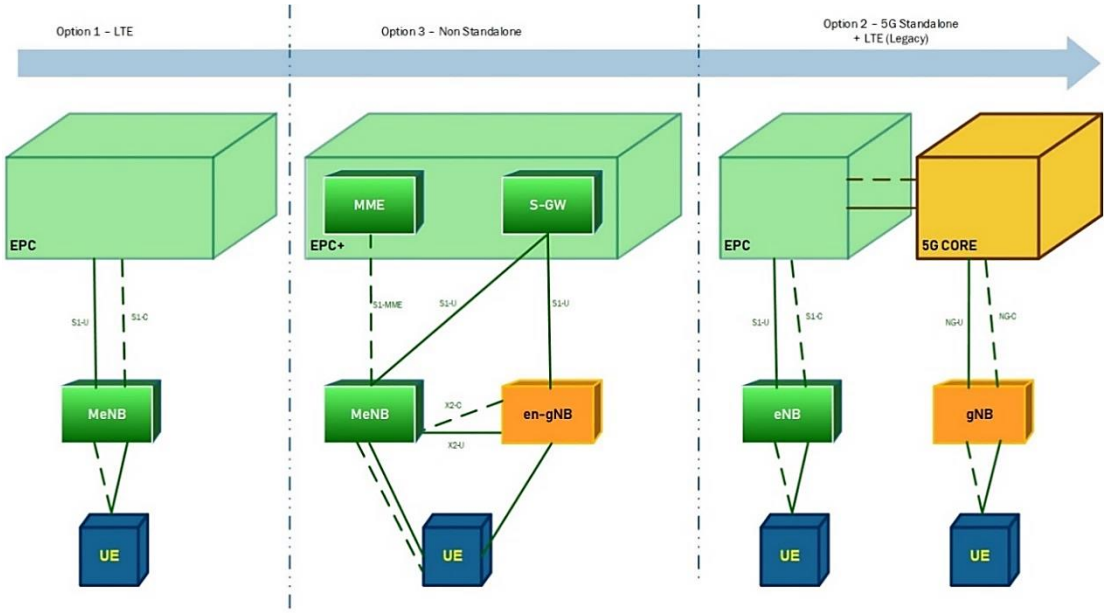
[68] Y. Arjoune and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2020, pp. 1010-1015, doi: 10.1109/CCWC47524.2020.9031175, accessed October 2020.
[69] GSMA - 5G Implementation Guidelines: NSA Option 3, February 2020 https://www.gsma.com/futurenetworks/wp-content/uploads/2019/03/5G-Implementation-Guidelines-NSA-Option-3-v2.1.pdf, accessed October 2020.

developed, the EPC may need to be retained longer than in the case of having EPS (Evolved Packet System) for 4G alone (instead of supporting NSA Option 3).

Standalone option 2 is where radio access network consists of only gNBs (gNode Bs) and connects to 5GC (5G Core), and the 5GC interworks with EPC. SA option 2 has no impact on LTE radio and can fully support all 5G use cases by enabling network slicing via cloud native service-based architecture. On the other hand, this option requires both NR and 5GC, making time-to-market slower and deployment cost higher than that of NSA option 3. Furthermore, the devices would need to support NR and core network protocols so it would take more time to develop devices.

Finally, as the standalone 5G System would need to interwork with EPS to ensure service continuity depending on coverage, the interworking between EPC and 5GC may be necessary.

Figure 11: Implementation options / Migration Paths



The elements of the Option 3 Non-standalone architecture are:

Element	Short description
EPC	Evolved Packet Core (EPC) is a framework for providing converged voice and data on a 4G Long-Term Evolution (LTE) network. 2G and 3G network architectures process and switch voice and data through two separate sub-domains: circuit-switched (CS) for voice and packet-switched (PS) for data. Evolved Packet Core unifies voice and data on an Internet Protocol (IP) service architecture and voice is treated as just another IP application.
EPC+	Evolved Packet Core (EPC) is the LTE Core Network. In order to support the Non-standalone deployments with LTE and NR technologies, the core network will need to undergo a series of improvements – hence the EPC+ designation. Envisaged improvements include increasing the bandwidth of the S1-U interface to meet the LTE/NSA transmission requirements. There are two typical scenarios for EPC upgrade to support 5G deployment. Scenario A: • Physical EPC is upgraded to support NSA; • Capacity expansion is based on physical EPC.

Element	Short description
	Scenario B: • Build a new virtualized EPC network to support NSA independently; • Interoperability is made between the new virtualized EPC and the physical EPC; • Capacity expansion is based on the virtualized EPC. At the time of this analysis, priority is given to Scenario B, which can be smoothly evolved to the target network through the expansion of virtualized EPC.
5G Core Network (5GC)	The core network is the central part of the 5G infrastructure and enables all functions related to multi-access technologies - see 5G Core Network zoom-in.
En-gNB	En-gNB is a node providing NR user plane and control plane protocol terminations towards the UE, and acting as Secondary Node in EN-DC. En-gNB is a gNB that supports legacy E-UTRAN interface.
MeNB (Master node)	The LTE eNB is referred to as the MeNB to indicate that it is the 'Master' (M) base station controlling the 'Secondary' (S) 5G NR base station. In MR-DC (Multi-Radio Dual Connectivity), the radio access node that provides the control plane connection to the core network. It may be a Master eNB (in EN-DC), a Master ng-eNB (in NGEN-DC) or a Master gNB (in NR-DC and NE-DC).
X2 Interface	X2 is an interface for the interconnection of two E-UTRAN NodeB (eNB) components and an E-UTRAN NodeB (eNB) and an E-UTRAN gNodeB (en-gNB) within the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) architecture. It is specified in the 3GPP 36.42x series of technical specifications. The X2 interface provides capability to support radio interface mobility and Dual Connectivity either between eNBs or between eNBs and en-gNBs of UEs having a connection with E-UTRAN. The list of functions on the X2 interface is the following: • Intra LTE-Access-System Mobility Support for ECM-CONNECTED UE; • Load Management; • Inter-cell Interference Coordination; • General X2 management and error handling functions; • Application level data exchange between eNBs • Trace functions; • Data exchange for self-optimisation; • E-UTRA-NR Dual Connectivity (EN-DC).
S1 Interface	S1 interface for the interconnection of the evolved NodeB (eNB) component of the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) to the Core Network (CN) of the Evolved Packet System (EPS). It is specified in the 3GPP 36.41x series of technical specifications. The S1 interface supports: • procedures to establish, maintain and release E-UTRAN Radio Access Bearers; • procedures to perform intra-LTE handover and inter-RAT handover; • the separation of each UE on the protocol level for user specific signalling management; • the transfer of NAS signalling messages between UE and EPC; • location services by transferring requests from the EPC to E-UTRAN, and location information from E-UTRAN to EPC; • mechanisms for resource reservation for packet data streams.
MME	Mobility Management Entity (MME) is the key control-node for the LTE access-network. It is responsible for idle mode User Equipment (UE) paging and tagging procedure including retransmissions. It is involved in the bearer activation/deactivation process and is also responsible for choosing the Serving Gateway for a UE at the initial attach and at time of intra-LTE handover involving Core Network (CN) node relocation. It is responsible for authenticating the user (by interacting with the Home Subscriber Server). The Non Access Stratum (NAS) signalling terminates at the MME and it is also responsible for generation and allocation of temporary identities to UEs. It checks the authorisation of the UE to camp on the service provider's Public Land Mobile Network (PLMN) and enforces UE roaming restrictions.

Element	Short description
SGW	The Serving Gateway (SGW) routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies (terminating S4 interface and relaying the traffic between 2G/3G systems and Packet Data Network Gateway). For idle state User Equipment, the Serving Gateway terminates the downlink data path and triggers paging when downlink data arrives for the User Equipment. It manages and stores UE contexts, e.g. parameters of the IP bearer service, network internal routing information.
User Equipment (UE)	User equipment is any device used by users to communicate within the 5G infrastructure. Besides a SIM, user equipment may be home appliances of any kind (e.g. computer, IoT devices, etc.).

3.12.1 SECURITY CONSIDERATIONS

Risks related to legacy technologies

LTE networks and 5G NSA networks based on LTE core networks will continue to operate in the operators' networks for years to come. Early 5G commercial launches are leveraging 3GPP's Non-Standalone 5G specifications, meaning these early 5G NSA networks are required to use the LTE control plane protocols and the LTE Evolved Packet Core (EPC) network. Initial 5G NSA launches will deliver only Enhanced Mobile Broadband (eMBB) service so, any LTE threats and vulnerabilities will also exist in the 5G NSA network.

Even after the operators upgrade their cell sites with 5G radios (gNBs) using the NSA architecture, some of these 5G NSA cell sites may operate as 5G NSA sites for years after Standalone 5G networks are operational. NSA architectures are expected to live alongside each other for a considerable period, so a series of legacy risks will remain active[70].

Affected components: EPC, eNB

INTER-RAT (Radio Access Technologies) Handover

3GPP has specified interworking that allows 5GC network functions to support interfaces to an EPC. Handover attempts to NR connected to 5GC from 4G LTE will occur, with active data sessions at risk of disruption if a roaming agreement exists for 4G, but not for 5G between PLMN's. The MME can prevent such handover attempts by including RAT and Core Network Type restrictions in the Handover Restriction List to E-UTRAN[71].

Roaming

5G NSA roaming is essentially 4G roaming because NSA uses the EPC for all Core Network functions. From a security perspective, a 5G NSA roaming connection introduces no new protection, since it continues to use Diameter, SIP/VoLTE and possibly SS7. Diameter and SS7 are vulnerable to eavesdropping including voice calls, reading text messages, and tracking phones. Note: This consideration is also relevant for 5G SA, as there will be a need for roaming agreements with non-5G networks, hence Diameter and SS7 attacks will still apply.

[70] A 5G AMERICAS White Paper – Security considerations for the 5G Era, June2020 https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-FINAL-Word.docx, accessed October 2020
[71] GSMA - 5G Roaming Guidelines, May 2020 https://www.gsma.com/newsroom/wp-content/uploads//NG.113-v2.0-1.pdf , accessed October 2020.

For 5G SA the roaming flows will be considerably different, as HTTP/2 and JavaScript Object Notation (JSON) will be used versus the legacy Diameter protocol. Voice over New Radio (VoNR) will replace VoLTE in the 5G network and Security Edge Protection Proxy (SEPP) will establish a secure, encrypted connection with the roaming partner's SEPP[72].

As regards inter-operators Roaming, the following considerations need to be taken into account:

-Authentication confirmation between 5G SA-Networks must be activated in order to address the voice&sms eavesdropping, as well as the tracking threats. But whether or not authentication confirmation will be activated/enforced depends on multiple parameters.
-According to 33.501, SUPI "should" be encrypted while ME attaches in roaming scenario, but there are exceptions to this rule, which may become the norm if care is not taken.

Affected components: EPC, eNB.
Note: In roaming, components and procedures not specified by 3GPP play a role, for example those involved with CDR (Calling Data Record) exchange, such as NRTRDE (Near Real Time Roaming Data Exchange), SS7 Firewalls and SMS Firewalls.

Failure to meet General Security Assurance Requirements

The security assured by the EPC / 5G Core functions and the security of the Core Network itself is built upon the permanent update of Security Assurance Requirements for critical network components.

Failure the ensure that early-deployed systems or sub-systems comply with updated security assurance requirements may lead to unsubstantiated trust in the security offered by the 5G system as a whole.

3.13 PROCESS MAP

Telecommunication network security is more than a sum of technical specifications. Security is built and maintained by security-relevant processes, in four major areas:

- Standardization: operators, vendors and other stake-holders set standards for how networks around the globe will work together. This also includes how best to protect networks and users against malicious actors.
- Network design: vendors design, develop and implement the agreed standards for functional network elements and systems only, and warrant that they have a complete control and responsibility over the whole delivered systems, which play a crucial part in making the end network product both functional and secure.
- Network configuration: at the deployment phase, networks are configured for a targeted security level, which is key to setting security parameters and further strengthening the security and resilience of the network.
- Network deployment and operation: the operational processes which allow networks to function and deliver targeted levels of security are highly dependent on the deployment and operations of the network itself.[73]

While all stakeholders are relevant to ensure that security is embedded in the 5G System, design, implementation and operation, two stakeholders are of particular relevance to the

[72] A 5G AMERICAS White Paper – Security considerations for the 5G Era, June2020 https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-FINAL-Word.docx, accessed October 2020.
[73] A guide to 5G network securityericsson.com; Conceptualizing security in mobile communication networks – how does 5G fit in?: Ericsson AB 2018; https://www.ericsson.com/48fcab/assets/local/news/2018/10201291-04_gir_report_broschure_dec2018_webb_181212.pdf, accessed October 2020.

cybersecurity of 5G network. On the one hand, mobile network operators (MNO) have a central, decision-making role, giving them leverage on the overall secure operation of their networks, and on the other hand, telecom equipment manufacturers, who are responsible for the provision of software and hardware required to operate networks and liable for any Trojan or uncontrolled piece of software delivered to MNO[74].

To reflect this, in this section we highlight MNO and Vendor lifecycle processes and the associated security considerations, along with Security Assurance processes that span across several relevant stakeholder groups.

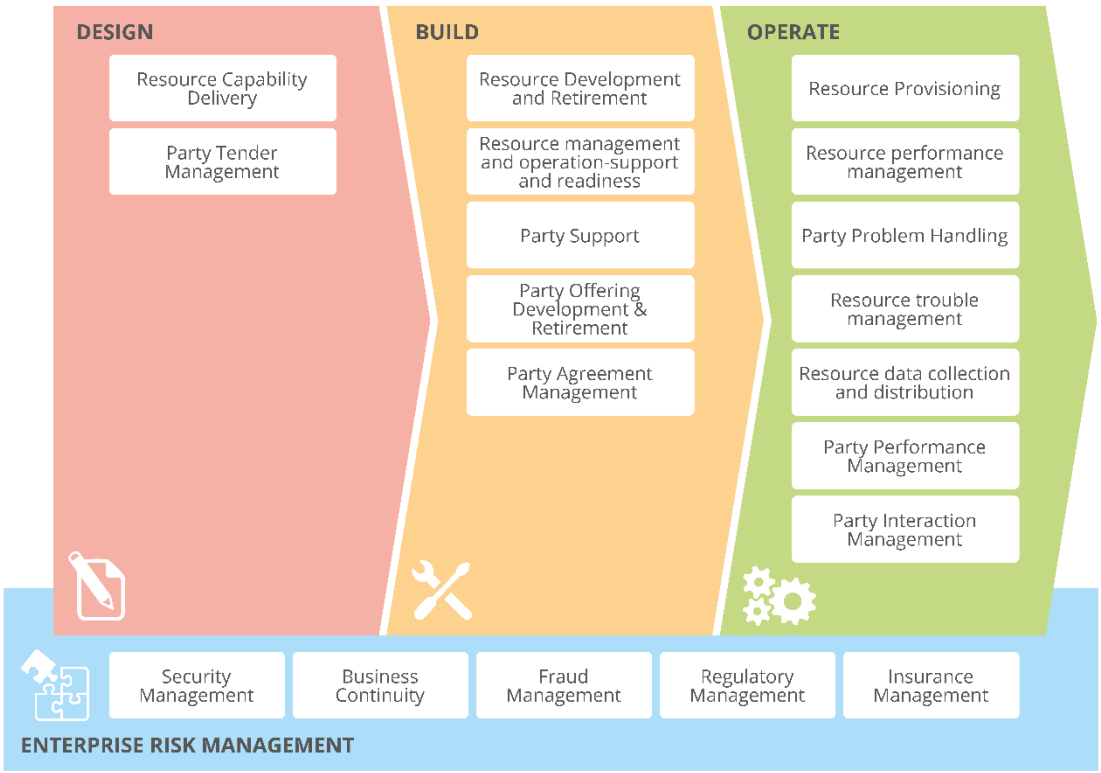
3.13.1 MNO Lifecycle Processes

MNO Lifecycle processes are aligned with eTOM – enhanced Telecom Operation Map[75], and include all actions necessary to Design, Build and Operate the 5G Network. eTOM makes available a standard structure, terminology and classification scheme for describing business processes and their constituent building blocks.[76]

Of increased importance for the Secure Design, Implementation and Operation of the 5G System are the Resource and Supply Chain Development, Management and Operation Processes, as well as the Enterprise Risk management Processes.

An overview of the MNO processes most critical to 5G system's security over the Design, Build, Operate phases is presented in the figure below:

Figure 12: MNO Lifecycle processes



[74] EU coordinated risk assessment of the cybersecurity of 5G networks Report 9 October2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132, accessed October 2020.
75 http://casewise.tmforum.org/evolve/statics/frameworx/#cwtype=index&cwview=index_diagrams_etom_start, accessed November 2020.
[76] M.3050 : Enhanced Telecom Operations Map (eTOM) – An eTOM primer, https://www.itu.int/rec/T-REC-M.3050-200702-I!Sup4/en, accessed November 2020

The description of MNO lifecycle processes in correlation with eTOM – enhanced Telecom Operation Map[77] is presented below:

Process	Short description of the process
Resource capability delivery	This category of processes coordinate and enact deployment of new technologies. These processes ensure that network and associated resources are deployed in timely and compliant manner. This is why well-functioning of these processes is critical to coordinate major system changes such as transition to 5G
Resource development and retirement	This category of processes encompasses all processes in the Build phase charged with development of new technologies and the associated resource types. These processes are also tasked with the initial decision to acquire external resources, therefore due needs to be taken to provide necessary controls that take into account all relevant risks. Last but not least, retirement or removal of certain technologies and associated resource types, are relevant in the context of transition to new technologies such as 5G.
Support Resource management and operation - Support & Readiness	Support & Readiness processes are to ensure that appropriate resources are available and ready to support the Operation Phase processes. Key responsibilities of these processes that directly impact security of the 5G System include: operations readiness testing and acceptance, Vulnerability Management, Threat Assessments, Risk Assessment and Mitigation and Secure Configuration Activities
Resource provisioning	Resource Provisioning process deal with allocation, installation, configuration, activation and testing of resources. Key responsibilities of these processes that directly impact security of the 5G System include: verification of resource availability; allocation of resources to requests from other processes such as incident recovery, vulnerability management or security function capability; configuration management, and; activation of resources and updating of resource inventory.
Resource Trouble Management	Resource Trouble Management processes are tasked with the management of undesired behaviour of specific resources, hence they are key for timely and effective management of security events. .
Resource data collection & distribution	Resource Data Collection & Distribution category of processes encompasses technical monitoring of resource and service instances and monitoring of enterprise processes to support to resource and service instances. Results of monitoring processes provide key input for other processes such as configuration management, performance management, security management.
Resource Performance Management	Resource Performance Management processes use information received from monitoring processes to analyse, control and report on the performance of specific resources, in order to maintain operational objectives such as service quality and security. Performance management processes should interface with other process classes such as Resource Trouble Management, Service Quality Management or Security Management.
Party Tender Management	Party Tender Management processes manage the entire tender lifecycle, from development of tender documents to tender decision-making. These processes are key for 5GS compliance and security, as due care should be taken to include all relevant requirements in tender documents and ensure adequateness of suppliers to risk classes of purchased products or services..
Party Offering Development & Retirement	Party Offering Development & Retirement manage the on-boarding and off-boarding of product specifications and thus are critical to ensure an adequate level of security at component and system level.

[77] http://casewise.tmforum.org/evolve/statics/frameworx/#cwtype=index&cwview=index_frameworx_processes, accessed November 2020.

Process	Short description of the process
Party Agreement Management	Party Agreement Management manages all aspects of agreements with suppliers and partners, from initiation to completion, to enable delivery of business and technical capabilities required by the 5G system.
Party Support	Management processes to engage parties who own and manage infrastructure, provide infrastructure capabilities, or otherwise provide value to the operator. Necessary facilities need to be in place to provide for interaction with parties in delivering products and/or services necessary for the operation of the 5G system.
Party Interaction Management	Interaction management deals with logging partners/supplier interaction, notification of interacting parties and matters such as communication channels and authentication/authorisation. These processes are key to ensure service level and security at all phases of the 5GS, but also an important element in preventing unauthorised dissemination of sensitive data.
Party Problem Handling	Tasked with timely and effective resolution of all problems related to the supplier/partner. It includes the entire problem lifecycle, from problem communication, management, to closure and reporting
Party Performance Management	Along with resource performance management, this process provides key input to manage performance of key activities and resources outsourced to external providers.
Business Continuity Management	Development of strategies, policies, plans, organizational roles, responsibilities and procedures for ensuring continuation of business processes and activities in the event of serious and/or sustained interruption. The relevant component of BCM for the 5G system are: • Infrastructure recovery planning which provides for recovery and backup procedures for all key infrastructure capabilities; • Serious incident management planning which defines the operational procedures and escalation criteria for operational and security incidents. Note: BCM practices might encompass ITIL Service continuity management.
Fraud Management	The general objective of the Fraud Management is prevention, detection and response to fraud risk, fraudulent activities and actors. The relevance of Fraud management processes for this document is given by the fact that they encompass interaction with Law Enforcement Agencies (LEA).
Enterprise risk audit management	Enterprise Risk Audit Management proactively works with the business to understand, assess, and report on risk. This category of processes provide assurance to senior management that the processes and controls to mitigate risk are effective and conform to reference standards. This process is relevant as the migration to 5G will expose the MNO to novel risks which must be correctly identified, evaluated and managed
Insurance management	Insurance management processes identify areas and activities within the enterprise where risk aspects are insurable and analyse the cost/benefits of undertaking specific insurance. This process is relevant as the migration to 5G will expose the MNO to novel risks, or may impact the operator's exposure to currently insured risks.
Regulatory management	Regulatory Management processes ensure that the enterprise complies with all applicable regulations. This might be sector-specific (telecommunications), or general, e.g. NIS Directive and subsequent national legislation. The relevant requirements must be fed in to the design and operation processes
Security Management	Security management processes as per ISO 27011 / ITU X.1051, including Incident Management.

3.13.2 VENDOR DEVELOPMENT AND PRODUCT LIFE CYCLE PROCESSES

Vendor Development and Product Lifecycle processes covers all aspects potentially impacting a Network Product's lifetime, including it being planned, designed, implemented, delivered, updated, and eventually ramped down.

For new Network Products and any modifications of Network Products, the Product Development phases are executed in a cyclical fashion, starting again from the beginning once finished for the previous Network Product release[78].

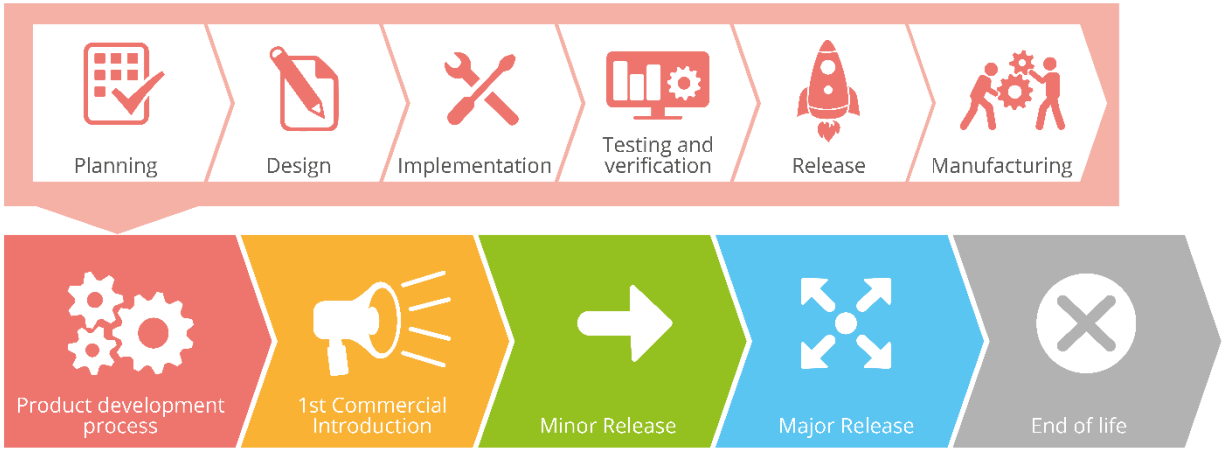
These processes must meet a clear set of security objectives and requirements to ensure that network products meet the baseline security criteria and capabilities necessary as building blocks for the overall security of the 5G network.

In addition, the network products themselves must meet baseline security criteria, tailored to their product class. These criteria are defined by 3GPP in the Security Assurance Specifications (SCASs) series of Technical Specification. Specific use cases and deployment scenarios may request additional security requirements, as defined by operators or regulators.

An objective assessment process that the network products and the processes at their origin meet baseline criteria is paramount for building trust in the 5G network, hence an important input for any procurement decisions.

The GSMA Network Equipment Security Assurance Scheme (NESAS)[79] and 3GPP Security Assurance Methodology (SECAM)[80] provide the blueprint for such an evaluation process and reference criteria. While the allocation of responsibilities among the actors of an assurance scheme might vary, the activities and their flow should be always based on the principles of independence, objectivity, competence. The vendor and product lifecycle processes are presented below:

Figure 13: Vendor and product lifecycle processes



[78] FS.16 – NESAS Development and Lifecycle Security Requirements v.1.1, GSMA, 20 July 2020, https://www.gsma.com/security/wp-content/uploads/2020/09/FS.16-NESAS-Development-and-Lifecycle-Security-Requirements-v1.1.pdf, accessed October 2020.
[79] FS.16 – NESAS Development and Lifecycle Security Requirements v.1.1, GSMA, 20 July 2020, https://www.gsma.com/security/wp-content/uploads/2020/09/FS.16-NESAS-Development-and-Lifecycle-Security-Requirements-v1.1.pdf, accessed October 2020.
[80] 3GPP TR 33.818 V0.7.0 (2020-05), Technical Report, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Assurance Methodology (SECAM); and Security Assurance Specification (SCAS); for 3GPP virtualized network products (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.

The description of the Vendor and product lifecycle processes is presented below.

Process	Sub-processes
Planning	In case of a completely new Network Product, the requirements for the first Release are planned. In the case of a new version of an existing Network Product, the requirements for the changes to be introduced by the next release are planned based on updated functional requirements as well as bug and vulnerability reports received against prior versions, if applicable.
Design	The implementation of the planned requirements for the Release is planned in detail.
Implementation	The planned requirements are implemented as per the design.
Testing and Verification	The fulfilment of the requirements by the implementation is verified. If the verification fails, the relevant requirement usually goes back to the "Implementation" phase. This phase also contains the security related testing and verification activities.
Release	The decision to release a given revision of a tested and verified implementation.
Manufacturing	In this phase, the development Release is converted into a deliverable Network Product. In the case of pure software delivery, this is the delivery of the Release to the provisioning process.
Delivery	The delivery of the manufactured Network Product.
Product development process	All the phases described above.
First Commercial Introduction	The Network Product starts its commercial lifetime by means of a first Release to be accepted for use in live commercial networks. Before that, earlier Releases may have been tested in test environments.
Update	The Network Product is updated by means of either a minor or a major Release. This phase is usually a cycle of such Releases.
Minor Release	A minor Release fixes vulnerabilities and other bugs found in earlier versions. It commonly introduces not more than minor feature enhancements and architectural changes.
Major Release	A major Release fixes vulnerabilities and other bugs found in earlier versions. It may introduce major feature enhancements and architectural changes.
End Of Life	No updates for the Network Product are supplied anymore. As this process occurs after contractual and regulatory requirements to maintain the Network Product have ceased, this commonly marks the end of a Network Product's lifetime.

3.13.3 SECURITY ASSURANCE PROCESSES

The operator can use as support for its purchasing decision the results of security conformity assessments integral to the Security Assurance Methodology, as defined by 3GPP33.916 Technical Specification[81].

The SECAM process provides the blueprint for any security assurance scheme such as product certification and vendor accreditation, and covers the following tasks:

[81] 3GPP TR 33.916 V16.0.0(2020-07) Technical Report 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Assurance Methodology (SCAS) for 3GPP network products (Release 16), https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-g40.zip, accessed October 2020.

- Vendor network product development and network product lifecycle management process assurance compliance (assessing if the method used to develop the products is compliant with the Vendor network product development and network product lifecycle management process assurance requirements).
- Security Compliance Testing (assessing if requested security requirements are correctly implemented in a network product). This includes Vulnerability Testing (running of a set of FOSS/COTS tools on external interfaces of the Network product).

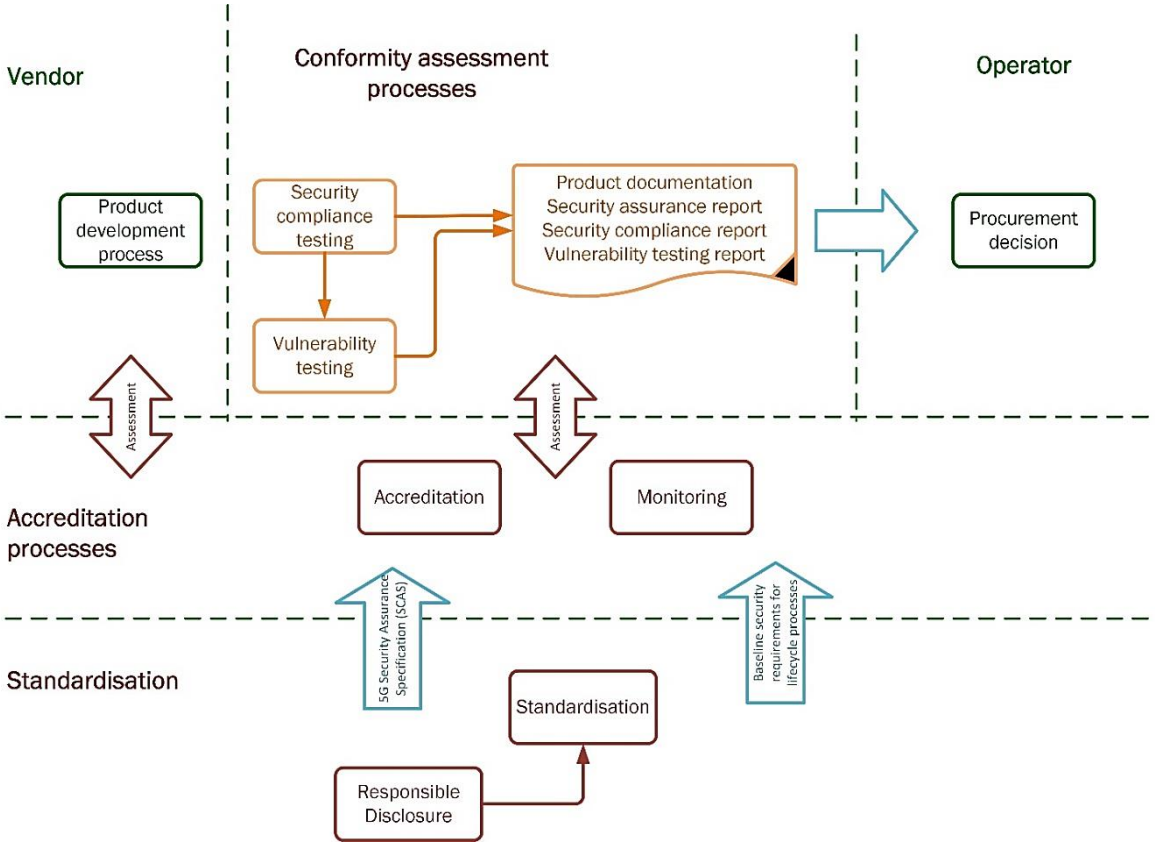
The ultimate output of the SECAM evaluation is:

- An evaluation report demonstrating compliance of the network product with the 3GPP security assurance specifications;
- Evidence to demonstrate to the test laboratory that the accredited vendor product and development lifecycle processes have been complied with for the network product;
- Evidence that the actors performing the evaluation tasks are accredited by the SECAM Accreditation Body.

The operator examines the evaluation reports together with the evidence that the actors performing the evaluation tasks have been accredited by the SECAM Accreditation Body.

Note: while the actors and distribution of tasks and responsibilities among actors may vary in different Assurance schemes, the general processes and sequence of tasks will stay generally unchanged, provided that criteria for impartiality and competence of actors that perform assessment tasks are maintained. The security assurance activities are presented below.

Figure 14: Security assurance activities



The description of the security assurance activities is presented below.

Activity	Description
Accreditation	Formal recognition by an accreditation body that a conformity assessment body is impartial and competent to carry out specific tests or types of assessments. The Accreditation Body defines requirements and processes for: • vendor network product development and network product lifecycle management processes accreditation; • test laboratory (vendor owned or third party) accreditation, and • dispute resolution.
Product development process	Vendor network product development and network product lifecycle management processes assurance requirements as well as related evaluation activities generic to all network product classes are defined by the Accreditation Body. In the SECAM scheme, the requirements are defined in the NESAS Security Assurance Requirements, but various conformity assessment schemes may define different criteria. Lifecycle management consists of establishing discipline and control in the updates of network product during its development and maintenance. Lifecycle management controls are important during normal improvement of network product as well as for vulnerability/security flaw remediation (documentation used to track vulnerability/security flaw, remediation procedure with relation to corrective actions for each identified vulnerability/security flaw…). The Vendor network product development and network product lifecycle management processes assessment covers a vendor's engineering processes and does not necessarily apply only to a single network product. This means that the results of one assessment may apply to more than one network product. Vendors can submit their generic network product development and network product lifecycle management processes or a subset of them for auditing and accreditation.
Security compliance testing	Evaluation process step used to describe activities for checking the compliance of a network product with applicable Security Assurance Specifications (SCAS).
Vulnerability testing	The process of running security tools against a network product. Vulnerability testing is defined by the use of Free and Open Source Software (FOSS) and Commercial off-the-shelf (COTS) security testing tools on the external interfaces of the network product, as well as manual testing procedures for specific attack scenarios.
Operator procurement decision	The operator examines the network product, the security compliance testing, including the vulnerability testing analysis reports, the self-declaration as well as the optional evidence of accreditation from the SECAM Accreditation Body for the actors performing the evaluation task and decides if the results are sufficient according to its internal policies. In particular, the operator can perform a sample of the security compliance testing and vulnerability testing, based on the delivered test procedures.
Audit	During an audit, the processes will be evaluated and their application on development activities in practice will be verified. An accreditation will be awarded, if the requirements are met. The accreditation processes consist of: • assessing the skills of the vendor‘s or third-party test laboratories in conducting an evaluation for conformance to Security Assurance requirements for a given network product class or range of classes, and • assessing the compliance to Test methodology (for security compliance testing and vulnerability testing laboratories).
Monitoring	The Accreditation Body monitors different kinds of accredited actors within the scheme: • Vendors development and product lifecycle processes, which are expected to comply with the Security Assurance requirements and • Test laboratories (for security compliance testing and vulnerability testing), which are expected to comply with the Test Methodology and skills requirements.

Activity	Description
Standardisation	5G security issues are addressed in the work undertaken by standards bodies, notably within the workgroup on Service and System Aspects 3 (SA3) of the 3rd Generation Partnership Project (3GPP). Other relevant standardisation bodies include ETSI and GSMA. Development of standards continuously evolve security specifications, taking into account ongoing research on security threats and vulnerabilities.
Responsible disclosure	Vulnerability Disclosure of security vulnerabilities is a well-established process which allows stakeholders such as security researchers to report details of security vulnerabilities in products and services. Vulnerability Disclosure Programmes, such as the GSMA Coordinated Vulnerability Disclosure (CVD) programme provide a framework that sets clear expectations for constructive engagement by all parties to remediate or mitigate notified vulnerabilities.[82] Results of vulnerability disclosure processes are an important input for standardization work, as security requirements are evolving to respond to identified vulnerabilities.

[82] GSM Association FS.23-GSMA Coordinated Vulnerability Disclosure Program, Version 3.016 July 2020, https://www.gsma.com/security/wp-content/uploads/2020/07/FS.23-v3.0.pdf , accessed September 2020

4. 5G VULNERABILITIES

4.1 VULNERABILITY ASSESSMENT METHOD AND SCOPE

This chapter provides the vulnerability assessment for the components of the 5G architecture. The chapter is structured according to the various zoom-ins: for each zoom-in, a set of vulnerabilities for all related components is being presented. These vulnerabilities detail the security considerations formulated for each zoom-in.

Due to the large number of vulnerabilities, and in order to facilitate readability, in this chapter we introduce vulnerability groups for the components of each zoom-in. The detailed vulnerabilities of each zoom-in are presented in a corresponding annex. While in the following sections a short description of vulnerability groups with highlights of the assessed weaknesses are presented, the annexes provide all details of each individual vulnerability, such as: detailed description, associated assets, threats exploiting the vulnerability, security controls to remove/reduce the exploitation surface, stakeholder responsible for the implementation of controls, as well as references to relevant sources.

For the sake of completeness of vulnerability assessment, some vulnerability groups that apply to multiple assets throughout several zoom-ins, are repeated in all relevant zoom-ins. This redundancy has been introduced in order to have a complete picture of the vulnerabilities at zoom-in level. Examples of such vulnerabilities are: virtualization vulnerabilities, vulnerabilities emerging from weak hardening of software, logging vulnerabilities, etc.

Each of the following sections is dedicate to a zoom-in. Besides the vulnerability groups applying to the assets of the zoom-in, it provides a reference to the cyberthreats that may lead to an exploitation, to the relevant measure foreseen in the Toolbox, as well as to references in relevant literature.

As regards the target groups of vulnerability assessment, the vulnerability groups presented in this chapter targets technical experts willing to have an overview of weaknesses of various technical components included in a zoom-in. This information can be used as a check-list in order to scrutinize the development of technical and organisation security measures and/or assess future actions to assess the priorities in the implementation of measures (e.g. depending on the current status of implementation of 5G functions).

The detailed vulnerabilities found in the annexes target technical experts working in the implementation of threat mitigation. It may be useful for checking the implementation status, planning/prioritizing implementation of security protection measures, assessing protection gaps, scoping of certification activities, etc.

4.2 VULNERABILITY GROUPS FOR CORE NETWORK

In the security considerations of core network, we have identified the following areas of vulnerabilities:

Service-based architecture: weaknesses are related with the protection of open source APIs, in particular with their integrity, authentication and protection for the data (in transit and stored).

Security update gap between new security requirements and deployment of updated versions of network functions in operational systems. Two major factors are relevant for this gap: a) vendors' responsiveness in issuing and validating new versions of the network functions that

address the updated requirements, and b) timeliness and effectiveness of MNO processes to update (e.g. UDM, AUSF, SEPP, NRF, NEF, SMF, AMF and UPF).

IP Based Protocol stack: the use of widely used IP protocols will lead to a shorted vulnerability exposure time and high impact of vulnerability disclosure.

Besides these areas of vulnerability, virtualization vulnerabilities are also applicable, as well as generic vulnerabilities related to soft- and hardware maintenance and hardening. The table below provides a more exhaustive view on vulnerabilities of core network components.

Name	Description	Relevant toolbox measures	Threat categories[83]
Vulnerabilities in implementation of AMF security functionalities	Relevant vulnerabilities in AMF implementation include: • Incorrect implementation of authentication and key agreement procedure; • Incorrect implementation of security mode command procedure; • Incorrect implementation of mechanisms for intra-RAT mobility; • Incorrect implementation of procedure for 5G-GUTI allocation; • Incorrect implementation of invalid or unacceptable UE security capabilities handling.	TM02, TM09	NAA-EXPL, NAA-ESH, NAA-AAA, NAA-DBLT, NAA-IFAS, NAA-AIL
Vulnerabilities in implementation of UPF security functionalities	Relevant vulnerabilities in UPF implementation include: • Incorrect user plane data protection; • Incorrect implementation of signalling data protection; • Failure to assign unique TEID for a session.	TM02, TM09	NAA-EXPL, NAA-AAA, NAA-DBLT, NAA-IFAS, NAA-AIL
Vulnerabilities in implementation of UDM security functionalities	Relevant vulnerabilities in UDM implementation include: • Incorrect implementation of synchronisation failure handling; • Incorrect implementation of protection SUCI de-concealment; • Incorrect implementation of authentication status handling by UDM.	TM02, TM09	NAA-EXPL, NAA-ESH, NAA-AAA, NAA-DBLT, NAA-IFAS, NAA-AIL, EIH
Vulnerabilities in implementation of SMF security functionalities	Relevant vulnerabilities in SMF implementation include: • implementation of user plane security policy handling; • Incorrect implementation of user plane security policy checking; • Incorrect implementation of unique Charging ID assignment.	TM02, TM09	NAA-EXPL, NAA-ESH, NAA-AAA, NAA-DBLT, NAA-IFAS
Vulnerabilities in implementation of SEPP security functionalities	Relevant vulnerabilities in SEPP implementation include: • Incorrect implementation of e2e core network interconnection security; • Incorrect implementation of cryptographic material handling; • Handling of cryptographic material beyond connection-specific scope • Incorrect implementation of protection policies mismatch handling.	TM02, TM09	NAA-EXPL, NAA-ESH, NAA-AAA, NAA-DBLT, NAA-IFAS, NAA-AIL

[83] To identify each threat category, use the taxonomy available in Table of Annex B.

Name	Description	Relevant toolbox measures	Threat categories[83]
Vulnerabilities in implementation of NEF security functionalities	Relevant vulnerabilities in NEF implementation include: • No authentication on application function; • No Authorisation on northbound APIs.	TM02, TM09	NAA-EXPL, NAA-ESH, NAA-AAA, NAA-DBLT, NAA-MND
Vulnerabilities in implementation of NRF security functionalities	Relevant vulnerabilities in NRF implementation include: • No slice specific authorisation for NF discovery	TM02, TM09	NAA-EXPL, NAA-ESH, NAA-AAA, NAA-DBLT, NAA-MND
SBA/SBI vulnerabilities of 5G Core components	Service-Based-Interfaces of network functions should provide adequate protection of access and of data in transit. Relevant vulnerabilities include: • Improper transport layer protection, and improper authentication mechanisms; • Vulnerable authorisation mechanisms on service access.	TM01, TM02, TM09	NAA-EXPL, NAA-AIL, NAA-AAA, NAA-DBLT, NAA-MND
Improper protection of Data and Information of 5G Core components	Adequate security controls are needed for protecting sensitive data stored, processed and transferred by 5G Core functions. Relevant vulnerabilities include: • Disclosure of confidential system internal data to users and administrators; • Improper protection of data and information in storage; • Improper protection of data and information in transfer; • Failure to log access to personal data.	TM01, TM02, TM09	NAA-DBLT, NAA-IFAS, NAA-CSVS, NAA-ESH
Improper protection of availability and integrity of 5G Core components	Adequate security controls are needed for upholding availability and integrity of 5G Core functions. Relevant vulnerabilities include: • Improper handling of overload situations; • Unrestricted boot memory devices; • Weaknesses in processing of unexpected input; • Lack of / improper mechanisms for Network Product software package integrity validation.	TM01, TM02, TM07, TM09	NAA-EXPL, NAA-ESH, NAA-MSH
Vulnerable mechanisms for authentication and authorisation of 5G Core components	System functions should not be used without appropriate authentication and authorisation and authorisation checks. Relevant vulnerabilities include: • Improper authentication policy; • Insecure / insufficient authentication attributes; • Insecure password policy; • Insecure authentication mechanisms to management / maintenance interfaces; • Failure to block consecutive failed login attempts; • Insecure authorisation and access control mechanisms.	TM01, TM02, TM09	NAA-DoS, NAA-AAA, NAA-DBLT, NAA-CSVS
Improper session protection mechanisms of 5G Core components	Systems should provide adequate mechanisms for user session protection. Relevant vulnerabilities include: • Lack of logout function; • Lack of inactivity timeout mechanisms.	TM01, TM02, TM09	NAA-AAA, NAA-IFAS, NAA-DBLT

Name	Description	Relevant toolbox measures	Threat categories[83]
Insufficient or improper monitoring mechanisms of 5G Core components	Adequate mechanisms for collection and processing of security events should be in place. Relevant vulnerabilities include: • Insufficient / inadequate logging of security events; • Logs not transferred to centralized storage; • Improper protection of security event log files.	TM01, TM02, TM05, TM09	NAA-{all}, UD, FM
Vulnerabilities in Operating Systems supporting 5G Core components	Operating systems supporting 5G Core components should provide a safe and stable environment for 5G Functions. Relevant vulnerabilities include: • Improper / insufficient mechanisms to protect availability and integrity; • Improper authentication and authorisation mechanisms.	TM01, TM02, TM09	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-DBLT, FM
Vulnerabilities in Web Servers supporting 5G Core components	Web servers serving functional and management services should provide adequate protection. Relevant vulnerabilities include: • Failure to encrypt communication between Web client and Web server; • Failure to log webserver activity; • Improper HTTP User sessions protection; • Improper validation of HTTP input.	TM01, TM02, TM09	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-DBLT, FM
Vulnerabilities of network devices running 5G Core components	The components of 5G Core may be implemented on dedicated network devices, which must be adequately protected. Relevant vulnerabilities include: • Improper mechanisms for data and information protection; • Improper mechanisms for protecting availability and integrity.	TM01, TM02, TM09	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-MND, FM
Improper hardening of 5G Core components	All 5G components, including the network functions in service-based architecture, should be hardened in order to reduce their respective surface of vulnerability. Relevant vulnerabilities include: • Unnecessary or insecure services / protocols; • Unrestricted reachability of services; • Presence of unused software / functions / components; • Unrestricted remote login for privileged users; • Excessive file-system authorisation privileges; • Vulnerable OS configuration; • Vulnerable Web server configuration; • Improper separation of traffic; • Improper hardening of 5G Core components.	TM01, TM02, TM07, TM09	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-MND, NAA-DBLT, FM
Virtualisation vulnerabilities of relevant core components	Vulnerabilities in the virtualisation layer may lead to risks such as unauthorised access to functions and data Virtualisation vulnerabilities include: • Vulnerabilities in virtualisation of OS layer; • Container vulnerabilities; • Vulnerabilities in function virtualization.	TM04	NAA-AVM, UD, FM

Name	Description	Relevant toolbox measures	Threat categories[83]
Physical and environmental vulnerabilities of relevant core components	Improper physical security of 5G Core Components infrastructure may impact the overall security and performance of the system. Relevant vulnerabilities include: • Improper physical security of Data-Centres / Telecommunication equipment room; • Improper isolation of physical secure perimeter between tenants; • Improper environmental protection controls; • Inadequate / defective security devices.	TM07	PA, FM, OUT, DIS

A detailed list of core network vulnerabilities can be found in the Annex (see C Annex).

4.3 VULNERABILITY GROUPS FOR NETWORK SLICING

In the security considerations of network slicing, we have identified the following areas of vulnerabilities:

Security-as-a-Service: While slices provide inherent security through segmentation, slices can also be used to provide additional security protection and security services specific to the use case and customer requirements. The implementation of slice security for use cases would rest ultimately with the Mobile Network Operator (MNO) to include such services in the offer, depending on its service strategy, market context, and in relation to vertical use-cases. This might the source of vulnerabilities, to be checked for each particular implementation.

Resource isolation: While network slicing offers the ability of isolation to be used in various scenarios, the proper isolation technique has to be suited to the use case at hand. Security requirements of the particular use case will be an important element of consideration for the selection of proper isolation mechanisms.

Secure Management and Orchestration: The architecture of the network slice MANO is challenging from a business model perspective. This high complexity and flexibility, which bring in higher security risks. Due to not finalized 3GPP specifications of authorisation of service management requests, implementation weaknesses may arise.

Trust Model: The building of trust to MNO capabilities for the various 5G operation models has to be based of the specified APIs. It needs to be assessed, if these APIs are sufficient for all three defined operation models and how implementation will use them, in order to avoid vulnerabilities in the management functions.

Besides these areas of vulnerability, virtualization vulnerabilities are also applicable, as well as generic vulnerabilities related to soft- and hardware maintenance and hardening. The following table provides a more exhaustive view on vulnerabilities of network slicing components.

Name	Description	Relevant toolbox measures	Threat categories
Vulnerabilities in implementation of NS security functionalities	Vulnerabilities in network segment negotiation procedures need to be secured in a standardized way to prevent malicious attacks, e.g. man-in-the-middle (MitM) attacks that could modify and downgrade slice capabilities.	TM01, TM02, TM05	NAA-EXPL, NAA-AAA
Service Based Vulnerabilities in Network Slicing Management	Network Slicing Management interface should be secured so that only authorized parties can create, alter, and delete network slice instances. If a malicious party gained access to an insecure management interface, or if it could replay or modify a valid message, then it would be able to spoof a genuine network manager to compromise slice security.	TM02, TM05	NAA-EXPL, NAA-AIL, NAA-AAA, NAA-DBLT, NAA-MND
Improper protection of Data and Information	Adequate security controls are needed to protect sensitive data stored, processed and transferred by NSI. Relevant vulnerabilities include: • Improper protection of Network Slice Instance supervision / reporting data; • Lack of / ineffective tamper-proofing of Network Slice Subnet Template (NSST).	TM02, TM05, TM07	NAA-AIL, NAA-MSH, NAA-DBLT
Vulnerable mechanisms for authentication and authorisation in Network Slicing Management	System functions should not be used without appropriate authentication and authorisation and authorisation checks. Relevant vulnerabilities include: • Improper slice-specific authentication mechanisms; • Lack of protection of NSSAI and home control; • Lack of protection of the User ID and credentials.	TM02, TM05	NAA-AAA, NAA-ARA
Improper hardening of network slicing components	All 5G components, including the network functions in service-based architecture, should be hardened in order to reduce their respective surface of vulnerability. Relevant vulnerabilities include: • Unnecessary or insecure services / protocols; • Unrestricted reachability of services; • Presence of unused software / functions / components; • Unrestricted remote login for privileged users; • Excessive file-system authorisation privileges; • Vulnerable OS configuration; • Vulnerable Web server configuration; • Improper separation of traffic.	TM01, TM02, TM07, TM09	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-MND, NAA-DBLT, FM, UD
Virtualisation vulnerabilities of relevant network slicing components	Vulnerabilities in the virtualisation layer may lead to risks such as unauthorised access to functions and data Virtualisation vulnerabilities include: • Vulnerabilities in virtualisation of OS layer; • Container vulnerabilities; • Vulnerabilities in function virtualization.	TM04	NAA-AVM, UD, FM
Insufficient or improper monitoring mechanism of Network Slice Instance (NSI)	Adequate mechanisms for collection and processing of security events should be in place. Relevant vulnerabilities include: • Insufficient / inadequate logging and auditing across NSI lifecycle; • Improper protection of security event log files; • Improper isolation of monitoring capabilities and data; • Improper or insufficient end-to-end monitoring capabilities for NSI.	TM02, TM05	NAA-{all}; UD, FM

A detailed list of network slicing vulnerabilities can be found in the Annex (see D Annex).

4.4 VULNERABILITY GROUPS FOR RADIO ACCESS NETWORK

In the security considerations of radio access network, we have identified the following areas of vulnerabilities:

Security of Ultra-Reliable Low-Latency Communication (URLLC): weaknesses in the implementation of QoS may impact low-latency requirements. Optimization issues of control and user plane will affect reliability and low latency of communications.

Vulnerability to Radio Jamming Attacks: an inherent weakness of wireless cellular communications is the free frequency space that allows for intentional or unintentional interferences. They can impact access of legitimate users and cause resilience issues in parts of the network.

Failure to meet General Security Assurance Requirements: a set of weaknesses will arise through the update requirements of various elements of RAN due to implementation of migration steps and the ability of early-deployed systems to comply with specification updates regarding security functions.

Optional nature of security controls for F1 interface: the optionality of security controls for this protocol may lead to security weaknesses in its implementation.

Besides these areas of vulnerability, virtualization vulnerabilities are also applicable, as well as generic vulnerabilities related to soft- and hardware maintenance and hardening. The table below provides a more exhaustive view on vulnerabilities of remote access network components.

Name	Description	Relevant toolbox measures	Threat categories
Incorrect implementation of gNB security functions	Relevant vulnerabilities in gNB implementation include: • Improper Ciphering and integrity checks of RRC-signalling; • Failure to ensure control plane data confidentiality protection over N2/Xn interface; • Improper ciphering of User data between UE and gNB; • Improper integrity protection and verification of user data; • Missing or improper replay protection mechanisms; • Lack of /improper mechanisms for prevention of bidding down at Xn-handover; • Improper Prevention of Key Reuse; • Improper mechanisms to enforce security policy.	TM02, TM09	NAA-AIL, NAA-AAA, NAA-UANI, NAA-SS, NAA-MND
Improper protection of Data and Information of gNB Components	Adequate security controls are needed for protecting sensitive data stored, processed and transferred by gNB components. Relevant vulnerabilities include: • Inadvertent disclosure of confidential system internal data; • Improper protection of data and information in storage; • Improper protection of data and information in transfer.	TM01, TM02, TM09	NAA-AIL, NAA-MSH, NAA-DBLT

Name	Description	Relevant toolbox measures	Threat categories
Improper protection of availability and integrity of gNB functionality	Adequate security controls are needed for upholding availability and integrity of gNB functions. Relevant vulnerabilities include: • Improper handling of overload situations; • Unrestricted boot memory devices; • Weaknesses in processing of unexpected input; • Lack of / improper mechanisms for software package integrity validation.	TM01, TM02, TM09	NAA-DoS, NAA-MSH, NAA-DBLT, UD
Vulnerable mechanisms for authentication and authorisation of gNB components	System functions should not be used without appropriate authentication and authorisation and authorisation checks. Relevant vulnerabilities include: • Improper authentication policy; • Insecure / insufficient authentication attributes, mechanisms and procedures; • Insecure authorisation and access control mechanisms.	TM01, TM02, TM09	NAA-DoS, NAA-AAA, NAA-ARA, NAA-DBLT
Improper session protection mechanisms of gNB components	Management interfaces and systems should provide adequate mechanisms for user session protection. Relevant vulnerabilities include: • Lack of logout function; • Lack of inactivity timeout mechanisms.	TM01, TM02, TM09	NAA-AAA, NAA-ARA, NAA-IFAS, NAA-DBLT
Insufficient or improper monitoring mechanisms of gNB components	Adequate mechanisms for collection and processing of security events should be in place. Relevant vulnerabilities include: • Insufficient / inadequate logging of security events; • Logs not transferred to centralized storage; • Improper protection of security event log files.	TM01, TM02, TM09	NAA-{all}, UD, FM
Vulnerabilities in Operating Systems supporting gNB components	Operating systems supporting gNB Components should provide a safe and stable environment for 5G Functions. Relevant vulnerabilities include: Improper / insufficient mechanisms to protect availability and integrity; Improper authentication and authorisation mechanisms.	TM01, TM02, TM09	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-DBLT, FM
Vulnerabilities in Web Servers supporting gNB components	Web servers serving functional and management services should provide adequate protection. Relevant vulnerabilities include: • Lack of or improper encryption of communication; • Failure to log webserver activity; • Improper HTTP User sessions protection; • Improper validation of HTTP input.	TM01, TM02, TM09	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-DBLT, FM
Vulnerabilities of network devices running gNB components	The components of gNB may be implemented on dedicated network devices, which must be adequately protected. Relevant vulnerabilities include: • Improper mechanisms for data and information protection; • Improper mechanisms for protecting availability and integrity.	TM01, TM02, TM09	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-MND, FM

Name	Description	Relevant toolbox measures	Threat categories
Improper hardening of gNB components	All 5G components should be hardened in order to reduce their respective surface of vulnerability. Relevant vulnerabilities include: • Unnecessary or insecure services / protocols; • Unrestricted reachability of services; • Presence of unused software / functions / components; • Unrestricted remote login for privileged users; • Excessive file-system authorisation privileges; • Vulnerable configuration of O.S. / Web server; • Improper separation of traffic.	TM01, TM02, TM07, TM09	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-MND, NAA-DBLT, FM, UD
Virtualisation vulnerabilities of relevant gNB components	Vulnerabilities in the virtualisation layer may lead to risks such as unauthorised access to functions and data. Virtualisation vulnerabilities include: • Vulnerabilities in virtualisation of OS layer; • Container vulnerabilities; • Vulnerabilities in function virtualization.	TM04	NAA-AVM, FM
Physical and environmental vulnerabilities of relevant gNB components	Improper physical security of gNB Components infrastructure may impact the overall security and performance of the system. Relevant vulnerabilities may include: • Improper physical security of telecommunications equipment rooms and equipment sited in partners' or users' premises; • Improper physical security of physically isolated operation areas; • Inadequate / defective security devices.	TM07	PA, FM, OUT, DIS
Vulnerability to Radio Jamming Attacks	As any wireless cellular networks, 5G networks are prone to radio interference. This inherent weakness can be used by adversary nodes to cause intentional interference and hinder legitimate user's communication over specific wireless channels. Jamming attacks are a special concern for mission-critical applications.	TM01	NAA-DoS

A detailed list of radio access network vulnerabilities can be found in the Annex (see E Annex).

4.5 VULNERABILITY GROUPS FOR NETWORK FUNCTION VIRTUALIZATION - MANO

In the security considerations of NFV - MANO, we have identified the following areas of vulnerabilities:

Management Interfaces / APIs: when developing management interfaces for the virtual functions, incomplete implementation of NVF security functions may lead to weaknesses related to access, storage and interception of network management data.

Localisation of functions: while physical functions of previous mobile networks have not allowed for mobility of functions, the introduced virtualization may lead to moving virtualized functions outside their original location, notably outside the perimeter of protecting measures/policies.

Besides these areas of vulnerability, virtualization vulnerabilities are also applicable, as well as generic vulnerabilities related to soft- and hardware maintenance and hardening. The following table provides a more exhaustive view on vulnerabilities of network function virtualization / MANO components.

Name	Description	Relevant toolbox measures	Threat categories
Service Based Vulnerabilities of NFV components	Service-Based-Interfaces of network functions should provide adequate protection of access and of data in transit. Relevant vulnerabilities include: • Improper transport layer protection for data transferred over internal interfaces to MANO; • Vulnerable authorisation mechanisms on authorisation server / resource server; • Improper message and session integrity checks on internal interfaces; • Vulnerabilities in legacy PNF; • Improper verification of identity and location of transmitting party on internal interfaces.	TM04	NAA-EXPL, NAA-AIL, NAA-AAA, NAA-DBLT, NAA-MND, EIH
Improper protection of Data and Information of NFV components	Adequate security controls are needed for protecting sensitive data stored, processed and transferred by NFV. Relevant vulnerabilities include: • Inability to provide proof of integrity of the data stores used for VM images; • Lack of encryption of control plane data; • Improper protection of data and information in storage; • Improper protection of data and information in transfer.	TM04	NAA-AIL, NAA-MSH, NAA-DBLT
Improper hardening of NFV components	All NFV components, should be hardened in order to reduce their respective surface of vulnerability. Hardening requirements must ensure that all the default configurations (including operating system software, firmware and applications) are appropriately set. Relevant vulnerabilities include: • Unnecessary or insecure services / protocols; • Unrestricted reachability of services; • Presence of unused software / functions / components; • Unrestricted remote login for privileged users; • Excessive file-system authorisation privileges; • Improper separation of traffic; • Improper patch management process; • Misconfiguration; • No mechanism to enforce geo-restrictions; • Vulnerabilities of NTP (VNF clock); • Improper hardening of MANO interfaces utilizing Service-Based Interfaces (SBI).	TM04	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-MND, NAA-DBLT, FM, UD
Virtualisation platform vulnerabilities for VNF	Vulnerabilities in the virtualisation layer may lead to risks such as unauthorised access to functions and data Virtualisation vulnerabilities include: • Inadequate access privileges in virtualized environments; • Improper key management system for encrypted virtual components; • Lack of mechanisms for ensuring a Hardware-Based Root of Trust (HBRT); • Vulnerabilities in cloud technology used for NFV implementation; • Hypervisor vulnerabilities conduct to cross-contamination of shared resources.	TM04, TM07	NAA-AVM, FM

Name	Description	Relevant toolbox measures	Threat categories
Physical security and environmental vulnerabilities of NFVI	Improper physical security of NFVI may impact the overall security and performance of the system. Relevant vulnerabilities include: • Improper physical security of telecommunications equipment rooms; • Improper physical security of physically isolated operation areas; • Inadequate / defective security devices.	TM04, TM06	PA, FM, OUT, DIS
Vulnerable mechanisms for authentication and authorisation of NFV Management	NFV Management and Orchestration should not be used without appropriate authentication and authorisation and authorisation checks. Relevant vulnerabilities include: • Improper authentication policy, such as unauthenticated access to system functions, use of generic accounts; • Insecure / insufficient authentication attributes, such as failure to protect accounts by at least one authentication attribute, active predefined authentication attributes; • Insecure password policy; • Insecure authentication mechanisms to management / maintenance interfaces; • Failure to block consecutive failed login attempts; • Insecure authorisation and access control mechanisms.	TM03, TM04	NAA-AAA, NAA-ARA, NAA-MSH, NAA-UANI, NAA-AVM
Insufficient or improper monitoring mechanisms of NFV	Adequate mechanisms for collection and processing of security events should be in place. Relevant vulnerabilities include: • Insufficient / inadequate logging of security events for MANO and NFVI; • Logs not transferred to centralized storage; • Improper protection of security event log files.	TM01, TM05	NAA, FM, UD

A detailed list of network function virtualization - MANO vulnerabilities can be found in the Annex (see F Annex).

4.6 VULNERABILITY GROUPS FOR SOFTWARE DEFINED NETWORKS

In the security considerations software defined networks, we have identified the following areas of vulnerabilities:

Control Plane: Recent practices to shift from single device controllers to distributed controllers, opens doors to control plane attacks. Such attacks are based on input buffer analysis to identify forwarding policy and eventually perform manipulations based on the analysis results.

Data Plane: As SDN data planes are just simple forwarding elements with no embedded intelligence, they may become targets of protocol attacks, exploiting protocol vulnerabilities in the forwarding devices.

Programmable Interfaces (APIs): The Southbound API may be misused for a series of attacks. These attacks are based on inferred flow rules in SDN through packet probing. Knowing the reactive rules, attackers can launch DoS attacks by sending numerous rule-matched packets which trigger packet-in packets to overburden the controller.

Besides these areas of vulnerability, virtualization vulnerabilities are also applicable, as well as generic vulnerabilities related to soft- and hardware maintenance and hardening. The table below provides a more exhaustive view on vulnerabilities of software defined networks components.

Name	Description	Relevant toolbox measures	Threat categories
Vulnerabilities in implementation of SDN security functionalities	Lack of functionality in the SDN control layer to support preventing flow rules confliction in order to avoid mandatory network policies from being bypassed.	TM01	NAA-MND, UD, FM
SBA/SBI vulnerabilities of SDN components	Service-Based-Interfaces of network functions should provide adequate protection of access and of data in transit. Relevant vulnerabilities include improper transport layer protection, improper authentication / authorisation mechanism for SDN controller, inadequate security of configuration data (including security policies and QoS policies) while being transported from SDN applications to the SDN controller over the application-control interface.	TM01	NAA-EXPL, NAA-AIL, NAA-AAA, NAA-DBLT, NAA-MND
Vulnerable mechanisms for authentication and authorisation of SDN components	SDN controller should not be used without appropriate authentication and authorisation checks. Relevant vulnerabilities are related to improper authentication and/or authorisation mechanism for SDN controller or defective implementations of these mechanisms.	TM01, TM03	NAA-AAA, NAA-ARA, NAA-MSH, NAA-UANI
Improper hardening of SDN components	All SDN components, should be hardened in order to reduce their respective surface of vulnerability. Relevant vulnerabilities include: • Operating system vulnerabilities; • Software vulnerabilities of SDN controller; • Improper cryptographic key management mechanisms or use of weak algorithms; • Lack of, or improper DoS protection mechanisms.	TM01, TM07	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-MND, NAA-DBLT, FM, UD
Insufficient or improper monitoring mechanisms of SDN components	Improper monitoring of SDN controller may lead to attacks or failures going undetected and therefore not mitigated. Improper hardware monitoring may compromise network security or bring down the SDN network.	TM05	NAA-{all}, FM, UD
Virtualisation vulnerabilities of relevant SDN components	Vulnerabilities in the virtualisation layer may lead to risks such as unauthorised access to SDN resources. Cloud solutions used for SDN implementation may lead to vulnerabilities specific to cloud technology.	TM01, TM07	NAA-AVM, FM
Physical security vulnerabilities of SDN	Improper physical security of SDN may impact the overall security and performance of the system. Relevant vulnerabilities may include unprotected Data Centre Interconnection channels, improper physical secure perimeter or isolation between tenants.	TM06	PA, FM, OUT, DIS

A detailed list of software defined networks vulnerabilities can be found in the Annex (see G Annex).

4.7 VULNERABILITY GROUPS FOR MULTI-ACCESS EDGE COMPUTING

In the security considerations of multi-access edge computing, we have identified the following areas of vulnerabilities:

Virtualization and containerization: Being based on virtualization and containerization, MEC may be vulnerable to a number of threats emerging from these technologies. Examples are: possible contamination of shared hardware resources, abuse of privilege elevation vulnerabilities of containers with higher levels of privileges, dependencies to central orchestration functions, high data and session volumes that can be subject of attacks, use of open-source APIs.

Physical security: flaws in physical security of MEC hardware may render such infrastructures vulnerable to physical attack. Given the fact of higher geographical distribution of such infrastructures, keeping a uniform level of physical security will be a challenge.

Application-Programming Interfaces (APIs): Though a dedicated architecture (CAPIF) is proposed to cope with access to APIs, it has to be ensured that these provisions are followed during API design and implementation phases. As being exposed to user access, usually such APIs are subject to multiple attacks.

Regulatory issues: European regulation (NIS-Directive), foresees an isolation of physical and logical components of critical services from services with low criticality. The implementation of requirement in MEC may lead to vulnerabilities of low criticality services, as they are going to be operated in a security domain with less security functions.

The table below provides a more exhaustive view on vulnerabilities of MEC components.

Name	Description	Relevant toolbox measures	Threat categories
Vulnerabilities in implementation of MEC security functionalities	Relevant vulnerabilities in MEC implementation include improper for collection, secure storage and transmission of charging-related information.	TM01, TM02	NAA-DoS, NAA-AIL,NAA-LIFA, NAA-DBLT, NAA-ARA, NAA-MSH, NAA-SHE, NAA-IFAS
Vulnerabilities in the Service-Based Interfaces of MEC components	Service-Based-Interfaces of network functions should provide adequate protection of access and of data in transit. Relevant vulnerabilities include improper implementation of MEC / CAPIF APIs, improper transport layer protection for data transferred over internal interfaces and improper verification of identity and access control to authorized mobile edge applications.	TM01, TM03	NAA-EXPL, NAA-AIL, NAA-AAA, NAA-DBLT, NAA-MND EIH, FM
Improper protection of Data and Information of MEC components	Adequate security controls are needed for protecting sensitive data stored, processed and transferred by MEC applications. The mobile edge platform shall only provide a mobile edge application with the information for which the application is authorized.	TM01, TM03	NAA-AIL, NAA-MSH, NAA-DBLT

Name	Description	Relevant toolbox measures	Threat categories
Vulnerabilities in Operating Systems supporting MEC components	Operating systems supporting MEC Host should provide a safe and stable environment for MEC Applications. Relevant vulnerabilities include: • Improper / insufficient mechanisms to protect availability and integrity; • Improper authentication and authorisation mechanisms.	TM01, TM07	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-DBLT, FM
Improper hardening of MEC components	All MEC components, should be hardened in order to reduce their respective surface of vulnerability. Hardening requirements must ensure that all the default configurations (including operating system software, firmware and applications) are appropriately set. Relevant vulnerabilities include: • Unnecessary or insecure services / protocols; • Unrestricted reachability of services • Presence of unused software / functions / components; • Unrestricted remote login for privileged users; • Excessive file system Authorisation privileges; • Improper separation of traffic; • Improper patch management process • Misconfiguration; • Lack of or improper DDoS Protection mechanism.	TM01, TM07	NAA-MAL, NAA-DoS, NAA-ARA, NAA-AAA, NAA-ESH, NAA-MSH, NAA-UANI, NAA-MND, NAA-DBLT, FM, UD
Software vulnerabilities in MEC applications	Vulnerabilities in MEC Applications may be used as an entry point for attacks aiming at exploiting other MEC components or internal interfaces. Relevant vulnerabilities include unauthorized access to data, elevation of privileges or cloud intrusion.	TM01, TM02	NAA-EXPL, NAA-ARA, NAA-AAA, NAA-ESH, NAA-DBLT
Vulnerabilities of the MEC virtualization platform	Vulnerabilities in the virtualization platform include inadequate isolation of resources in operating system / container layers and vulnerabilities specific to cloud technologies widely used in MEC implementations.	TM01, TM02	NAA-AVM, FM
Physical security and environmental vulnerabilities of MEC hosts	Improper physical security of MEC host may impact the overall security and performance of the system. Relevant vulnerabilities include: • Improper physical and environmental security of edge computing facilities; • Improper security monitoring of edge computing facilities; • Insecure service environment.	TM06	PA, FM, OUT, DIS
Vulnerable mechanisms for authentication and authorisation of MEC components	MEC authentication functions – LCM Proxy and MEC Orchestrator – should not be used without appropriate authentication and authorisation and authorisation checks. Relevant vulnerabilities include: • Improper authentication policy, such as unauthenticated access to system functions, use of generic accounts; • Insecure / insufficient authentication attributes, such as failure to protect accounts by at least one authentication attribute, active predefined authentication attributes; • Insecure password policy; • Insecure authentication mechanisms to management / maintenance interfaces; • Failure to block consecutive failed login attempts; • Insecure authorisation and access control mechanisms.	TM01, TM03	NAA-AAA, NAA-ARA, NAA-DoS, NAA-DBLT

Name	Description	Relevant toolbox measures	Threat categories
Insufficient or improper monitoring mechanisms of MEC components	Adequate mechanisms for collection and processing of security events should be in place. Relevant vulnerabilities include: • Insufficient / inadequate logging of security events for MEC App and MEC host; • Logs not transferred to centralized storage; • Improper protection of security event log files.	TM01, TM05	NAA-{all}, FM, UD

A detailed list of multi-access edge computing vulnerabilities can be found in the Annex (see H Annex).

4.8 VULNERABILITY GROUPS FOR SECURITY ARCHITECTURE

Given the fact that vulnerabilities in all zoom-ins cover security issues of the 5G architecture in a horizontal manner, no additional security vulnerabilities have been developed for the components of the security zoom-in. Hence, it can be considered that the entire set of vulnerabilities assessed for all other zoom-ins cover the full set of security vulnerabilities.

4.9 VULNERABILITY GROUPS FOR PHYSICAL INFRASTRUCTURE

In the security considerations of physical infrastructure, we have identified some areas of vulnerabilities. Given the fact that the physical infrastructure is the common basis for the implementation of all other zoom-ins, the assessed physical vulnerabilities are derived by the vulnerabilities of all zoom-ins by means of their relevance to the physical components. Hence, the vulnerabilities below draw consequences of the vulnerabilities mentioned in other zoom-ins, by concentrating on their physical aspects:

Impact of virtualisation: The physical measures/controls will need to be derived by and be complementary to weaknesses encountered by the implementation of functions in containerized and virtualized environments (see also vulnerabilities of MEC in section 4.7 above). This will mainly impact physical availability measures for the concerned functions.

General physical security considerations: General physical measures need to be developed based on vulnerabilities and resulting risk-exposure that are related to the operational needs, supply chain of various components (delivery, operation, implementation, maintenance) and criticality of services. Given the large number of roles involved in 5G infrastructures, the identification of physical vulnerabilities requires a holistic approach.

Threats to edge cloud computing resources: attack surface reduction of MEC services will rely on physical measures taken for the relevant components (see also vulnerabilities in section 4.7 above).

Vulnerability of wireless frequencies to jamming attacks: as a high number of wireless connections are involved in the communication within the 5G infrastructure, both in the public and non-public domain, physical measures for the reduction of impact of jamming attacks need to be taken into account, especially on availability of communication channels.

The following table provides a more exhaustive view on vulnerabilities of physical infrastructure.

Name	Description	Relevant toolbox measures	Threat categories
Improper physical security of communication centres	Communication centres should provide a full set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters. Failure to do so may lead to unauthorised access, destruction of assets and impairment of operations.	TM06	PA, DIS, OUT, NAA-CSVS
Improper physical security of telecommunications equipment room	Telecom equipment rooms should provide a risk-calibrated set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters. Failure to do so may lead to unauthorised access, destruction of assets and impairment of operations.	TM06, TM11	PA, DIS, OUT, NAA-CSVS
Improper physical security of physically isolated operation areas	Remote equipment facilities should provide a set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters, taking into account its remoteness and lack of human presence. Failure to do so may lead to unauthorised access, destruction of assets and impairment of operations.	TM06, TM11	PA, DIS, OUT, FM, NAA-CSVS
Improper physical security of equipment sited in other carrier's or partner's premises	Equipment located in third party facilities rooms should be protected using a risk-calibrated set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters. Failure to do so may lead to unauthorised access, destruction of assets and impairment of operations.	TM06, TM11	PA, DIS, OUT, NAA-CSVS
Vulnerability to Radio Jamming Attacks	Wireless cellular networks are inherently vulnerable to interference. This weakness can be used to cause intentional interference and hinder legitimate user's communication over specific wireless channels. 5G improves resilience against jamming attacks over the 4G LTE, but remains vulnerable to customised attacks. Jamming attacks are a special concern for mission-critical applications, in particular for their availability.		NAA-DoS
Vulnerabilities related to virtualisation technologies	Softwarisation and virtualization of functions only increase availability and integrity requirements for shared physical resources, some of them placed in remote locations. Relevant vulnerabilities include: • Improper protection of access to physical interfaces; • Shared resource contamination; • Vulnerable mechanisms for Hardware-Based Root of Trust (HBRT); • Hypervisor vulnerabilities conduct to cross-contamination of shared resources; • Improper availability arrangements for hardware infrastructure.	TM04, TM06	NAA-AVM, FM

A detailed list of physical infrastructure vulnerabilities can be found in the Annex (see I Annex).

4.10 VULNERABILITY GROUPS FOR IMPLEMENTATION OPTIONS

In the security considerations of 5G implementation options – migration paths, we have identified the following areas of vulnerabilities:

Risks related to legacy technologies: these risks materialize through exploitation of vulnerabilities that are concerned with mismatches of functionalities of non-standalone 5G networks (NSA) to the current specifications. An example hereto are the use of the LTE Evolved Packet Core (EPC) and the LTE control panel. In this way, for NSA 5G networks, threats and vulnerabilities of the LTE technology will persist.

Roaming: during migration, 4G roaming is being used for 5G. This roaming does not include the new 5G security functions, while maintaining Diameter, SIP/VoLTE and possibly SS7. These protocols are vulnerable to eavesdropping and tracking.

Security update gap between new security requirements and deployment of updated versions of network functions in operational systems. Two major factors are relevant for this gap: a) vendors' responsiveness in issuing and validating new versions of the network functions that address the updated requirements, and b) timeliness and effectiveness of MNO processes to update. This may lead to vulnerabilities in operational NSA 5G infrastructures.

Besides these areas of vulnerability, virtualization vulnerabilities are also applicable to implementation options. The table below provides a more exhaustive view on vulnerabilities of components used within 5G implementation options.

Name	Description	Relevant toolbox measures	Threat categories
Vulnerabilities of legacy technologies	Vulnerabilities inherited from the LTE system include: • Lack of integrity protection of over-the-air User Plane traffic; • Exposure of international mobile subscriber identities (IMSI) over the air; • Weaker cryptographic algorithms.	TM05	NAA-AIL, NAA-SGN, EIH
Improper implementation of updated security functions	The updated requirements for LTE critical components involved in Non-standalone implementations include security controls for known vulnerabilities and allow interoperability by the 5G Components. Failure to meet assurance specification as defined in the Security Assurance Specification for critical components leave open vulnerabilities. The affected components are: • Vulnerabilities in MME implementation; • Vulnerabilities in evolved Node B (eNB) implementation.	TM02	NAA-{all}, EIH, UD, FM

Name	Description	Relevant toolbox measures	Threat categories
Vulnerabilities in the technical baseline of EPC+ functions	Similar to 5G Core functions, the security of EPC+ functions relies on a secure technical baseline. Vulnerabilities relevant for 5G Core functions as detailed in the respective section apply similarly. Relevant vulnerabilities include: • Improper protection of Data and Information of EPC+ components; • Improper protection of availability and integrity of EPC+ components; • Vulnerable mechanisms for authentication and authorisation of EPC+ components; • Improper session protection mechanisms of EPC+ components; • Insufficient or improper monitoring mechanisms of EPC+ components; • Vulnerabilities in Operating Systems supporting EPC+ components; • Vulnerabilities in Web Servers supporting EPC+ components; • Vulnerabilities of network devices running EPC+ components; • Improper hardening of EPC+ components.	TM01, TM02	NAA-{all}, EIH, FM, UD
5G New Radio Vulnerabilities	Vulnerabilities for 5G New Radio components are referred in the 5G RAN Vulnerabilities section.	TM02	See section above
SBA/SBI vulnerabilities of components	Service-Based-Interfaces are a common feature of 4G and 5G NR components. Relevant vulnerabilities include: • Improper transport layer protection, such as incorrect TLS profile and improper authentication mechanisms; • Vulnerable authorisation mechanisms on service access. Detailed information is presented in the 5G Core Section.	TM01	NAA-EXPL, NAA-AIL, NAA-AAA, NAA-DBLT, NAA-MND EIH, FM
Virtualisation Vulnerabilities	One of the main implementation scenarios focuses on building a new virtualized EPC network to support the Non-Standalone implementation. In this scenario, virtualization vulnerabilities are highly relevant. Virtualisation vulnerabilities are detailed in Section NFV and 5G Core.	TM04	NAA-AVM, FM
LTE Roaming vulnerabilities	5G NSA roaming is essentially 4G roaming. From a security perspective, a 5G NSA roaming connection introduces no new protections since it continues to use Diameter, SIP/VoLTE and possibly SS7. Relevant vulnerabilities may include: • Improper protection of Data and Information of EPC+ components; • SS7 Vulnerabilities; • Diameter vulnerabilities; • VoLTE vulnerabilities[84].	TM01, TM02, TM05	NAA-AIL, NAA-SGN, EIH

A detailed list of implementation options – migration path vulnerabilities can be found in the Annex (see J Annex).

[84] David Rupprecht and Katharina Kohls and Thorsten Holz and Christina Popper, Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE, 29th USENIX Security Symposium Proceedings, 2020. isbn 978-1-939133-17-5, pages 73-88, accessed October 2020.

4.11 VULNERABILITY GROUPS FOR PROCESSES

In this section we develop a set to vulnerabilities/weaknesses that arise from the absence of processes pertinent to life-cycle maintenance of systems and applications of the entire 5G infrastructure. As mentioned in section 3.13, the processes considered are MNO life-cycle processes, vendor development and product life-cycle, as well as security assurance.

Though we have not developed any security considerations in section 3.13 – as we did for the 3GPP specified components - in the discussion below we enlist weaknesses that may arise from the absence of maintenance processes for life-cycle considerations regarding the entire 5G infrastructure.

4.11.1 MNO processes

Security of the 5G System is achieved and maintained by upholding security objectives across the entire lifecycle of the system, in particular from the side of Mobile Network Operator (MNO). In this section, we have identified operational process weaknesses that can directly impact the security of the 5G System. As a reference model for operational processes, we used the eTOM Business Framework[85] which defines comprehensive, industry-agreed, multi-layered view of the key business processes in the Telecommunications sector. Any other process framework could be used for this purpose.

Name	Description	Relevant toolbox measures	Threat categories
Improper Resource Capability Delivery Processes	Process weaknesses that may directly impact the security of 5G system include: • Improper processes to map and analyse resource requirements; • Failure to adapt resource support and operations; • Inability to capture resource capability shortfalls; • Improper Resource Capabilities design and management of delivery; • Improper management of Handover to Resource Operations.	TM01, TM09, TM10	NAA-CSVS, NAA-AIL, NAA-DBLT, EIH, PA, UD, FM, OUT, DIS
Improper Party Tender Management Processes	Process weaknesses that may directly impact the security of 5G system include: • Inadequate definition of sourcing requirements; • Improper process to determine Potential Suppliers/Partners; • Inadequate management of the Tender Process.	TM08, TM09, TM10	NAA-CSVS, NAA-AIL, NAA-DBLT, EIH, PA, UD, FM, OUT, DIS
Improper Resource Development & Retirement Processes	Process weaknesses that may directly impact the security of 5G system include: • Improper control of Detailed Resource Specifications development; • Inadequate coordination of resource development; • Improper management of resource deployment; • Improper storage media sanitisation; • Improper management of resource exit.	TM01	NAA-CSVS, NAA-AIL, NAA-DBLT, EIH, PA, UD, FM, OUT, DIS

[85] http://casewise.tmforum.org/evolve/statics/frameworx/#cwtype=index&cwview=home, accessed November 2020.

Name	Description	Relevant toolbox measures	Threat categories
Improper Resource management and operation Support & Readiness processes	Process weaknesses that may directly impact the security of 5G system include: • Improper processes to support resource provisioning; • Improper processes to support resource performance management; • Improper processes to support resource trouble management; • Improper management of resource inventory.	TM01	NAA-CSVS, NAA-AIL, NAA-DBLT, EIH, PA, UD, FM, OUT, DIS
Improper Party Agreement processes	Process weaknesses that may directly impact the security of 5G system include: • Insufficient / improper definition of relevant operational and security clauses in agreements with suppliers and partners; • Improper management of contract variations.	TM08	NAA-CSVS, NAA-AIL, NAA-DBLT, EIH, PA, UD, FM, OUT, DIS
Improper Party Support processes	Process weaknesses that directly impact the security of 5G system include: • Improper processes to support Party Requisition Management; • Support Party Performance Management; • Support Party Interface Management.	TM01	NAA-CSVS, EIH, PA, UD, FM, OUT, DIS
Improper resource provisioning processes	Process weaknesses that directly impact the security of 5G system include: • Improper processes for resource allocation and installation; • Improper / obsolete processes to Configure & Activate Resources; • Improper tracking & management of resource provisioning.	TM01, TM02	NAA-CSVS, NAA-AIL, NAA-DBLT, EIH, PA, UD, FM, OUT, DIS
Resource Trouble Management	Process weaknesses that directly impact the security of 5G system include: • Improper survey and analysis of resource trouble; • Improper processes for localisation of resource trouble; • Improper processes for correction and resolution of resource trouble.	TM05	NAA-CSVS, NAA-AIL, NAA-DBLT, EIH, PA, UD, FM, OUT, DIS
Resource data collection & distribution	Process weaknesses that directly impact the security of 5G system include: • Improper processing of management and Security Information & Data; • Inadequate processes for audit of Management and Security Data Collection & Distribution.	TM05	NAA-CSVS, NAA-AIL, NAA-DBLT, EIH, PA, UD, FM, OUT, DIS
Resource Performance Management	Process weaknesses that directly impact the security of 5G system include: • Improper monitoring of resource performance; • Improper processes for controlling resource performance.	TM05	UD, FM, OUT

Name	Description	Relevant toolbox measures	Threat categories
Party Interaction Management	Process weaknesses that directly impact the security of 5G system include improper Tracking, Management and Handling of Interaction with suppliers and partners.	TM05	NAA-CSVS, NAA-AIL, NAA-DBLT, EIH, PA, UD, FM, OUT, DIS
Party Problem Handling	Process weaknesses that directly impact the security of 5G system include improper processes to Receive, Assess and Track problems related to relevant Suppliers/Partners, as well as failure to capture trends in problems related to third-parties.	TM05	UD, FM, OUT
Party Performance Management	Process weaknesses that directly impact the security of 5G system include improper processes to Monitor & Control Supplier/Partner Performance and to track & manage party performance resolution.	TM05	NAA-CSVS, UD, FM, OUT
Party Inventory Management	Process weaknesses that directly impact the security of 5G system include improper processes for manage S/P Inventory Repository and to manage and administer S/P Inventory.	TM05	NAA-CSVS, NAA-AIL, NAA-DBLT, EIH, PA, UD, FM, OUT, DIS
Business Continuity Management	Process weaknesses that directly impact the security of 5G system include failure to update and adapt Business Continuity plans, Infrastructure Recovery plans and Incident Management plans.	TM11	OUT, DIS
Fraud Management	Process weaknesses that directly impact the security of 5G system include failure to adapt fraud management policies and controls.	TM05	NAA-IFAS, LEG
Regulatory Management	Process weaknesses that directly impact the security of 5G system include failure to identify and comply with updated compliance requirements	TM05	LEG
Insurance Management	Process weaknesses that directly impact the security of 5G system include failure to identify insurable risks.	TM05, TM11	NAA-CSVS, EIH, PA, UD, FM, OUT, DIS, LEG
Security Management	Failure to adapt security management processes to new technologies, business models and associated risks will directly impact the security of the 5G System.	TM05, TM11	NAA, EIH, PA, UD, FM, OUT, DIS, LEG

A detailed list of vulnerabilities emerging from improper operational processes at the level of mobile network operator can be found in the Annex (see K Annex).

4.11.2 Vendor, development and product life-cycle processes

Vendor Development and Product Lifecycle covers all aspects potentially impacting a Network Product's lifetime. Vulnerabilities in vendor development and product lifecycle processes impact directly the security of 5G system components. While some vulnerabilities are directly connected to a specific phase in the Product Lifecycle, other process vulnerabilities are relevant for the entire Development and Product lifecycles.

Name	Description	Relevant toolbox measures	Threat categories
Design Phase Vulnerabilities	Failure to apply security architectural and security design principles and follow them throughout the entire development lifecycle leads to structural security problems that imperil the security of the components and of the 5G system.	TM08	NAA-EXPL, UD, FM
Implementation Phase Vulnerabilities	Relevant implementation phase vulnerabilities include: • Ineffective code governance and improper code review; • Vulnerabilities in Build process and environment.	TM08	NAA-CSVS, UD, FM
Testing Phase Vulnerabilities	The relevant vulnerability in the testing phase refers to lack of or improper security testing. This in turn leaves the network products exposed to vulnerabilities and unexpected and unspecified behaviour.	TM08	NAA-EXPL, NAA-DBLT, UD, FM
Release Phase Vulnerabilities	Relevant release phase vulnerabilities include: • Improper verification of software integrity; • Ambiguous software release identifiers; • Inaccurate / obsolete documentation.	TM08	NAA-EXPL, NAA-DBLT, UD, FM
Operation Phase Vulnerabilities	Relevant operation phase vulnerabilities include: • Failure to provide a security contact; • Insufficient vulnerability awareness; • Ineffective vulnerability remedy process; • Unreliable communication of software fixes.	TM08, TM11	NAA-EXPL, NAA-DBLT, NAA-EXPL, NAA-DBLT, UD, FM
Vulnerabilities relevant for the entire lifecycle	The following vulnerabilities impact the security of network product across its entire development and product lifecycle: • Improper version control system; • Improper change management process; • Insufficient security education and awareness of staff; • Ineffective Information Security Management System.	TM11	NAA-EXPL, NAA-DBLT, NAA-EXPL, NAA-DBLT, UD, FM

A detailed list of vulnerabilities emerging from improper vendor, product, development life-cycle processes can be found in the Annex (see L Annex).

4.11.3 Security assurance processes

A solid and objective assessment process can contribute towards identification baseline security requirements to be met for network products and the implemented processes. This is an additional dimension to technological and operational security mitigation controls, contributing towards the assurance of their implementation levels.

Following conclusions of the Toolbox, security assurance processes can only help mitigate certain risks to a limited extent given the constant need to update products and systems-making it impossible to create 'trust' through these mechanisms only. Hence, assurance

processes and related measures need to be seen in combination to implementation of technical and operational ones.

In this context, a series of vulnerabilities must be taken into consideration when assessing the fitness for purpose of a security assurance scheme for 5G Systems:

Name	Description	Relevant toolbox measures	Threat categories
Standardisation vulnerabilities	Agreed-upon and recognized standards are paramount for ensuring a security baseline. Potential vulnerabilities include: • Obsolescence of standards; • Alignment of standards; • Missing security requirements reference for verticals.	TM02, SA03, SA04	NAA-{all}, UD, FM
Accreditation vulnerabilities	Accreditation provides trust in the results of conformity and security assessment results. Potential vulnerabilities include: • Recognition of accreditation scheme; • No alignment with internationally recognized standards for accreditation and conformity assessment; • Lack of control by regulatory and supervisory bodies.	TM09, TM10, SA05	NAA-{all}, UD, FM, LEG
Conformity Assessment vulnerabilities	Security assessment activities and their results need to be trustworthy, relevant and sufficient for meeting the overall security objectives and regulatory requirements. Potential vulnerabilities include: • Not appropriate to address risks stemming from non-technical risks related to the supplier's risk profile; • No common reference for security requirements for Mobile Network Operators; • No security evaluation of the operational environment; • Insufficient assurance of environmental assumptions; • Certification overhead and relevance; • No assessment scheme for evaluation of virtualized products; • Insufficient security assurance level; • Re-use of evidence created by conformity assessment bodies.	TM09, TM10, SA05, SA06	NAA-{all}, UD, FM, LEG

A detailed list of vulnerabilities emerging from the absence of an effective security assurance process can be found in the Annex (see M Annex).

5. ASSETS

5.1 ASSET CLASSIFICATION AND MAPPING

One critical and initial step in any threat assessment is to identify and classify the most sensitive assets that, if compromised, may pose a certain level of risk to an individual or organisation. These activities are part of the asset security domain that focus on collecting and handling the information required to define the model and a strategy to protect the attribute and value it represents. In the 5G context, the monetisation of asset attributes such as network slicing, cloud and Edge computing are in the centre of the value concept of this new generation of mobile communications.

The 5G architecture considers four main areas that includes user equipment, radio access network, core network and data network. In this report, we cover two main areas which are the most significant on 5G evolution: the core network and radio access. We leave user equipment and data network for future analysis. In the context of this report, we consider various asset categories that relate to critical components or entities in a 5G network. These components and entities are of a heterogeneous nature and require differentiated asset security strategies from owners and/or stakeholders. For example, the interoperability, multi-level and seamless usage may result in unauthorised and opportunistic access to the network.

We also identify differentiated roles assumed by various actors (presented in chapter2.1 above2.1 of this report), in the definition and implementation of these asset security strategies. These however, may change in importance, sensitivity and relevance over time, depending on the product or service lifecycle stage. Each mapped asset may expose certain vulnerabilities or weaknesses during the lifecycle that if exploited may pose a threat to the confidentiality, integrity and availability (CIA triad) of systems and data transmitted of parts or the entire 5G network.

The scope of this document is not to report on a specific asset inventory but to direct the reader on where to look when conducting such exercises. The responsibility of mapping the sensitive assets of network relays with the operator since it depends on the technology used, network product implemented, processes adopted, type of organisations and the services offered. A mapping of assets and the CIA Triad is presented Table 3.

In the first version of the ENISA Threat Landscape Report for 5G Networks (ETL5G), we prepared a categorisation of assets based on a high-level architecture presented in the document. We also review the importance and relevance of these assets to the CIA triad properties. The categorisations considered a specific definition of assets based on a GNP (Generic Network Product) class description. A GNP is a class of network products that implement a common set of 3GPP-defined functionalities for a particular component. According to 3GPP, the critical assets of GNP to be protected are:

- User account data and credentials (e.g. passwords);
- Log data;
- Configuration data, e.g. GNP's IP address, ports, VPN ID, Management Objects (e.g. user group, command group) etc.
- Operating System (OS), i.e. the files that make up the OS and its processes (code and data);

- GNP Application;
- Sufficient processing capacity: that processing powers are not consumed close to limits;
- Hardware, e.g. mainframe, board, power supply unit etc.
- The interfaces of GNP to be protected and which are within SECAM scope: for example
    - Console interface, for local access: local interface on MME
    - OAM interface, for remote access: interface between MME and OAM system
    - GNP Software: binary code or executable code

All the above critical assets from release 15 of the 3GPP Security Assurance Specification (SCAS) fit in the asset categories defined in the first edition of the ETL5G.

In this edition, we update the asset categorisations based on new requirements introduced by release 16 of the 3GPP technical specifications and the new 5G use cases. We classified the sensitive assets considering the stages of the implementation lifecycle using the eTOM – enhanced Telecom Operation Map[86] as a guide. We assume that certain assets gain a particular importance or sensitiveness during different stages of the GNP lifecycle. We also update the information about stakeholders from the previous edition and correlate it with the new asset categorisation.

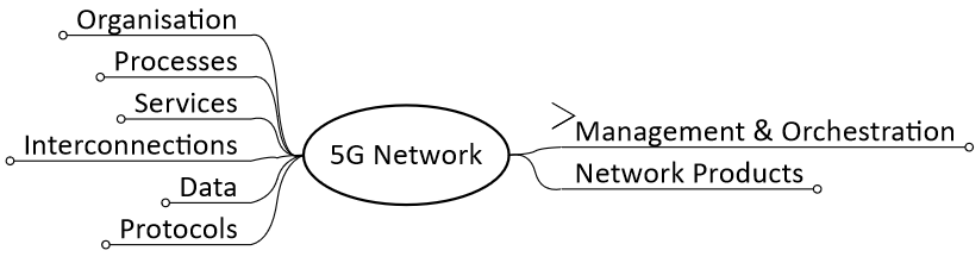
5.2 NEW ASSET CATEGORIES

The following 5G asset categories derive from the high-level architecture presented in chapter 3.2 of this report and classification based on release 16 of the 3GPP technical specifications. The high number of sensitive assets identified from the architecture resulted in a complex and large diagram, making it difficult to read and display in this report. We use part of the diagram to depict each asset group. The diagram is structured using asset groups according to their exposure to threats. By taking into account the role of assets in maintaining the security-related properties of confidentiality, availability and integrity (known as CIA triad), an initial assessment of their importance has been developed. In doing so, the emphasis has been given to asset groups responsible for maintaining the overall security and availability of the 5G infrastructure and that are known targets of cyber-attacks.

This new categorisation introduces new groups at the lower or more detailed level of the asset classification, deriving from the requirements of release 16. Another important aspect is the definition of a high-level classification introducing main categories. These main categories, depicted in Figure 15, include components and entities from management & orchestration, network products, protocols, data, interconnections, services, processes and organisation. The main advantage of having this new upper level is to allow the possibility to define different asset security strategies depending on the characteristics of each asset group. The assets in these groups share important characteristics such as type of vulnerabilities, stakeholders and controls. These characteristics change quite substantially and require differentiated approaches in the asset security strategy. A complete diagram of the asset map is present in Figure in Annex A.

[86] http://casewise.tmforum.org/evolve/statics/frameworx/#cwtype=index&cwview=home, accessed November 2020.

Figure 15: Main categories of 5G network assets



Network Products: This main category includes network planes, functions and elements. These derive into multiple asset groups that could be found in the previous asset mapping like core functions, physical infrastructure, security, software-defined networking (SDN), among others. The main category is a core part of the 5G architecture and one of the most critical in any 5G asset mapping.

Figure 16: 5G Asset groups from the Network Products category

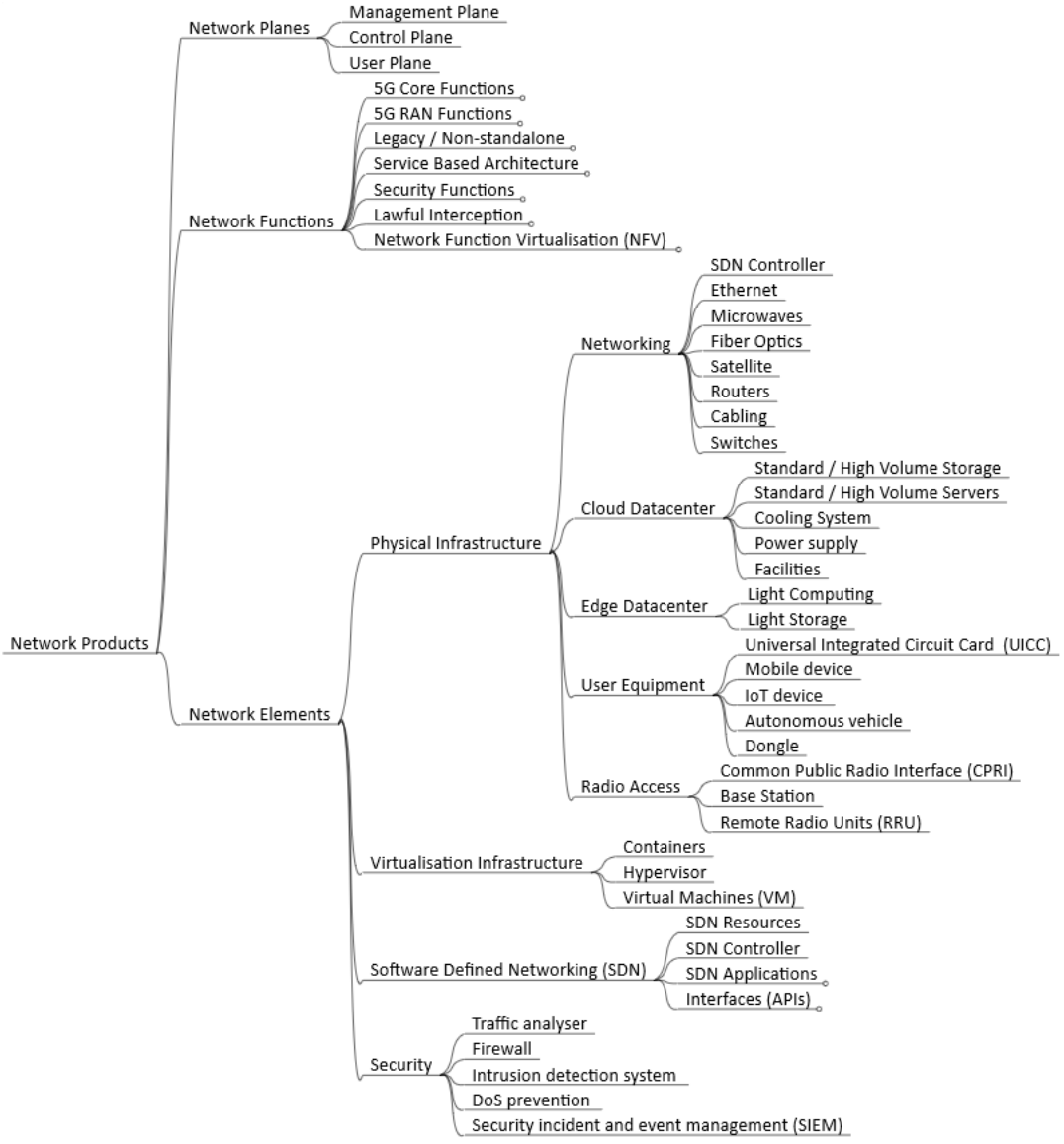
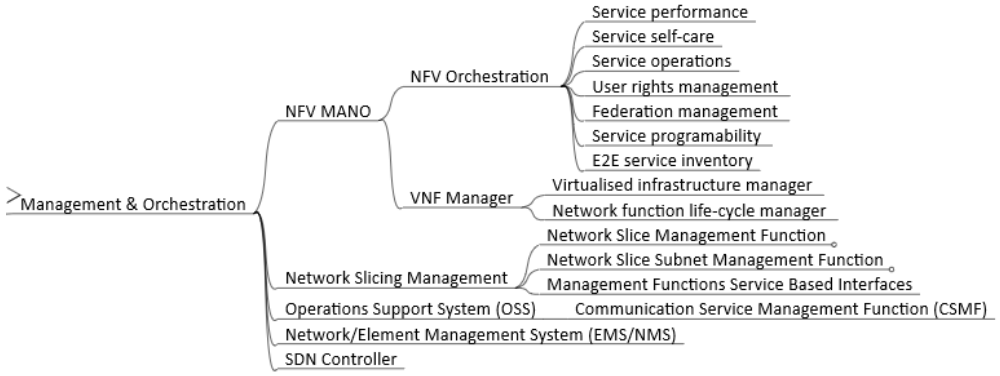


Figure 16 depicts the second, third and fourth level groups of the Network Products asset category. However, not all levels are displayed; hence, we present the full diagram at ENISA website[87] using an interactive tool to explore the inwards of the different asset categories.

Management and orchestration: This main category includes the management of network functions, network slicing, operations support system, network/element (EMS/NMS) and SDN Controller. Figure 17 depicts the different asset groups of MANO.

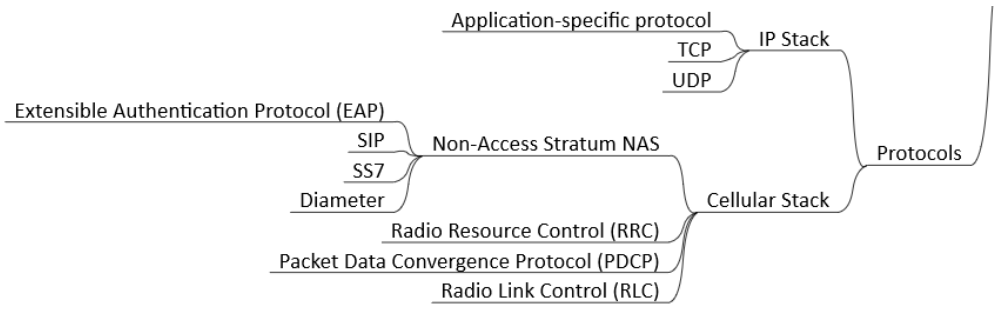
MANO is the most vital part of the 5G infrastructure since is responsible for controlling the entire set of network functions, their virtualisation and entire software lifecycle related hereto. The main parts of MANO are the Network Function Virtualisation (NFV) orchestrator, the Virtual Network Function (VNF) manager, and the virtualised infrastructure manager. Given its important role, MANO is going to be exposed to numerous attacks with potential major impact on the entire managed 5G infrastructure environment. The assets of MANO are also depicted in detail in the corresponding 'Zoom-in' in the 5G architecture chapter 3.5.

Figure 17: Asset groups from the Management & Orchestration category



Protocols: This main category of 5G assets include IP and cellular stack. ENISA reviewed the legacy protocols SS7 and Diameter in a study conducted in 2018[88]. Early generations of mobile networks such as 2G and 3G rely on these protocols that still contain many critical vulnerabilities yet to be resolved. 5G networks will need to support SS7 and Diameter for the foreseeable future (decades) in order to maintain global connectivity (roaming). Figure 18 depicts the various groups of assets associated with protocols typically implemented in a 5G Network.

Figure 18: Asset groups from the Protocols category

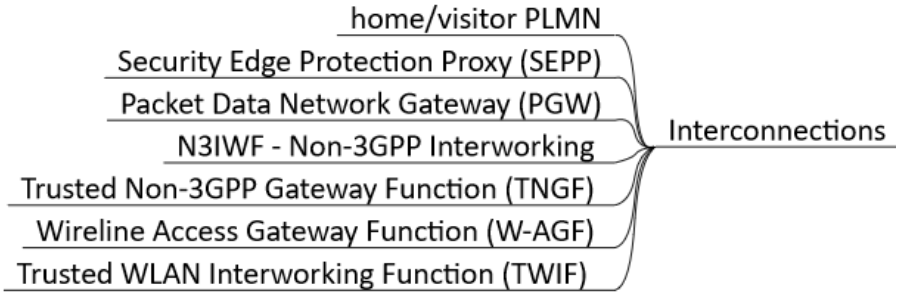


Interconnections: This main category of 5G assets include home/visitor PLMN, security Edge Protection Proxy (SEPP), packet data network gateway (PGW), N3IWF - Non-3GPP

[87] https://www.enersec.net/Asset_MM/ accessed October 2020.
[88] https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g, accessed October 2020.

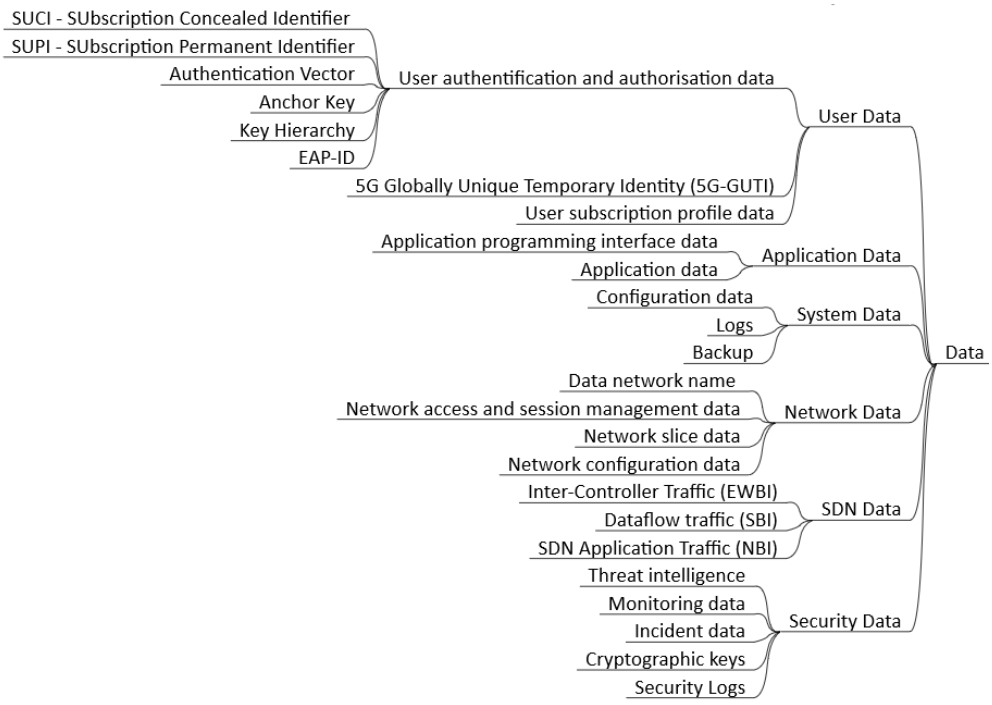
Interworking, trusted non-3GPP Gateway Function (TNGF), wireline Access Gateway Function (W-AGF) and trusted WLAN Interworking Function (TWIF) asset groups. Figure 19 depicts the various assets groups associated with interconnections that could be implemented in a 5G Network.

Figure 19: Asset groups from the Interconnections category



Data: This main category of 5G assets include user, application, system, network, SDN and security data. This asset group includes the entire data catalogue required in any 5G operation combined with used data. Though not necessarily exhaustive at this stage of the analysis, this asset group covers information related to: user data, system and configuration data, security-related data, network data (configuration, edge, logs, API-data, SDN-data, etc.). It is expected that 5G data such as user, security and configuration information will be subject to cyber-attacks with the aim to breach them. Main motives are monetisation and unnoticed access to the network.

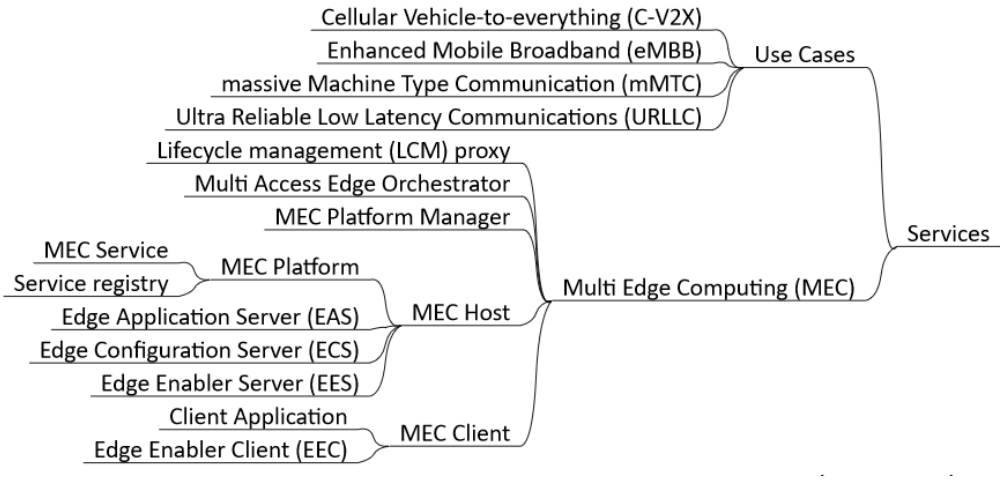
Figure 20: Asset groups from the data category



Services: This main of 5G assets include the use cases, multi-edge computing (MEC) and cloud service asset groups. These services are directly related with the asset monetisation model of a 5G Network and consequently represents part of the value generated that needs to be protected. In this version of the 5GTL we review assets that support the value generation model but not the

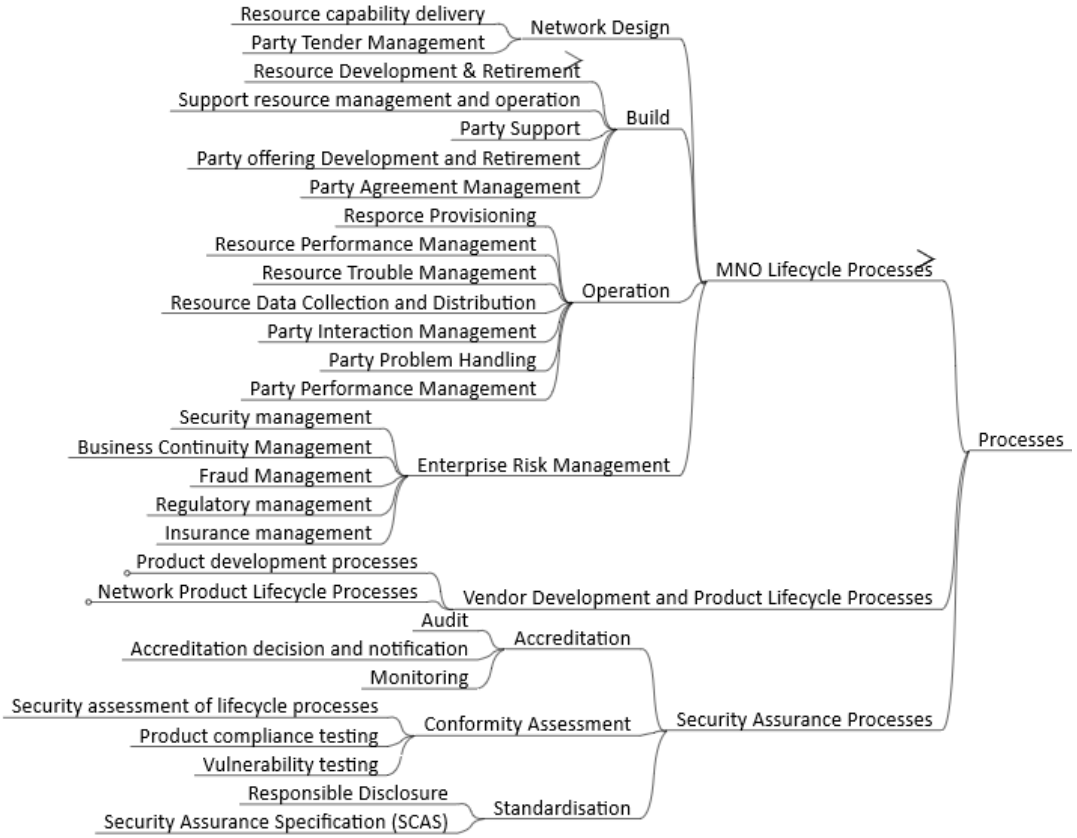
model itself. These were already covered by ENISA in previous work (cloud computing, autonomous vehicles, IIOT[89]) or are part of recommendations for future research work.

Figure 21: Asset groups from the Services category



Processes: This main category of 5G assets include the MNO and the product development lifecycle processes. All these processes are vital in a secure and reliable implementation of a 5G Network.

Figure 22: Asset groups from the Processes category

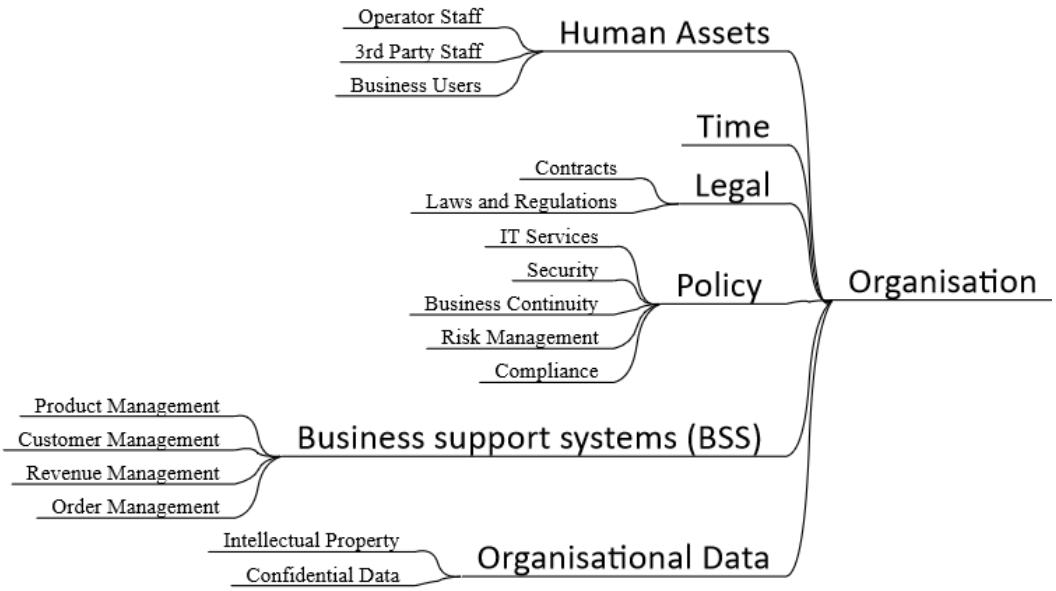


[89] https://www.enisa.europa.eu/publications accessed October 2020.

Organisation: This main category of 5G assets include time, legal, policy, business support systems (BSS) and human assets.

Many components in this asset category were also included in the previous mapping. For example, human assets are considered an important group since humans represent all individuals involved in the operation and use of the 5G network. Time for example plays a significant role in many time-dependent functions. With release 16 and the introduction of mission-critical uses cases requiring constant time synchronisation (e.g. ITS, V2X, IIoT and URLLC), this asset plays an even more important role in a 5G Network.

Figure 23: Asset groups from the Organisation category



5.3 ASSET CLASSIFICATION AND THE CIA TRIAD

In the following table, we provide the relevance of the identified asset groups with regard to the CIA triad.

Table 3: Relevance of asset groups to the maintenance of CIA properties

Asset C	CIA Triad		
	Confidentiality	Integrity	Availability
Management & orchestration	🔴	🔴	🔴
Network products	🔴	🔴	🔴
Protocols	🔵	🔴	
Data	🟡	🟡	🟡
Interconnections	🔴	🔴	🔴
Services	🔴	🔴	🔴
Processes	🟡	🟡	🟡
Organisation	🔴	🔴	🟡

Legend:
Very high relevance of asset group to maintain the property: 🔴
High relevance of asset group to maintain the property: 🟡
Medium relevance of asset group to maintain the property: 🔵
Low relevance of asset group to maintain the property: 🟢
Very low relevance of asset group to maintain the property: 🟢

The assignment of these security properties has been performed at the level of asset groups. We recommend performance of this exercise in higher detail, depending on the focus of prospective threat assessments. In this case, to achieve a more precise mapping, users of this document should obtain a more accurate internal evaluation of these properties.

Concluding this chapter, it is worth mentioning that due to its complexity and the early stage of 5G networks (development, deployment, specification) the asset mapping is an ongoing task that will need some time to reach a mature stage. This is due to a variety of reasons/issues regarding the parameters of current 5G activities (narrow time windows for the creation of reports, resource issues, knowledge transfer, vendor's enrolment, etc.). These challenges will be sufficiently managed in future assessment of 5G threats.

5.4 THE RELEVANCE OF ASSETS THROUGHOUT THE LIFECYCLE

The following table presents the relevance of the identified asset groups with regard to the 5G network lifecycle.

Table 4: Relevance of asset categories throughout the 5G network lifecyle

Asset category	Lifecycle process (eTOM)			
	Design	Build	Operation support & readiness	Operations (fulfilment and assurance)
Network products	The technical requirements and specifications of the network	The network planes, functions and elements	The testing capabilities for physical infrastructure, SDN and Network functions	Management plane, control plane, user plane, 5G core functions, 5G RAN functions, legacy / non-standalone, service-based architecture, security functions, network function virtualisation (NFV), physical infrastructure, virtualisation infrastructure, software defined networking (SDN) and security functions.
Management & orchestration	The infrastructure and virtualisation requirements	Virtualisation related (build) components such as scripts, templates and schemas	User rights management, service programmability, E2E service inventory and federation management.	NFV MANO, network slicing management, operations support system (OSS), network/element management system (EMS/NMS) and SDN controller
Protocols	Protocols requirements	Protocol configuration data	N/A	IP and cellular stack
Data	The technical, security, legal, processual and business data generated.	The technical and security configuration data	Test and application data	User data, application data, system data, network data, SDN data and security data
Inter-connections	The interconnection requirements between technologies, services and operators	The interconnection APIs and proprietary interfaces	Testing interfaces between technical infrastructures, operators and with providers and customers.	Home/visitor PLMN, security Edge protection proxy (SEPP), packet data network gateway (PGW), N3IWF - Non-3GPP interworking, trusted non-3GPP gateway function (TNGF), wireline access gateway function (W-AGF), trusted WLAN interworking function (TWIF)
Services	The use cases requirements, (Verticals including on premises and cloud requirement	Cloud and tenant configuration	Use cases and verticals testing with vendors, operators and customers	Use cases, multi edge computing (MEC) and cloud computing
Processes	The product design and procurements requirements. Vendor review data. Risk and threat assessments	Product development and security implementation	Security assurance and auditing, product road mapping.	MNO lifecycle processes, vendor development and product lifecycle processes, security assurance processes
Organisation	The legal aspects related with the procurement of network product including tender specifications, budget, contracts, laws and regulations	Organisational data and human assets	Time, policies and human assets	Business support systems, organisational data, synchronisation systems and policy monitoring systems

6. 5G THREATS

In the first edition of the threat landscape for 5G Networks, we identified and described multiple threat types distributed by asset categories from the network architecture (core, access and edge), traditional IP-based threats, insecure legacy 2/3/4G generations and the ones introduced by the virtualisation technology. To complement the analysis, we added the potential impact and information about the affected assets. We used ENISA threat taxonomy to group these threats in one common list. In this edition, we continued reviewing the threat landscape by updating the information from the previous edition and added new elements to the analysis. In summary, we:

1. reviewed the network architecture based on the specifications defined in release 16 for a generic network product (GNP);
2. reviewed the asset map based on the revised architecture and product lifecycle;
3. added information about vulnerabilities;
4. made a correlation between sensitive assets and vulnerabilities to look for exploitation opportunities;
5. used STRIDE[90] model to structure the information about threats and;
6. prepared a list combining all the information available about threats, including the ones from the previous edition and other sources such as 3GPP and GSMA.

As previously mentioned, we used the STRIDE model to structure information about threats. According to ISO 27001[91], a threat can be defined as “the potential cause of an incident that may result in a breach of information security or compromise business operations.”. In the context of this report, we collected information about various potential causes of an incident during the design, build, operation support & readiness and operations (fulfilment and assurance) of a 5G Network structured in 6 main categories (spoofing identity, tampering, repudiation, information disclosure, denial of service and elevation of privilege).

6.1 TAXONOMY OF THREATS

With the proliferation of methods, taxonomies and models, it is imperative to establish a common understanding of the different terms used to describe the threat landscape. It should start with the categorization of important elements such as assets, vulnerabilities and threats. For example, the adoption of a common taxonomy in 5G security will help improving communication among the various stakeholders in policymaking, regulation, product development, system implementation and operation. For that purpose, ENISA presents a threat taxonomy in Table 5 Annex B.

6.2 THREAT MAP

At this stage, we have completed the security risk management triangle with information about assets, vulnerabilities and threats. Conducting a more detailed assessment for a particular context and use case, it will be possible to complete the entire model. In this revision of the threat map, we structured the information from the previous edition of this report and generic threats from 3GPP security assurance specification (SCAS) using the STRIDE model.

[90] https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN, accessed October 2020.
[91] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-27001, accessed October 2020/

Threat Type	Threats	Potential Impact	Affected Assets
Nefarious Activity/ Abuse of assets (NAA)	**Manipulation of network configuration/data forging** - Routing tables manipulation - CORE configuration data tampering - DNS manipulation - Manipulation of access network and radio technology configuration data - Exploitation of misconfigured or poorly configured systems/networks - Registration of malicious network functions - Security data tampering (cryptography keys, security policies, access rules, etc,). - Network implementation data tampering - Operating system (OS) services tampering	- Information integrity - Information destruction - Service unavailability	- SDN, NFV, MANO - RAN, RAT - System configuration data - Network configuration data - Security configuration data - Business services
	Exploitation of software, hardware vulnerabilities - Zero-day exploits - Abuse of edge open application programming interfaces (APIs) - Application programming interface (API) exploitation - Software tampering - System execution hijack	- Information integrity - Information destruction - Service unavailability	- SDN, NFV, MANO, RAN, RAT, MEC, API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation - Subscribers' data - Application data - Security data - Network data - Business services
	Denial of service (DoS) - Distributed denial of service (DDoS) - Flooding of core network components - Flooding of base stations - Amplification attacks - MAC layer attacks - Jamming the network radio - Jamming device radio interface - Jamming base station radio interface - Edge node overload - Authentication traffic spikes	- Service unavailability - Outage	- SDN, NFV - RAN, RAT - MEC - CLOUD - Network services - Business services
	Remote access exploitation - intra-RAT mobility mechanism hijack - RAT session hijack	- System integrity - Data confidentiality	- RAT, SDN, NFV, MANO, CLOUD - Intra-RAT

Threat Type	Threats	Potential Impact	Affected Assets
	Malicious code/software - Injection attacks (SQL, XSS) - Rootkits - Rogueware - Worms/trojan - Botnet - Ransomware - Malicious network functions - Malware attacks on network products - Malware attacks on business applications	- Service unavailability - Information integrity - Information destruction - Other software asset integrity - Other software asset destruction	- Data network - Business applications - Security controls - Cloud, virtualisation - Subscribers' data - Application data - Security data - Network data - Business services - Network services
	Abuse of remote access to the network - Abuse on external remote services to network products (e.g. VPN)	- Information integrity - System integrity - Information confidentiality - Initial unauthorised access - Persistence	- SDN, NFV, RAN, RAT - Intra-RAT - Subscribers' data - Application data - Security data - Network data
	Abuse of information leakage - Theft and/or leakage from network traffic - Theft and/or leakage of data from cloud computing - Abuse on security data from audit tools - Theft/breach of security keys - Unauthorised access to user plane data - Unauthorised access to signalling data	- Information integrity - Information destruction - Information confidentiality	- Data storage/ repository - Subscribers' data - Cryptographic keys - Monitoring data - User subscription profile data - User plane data - Signalling data
	Abuse of authentication - Authentication traffic spikes - Abuse of user authentication/authorisation data by third parties' personnel - Abuse of the application management function (AMF) authentication and key agreement procedure - Abuse the credentials of existing accounts	- Information integrity - Information destruction - Service unavailability - Initial unauthorised access - Persistence	- Security data - Network service - Network functions - Subscribers' data - Application data - Security data - Network data
	Lawful interception function abuse	- Information integrity - Information destruction	- Subscribers' data - User subscription profile data

Threat Type	Threats	Potential Impact	Affected Assets
	Manipulation of hardware and software - Manipulation of hardware equipment - Manipulation of the network resources orchestrator - Memory scraping - Side channels attacks - Fake access network node - False or rogue MEC gateway - UICC format exploitation - UE compromising - Unacceptable UE security capabilities - Software backdoor	- Service unavailability - Information integrity - Information destruction	- Cloud data centre equipment - User equipment - Radio access/units - Light data centres - SDN, MANO, NF, - RAN, RAT - Virtualisation - Subscribers' data - Network services
	Data breach, leak, theft and manipulation of information - Network product log tampering - File Write Permission Abuse - Ownership file misuse - Breach of customer data - Theft of personal data	- Information integrity - Information destruction - Information confidentiality	- Subscribers' data - Subscriber geo locations - Financial data - Commercial data, IP - Configuration data - Service data - Network data
	Unauthorised activities/network intrusions - IMSI catching attacks - Lateral movement - Brute force - Port knocking	- Information integrity - System integrity	- User equipment - Network services - Business services
	Identity fraud/account or service - Identity theft - Identity spoofing - IP spoofing - MAC spoofing	- Service unavailability - Information destruction - Information integrity	- User subscription profile data - Subscribers' data
	Spectrum sensing	- Service unavailability	- RAT - Radio access units

Threat Type	Threats	Potential Impact	Affected Assets
	Compromised supply chain, vendor and service providers - Abuse on third parties' personnel access to MNO's facilities - Network product development tools tampering - Network product configuration tools tampering - Network product source code tampering - Manipulation of network product updates	- Service unavailability - Information integrity - Information destruction - Initial unauthorised access	- SDN, NFV, MANO, RAN, RAT, MEC, API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation - Network services - Business services
	Abuse of virtualisation mechanisms - Network virtualisation bypassing - Virtualised host abuse - Virtual machine manipulation - Data centre threats - Cloud container image implant - Cloud container image backdoor - Abuse of cloud computational resources	- Service unavailability - Information integrity - Information destruction	- Virtualisation - MANO - Cloud - Network services - Business services
	Signalling threats - Signalling storms - Signalling fraud	- Service unavailability - Information integrity - Information destruction	- RAT - Radio access units - Protocols - Network services - Business services
	Traffic Tampering	-	- RAT - SDN, NFV, MANO
Eavesdropping/ Interception/ Hijacking (EIH)	**Nation state espionage**	- Information integrity - Information confidentiality	- Subscribers' data - Subscriber geo locations
	Corporate espionage	- Information integrity - Information confidentiality	- Financial data - Commercial data - IP
	Traffic sniffing	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data - Subscriber geo location

Threat Type	Threats	Potential Impact	Affected Assets
	Manipulation of network traffic, network reconnaissance and information gathering - Radio network traffic manipulation - Malicious diversion of traffic - Traffic redirecting - Abuse of roaming interconnections	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data - Subscriber geo locations
	Man in the middle/ Session hijacking - Session hijacking via rogue base station - Downgrade attacks via rogue base station	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data - Subscriber geo locations
	Interception of information - Data eavesdropping via compromised small cell - Air interface eavesdropping - Device and identity tracking via rogue base station - Eavesdropping on unencrypted message content	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data - Subscriber geo locations
Physical Attacks (PA)	**Sabotage of network infrastructure (radio access, edge servers, etc.)** - Hardware additions	- Service unavailability - Information destruction - Information integrity - Initial unauthorised access	- Radio access units - ICT equipment - Light data centre - Cloud data centre - Network services - Business services
	Vandalism of network infrastructure (radio access, edge servers, etc.)	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data centre - Cloud data centre - Network services - Business services
	Theft of physical assets	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data centre - Cloud data centre - Network services - Business services

Threat Type	Threats	Potential Impact	Affected Assets
	Terrorist attack against network infrastructure	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data centre - Cloud data centre - Network services - Business services
	Fraud by MNO employees	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center - Network services - Business services
	Unauthorised physical access to based stations in shared locations	- Service unavailability - Information destruction - Information integrity	- RAT - Radio access units - Network services - Business services
Unintentional damages (accidental) (UD)	**Misconfigured or poorly configured systems/networks**	- Service unavailability - Information integrity	- Management processes - Policies - Legal - Human assets - SDN, NFV, MANO, API - RAN, RAT, MEC - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation
	Inadequate designs and planning or lack of adaption - Outdated system or network from the lack of update or patch management - Errors from the lack of configuration change management - Poorly design network and system architecture	- Service unavailability - Information integrity	- Management processes - Policies - Human assets - SDN, NFV, MANO, RAN, RAT, MEC, API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation

Threat Type	Threats	Potential Impact	Affected Assets
Failures or Malfunctions (FM)	**Erroneous use or administration of the network, systems and devices**	- Service unavailability - Information integrity	- Management processes - Policies - Human assets - SDN, NFV, MANO, RAN, RAT, MEC, UE, API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation
	Information leakage/sharing due to human error	- Information integrity - Information confidentiality	- Data storage/repository - Management processes - Policies - Legal - Human assets - Subscribers' data - Application data - Security data - Network data
	Data loss from unintentional deletion	- Information integrity - Information confidentiality	- Management processes - Policies - Human assets
	Failure of the network, devices or systems	- Service unavailability - Information destruction - Information integrity	- Cloud data centre - User equipment - RAT, Radio unit - Light data centre - Subscribers' data - Application data - Security data - Network data
	Failure or disruption of communication link	- Service unavailability - Information destruction - Information integrity	- Cloud data centre - Network services - Business services

Threat Type	Threats	Potential Impact	Affected Assets
	Failure or disruption of main power supply	- Service unavailability - Information destruction - Information integrity	- Cloud data centre - Network services - Business services
	Failure or disruption from service providers (supply chain)	- Service unavailability - Information destruction - Information integrity	- Network services - Business services
	Malfunction of equipment (devices or systems)	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data centre - Cloud data centre - Network services - Business services
Outages (OUT)	**Loss of resources** - Human resources - Physical resources	- Service unavailability - Information destruction - Information integrity	- Human assets - Legal - Network services - Business services
	Support services	- Service unavailability - Information destruction - Information integrity	- Human assets - Management processes - Policies - Legal - Network services - Business services
	Data network (access)	- Service unavailability - Information destruction - Information integrity	- Cloud data centre - Network services - Business services
	Interfering radiation	- Service unavailability - Information destruction - Information integrity	- CORE, RAN, MANO, UE - Network services - Business services - Cloud data centre - Network services - Business services

Threat Type	Threats	Potential Impact	Affected Assets
Disasters (DIS)	**Natural disasters** - Earthquakes - Landslides	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data centre - Cloud data centre - Network services - Business services
	Environmental disaster - Floods, storms - Pollution, dust, corrosion - Fires, heavy winds - Unfavourable climatic conditions	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data centre - Cloud data centre - Network services - Business services
Legal (LEG)	**Breach of service level agreement (SLA)**	- Service unavailability - Information destruction - Information integrity	- Network services - Business services
	Breach of legislation	- Service unavailability - Information destruction - Information integrity	- Network services - Business services
	Failure to meet contractual requirements and/or legislation	- Service unavailability - Information destruction - Information integrity	- Network services - Business services

In the following table we provide a mapping between the ENISA 5G threat taxonomy and the vulnerabilities/threats identified by 3GPP.
This mapping establishes the correspondence between the threats assigned to the assessed vulnerabilities.

	Spoofing Identity	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
NEFARIOUS ACTIVITY/ ABUSE OF ASSETS (NAA)						
Malicious Code or SW (NAA-MAL)	Malware	· Software Tampering · Log Tampering		Malware		Over-Privileged Processes/Services
Exploitation of flaws in the architecture, design and configuration of the network. (NAA-EXPLO)	· Default Accounts · Weak Password Policies · Malware · Eavesdropping	· Software Tampering · Ownership File Misuse · External Device Boot · Log Tampering · OAM Traffic Tampering · File Write Permission Abuse · User Session Tampering	· Lack of User Activity Trace	· Poor Key Generation · Poor Key Management · Weak Cryptographic Algorithms · Insecure Data Storage · System Fingerprinting · Malware · Insecure Default Configuration · File/ Directory Read Permissions Misuse · Insecure Network Services · Unnecessary Services · Unnecessary Applications · Eavesdropping · Security threat caused by lack of GNP traffic isolation.	· Compromised/ Misbehaving User Equipment · Implementation Flaw · Insecure Network Services	· Misuse by Authorized Users · Over-Privileged Processes/Services · Folder Write Permission Abuse · Root-Owned File Write Permission Abuse · High-Privileged Files · Insecure Network Services · Elevation of Privilege via Unnecessary Network Services
Denial of Service (NAA-DoS)		· Software Tampering · File Write Permission Abuse		· File/ Directory Read Permissions Misuse	· Compromised/ Misbehaving User Equipment · Implementation Flaw · Insecure Network Services · Human Error	· High-Privileged Files

	Spoofing Identity	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Abuse of information leakage (NAA-AIL)	· Malware · Eavesdropping	· Software Tampering · Ownership File Misuse		· Poor Key Generation · Weak Cryptographic Algorithms · Insecure Data Storage · System Fingerprinting · Malware · Personal Identification Information Violation · Security threat caused by lack of GNP traffic isolation. · Insecure Default Configuration · File/ Directory Read Permissions Misuse · Insecure Network Services · Unnecessary Services · Log Disclosure · Unnecessary Applications · Eavesdropping · Security threat caused by lack of GNP traffic isolation.		
Abuse of remote access to the network. (NAA-ARA)	· Direct Root Access			· Unnecessary Services		· Elevation of Privilege via Unnecessary Network Services
Exploitation of software, and/or hardware vulnerabilities. (NAA-ESHV)		· Software Tampering · External Device Boot · File Write Permission Abuse · User Session Tampering	· Lack of User Activity Trace	· System Fingerprinting · Unnecessary Applications · Poor Key Generation · Insecure Default Configuration · Unnecessary Services	· Compromised/ Misbehaving User Equipment · Implementation Flaw · Insecure Network Services · Human Error	· Insecure Network Services · Elevation of Privilege via Unnecessary Network Services

	Spoofing Identity	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Abuse of authentication (NAA-AA)	· Default Accounts · Weak Password Policies · Password Peek · Direct Root Access · IP Spoofing	· OAM Traffic Tampering · File Write Permission Abuse	· Lack of User Activity Trace	· Poor Key Generation · Poor Key Management · Weak Cryptographic Algorithms · Insecure Data Storage · Insecure Default Configuration · File/ Directory Read Permissions Misuse · Unnecessary Applications		· Misuse by Authorized Users · Over-Privileged Processes/Services · Folder Write Permission Abuse · Root-Owned File Write Permission Abuse · High-Privileged Files · Insecure Network Services · Elevation of Privilege via Unnecessary Network Services
Lawful interception function abuse (NAA-LIFA)		· File Write Permission Abuse		· Insecure Default Configuration · Unnecessary Applications		· Folder Write Permission Abuse · Root-Owned File Write Permission Abuse
Manipulation of hardware and software (NAA-MSH)	· Default Accounts · IP Spoofing · Malware	· Software Tampering · External Device Boot · File Write Permission Abuse · User Session Tampering	· Lack of User Activity Trace	· Insecure Default Configuration · Unnecessary Applications	· Compromised/ Misbehaving User Equipment · Implementation Flaw · Insecure Network Services · Human Error	· Insecure Network Services · Elevation of Privilege via Unnecessary Network Services

	Spoofing Identity	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data, breach, leak, theft and manipulation of information (NAA-DBLT)	· Default Accounts · Weak Password Policies · Password Peek · Malware · Eavesdropping	· OAM Traffic Tampering	· Lack of User Activity Trace	· Poor Key Generation · Poor Key Management · Weak Cryptographic Algorithms · Insecure Data Storage · Malware · Personal Identification Information Violation · Insecure Default Configuration · File/ Directory Read Permissions Misuse · Insecure Network Services · Security threat caused by lack of GNP traffic isolation. · Unnecessary Services · Log Disclosure · Unnecessary Applications · Eavesdropping		· Folder Write Permission Abuse · Root-Owned File Write Permission Abuse · Insecure Network Services · Elevation of Privilege via Unnecessary Network Services
Unauthorised activities/network intrusions (NAA-UANI)	· Default Accounts · Weak Password Policies · Password Peek · Direct Root Access · IP Spoofing · Malware · Eavesdropping			· Personal Identification Information Violation · Insecure Network Services · Unnecessary Services · Eavesdropping	· Compromised/ Misbehaving User Equipment · Insecure Network Services · Human Error	· Misuse by Authorized Users · Insecure Network Services · Elevation of Privilege via Unnecessary Network Services
Identity fraud/account or service (NAA-IFAS)	· Default Accounts · Weak Password Policies · Password Peek · Direct Root Access · IP Spoofing · Malware · Eavesdropping		· Lack of User Activity Trace	· System Fingerprinting · Malware · Insecure Network Services · Unnecessary Services	· Compromised/ Misbehaving User Equipment · Insecure Network Services · Human Error	· Misuse by Authorized Users · Folder Write Permission Abuse · Over-Privileged Processes/Services · Insecure Network Services · Elevation of Privilege via Unnecessary Network Services

	Spoofing Identity	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Spectrum sensing (NAA-SS)					· Compromised/ Misbehaving User Equipment · Implementation Flaw · Insecure Network Services · Human Error	
Compromised supply chain, vendor and service providers (NAA-CSVS)	· Direct Root Access	· External Device Boot	· Lack of User Activity Trace	· Unnecessary Applications · Unnecessary Services	· Human Error	· Elevation of Privilege via Unnecessary Network Services
Abuse of virtualization mechanisms (NAA-AVM)						
Signalling threats (NAA-ST)				· Insecure Default Configuration · Security threat caused by lack of GNP traffic isolation.	· Compromised/ Misbehaving User Equipment	
Manipulation of network configuration/data forging. (NAA-MND)	· Default Accounts · Weak Password Policies · Password Peek · Direct Root Access · Eavesdropping			· Insecure Default Configuration · Personal Identification Information Violation · Insecure Network Services · Unnecessary Services · Eavesdropping	· Compromised/ Misbehaving User Equipment · Insecure Network Services · Human Error	
EAVESDROPPING/ INTERCEPTION/ HIJACKING (EIH)						
Eavesdropping/ interception/ hijacking (EIH-EV)	· Eavesdropping			· Insecure Default Configuration · Eavesdropping · Security threat caused by lack of GNP traffic isolation		

	Spoofing Identity	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
PHYSICAL ATTACKS (PA)						
PHYSICAL ATTACKS (PA-1)		· Software Tampering · Ownership File Misuse · External Device Boot · Log Tampering · OAM Traffic Tampering · File Write Permission Abuse · User Session Tampering		· File/ Directory Read Permissions Misuse · Security threat caused by lack of GNP traffic isolation.		· Folder Write Permission Abuse · High-Privileged Files

7. THREAT AGENTS

The assessed threat agents engaged in attacks of 5G infrastructures remain identical to the previous edition of the 5G Threat Landscape[8]. This is due to the fact that there are no insights about malicious activities targeting 5G infrastructures. Main reasons for this are:

- Due to the early stages of 5G deployments, no incidents of attacks to 5G infrastructures have been identified during 2020;
- The threat agent assessment is based on hypothetical attacks;
- The current threat landscape is done at the level of specifications. Real attacks will happen against implementations. This will influence modus operandi;
- As business processes that will run of 5G infrastructures are still unknown, it is difficult to assess threat actor motives other than the obvious state-sponsored interventions. There are no indications about the most frequent threat of cybercrime.

These points make clear that as the next generation of Mobile Networks (5G) are being deployed, existing threat agent profiles will develop towards a new set of capabilities and motives. Nonetheless, without any analysis of specific implementations of 5G infrastructures and business processes running on these infrastructures, a threat agent assessment can be performed only at a generic hypothetical level.

Given this the complexity of 5G infrastructures and the ambiguity regarding 5G related attack vectors, it is expected that the following facts will influence the attacker profile:

- A whole set of new vulnerabilities related to individual 5G deployments will expand the attack surface, exposure, number and nature of critical assets.
- New tools/methods to exploit those vulnerabilities will be developed.
- New motives/ impacted targets are going to be observed due to the interconnected verticals/applications.
- Existing threat agent groups may be expanded with ones that have an interest in novel malicious objectives emerging from the upcoming 5G use-cases.

These facts may cause an unprecedented shift of capabilities and objectives of existing threat agent groups in ways that have not been seen in the past.

Having regard to the above mentioned facts, in the current 5G Threat Landscape, we stick to the threat agent groups assessed in the previous edition taking into account the following threat agent groups:

- Cyber criminals
- Insider (own, third parties)
- Nation states
- Hacktivists
- Cyber-fighters
- Cyber-terrorists
- Corporations
- Script kiddies

Interested readers should revisit the previous 5G Threat Landscape edition[8] to find the descriptions and motives of these threat agent groups.

For the sake of completeness, we provide below a mapping between threat agents and cyber-threats used in this report.

Table 5: Involvement of threat agents in cyberthreats[92]

	Cyber-criminals	Insiders	Nation States	Cyber-warriors	Hacktivists	Corporations	Cyber-terrorists	Script-kiddies
Nefarious activity/Abuse	✓	✓	✓	✓	✓	✓	✓	✓
Eavesdropping/ Interception/ Hijacking	✓	✓	✓	✓	✓	✓	✓	✓
Disasters			✓	✓			✓	
Unintentional Damage	✓	✓	✓	✓				✓
Outages	✓	✓	✓	✓	✓		✓	
Failures/ malfunctions	✓	✓	✓	✓	✓	✓	✓	✓
Legal	✓	✓	✓	✓	✓	✓	✓	
Physical attacks	✓	✓	✓	✓	✓	✓	✓	

Legend:

Primary group for threat: ✓

Secondary group for threat: ✓

[92] It is worth mentioning that the involvement is indicative and at a high level of abstraction (i.e. threat categories). Given the detailed vulnerability analysis presented in this document (see Annexes C-M), it is possible to infer the potential engagement of these threat agent groups in exploitation campaigns. In this way, a detailed threat agent profiling can be performed. This task has not been performed in this report. However, it will be subject of prospective ENISA activities in detailed threat/risk assessments.

8. RECOMMENDATIONS/ CONCLUSIONS

8.1 RECOMMENDATIONS

Based on the assets, threats and the state-of-play of current developments, the following recommendations/courses of actions can be made for various stakeholders of the 5G ecosystem:

Recommended courses of action at EU level (e.g. Member States, European Commission and ENISA)

- It is essential that the EU continues to facilitate the definition of common security standards across for 5G Networks and its use cases by supporting further cooperation and information sharing among Member States.
- The existing EU 5G observatory[93] is a very useful/important resource for dissemination of content related to 5G, in support of activities of EU 5G Stakeholders. It covers developments in various areas of 5G, such as status of 5G deployments, relevant MS-actions, market uptakes, economic aspects of 5G infrastructure development, etc. Besides this information offering, it is recommended to collect cybersecurity-related market information, such as the status of specifications, and certification activities, more systematically, through the appropriate mechanism or forum.
- Relevant work of stakeholders (e.g. Member States, MNOs, etc.) regarding prioritisation of implementation, service criticality assessments, security requirements, etc. should be consolidated and made available to the 5G community. This could be one of the tasks of the 5G observatory mentioned above.
- It is important to deliver developed CTI in a form that can be more easily utilised by interested stakeholders. A possible way to achieve this can be by means of a 5G CTI repository offering querying facilities based on various criteria (i.e. such as threat exposure, vulnerabilities per asset type, threats per attacker type, mapping of roles and assets, etc.).
- In orchestration with the above-mentioned recommendations, critical 5G services should be identified and implemented. Main objective of this action is could be to develop a security assurance scheme that could drive certifications on 5G equipment, software and processes. In all cases, a risk-based approach should be followed. CTI provided within this report should be adapted where necessary and taken into account within the risk assessment and the evaluation of attacker potential.
- As the proliferation of AI algorithms has reached components used in the 5G ecosystem, it is proposed to assess the threat exposure such functions throughout the components of the entire 5G ecosystem (devices, EPROMs, software, sensors, actuators, etc.). This activity overlaps with current ENISA work on an AI Threat Landscape, whereas a more deep assessment w.r.t. 5G could be done in prospective versions of the 5G Threat Landscape, when more information about such functions will be available.
- Through the performed threat analysis, it has been recognised that some work needs to be done in the area of 5G threat agent profiling and in the identification of possible attack vectors. Given the rudimentary information available for both topics and the level of

[93] https://5gobservatory.eu, accessed November 2020.

available information processed (mainly specification level), at this point of time a profiling would be premature. Nonetheless, this work is considered as a priority for future versions of the 5G Threat Landscape, given the availability of more information on both threat agents and attack vectors.

Recommendations for 5G market stakeholders (e.g. vendors, MNOs, Operators of Services, Standardisation Bodies, 5G Test Labs, etc.)

- More detailed mappings of asset/role responsibilities and vulnerabilities/threats could enhance the utilisation of the produced CTI. This process could be steered by means of identified priorities and asset criticalities assessed via market analysis, stakeholder surveys and 5G rollout activities of MNOs.
- A detailed cap analysis for the protection of various 5G assets needs to be performed. Besides organisational issues, such a gap analysis will be needed for migration/implementation options.
- The specification of 5G provides a solid basis for the security of the entire system. Nonetheless, the final security level will heavily depend on implementation/coding practices. The development of good practices/guidelines for the secure implementation of network functions is an important step towards maintaining the security level of the specification in the resulting code-base. Such guidelines do not yet exist.
- The terminology used in various published 5G documents (specifications, standardisation documentation, research projects, etc.) needs to be consolidated. This will facilitate homogeneity in references to important security concepts (e.g. threats, vulnerabilities, impact, responsibilities, stakeholders, etc.) and will contribute to an elevation of understanding and utilization of the produced material.
- Some operational, general-purpose process models and frameworks do exist in the area of telecommunication. They cover network management, vendor and security assurance processes. Though making up a very good starting point for 5G infrastructures, they might entail gaps w.r.t. specialised 5G operational issues. It is proposed to perform a systematic gap analysis of these frameworks to test their 5G adequacy and fill the identified gaps.

Recommendations for national competent bodies in the area of 5G cybersecurity (e.g. NRAs, NCSCs, National 5G Test Centres, etc.)

- With guidance from current 5G deployments (including migration options), more exhaustive gap analysis on various areas of cybersecurity measures, should be performed. This information will contribute to the advancement of current cybersecurity practices. The delivered CTI of this report can serve as key input towards a risk and threat based approach.

While the above may be advisable future actions for various stakeholder groups, ENISA envisages an involvement in the following actions e.g. on behalf/on request of EU, MS

- It is important to deliver developed CTI in a form that can be more easily utilised by interested stakeholders. A possible way to achieve this can be by means of a 5G CTI repository offering querying facilities based on various criteria (i.e. such as threat exposure, vulnerabilities per asset type, threats per attacker type, mapping of roles and assets, etc.).
- Fostering the use of the released CTI within implementation projects and establishment of feedback will be an important element for the improvement of the presented material and enhancement of 5G technical and operational cybersecurity.
- Performance of risk assessments for specific parts of the 5G infrastructure will lead to better utilisation of the information delivered in the present report and will reveal areas of improvement of the provided analysis. A pilot on a security assurance scheme for

certification of identification service is planned by ENISA for the coming semester. Information from the present report will flow into this activity during the risk assessment phase.

- Besides integrating feedback from implementations, processes and detailed assessments, prospective versions of the 5G threat landscape need to be linked to planned versions of 5G specification activities, in particular regarding the work of 3GPP group.

8.2 CONCLUSIONS

Having reached a good degree of comprehensiveness and detail within this version of the 5G Threat Landscape, it is proposed to put the focus on utilization within upcoming activities at EU level, Member States and MNOs. By means of the identified recommendations, this objective can be achieved. Just as in the previous edition of the 5G Threat Landscape, it will be important to use this material in various stakeholder activities, identify current and future developments and try to accommodate those in future versions of the present report.

Such activities, if performed in a coordinated manner, will speed up implementation of measures developed by various actors (i.e. EU toolbox measures, specified security measures, development of 5G good practices for operation and security assurance).

ENISA will continue engaging within cybersecurity activities of 5G. Coordination with EU-wide activities will be key to the success of this attempt.

Future ENISA actions on this matter will be agreed upon, mandated and coordinated with European Commission and Member States (NIS CG SG on 5G) as deemed necessary.

A ANNEX: ASSETS MAP

Figure 24: 5G Asset Mind Map (FULL)

A full diagram of the Asset Mapping will be made available at ENISA website[94].

[94] https://www.enersec.net/Asset_MM/ accessed October 2020.

B ANNEX: THREAT TAXONOMY

The references presented in Table 5 will help the reader relating ENISA Threat Taxonomy with the vulnerabilities presented in Annexes from C to M. These references result from the intersection between ENISA and ITU threat Taxonomies.

ENISA Threat Taxonomy Categories are the following:

- **Nefarious activity/abuse (NAA):** This threat category is defined as “intended actions that target ICT systems, infrastructure, and networks by means of malicious acts with the aim to either steal, alter, or destroy a specified target”.
- **Eavesdropping/Interception/ Hijacking (EIH)**: This threat category is defined as “actions aiming to listen, interrupt, or seize control of a third party communication without consent”.
- **Physical attacks (PA):** This threat category is defined as “actions which aim to destroy, expose, alter, disable, steal or gain unauthorised access to physical assets such as infrastructure, hardware, or interconnection”.
- **Damage (DAM):** This threat category is defined as intentional actions aimed at causing “destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness”.
- **Unintentional Damage (UD):** This threat category is defined as unintentional actions aimed at causing “destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness”.
- **Failures or malfunctions (FM):** This threat category is defined as “Partial or full insufficient functioning of an asset (hardware or software)”.
- **Outages (OUT):** This threat category is defined as “unexpected disruptions of service or decrease in quality falling below a required level“.
- **Disaster (DIS):** This threat category is defined as “a sudden accident or a natural catastrophe that causes great damage or loss of life”.
- **Legal (LEG):** This threat category is defined as “legal actions of third parties (contracting or otherwise), in order to prohibit actions or compensate for loss based on applicable law”.

Figure 25: 5G Threat Taxonomy Categories

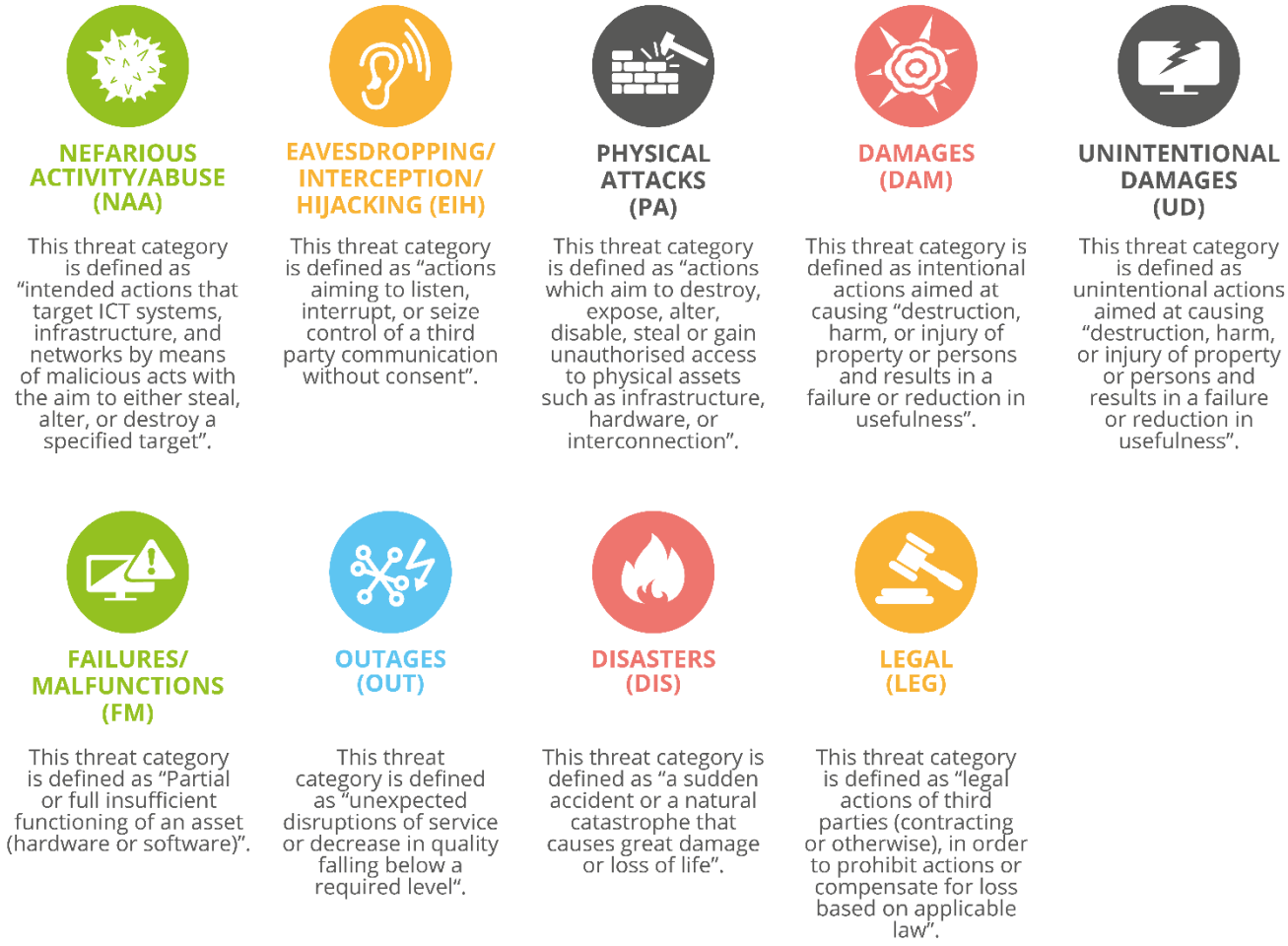
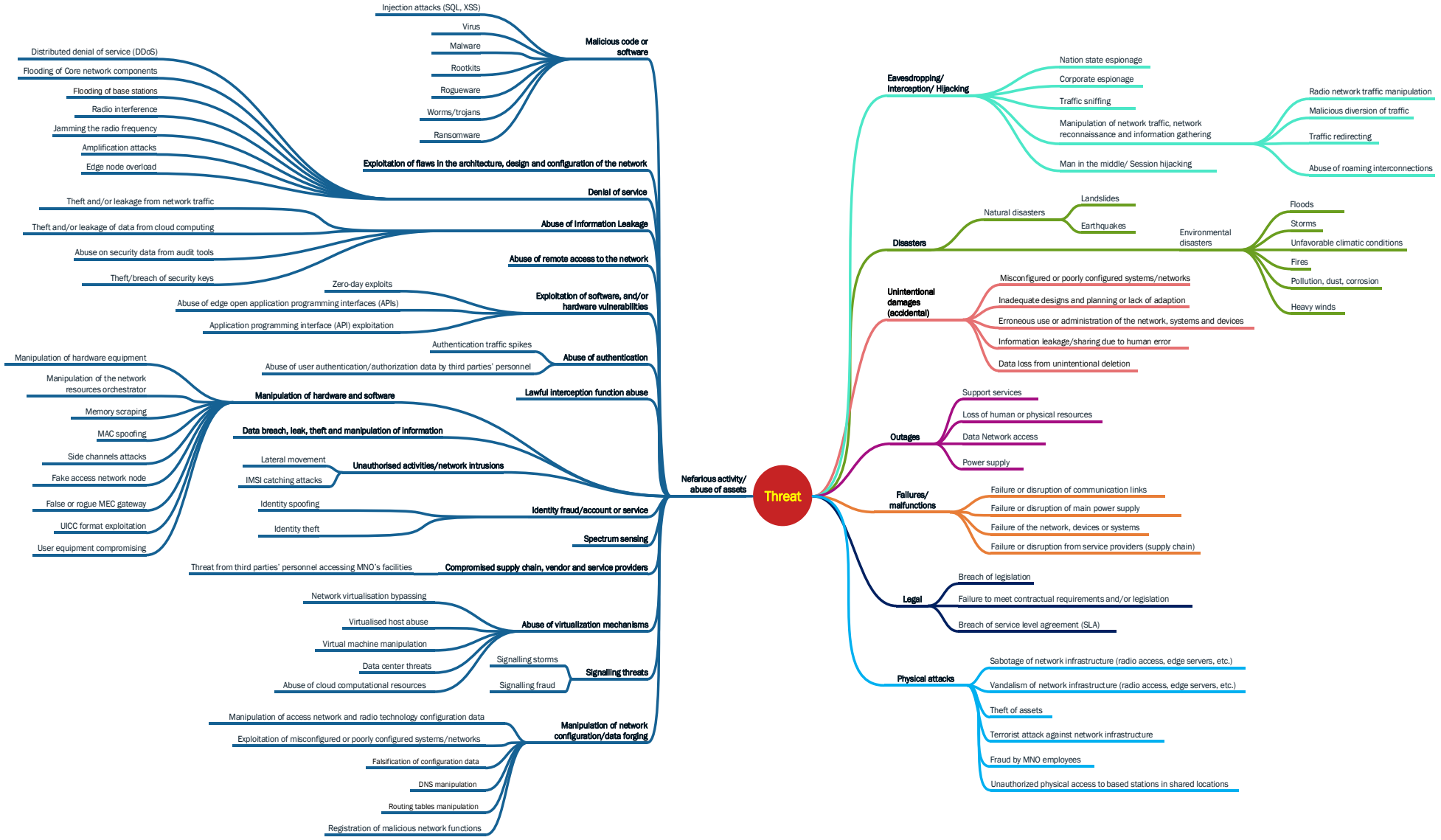


Table 5: ENISA and ITU Threat Taxonomies

ENISA THREAT TAXONOMY	THREAT TAXONOMY DETAILED (ITU)				
	DESTRUCTION OF INFORMATION AND OTHER RESOURCES	CORRUPTION OR MODIFICATION OF INFORMATION	THEFT, REMOVAL OR LOSS OF INFORMATION AND OTHER RESOURCES	DISCLOSURE OF INFORMATION	INTERRUPTION OF SERVICES.
Nefarious Activity/ Abuse of assets (NAA)					
Malicious Code or SW **(NAA-MAL)**	NAA-MAL1	NAA-MAL2	NAA-MAL3	NAA-MAL4	NAA-MAL5
Exploitation of flaws in the architecture, design and configuration of the network. **(NAA-EXPLO)**		NAA-EXPLO2	NAA-EXPLO3	NAA-EXPLO4	NAA-EXPLO5
Denial of Service **(NAA-DoS)**	NAA-DoS1				NAA-DoS5
Abuse of information leakage **(NAA-AIL)**			NAA-AIL3	NAA-AIL4	
Abuse of remote access to the network. **(NAA-ARA)**	NAA-ARA1	NAA-ARA2	NAA-ARA3	NAA-ARA4	NAA-ARA5
Exploitation of software, and/or hardware vulnerabilities. **(NAA-ESHV)**	NAA-ESHV1	NAA-ESHV2	NAA-ESHV3	NAA-ESHV4	NAA-ESHV5
Abuse of authentication **(NAA-AA)**	NAA-AA1	NAA-AA2	NAA-AA3	NAA-AA4	NAA-AA5
Lawful interception function abuse **(NAA-LIFA)**					NAA-LIFA5
Manipulation of hardware and software **(NAA-MSH)**	NAA-MSH1	NAA-MSH2	NAA-MSH3	NAA-MSH4	NAA-MSH5
Data, breach, leak, theft and manipulation of information **(NAA-DBLT)**		NAA-DBLT2	NAA-DBLT3	NAA-DBLT4	
Unauthorised activities/network intrusions **(NAA-UANI)**	NAA-UANI1	NAA-UANI2	NAA-UANI3	NAA-UANI4	NAA-UANI5
Identity fraud/account or service **(NAA-IFAS)**	NAA-IFAS1	NAA-IFAS2	NAA-IFAS3	NAA-IFAS4	NAA-IFAS5
Spectrum sensing (NAA-SS)					NAA-SS5
Compromised supply chain, vendor and service providers **(NAA-CSVS)**				NAA-CSVS4	NAA-CSVS5

Abuse of virtualization mechanisms **(NAA-AVM)**					
Signalling threats **(NAA-ST)**					NAA-ST5
Manipulation of network configuration/data forging. **(NAA-MND)**	NAA-MND1	NAA-MND2			NAA-MND5
Eavesdropping/ Interception Hijacking (EIH)				EIH4	
Physical Attacks (PA)	PA1		PA3		PA5
Unintentional damages (accidental) (UD)	UD1	UD2		UD3	UD4
Failures or Malfunctions (FM)	FM1	FM2			FM5
Outages (OUT)	OUT				
Disasters (DIS)	DIS				
Legal (LEG)	LEG				

Figure 26: 5G Threat Taxonomy



C ANNEX: DETAILED VULNERABILITIES IN THE CORE NETWORK

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper protection of Service Based Interfaces							
Improper transport layer protection of service-based interfaces (SBI)	Use of TLS profiles forbidden in TS 33.310 for NF mutual authentication and NF transport layer protection. May lead to sensitive information/data being disclosed and eventually tampered.	all Network Function (NF) within the 5G Core (5GC) utilizing Service-Based Interfaces (SBI)	TS 33.501 / 13.1 Protection at the network or transport layer TS 33.501 / 13.3 Authentication and static authorisation	All network functions shall support TLS. Network functions shall support both server-side and client-side certificates. The TLS profile shall follow the profile given in clause 6.2 of TS 33.210 with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540. TLS shall be used for transport protection within a PLMN unless network security is provided by other means. NRF and NF shall authenticate each other during discovery, registration, and access token request. If the PLMN uses protection at the transport layer, authentication provided by the transport layer protection solution shall be used for mutual authentication of the NRF and NF.	Information Disclosure, Rogue base station NAAx, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.310 3GPP TR 33.926 4.2.2.2.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Incorrect Verification of Access Tokens	There are the following threats if the generic NF cannot correctly verify the access tokens: - An access token may be tampered so that an attacker can arbitrarily access any services from any NF service providers within the same PLMN or in different PLMNs, which leads to elevation of privilege and consequently information disclosure. - An access token may be tampered so that an attacker can block service access by replacing the granted services/NF service providers with unavailable services/NF service providers, which leads to denial of service.	all Network Function (NF) within the 5G Core (5GC) utilizing Service-Based Interfaces (SBI)	TS 33.501 13.4.1. OAuth 2.0 based authorisation of Network Function service access	The authorisation framework uses the OAuth 2.0 framework as specified in RFC 6749. Access tokens shall be JSON Web Tokens as described in RFC 7519 and are secured with digital signatures or Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in RFC 7515.	Elevation of Privilege, Information Disclosure, Denial of Service. NAAx, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 4.2.2.2.3, 4.2.2.2.4
Vulnerabilities in implementation of AMF security functionalities							
Incorrect implementation of bidding down prevention at Xn-handover	If the gNB does not send the UE 5G security capabilities, the AMF cannot verify 5G security capabilities are the same as the UE security capabilities that the AMF has stored, the attacker may force the system to accept a weaker security algorithm than the system is allowed, forcing the system into a lowered security level making the system easily attacked and/or compromised	gNB, AMF	TS 33.501/6.7.3.1 Xn-handover	The AMF shall verify that the UE's 5G security capabilities received from the target gNB are the same as the UE's 5G security capabilities that the AMF has locally stored. If there is a mismatch, the AMF shall send its locally stored 5G security capabilities of the UE to the target gNB in the Path-Switch Acknowledge message. The AMF shall support logging capabilities for this event and may take additional measures, such as raising an alarm	Tampering Data, Information Disclosure, Denial of Service. NAAx, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511 3GPP TS 33.512 4.2.2.1.14 4.2.2.4
Incorrect implementation of NAS signalling messages replay protection	If SMC does not include the complete initial NAS message if either requested by the AMF or the UE sent the initial NAS message unprotected, the UE can force the system to reduce the security level by using weaker security algorithms or turning security off, making the system easily attacked and/or compromised	AMF	TS 33.512/ 4.2.2.3.1 Replay protection of NAS signalling messages	AMF shall support replay protection of NAS signalling messages between UE and AMF on N1 interface." as specified in TS 33.501 [2], clause 5.5.1.	Tampering of Data, Information Disclosure NAAx, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	TS 33.512 4.2.2.3.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Incorrect implementation of cryptographic protection for NAS signalling messages	If NAS NULL integrity protection is used outside of emergency call scenarios, an attacker can initiate unauthenticated non-emergency calls	AMF	TS 33.117 / 5.5.2 Signalling data integrity	NIA0 shall be disabled in AMF in the deployments where support of unauthenticated emergency session is not a regulatory requirement." as specified in TS 33.501 [2], clause 5.5.2	Elevation of Privilege NAAx, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.512 4.2.2.3
Incorrect implementation of procedures for NAS Algorithm selection	If the highest priority NAS integrity protection is not selected by the new AMF in AMF change, the new AMF could end up using a weaker algorithm forcing the system into a lowered security level making thee system easily attacked and/or compromised	AMF	TS 33.501, 6.7.1 Procedures for NAS algorithm selection	To establish the NAS security context, the AMF shall choose one NAS ciphering algorithm and one NAS integrity protection algorithm. The AMF shall then initiate a NAS security mode command procedure and include the chosen algorithm and UE security capabilities (to detect modification of the UE security capabilities by an attacker) in the message to the UE. The AMF shall select the NAS algorithm which have the highest priority according to the ordered list.	Tampering of Data, Information Disclosure NAAx, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.512 4.2.2.5
Incorrect implementation of invalid or unacceptable UE security capabilities handling	A flawed AMF implementation accepting insecure or invalid UE security capabilities may put User Plane and Control Plane traffic at risk, without the operator being aware of it. If NULL ciphering algorithm and/or NULL integrity protection algorithm of the UE security capabilities is accepted by the AMF, all the subsequent NAS, RRC, and UP messages will not be confidentiality and/or integrity protected. The attacker can easily intercept or tamper control plane data and the user plane data. This can result in information disclosure as well as tampering of data.	AMF	TS 24.501/ 5.5.1.2.8 Abnormal Cases on the network side	If the REGISTRATION REQUEST message is received with invalid or unacceptable UE security capabilities (e.g. no 5GS encryption algorithms (all bits zero), no 5GS integrity algorithms (all bits zero), mandatory 5GS encryption algorithms not supported or mandatory 5GS integrity algorithms not supported, etc.), the AMF shall return a REGISTRATION REJECT message."	Tampering of Data, Information Disclosure NAAx, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.512 4.2.2.6

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Incorrect implementation of RES* verification failure handling	If a malicious UE initiates a registration request using a SUCI and this request is followed by primary authentication in which an incorrect RES* is sent to the network, then the RES* verification will fail. In this case, if the RES* verification failure is not handled correctly, e.g., AMF/SEAF does not reject the registration request directly, or initiates a new authentication procedure with the UE, this would result in waste of system resources.	AMF/SEAF, AUSF	TS 33.501 6.1.3.2. Authentication procedure for 5G AKA	Handling of RES* verification failure in the SEAF or in the AUSF is defined in detail in sub-clause 6.1.3.2.2	Denial of Service NAA5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.512 3GPP TS 33.516 4.2.2.1.2
Incorrect implementation of synchronisation failure handling	The Security Anchor Function should handle authentication failure message with synchronisation failure (AUTS) from the UE, as to prevent possible exploitation from denial of service / resource exhaustion attacks / incidents. Complementary procedures have to be performed at USIM level. Synchronization failure handling and/or Storing of authentication status of UE by UDM could conduct to access denial to resources	AMF/SEAF; USIM; UDM	TS 33.501 6.1.3.3. Handling of synchronization failure or MAC failure	The Security Anchor Function should handle authentication failure message with synchronisation failure (AUTS) from the UE, as to prevent possible exploitation from denial of service / resource exhaustion attacks / incidents. Complementary procedures have to be performed at USIM level.	Denial of Service (TR 33.926 K.2.2.1., TR 33.926 E.2.2.2) NAA5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.512 3GPP TS 33.514 4.2.2.1.

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerabilities in implementation of UPF security functionalities							
Inconsistent allocation of Tunnel Endpoint Identifier	TEID, as part of the CN Tunnel information, is used by the UPF and gNB/ng-eNB for user plane routing. The failure to guarantee the uniqueness of the TEID for a PDU session interrupts the routing of user traffic. It also interrupts charging. If multiple PDU sessions were to share the same TEID at the same time, the counts for the network usage of a single PDU session will be in fact the counts for the network usage of multiple sessions, creating charging errors.	UPF	TS 23.501/5.8.2.3.1 TS 29.281 / 5.1 TS 23.060 /14.6	Allocation and release of CN Tunnel Info is performed when a new PDU Session is established or released. This functionality is supported either by SMF or UPF, based on operator's configuration on the SMF as specified in TS 23.501, clause 5.8.2.3.1. Tunnel Endpoint Identifier (TEID): This field unambiguously identifies a tunnel endpoint in the receiving GTP U protocol entity. The receiving end side of a GTP tunnel locally assigns the TEID value the transmitting side has to use as specified in TS 29.281, clause 5.1. The TEID is a unique identifier within one IP address of a logical node." As specified in TS 23.060, clause 14.6	Tampering. (33.926/L.2.4, J.2.2.2) NAA2, NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP 33.513 3GPP 33.515 4.2.2.6 4.2.2.1.2.
Improper allocation of security policy determined by SMF	It is required that user Plane Security Policy from UDM takes precedence over locally configured User Plane Security Policy in SMF. If SMF fails to comply with the requirement, user plane security may be degraded. For example, if the UP security policy from the UDM mandates the ciphering and integrity protection of the user plane data, but no protection is indicated in the local UP security policy at the SMF, and the local UP security policy takes the priority, then the user plane data will be sent over the air without any protection.	User Plane Data	TS23.501, 5.10.3	It is required that user Plane Security Policy from UDM takes precedence over locally configured User Plane Security Policy in SMF. If SMF fails to comply with the requirement, user plane security may be degraded. For example, if the UP security policy from the UDM mandates the ciphering and integrity protection of the user plane data, but no protection is indicated in the local UP security policy at the SMF, and the local UP security policy takes the priority, then the user plane data will be sent over the air without any protection.	Tampering data, Information Disclosure (TR 33.926 / J.2.2.1) NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.515 4.2.2.1.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Incorrect implementation of user plane data protection	It is required that the SMF verifies that the UP security policy received from the ng-eNB/gNB is the same as that stored locally at the SMF. If the SMF fails to check, security degradation of UP traffic may occur. For example, if the UP security policy received from the ng-eNB/gNB indicates no security protection, while the local policy mandates the opposite, and SMF uses the received UP security policy without validation, then the user plane data will be unprotected	User Plane Data	TS 33.501/6.6.1	The SMF must provide UP security policy for a PDU session to the ng-eNB/gNB during the PDU session establishment procedure. In particular, The SMF shall verify that the UE's UP security policy received from the target ng-eNB/gNB is the same as the UE's UP security policy that the SMF has locally stored. If there is a mismatch, the SMF shall send its locally stored UE's UP security policy of the corresponding PDU sessions to the target gNB. Failure to do so may result in manipulation of UP Security policy and compromise of data	Tampering data, Information disclosure (TR 33.926/ J.2.2.4) NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.515 4.2.2.1.3
Vulnerabilities in implementation of UDM security functionalities							
Incorrect implementation of SUCI de-concealment	If the SUPI in the UE and the SUPI retrieved from Nudm_Authentication_Get Response message are not the same, the AMF key generated based on the SUPI in the UE is also not the same as the AMF key generated in the AMF/SEAF. As a result the subsequent NAS SMC procedure will always fail. Hence, UE will never be able to use the services provided by the serving AMF	UDM	TS 33.501/5.8.2. Subscriber privacy related requirements to UDM and SIDF	The SIDF is responsible for de-concealment of the SUCI - The SIDF shall be a service offered by UDM. - The SIDF shall resolve the SUPI from the SUCI based on the protection scheme used to generate the SUCI. The Home Network Private Key used for subscriber privacy shall be protected from physical attacks in the UDM. The UDM shall hold the Home Network Public Key Identifier(s) for the private/public key pair(s) used for subscriber privacy. The algorithm used for subscriber privacy shall be executed in the secure environment of the UDM.	Denial of Service (33.926/E.2.2.1) NAA5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.514 4.2.1.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Incorrect implementation of handling of authentication status by UDM	If the UDM does not store the authentication status of a UE, the 5G network cannot support the increased home control, which is useful in preventing certain types of fraud, e.g. fraudulent Nudm_UECM_Registration Request sending a malicious AMF for registering the malicious AMF in UDM that is not actually present in the visited network. Without the authentication status in the UDM, or if the stored authentication status is incorrect, the Nudm_UECM_Registration Request sent from malicious AMF may be accepted.	UDM	TS 33.501 / 6.1.4.1a Linking authentication confirmation to Nudm_UECM_Registration procedure from AMF	When 3GPP credentials are used in above cases, the result of the authentication procedure is reported to the UDM. The feature of increased home control is useful in preventing certain types of fraud, e.g. fraudulent Nudm_UECM_Registration Request for registering the subscriber's serving AMF in UDM that are not actually present in the visited network. But an authentication protocol by itself cannot provide protection against such fraud. The authentication result needs to be linked to subsequent procedures, e.g. the Nudm_UECM_Registration procedure from the AMF in some way to achieve the desired protection.	Denial of Service (33.926/E.2.2.3) NAA5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.514 4.2.2.2
Incorrect implementation of handling of synchronisation failure	The Security Anchor Function should handle authentication failure message with synchronisation failure (AUTS) from the UE, as to prevent possible exploitation from denial of service / resource exhaustion attacks / incidents. Complementary procedures have to be performed at USIM level. Synchronization failure handling and/or Storing of authentication status of UE by UDM could conduct to access denial to resources	AMF/SEAF; USIM; UDM	TS 33.501 6.1.3.3. Handling of synchronization failure or MAC failure	The Security Anchor Function should handle authentication failure message with synchronisation failure (AUTS) from the UE, as to prevent possible exploitation from denial of service / resource exhaustion attacks / incidents. Complementary procedures have to be performed at USIM level.	Denial of Service (TR 33.926 K.2.2.1., TR 33.926 E.2.2.2) NAA5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.512 3GPP TS 33.514 4.2.2.1.

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerabilities in implementation of SMF security functionalities							
Incorrect implementation of checking of user plane security policy by SMF	It is required that user Plane Security Policy from UDM takes precedence over locally configured User Plane Security Policy in SMF. If SMF fails to comply with the requirement, user plane security may be degraded. For example, if the UP security policy from the UDM mandates the ciphering and integrity protection of the user plane data, but no protection is indicated in the local UP security policy at the SMF, and the local UP security policy takes the priority, then the user plane data will be sent over the air without any protection.	SMF	TS23.501, 5.10.3	It is required that user Plane Security Policy from UDM takes precedence over locally configured User Plane Security Policy in SMF. If SMF fails to comply with the requirement, user plane security may be degraded. For example, if the UP security policy from the UDM mandates the ciphering and integrity protection of the user plane data, but no protection is indicated in the local UP security policy at the SMF, and the local UP security policy takes the priority, then the user plane data will be sent over the air without any protection.	Tampering data, Information Disclosure (TR 33.926 / J.2.2.1) NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.515 4.2.2.1.1
Incorrect implementation of handling of user plane security policy by SMF	It is required that the SMF verifies that the UP security policy received from the ng-eNB/gNB is the same as that stored locally at the SMF. If the SMF fails to check, security degradation of UP traffic may occur. For example, if the UP security policy received from the ng-eNB/gNB indicates no security protection, while the local policy mandates the opposite, and SMF uses the received UP security policy without validation, then the user plane data will be unprotected	SMF	TS 33.501/6.6.1	The SMF must provide UP security policy for a PDU session to the ng-eNB/gNB during the PDU session establishment procedure. In particular, The SMF shall verify that the UE's UP security policy received from the target ng-eNB/gNB is the same as the UE's UP security policy that the SMF has locally stored. If there is a mismatch, the SMF shall send its locally stored UE's UP security policy of the corresponding PDU sessions to the target gNB. Failure to do so may result in manipulation of UP Security policy and compromise of data	Tampering data, Information disclosure (TR 33.926/ J.2.2.4) NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.515 4.2.2.1.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Failure to assign unique Charging ID for a session	At the SMF if more than one PDU session were to share the same charging ID, the charging information for a PDU session would be wrongly correlated, creating charging errors.	SMF; Charging data	TS 32.255/5.1	Requirements for handling of charging data, including identifiers by the SMF are defined in TS 32.255. / Clause 5.1.	Tampering data, Information disclosure (TR 33.926/J.2.2.3) NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.515 4.2.2.1.4
Vulnerabilities in implementation of SEPP security functionalities							
Incorrect implementation of e2e core network interconnection security requirements	Incorrect / incomplete implementation of requirements for E2E interconnection between core network functions, as defined in 3GPP TS 33.501 clause 5.9.3. open confidentiality, integrity and availability risk to all data passed across networks and to unprotected access to network functions	SEPP, IPX	TS 33.501 5.9.3 Requirements for e2e core network interconnection security	3GPP TS 33.501 clause 5.9.3. defines security requirements for E2E interconnection between core network, requirements to be covered generally by the SEPP.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.517 4.2.2.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Incorrect handling of cryptographic material of peer SEPPs and IPX providers	There are the following risks if cryptographic material of peer SEPPs and cryptographic material of IPX providers are not clearly differentiated and misused: - The SEPP using the wrong cryptographic material will lead to the failure of N32-c TLS connection establishment with the peer SEPP; or lead to rejecting genuine N32-f JSON patches from an authentic intermediate IPX provider. This can result in service interruption as well as waste of system resources. - The SEPP will wrongly accept forged N32-f JSON patches signed by a peer SEPP, which maliciously impersonates an intermediate IPX provider. This can result in service data tampering as well as waste of system resources. - The SEPP will wrongly establish N32-c TLS connection with an intermediate IPX entity, which maliciously impersonates a peer SEPP. This can result in information disclosure as well as waste of system resources. - Threatened Asset: SEPP Application, N32-c, N32-f, Application layer security data, Sufficient Processing Capacity	SEPP	TS 33.501 / 5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP)	The SEPP shall protect application layer control plane messages between two NFs belonging to different PLMNs that use the N32 interface to communicate with each other. The SEPP shall perform mutual authentication and negotiation of cipher suites with the SEPP in the roaming network. The SEPP shall handle key management aspects that involve setting up the required cryptographic keys needed for securing messages on the N32 interface between two SEPPs.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.517 4.2.2.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Incorrect implementation of cryptographic material handling beyond connection-specific scope	There are following risks if the SEPP authenticates N32-f message modifications using the cryptographic material from an IPX provider which was not exchanged as part of the IPX security information list via the related N32-c connection: - The SEPP using the wrong cryptographic material will lead to failed authentication of N32-f message modifications signed by the authentic IPX provider, who is a part of the related N32-c connection. This can result in service interruption as well as waste of system resources. - The SEPP will wrongly accept N32-f JSON patches signed by an IPX provider, who is a part of a different N32-c connection. This can result in service data tampering as well as waste of system resources. - Threatened Asset: SEPP Application, N32-c, N32-f, Sufficient Processing Capacity	SEPP	TS 33.501 / 5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP)	The SEPP shall protect application layer control plane messages between two NFs belonging to different PLMNs that use the N32 interface to communicate with each other. The SEPP shall perform mutual authentication and negotiation of cipher suites with the SEPP in the roaming network. The SEPP shall handle key management aspects that involve setting up the required cryptographic keys needed for securing messages on the N32 interface between two SEPPs.	Denial of Service, Tampering of Data, Information Disclosure NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.517 4.2.2.3
Incorrect implementation of handling of serving PLMN ID mismatch	Wrong handling of serving PLMN ID mismatch could affect the authentication process giving unauthorized access to an attacker	SEPP	TS 33.501/13.2.4.7 Message verification by the receiving SEPP TS 33.501/13.4.1.2 Service access authorisation in roaming scenarios	The receiving SEPP shall verify that the PLMN-ID contained in the incoming N32-f message matches the PLMN-ID in the related N32-f context" as specified in TS 33.501 , clause 13.2.4.7. The pSEPP shall check that the serving PLMN ID of subject claim in the access token matches the remote PLMN ID corresponding to the N32-f context Id in the N32 message as specified in TS 33.501 , clause 13.4.1.2.	Denial of Service, Information Disclosure, Spoofing Identity NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.517 4.2.2.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Failure to replace confidential IEs with NULL in original N32-f message	Failure to replace confidential IEs with NULL in original N32-f message may lead to exposure of confidential IEs in N32-f message	SEPP	TS 33.501/13.2.4.3.1.1 clearTextEncapsulatedMessage	If there is any attribute value that requires encryption, the value shall be replaced by null. The SEPP shall calculate a JSON patch document, dataToIntegrityProtectAndCipher (clause 13.2.4.3.2), that replaces any nulls with the required values.	Information Disclosure. NAA4, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.517 4.2.2.5
Incorrect implementation of handling for protection policies mismatch	there are the following risks if the SEPP cannot detect the mismatch between the policies received on N32-c connection from a specific roaming partner and the policies manually configured on it for this specific roaming partner and IPX provider: - The policies received on N32-c connection from a peer SEPP could be tampered by an attacker, which is however not detected. Or the policies manually configured on the SEPP could be misconfigured, which is however not detected. a) If Data-type encryption policies are tampered or misconfigured, the IEs on N32-f which shall be encrypted may be disclosed due to policy tampering. This can result in information disclosure. b) If Modification policies are tampered or misconfigured, the IEs on N32-f which cannot be modified/added/removed by IPX provider may be tampered. This can result in tampering of data. - As the data-type encryption policies in the two partner SEPPs are not equal, a consistent ciphering of IEs on N32-f cannot be enforced.	SEPP, Protection Policies	TS 33.501/13.2.3.6 Precedence of policies in the SEPP	When a SEPP receives a data-type encryption or modification policy on N32-c as specified in clause 13.2.2.2, it shall compare it to the one that has been manually configured for this specific roaming partner and IPX provider. If a mismatch occurs for one of the two policies, the SEPP shall perform one of the following actions, according to operator policy: a) Send the error message <TBD> to the peer SEPP; b) Create a local warning	Information Disclosure. Tampering of Data, Denial of Service NAA2, NAA3, NAA4, NAA5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.517 4.2.2.6
Failure to comply with JWS profile restriction	Use of weak JWS algorithm instead of specific algorithm	SEPP	TS 33.501/13.2.4.9 JWS profile restriction	SEPPs and IPXs shall follow the JWS profile as defined in TS 33.210 [3] with the restriction that they shall only use ES256 algorithm	Information Disclosure. NAA4, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.517 4.2.2.7

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Misplacement of encrypted IEs in JSON object by IPX	Basic validation rules fail to be applied irrespective of the policy exchanged between two roaming partners	SEPP	TS 33.501/13.2.3.4 Modification policy for N32 application layer solution TS 33.501/13.2.4.1 N32-f connection between SEPPs	The following basic validation rule shall always be applied irrespective of the policy exchanged between two roaming partners: IEs requiring encryption shall not be inserted at a different location in the JSON object. - as specified in TS 33.501, clause 13.2.3.4. A SEPP shall verify that an intermediate IPX has not moved or copied an encrypted IE to a location that would be reflected from the producer NF in an IE without encryption - as specified in TS 33.501, clause 13.2.4.1.	Information Disclosure. NAA4, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.517 4.2.2.8
Vulnerabilities in implementation of NRF security functionalities							
No slice specific authorisation for NF discovery	If NF discovery authorisation for specific slice is not supported by the NRF, the NF instance in one slice can discover NF instances belonging to other slices. This can result in reduced assurance level of slice data isolation, making the system easily attacked as well as wasting resource	NRF, NF profile of available NF instances	TS 33.501 / 5.9.2.1 TS 23.502 / 4.17.4.	NRF shall be able to ensure that NF Discovery and registration requests are authorized - as specified in TS 33.501, clause 5.9.2.1. The NRF authorizes the Nnrf_NFDiscovery_Request. Based on the profile of the expected NF/NF service and the type of the NF service consumer, the NRF determines whether the NF service consumer is allowed to discover the expected NF instance(s). If the expected NF instance(s) or NF service instance(s) are deployed in a certain network slice, NRF authorizes the discovery request according to the discovery configuration of the Network Slice, e.g. the expected NF instance(s) are only discoverable by the NF in the same network slice - as specified in TS 23.502, clause 4.17.4.	Information Disclosure, Elevation of privilege (TR 33.926 / H.2.2.1) NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.518 4.2.2.2.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerabilities in implementation of NEF security functionalities							
No authentication on application function	If the authentication of the Application Function is not supported, the application function without legal certificates, or pre-shared key could be able to establish a TLS connection with the NEF. The data stored in the NEF may be exposed to an attacker	NEF	TS 33.501/5.9.2.3 NEF security requirements	- Integrity protection, replay protection and confidentiality protection for communication between the NEF and Application Function - Mutual authentication between the NEF and Application Function - Internal 5G Core information such as DNN, S-NSSAI etc., shall not be sent outside the 3GPP operator domain. - SUPI shall not be sent outside the 3GPP operator domain by NEF The NEF shall be able to determine whether the Application Function is authorized to interact with the relevant Network Functions..	Information Disclosure, tampering (33.926/I.2.2.1) NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.519 4.2.2.1.1
No Authorisation on northbound APIs	A malicious AF without OAuth-based authorisation or with an incorrect access token may invoke the NEF services arbitrarily. For example, an attacker may invoke the Nnef_EventExposure Subscriber service provide by the NEF without authorisation. The Event data related with this subscribe will be leaked to the attacker.	NEF	TS 33.501/12.4 Authorisation of Application Function's requests	Network Entity. The NEF shall authorize the requests from Application Function using OAuth-based authorisation mechanism, the specific authorisation mechanisms shall follow the provisions given in RFC 6749	Elevation of Privilege, Information Disclosure (33.926/I.2.2.2) NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.519 4.2.2.1.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper protection of Data and Information of 5G Core components							
System functions revealing confidential data	Presence of active system function(s) that reveal confidential system internal data in the clear to users and administrators. Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).	UPF; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.2.2 Protecting data and information – Confidential System Internal Data	When the system is not under maintenance, there shall be no system function that reveals confidential system internal data in the clear to users and administrators. Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).	Elevation of Privilege, Information Disclosure, Tampering NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.2.2
Improper protection of data and information in storage	For sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of a system that are needed for the functionality shall be protected against manipulation. In addition, the following rules apply for: - Systems that need access to identification and authentication data in the clear, e.g. in order to perform an authentication. Such systems shall not store this data in the clear, but scramble or encrypt it by implementation-specific means. - Systems that do not need access to sensitive data (e.g. user passwords) in the clear. Such systems shall hash this sensitive data - Stored files on the network product: examples for protection against manipulation are the use of checksum or cryptographic methods.]	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.2.3 Protecting data and information in storage	For sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of a system that are needed for the functionality shall be protected against manipulation.	Elevation of Privilege, Information Disclosure, Tampering NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.2.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Lack of or improper cryptographic protection of data in transfer	The transmission of data is done without proper protection (industry standard network protocols with sufficient security measures and industry accepted cryptographic algorithms), as defined in TS33.310/33.210	UPF/User Data; UPF/Signalling Data; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.2.4 Protecting data and information in transfer	Usage of cryptographically protected network protocols is required. The transmission of data with a need of protection shall use industry standard network protocols with sufficient security measures and industry accepted algorithms. In particular, a protocol version without known vulnerabilities or a secure alternative shall be used.	Spoofing, Information disclosure NAA3, NAA4, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.2.4
No traceability of access to personal data	In some cases, access to personal data in clear text might be required. If such access is required, access to this data shall be logged, and the log shall contain who accessed what data without revealing personal data in clear text. When for practical purposes such logging is not available, a coarser grain logging is allowed. In some cases, the personal data stored in the log files may allow the direct identification of a subscriber. In such cases, the revealed personal information may not expose the subscriber to any kind of privacy violation	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.2.5 Logging access to personal data	In some cases, access to personal data in clear text might be required. If such access is required, access to this data shall be logged, and the log shall contain who accessed what data without revealing personal data in clear text. When for practical purposes such logging is not available, a coarser grain logging is allowed. In some cases, the personal data stored in the log files may allow the direct identification of a subscriber. In such cases, the revealed personal information may not expose the subscriber to any kind of privacy violation.	Information disclosure NAA4, LEG	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.2.5

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper protection of availability and integrity of 5G Core components							
Failure to address overload situation	Overload situation could appear in the case of DoS attack or increased traffic. Lack to deal with such events affects availability of information or security functionalities	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.3.1 System handling during overload situations TS 33.117 /4.2.3.3.3 System handling during excessive overload situations	The system shall provide security measures to deal with overload situations which may occur as a result of a denial of service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided. In the situation where the security measures are no longer sufficient., it shall be ensured that the system cannot reach an undefined and thus potentially insecure state. In an extreme case this means that a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.	Denial of service attacks NAA5, UD5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.3.1, 4.2.3.3.3
Boot from unauthorized memory devices	The network product can boot only from the memory devices intended for this purpose	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.3.2 Boot from intended memory devices only	The network product can boot only from the memory devices intended for this purpose	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.3.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper handling of unexpected input	During transmission of data to a system it is necessary to validate input to the network product before processing. This includes all data which is sent to the system. Examples of this are user input, values in arrays and content in protocols. The following typical implementation errors shall be avoided: - No validation on the lengths of transferred data - Incorrect assumptions about data formats - No validation that received data complies with the specification - Insufficient handling of protocol errors in received data - Insufficient restriction on recursion when parsing complex data formats - White listing or escaping for inputs outside the values margin	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.3.4 System robustness against unexpected input	During transmission of data to a system it is necessary to validate input to the network product before processing. This includes all data which is sent to the system. Examples of this are user input, values in arrays and content in protocols.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.3.4
Insufficient assurance of software package integrity	Lack of software package integrity could affect CIA of data, services, hardware and policies during installation or upgrade phases for the envisioned product/system. Missing information regarding software package integrity checks, including details of how the integrity check is carried out. Missing authentication and access control mechanisms for software package installation.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.3.5 Network Product software package integrity validation	1) Software package integrity shall be validated in the installation/upgrade stage; 2) Network product shall support software package integrity validation via cryptographic means, e.g. digital signature. To this end, the network product has a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software update is originated from only these sources; 3) Tampered software shall not be executed or installed if integrity check fails; 4) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update, and modify the list mentioned in bullet 2.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.3.5

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerable mechanisms for authentication and authorisation of 5G Core components							
Unauthenticated access to system functions	The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) opens the opportunity of exploitation and limits accountability. This includes M2M communication	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.4.1.1 System functions shall not be used without successful authentication and authorisation.	The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems. An exception to the authentication and authorisation requirement are functions for public use such as those for a Web server on the Internet, via which information is made available to the public	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.1.1
Improper authentication mechanisms	Depending of information sensitivity different level of strong authentication mechanisms are required. Fail to identify the proper correspondence between levels of protection and authentication mechanisms implemented creates the possibility to allow unauthorized entities to access unallocated resources	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.4.1.2 Accounts shall allow unambiguous identification of the user TS 33.117 / 4.2.3.4.2.1 Account protection by at least one authentication attribute	The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.1.2, 4.2.3.4.2.1 4.2.3.4.3.

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Predefined/ default accounts and/or authentication attributes	All predefined or default accounts and/or or default authentication attributes shall be deleted or disabled	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.4.2.2 Predefined accounts shall be deleted or disabled TS 33.117 / 4.2.3.4.2.3 Predefined or default authentication attributes shall be deleted or disabled	All predefined or default accounts shall be deleted or disabled. Should this measure not be possible the accounts shall be locked for remote login. Preconfigured authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the vendor provides instructions on how to manually change it	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.2.2 4.2.3.4.2.3
Weak or missing password policy	A password policy shall address the password structure, password change, hiding password display capabilities, consecutive failed login attempts. A week password structure and/or a long validity password period could lead to a successful brute force attack. Password display is vulnerable to eavesdropping attack. Password policy is a security policy component.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.4.3 Password policy	Password policy requirements include requirements regarding Password complexity, password change, Protection against brute force and dictionary attacks, hiding password display	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.3.
Lack of mutual authentication of entities for management interfaces	The network product management shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.4.4.1 Authentication on Network Product Management and Maintenance interfaces	The network product management shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.4.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper authorisation and access control policy	The authorisations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.4.6 Authorisation and access control	The authorisations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform. Authorisations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.6
Improper session protection mechanisms of 5G Core components							
Improper / missing functionality for session protection	The system shall have a function that allows a signed in user to logout at any time. All processes under the logged in user ID shall be terminated on log out. A permanent exposed session increases the vulnerability of the system as an entry point for unauthorized person. OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.5 Protecting sessions	The system shall have a function that allows a signed in user to logout at any time. All processes under the logged in user ID shall be terminated on log out. The network product shall be able to continue to operate without interactive sessions. An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx"	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.5.

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Insufficient or improper monitoring mechanisms of 5G Core components							
Lack of or improper security event logging	lack of security events logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred do not allow a correct and rapid audit in case of security incident occurrence. Security restauration is delayed.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.6.1 Security event logging	Security events shall be logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred. For each security event, the log entry shall include user name and/or timestamp and/or performed action and/or result and/or length of session and/or values exceeded and/or value reached. IETF RFC 3871, section 2.11.10 specifies the minimum set of security events.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx"	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.6.1
Vulnerabilities in Operating Systems supporting 5G Core components							
Improper / missing controls for protection of security event log files	Security event logs should be forwarded or uploaded to a central location or external systems. Security event log files shall be protected in storage and transfer states, too. Availability and integrity of security event log files could conduct to delays, wrong audit results, delays in security restauration, threats persistence.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.3.6.2 Log transfer to centralized storage TS 33.117 / 4.2.3.6.3 Protection of security event log files	Log functions should upload securely of log files to a central location or to an external system for the Network Product that is logging. Secure transport protocols shall be used. The security event log shall be access controlled (file access rights) so only privileged users have access to the log files.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.6.2 4.2.3.6.3
Improper handling of growing content by file system	Growing or dynamic content (e.g. log files, uploads) could influence system functions. A file system that reaches its maximum capacity could stop a system from operating properly.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.4.1.1.1 Handling of growing content	Growing or dynamic content (e.g. log files, uploads) shall not influence system functions. A file system that reaches its maximum capacity shall not stop a system from operating properly. Therefore, countermeasures shall be taken such as usage of dedicated file systems, separated from main system functions, or quotas, or at least a file system monitoring to ensure that this scenario is avoided.	Denial of service attacks, equipment / software errors, growing dynamic content NAA5, UD5, FM5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.4.1.1.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Processing of ICMP packets not required for operation	Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the network product. In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.4.1.1.2 Processing of ICMPv4 and ICMPv6 packets	Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the network product. In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk. Permitted, forbidden and optional ICMP packets are detailed in TS 33.117 clause 4.2.4.1.1.2	Denial of service attacks, equipment / software errors, misconfiguratio ns NAA5, UD5, FM5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.4.1.1.2
Processing of IP packets with unnecessary options or extensions	IP packets with unnecessary options or extension headers could be used by attackers to get unauthorized access to system resources.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.4.1.1.3 IP packets with unnecessary options or extension headers shall not be processed	IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g. source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.4.1.1.3
Privilege Escalation allowed without re-authentication	Authenticated Privilege Escalation allowed without re-authentication could permit to an authorized user to gain unallocated higher rights to resources, violating security policy	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.4.1.2.1 Authenticated Privilege Escalation only	There shall not be a privilege escalation method in interactive sessions (CLI or GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication. Implementation example: Disable insecure privilege escalation methods so that users are required to (re-)login directly into the account with the required permissions.	Privilege escalation NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.4.1.2.1
Recurrent UIDs for UNIX System accounts	Each system account in UNIX shall have a unique UID, to provide for system account accountability	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.4.2.2 System account identification	Each system account in UNIX shall have a unique UID. The term 'UNIX' includes all major derivatives, including Linux.	Authorisation attacks NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.4.2.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerabilities in Web Servers supporting 5G Core components							
Unsecure Https connection to web servers	The communication between Web client and Web server shall be protected using TLS. TLS profile should be defined in compliance Annex E of TS 33.310, with the following additional requirement: cipher suites with NULL encryption shall not be supported	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.5.1 HTTPS	The communication between Web client and Web server shall be protected using TLS. Cipher suites with NULL encryption shall not be supported	Spoofing identity, Tampering of Data, Information Disclosure NAA2, NAA3, NAA4, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.5.1
Lack of / improper logging of access to the webserver	When logging information lacks completeness, integrity or timeliness it is impossible to detect, analyse and respond to system faults and relevant security events.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.5.2 Webserver logging	Access to the webserver shall be logged. The web server log shall contain the following information: Access timestamp / Source (IP address) / (Optional) Account (if known) / (Optional) Attempted login name (if the associated account does not exist) / Relevant fields in http request. The URL should be included whenever possible / Status code of web server response	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.5.2
Lack of / improper http user session protection	Improper session protection mechanisms may lead to session hijacking, disclosure of confidential information, including authentication attributes	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.5.3 HTTP User sessions	To protect user sessions the Network Product shall support the following session ID and session cookie requirements: 1. The session ID shall uniquely identify the user and distinguish the session from all other active sessions. 2. The session ID shall be unpredictable. 3. The session ID shall not contain sensitive information in clear text (e.g. account number, social security, etc.). 4. In addition to the Session Idle Timeout, the Network Product shall automatically terminate sessions after a configurable maximum lifetime 5. Session ID's shall be regenerated for each new session (e.g. each time a user logs in). 6. The session ID shall not be reused or renewed in subsequent sessions. 7. The Network Product shall not use persistent cookies to manage sessions but only session cookies. This means that	Session hijacking NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.5.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
				neither the "expire" nor the "max-age" attribute shall be set in the cookies. 8. Where session cookies are used the attribute 'HttpOnly' shall be set to true. 9. Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain. 10. Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory. 11. The Network Product shall not accept session identifiers from GET/POST variables. 12. The Network Product shall be configured to only accept server generated session ID's.			
Improper validation of HTTP input	The Network Product shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.5.4 HTTP input validation	The Network Product shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.	Injection, cross-site scripting NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.5.4
Vulnerabilities of network devices running 5G Core components							
Lack of packet filtering functionality	Lack of, or improper mechanisms to filter incoming IP packets on any IP interface according to defined and manageable rules leaves the network device vulnerable to denial-of-service attacks, service degradation or attack aimed at leading the device to an exception state.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.6.2.1 Packet filtering	The Network Product shall provide a mechanism to filter incoming IP packets on any IP interface, as defined in RFC 3871 and TS 33.117 clause 4.2.6.2.1	Denial of service, packet flooding NAA5, FM5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.6.2.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Lack of robustness against unexpected input	If a network device does not have the capability to detect and drop by incoming packets, from other network element, that are manipulated or differing the norm, it can lead to an impairment of availability.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.6.2.2 Interface robustness requirements	All incoming packets, from other network element, that are manipulated or differing the norm shall be detected as invalid and be discarded. The process shall not be affecting the performance of the network device. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets.	Malware, denial-of-service, packet flood NAA5, FM5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.6.2.2
Improper or absent GTP-C Filtering	In the absence of an effective GTP-C filtering mechanisms, the network device is vulnerable to Border gateway bandwidth saturation or GTP flood.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.6.2.3 GTP-C Filtering	For each message of a GTP-C-based protocol, it shall be possible to check whether the sender of this message is authorized to send a message pertaining to this protocol. At least the following actions should be supported when the check is satisfied: Discard: the matching message is discarded /Accept: the matching message is accepted./ Account: the matching message is accounted for, i.e. a counter for the rule is incremented.	Authorisation attacks, man-in-the-middle attacks NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.6.2.3
Improper or absent GTPU Filtering	In the absence of effective GTP-U filtering mechanisms, the network is exposed to malformed GTP packets, denial of service attacks, and out-of-state GTP messages, and also vectors such as spoofed IP packets.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.2.6.2.4 GTP-U Filtering	For each message of a GTP-U-based protocol, it shall be possible to check whether the sender of this message is authorized to send a message pertaining to this protocol.	Authorisation attacks, man-in-the-middle attacks NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.6.2.4
Improper hardening of 5G Core components							
Unnecessary or insecure services / protocols	Should the network product run protocol handlers and services which are not needed for its operation, or which have known security vulnerabilities, they may be manipulated to gain unauthorized access to the system, impair its availability or other forms of manipulation.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.2.1 No unnecessary or insecure services / protocols	The network product shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Software errors NAAx, FMx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Unrestricted reachability of services	The network product shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. The absence of appropriate mechanisms expose the services to risk of exploitation of known or unknown vulnerabilities by malicious parties or technical faults.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.2.2 Restricted reachability of services	The network product shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. On interfaces were services are active, the reachability should be limited to legitimate communication peers. This limitation shall be realized on the network product itself (without measures (e.g. firewall) at network side) according to the requirement detailed in clause 4.2.6.2.1 Packet Filtering.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.2
Unused software components	Unused software components or parts of software which are not needed for operation or functionality of the network product create an unnecessary attack surface. Such unused software components have a high susceptibility of falling outside patching and vulnerability management processes and therefore are increasingly exposed to malicious attacks and technical faults.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.2.3 No unused software	Unused software components or parts of software which are not needed for operation or functionality of the network product shall not be installed or shall be deleted after installation. This includes also parts of a software, which will be installed as examples but typically not be used (e.g. default web pages, example databases, test data).	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.3
Unused software or hardware functions	During installation of software and hardware often functions will be activated that are not required for operation or function of the system. Such hardware and software functions increase the IT attack surface and their exposure is increased by their susceptibility of falling outside access control policies.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.2.4 No unused functions	During installation of software and hardware often functions will be activated that are not required for operation or function of the system. If unused functions of software cannot be deleted or de-installed individually, such functions shall be deactivated in the configuration of the network product permanently. Also, hardware functions which are not required for operation or function of the system (e.g. unused interfaces) shall be permanently deactivated. Permanently means that they shall not be reactivated again after network product reboot.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Unsupported components	Unsupported components incur a high risk of unmitigated vulnerabilities that can be exploited by malicious actors or technical faults.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.2.5 No unsupported components	The network product shall not contain software and hardware components that are no longer supported by their vendor, producer or developer, such as components that have reached end-of-life or end-of-support. Excluded are components that have a special support contract. This contract shall guarantee the correction of vulnerabilities over components' lifetime.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Component malfunctions NAAx, FMx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.5
Remote login of privileged users	Unrestricted remote login for privileged users expose the network element to increased risk of unauthorized access and manipulation.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.2.6 Remote login restrictions for privileged users	Description: Direct login as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to the system remotely.	Authorisation attacks, elevation of privilege NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.6
Excessive file system Authorisation privileges	In the presence of excessive files stem authorisation privileges, application and configuration data is exposed to risks of unauthorised disclosure, tampering, or destruction.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.2.7 file system Authorisation privileges	The system shall be designed to ensure that only users that are authorized to modify files, data, directories or file systems have the necessary privileges to do so.	Unauthorised / erroneous data element modification / deletion NAA1, NAA2, NAA3, UD1, UD2	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.7
Lack of protection against IP-Source address spoofing	IP address spoofing involving the use of a trusted IP address can be used by network intruders to overcome network security measures, such as authentication based on IP addresses. IP address spoofing is most frequently used in denial-of-service attacks, where the objective is to flood the target with an overwhelming volume of traffic, and the attacker does not care about receiving responses to the attack packets.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.3.1.1 IP-Source address spoofing mitigation	Systems shall not process IP packets if their source address is not reachable via the incoming interface.	Packet flood NAA5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Unneeded kernel network functions	Kernel based network functions not needed for the operation of the network element offer an unnecessary attack surface. Particularly vulnerable services are: IP Packet Forwarding between different interfaces of the same equipment, Proxy ARP (resource exhaustion attacks and man-in-the-middle attacks), Directed broadcast (Smurf, Denial of Service attack), IPv4 Multicast handling (smurf and fraggle attacks), gratuitous ARP messages (ARP Cache Poisoning attack)	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.3.1.2 Minimized kernel network functions	Kernel based network functions not needed for the operation of the network element shall be deactivated	Exploitation of vulnerable kernel functions NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.2
automatic launch of removable media	Automatic launch of removable media provides a potential vector for unauthorized or malicious payloads	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.3.1.3 No automatic launch of removable media	The network product shall not automatically launch any application when removable media device such as CD-, DVD-, USB-Sticks or USB-Storage drive is connected. If the operating system supports an automatic launch, it shall be deactivated unless it is required to support availability requirements.	Malware, bypassing of security controls, running unauthorised operating system NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.3
No SYN Flood Prevention	A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.3.1.4 SYN Flood Prevention ; RFC 4987	The network product shall support a mechanism to prevent Syn Flood attacks (e.g. implement the TCP Syn Cookie technique in the TCP stack by setting net.ipv4.tcp_syncookies = 1 in the linux sysctl.conf file). This feature shall be enabled by default.	Syn Flood attacks NAA5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.4
No protection against buffer overflows	In information security and programming, a buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. Buffers are areas of memory set aside to hold data, often while moving it from one section of a program to another, or between programs. Buffer overflows can	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.3.1.5 Protection from buffer overflows	The system shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided.	Buffer overflow attacks NAA2, NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.5

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
	often be triggered by malformed inputs; if one assumes all inputs will be smaller than a certain size and the buffer is created to be that size, then an anomalous transaction that produces more data could cause it to write past the end of the buffer. If this overwrites adjacent data or executable code, this may result in erratic program behaviour, including memory access errors, incorrect results, and crashes. Exploiting the behaviour of a buffer overflow is a well-known security exploit. By sending in data designed to cause a buffer overflow, it is possible to write into memory areas known to hold executable code and replace it with malicious code, or to selectively overwrite data pertaining to the program's state, therefore causing behaviour that was not intended by the original programmer. Buffers are widespread in operating system (OS) code, so it is possible to make attacks that perform privilege escalation and gain unlimited access to the computer's resources.						
No/improper external file system mount restrictions	In the absence of effective external file systems mount restrictions, the system is exposed to privilege escalation and excessive access permissions due to the contents of the mounted file systems.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.3.1.6 External file system mount restrictions	If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.	Malware, bypassing of security controls, running unauthorised operating system NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.6

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Directory listings	Web servers can be configured to automatically list the contents of directories that do not have an index page present. This can aid an attacker by enabling them to quickly identify the resources at a given path, and proceed directly to analysing and attacking those resources. It particularly increases the exposure of sensitive files within the directory that are not intended to be accessible to users, such as temporary files and crash dumps.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.10 No directory listings	Directory listings (indexing) / "Directory browsing" shall be deactivated.	Scanning of vulnerable resources NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.10
Web server information in HTTP headers	The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version and languages used by the web server.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.11 Web server information in HTTP headers	The HTTP header shall not include information on the version of the web server and the modules/add-ons used.	Exploitation of vulnerable components NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.11
Web server information in error pages	The error page sent by the web server discloses information that can aid an attacker, such as the server version, modules/add-ons used or information revealing inner workings such as internal server names, error codes, etc.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.12 Web server information in error pages	User-defined error pages shall not include version information about the web server and the modules/add-ons used. Error messages shall not include internal information such as internal server names, error codes, etc. Default error pages of the web server shall be replaced by error pages defined by the vendor.	Exploitation of vulnerable components NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.12
Unused file type- or script-mappings	Unused File type- or script-mappings can be used in attacks based on delivery of malicious payloads, such as code-injection attacks.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.13 Minimized file type mappings	File type- or script-mappings that are not required shall be deleted, e.g. php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs	Code injection NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.13

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Unrestricted access to files	Improperly restricted file access rights may lead to unauthorized delivery of files which are not meant to be delivered, and to path traversal attacks.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.14 Restricted file access	Restrictive access rights shall be assigned to all files which are directly or indirectly (e.g. via links or in virtual directories) in the web server's document directory. In particular, the web server shall not be able to access files which are not meant to be delivered.	Direct access to restricted data from public domain NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.14
Execution rights outside CGI/Scripting directory	Improper restriction of execute rights may lead to Remote Command Execution by unauthorized delivery of malicious payload through various vectors.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.15 Execute rights exclusive for CGI/Scripting directory	If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights	Code injection NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.15
System privileges for web server processes	If the web server runs under privileged accounts, web server compromise caused by malicious action or technical fault has an increased chance to compromise the host operating system's integrity and availability.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 /4.3.4.2 No system privileges for web server	No web server processes shall run with system privileges. This is best achieved if the web server runs under an account that has minimum privileges. If a process is started by a user with system privileges, execution shall be transferred to a different user without system privileges after the start.	Elevation of privileges NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.2
Active and unused HTTP methods	Unused http methods provide an unnecessary attack surface that can lead to security compromise of the system	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.3 No unused HTTP methods	HTTP methods that are not required shall be deactivated. Standard requests to web servers only use GET, HEAD, and POST. If other methods are required, they shall not introduce security leaks such as TRACK or TRACE.	Abuse of unused vulnerable methods NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.3
Unused web server addons	Unused server addons provide an unnecessary attack surface that can lead to security compromise of the system	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.4 No unused add-ons	All optional add-ons and components of the web server shall be deactivated if they are not required. In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.	Code injection NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Access to compiler, interpreter, or shell via CGI or other server-side scripting	CGI and other server-side scripting specifications provide opportunities to read files, acquire shell access, and corrupt file systems on server machines and their attached hosts. Means of gaining access include: exploiting assumptions of the script, exploiting weaknesses in the server environment, and exploiting weaknesses in other programs and system calls. Presence in the scripting directory of compilers, interpreters or operating system shells renders the system particularly vulnerable.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.5 No compiler, interpreter, or shell via CGI or other server-side scripting	If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory - or other corresponding scripting directory - shall not include compilers or interpreters (e.g. PERL interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells).	Code injection NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.5
Common directory for uploads and CGI/Scripting	In upload is permitted in the CGI/Scripting, the system is vulnerable to code injection / shell upload attacks.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.6 No CGI or other scripting for uploads	If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.	Code injection NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.6
Execution of system commands with server side includes (SSI)	SSIs are directives present on Web applications used to feed an HTML page with dynamic contents. The Server-Side Includes attack allows the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary codes remotely. It can be exploited through manipulation of SSI in use in the application or force its use through user input fields.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.7 No execution of system commands with SSI	If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.	Code injection NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.7
Excessive / improper access rights for web server configuration files	Improper setting of access rights for web server configuration files may lead to unauthorized disclosure or modification of configuration information.	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.8 Access rights for web server configuration	Access rights for web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges. Implementation example: Delete "read" and "write" access rights for "others." Only grant "write" access to the user who configures the web server	Manipulation of server configuration files NAA2, NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.8

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Presence of default content	Presence of default content may disclose information on the web server version, add-ons and configuration or information/file structure, and thus facilitate information gathering for a malicious party. Also, default content may include known vulnerabilities (such as the case of IIS Default Page).	UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.4.9 No default content	Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the web server shall be removed.	Abuse of vulnerable content, collection of system information NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.9
Inadequate traffic separation of traffic belonging to different network domains	Unsegregated traffic belonging to different planes (data, control, management) increases the risk that unauthorized individuals will be able to observe management traffic and/or compromise the device.	O&M; control plane; UPF; gNB; AMF; UDM; SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.5.1 Traffic Separation RFC 3871 / 2.3.5. Support Separate Management Plane IP Interfaces	The network product shall support physical or logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See RFC 3871 [3] for further information.	Lateral movement, elevation of privileges, eavesdropping NAA2, NAA3, NAA4, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.5.1
Code execution or inclusion of external resources by JSON parsers	Execution of JavaScript or any other code contained in JSON objects received on Service Based Interfaces (SBI) expose the system to execution of malicious code delivered over the SBI.	Network Function (NF); 5G Core (5GC); Service-Based Interfaces (SBI); UPF; AMF; UDM, SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.6.2 No code execution or inclusion of external resources by JSON parsers	Parsers used by Network Functions (NF) shall not execute JavaScript or any other code contained in JSON objects received on Service Based Interfaces (SBI). Further, these parsers shall not include any resources external to the received JSON object itself, such as files from the NF's file system or other resources loaded externally	Code injection NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.512-519 4.3.6.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
JSON Parser not robust	For data structures where values are accessible using names (sometimes referred to as keys), e.g. a JSON object, if the names/keys are not unique and duplicated names/keys occur within such a structure, it can result in inconsistent values for that names (or keys), which leads to Denial of Service. - If the format and range of values for the IEs in API messages are not implemented as required (e.g. when the number of leaf IEs exceeds the maximum number or when the size of the JSON body of any HTTP request exceed the maximum size), security vulnerabilities may be introduced such as buffer overflow flow, which may lead to Denial of Service.	Network Function (NF); 5G Core (5GC); Service-Based Interfaces (SBI); UPF; AMF; UDM, SMF; AUSF; SEPP; NRF; NEF	TS 33.117 / 4.3.6.3 Validation of the unique key values in IEs. TS 33.117 / 4.3.6.4 Validation of the IEs limits.	For data structures where values are accessible using names (sometimes referred to as keys), e.g. a JSON object, the name shall be unique. The occurrence of the same name (or key) twice within such a structure shall be an error and the message shall be rejected The valid format and range of values for each IE, when applicable, shall be defined unambiguously.	Software error FMx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.512-519 4.3.6.3, 4.3.6.4

D ANNEX: DETAILED VULNERABILITIES IN NETWORK SLICING

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref/Code Spec
Service Based Vulnerabilities in Network Slicing Management							
Unsecured management exposure interface	This management interface will need to be secured so that only authorized parties can create, alter, and delete network slice instances. Without secure protection, an attacker could: - use charged for services in an unauthorized way - create a network slice instance to deny services to or track customers who expect to use a specific network instance - deny services to customers using an existing slice instance by modifying slice services - perform a man-in-the-middle attack by modifying a slice instance to reroute the traffic maliciously - deny services by deleting a slice instance	Service Based Interfaces, OS-Ma-NFVi	Secure configuration of Management Exposure Interface	A communication service customer shall be authenticated by the network before accessing to the slice management interface. A communication service customer shall authenticate the network before accessing to the slice management interface. The slice management interface shall only be accessed by authorized communication service customers. The management capabilities that a communication service customer is allowed to use are defined by the HPLMN. The slice management interface shall be designed securely to ensure that security features cannot be bypassed. It shall be possible to integrity protect the slice management interface messages. It shall be possible to confidentiality protect the slice management interface messages. It shall be possible to protect the slice management interface messages against replay attacks.	Attackers may gain access to capabilities for the network management without authorisation. Attackers may create network slice instances requiring significant network resources or a large number of network slice instances to exhaust the network resources and potentially bring down the network. Attackers may also modify the configuration of other customers' slice instances to fail their SLA. Attackers could replay management messages causing repeated management operations (e.g. creating duplicated network slices) and false charging etc. NAA2, NAA3, NAA4	MNO, CSP	3GPP TR 33.811 V15.0.0 4.1.1.

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref/Code Spec
Improper protection of Data and Information							
Improper protection of Network Slice Instance supervision / reporting data	During the operation phase of management aspects of a Network Slice Instance, supervision and performance reporting (e.g. for KPI monitoring) are included. NSI modification can be triggered by the result of supervision/reporting, so protecting the integrity of the result of the supervision/reporting data is important. A tampered result may cause an unnecessary or improper NSI modification action such as creation or modification of NSI constituents. If supervision and reporting data is not protected by encryption, an attacker may be able to extract sensitive information such as topology.	Network Slice Instance	Encryption, integrity verification	The result of supervision/reporting should be integrity protected. The supervision and reporting data may be confidentiality protected.	An attacker can tamper the result of supervision/reporting to cause a modification of an NSI. This may cause consumption of network resource or changes to a running slice instance. An attacker can eavesdrop the transmission of supervision and reporting data and extract sensitive information that can be used to execute attacks of running network slice instances.	MNO, CSP	3GPP TR 33.811 V15.0.0 4.2.1.
Lack of / ineffective tamper-proofing of Network Slice Subnet Template (NSST)	A network Slice Subnet Template (NSST) is used during on-boarding and creation of a slice instance. The template describes the structure (i.e. contained components and connectivity between them) and configuration of the network slice subnet, as well as network capability and other artifacts necessary to provision an instance based on the template. To detect a tampered template which could create a compromised NSI, the integrity of template should be protected. The correctness and source of template should also be verified. The confidentiality of an NSST should be protected to prevent attackers getting sensitive information such as topology and configuration about the running NSI.	Network Slice Subnet Instance	Integrity protection of NSST	The network slice subnet template should be integrity protected The management system should verify the correctness and source of the network slice subnet template. The network slice subnet template should be confidentiality protected during transmission and in storage.	Attackers can tamper network slice subnet template during on-boarding, transmission, and storage. Based on a tampered NSST, a slice instance may not be created correctly or successfully. Attackers can get sensitive information about NSIs if NSSTs can be read in clear text during transmission and in storage - later to be used to attack a running NSI. NAA2, NAA3, NAA4	MNO, CSP	3GPP TR 33.811 V15.0.0 4.3.1.

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref/Code Spec
Vulnerabilities in implementation of NS security functionalities							
Insecure procedure for capability negotiation	The services or network slice characteristics include radio access technology, bandwidth, latency, reliability, guaranteed/non-guaranteed QoS, security level etc. It should be possible for these items to be securely negotiable in a standardized way. If the network slice negotiation procedures are not secured in a standardized way, the slice management may be subject to malicious attacks, e.g. man-in-the middle (MitM) attacks to modify and downgrade the slice capabilities.	Network Slice Instance	Protection of negotiation procedure	The negotiation procedure shall be authenticated The negotiation procedure shall be integrity, replay and confidentiality using TLS (recommended TLS 1.2 or TLS 1.3) Access to the network management interface shall be authorised using OAuth 2.0	Man-in-the middle (MitM) attacks to modify and downgrade the slice capabilities NAA2, NAA3, NAA4	MNO, CSP	3GPP TR 33.811 V15.0.0 4.4.1.
Vulnerable mechanisms for authentication and authorisation in Network Slicing Management							
Improper slice-authentication mechanisms	Access control to Network Slices may require additional authorisation and authentication different from the 3GPP SUPI. This will take place after the primary authentication which is still required between the UE and the 5GS for PLMN access authorisation and authentication. If Slice specific authentication is not performed, unauthorized UEs may access the Slice which those UEs are not entitled to access. The unauthorized UEs may consume resources of the Network Slice and they may cause DoS to legitimate UEs.	Network Slice Instance	Additional authentication mechanism	Configure Network Slice to perform access authentication and authorisation in addition to primary authentication. Perform the additional authentication after primary authentication using credentials other than credentials used for primary authentication used for 3GPP access.	Unauthorized access to NSI, DoS for legitimate users NAAx	MNO, CSP	3GPP TR 33.813 V16.0.0 6.2
Lack of protection of NSSAI and home control	Without confidentiality or integrity protection of the User ID and corresponding credentials, sensitive information may leak, and user data may be obtained by attackers.	NSSAAI	Secure authentication mechanisms	Protect the security of the User ID and credentials in UE storage, transition and network storage. Protect the security of the interaction between the 3rd party entities and the network functions performing slice authorisation and authentication. Interaction between the network functions performing slice authorisation and authentication and the related MNO NFs such as AMF, SMF or NSSF	Unauthorized access to User ID, theft of access credentials NAAx	MNO, CSP	3GPP TR 33.813 V16.0.0 6.5

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref/Code Spec
Lack of protection of the User ID and credentials	Network Slice Selection Assistance Information (NSSAI) may contain sensitive information that causes privacy concerns when transmitted in clear. If a Single – Network Slice Selection Assistance Information (S-NSSAI) is sent in the clear text during the Radio Resource Control (RRC) connection establishment procedure, then the user privacy is lost. A non-compliant serving PLMN may transmit NSSAI in clear, leading to a leak of NSSAI.	NSSAAI	Protect S-NSSAI during transmission	5G system shall provide confidentiality protection for NSSAI transmission: - Cryptographic key available from an earlier authentication run, - Use of existing NAS or AS security contexts.	Man-in-the middle (MitM) attacks may disrupt the services, leak of NSSAI NAAx	MNO, CSP	3GPP TR 33.813 V16.0.0 6.7
Insufficient or improper monitoring mechanism of Network Slice Instance (NSI)							
Insufficient / inadequate logging and auditing across NSI lifecycle	Security must be enforced in all phases of the NSI lifecycle because a vulnerability in one phase can introduce vulnerabilities in other phases. Without proper monetarization of all phases, security events remain undetected	Network Slice Instance	Security event logging	Appropriate logging and auditing mechanisms should be implemented throughout the slice life cycle. Real-time analysis of security events to immediately detect any attempted attack. Slice life-cycle includes: 1) Preparation phase; 2) Installation, Configuration, and Activation phase; 3) Run-time phase; 4) Decommissioning phase.	Create fake slices. Delete/deactivate slices. Expose/change the configuration of the network slice. DoS/consume resources and network functions. (NAAx, FMx)	MNO, CSP	5G Network Slicing: A Security Overview[95]
Improper protection of security event log files	Logs and audit trails can assist in detecting security violations, performance problems, and flaws. It is important that audit records are available and complete. For this reason, protection is required for all security events.	Network Slice Management	Protection of log information	Establish policies and procedures for log management. Logs must be protected from breaches of their confidentiality and integrity.	Logs that are secured improperly in storage or in transit might be susceptible to intentional and unintentional alteration and destruction. (NAAx, FMx)	MNO, CSP	NIST 800-92

[95] R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in IEEE Access, vol. 8, pp. 99999-100009, 2020, doi: 10.1109/ACCESS.2020.2997702, accessed October 2020.

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref/Code Spec
Improper isolation of monitoring capabilities and data	A correct level of isolation must be implemented among the services and between the slice and the consuming services. Security is one dimension of isolation, together with performance and dependability. Isolation must be considered from different perspectives: isolation between network slices, isolation between network functions, isolation between users, isolation of data. The measurement of isolation remains an open problem.	Network Slice Instance	Isolation of data	Proper isolation between distinct slices in the slice manager and restriction to perform changes on parameters shared among slices belonging to different tenants. Strong authentication and access control procedures must be in place. If a 5G customer device is allowed to simultaneously attach to multiple slices, isolation of data should be possible at the customer device too.	Unauthorized access, leakage of shared parameters, sensitive data transmitted between the slices. (NAAx, FMx)	MNO, CSP	5G Network Slicing: A Security Overview
Improper or insufficient end-to-end monitoring capabilities for NSI	The concept of end-to end security is closely connected to the concepts of isolation and orchestration. Without end-to-end security monitoring, it is not possible to ensure adequate protection of the service provided by the network slice. All communication (e.g., between the slice and the resource layer, the slice and the slice manager, the sub-slices of a slice, the customer device and the access point in the network) should use adequate mechanisms to assure the target security level.	Network Slice Instance	End-to-end monitoring	Slices are end-to-end logical networks, so end-to-end security should be considered. All resources and network functions consumed by a slice should be monitored.	Availability of the service, sensitive data transmitted between the slices. (NAAx, FMx)	MNO, CSP	5G Network Slicing: A Security Overview
Insufficient / inadequate logging and auditing across NSI lifecycle	Security must be enforced in all phases because a vulnerability in one phase can introduce vulnerabilities in other phases. Slice life-cycle include: 1) Preparation phase; 2) 2) Installation, Configuration, and Activation phase; 3) Run-time phase; 4) Decommissioning phase. Without proper monetarization of all phases, security events remain undetected	Network Slice Instance	Security event logging	Appropriate logging and auditing mechanisms should be implemented throughout the slice life cycle. Real-time analysis of security events to immediately detect any attempted attack.	Create fake slices. Delete/deactivate slices. Expose/change the configuration of the network slice. DoS/consume resources and network functions. (NAAx, FMx)	MNO, CSP	5G Network Slicing: A Security Overview

E ANNEX: DETAILED VULNERABILITIES IN THE RADIO ACCESS NETWORK

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper implementation of gNB security functions							
Improper Ciphering of RRC-signalling	RRC-signalling data sent between UE and gNB over the NG RAN is not encrypted or encrypted using a non-compliant ciphering algorithm	gNB, UE	TS 33.501/5.3.2 User data and signalling data confidentiality	The gNB shall implement the following ciphering algorithms: - NEA0, 128-NEA1, 128-NEA2, 128-NEA3	Tampering data, Information Disclosure, Denial of Service (NAAx)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.6
Failure to ensure control plane data confidentiality protection over N2/Xn interface	If the gNB does not provide confidentiality protection for control plane packets on the N2/Xn reference points, then the control plane packets sent between gNBs (e.g. inter-gNB handover) and from gNB to AMF (e.g. handover on AMF change) can be intercepted and/or modified and the gNB can be compromised by attackers to prevent service to legitimate users (e.g. Handover failure) or to perform masquerading by making use of the legitimate users' UE identifiers to gain access to the network.	gNB, N2/Xn interface	TS 33.501/9.2 and 9.4 Security mechanisms for N2 and Xn interfaces	In order to protect the reference points, it is required to implement IPsec ESP and IKEv2 certificates-based authentication. IPsec is mandatory to implement on the gNB and the ng-eNB. In addition to IPsec, DTLS shall be supported to provide integrity protection, replay protection and confidentiality protection.	Tampering data, Information Disclosure, Denial of Service (NAAx)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.16
Improper mechanisms to protect RRC signalling data integrity	If the gNB does not provide integrity protection for control plane packets, they risk being exposed and/or modified. The intruder manipulations on control plane packets can lead to denial of service to legitimate users.	gNB	TS 33.501/5.3.3 User data and signalling data integrity	The gNB shall support integrity protection and replay protection of RRC-signalling.	Tampering data, Denial of Service, Rogue base station (NAAx, EIH4)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
RRC integrity check failure	Failure in RRC integrity check affects the data/message exchange between gNB and UE	gNB, UE	TS 33.501/6.5.1 RRC integrity mechanisms	RRC integrity protection shall be provided by the PDCP layer between UE and gNB and no layers below PDCP shall be integrity protected. Replay protection shall be activated when integrity protection is activated. Full mechanism is described in TS 33.501/6.5.1 RRC integrity mechanisms	Tampering data, Denial of Service, Rogue base station (NAAx)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.4
Failure to ensure control plane data integrity protection over N2/Xn interface	The integrity and replay-protection of transport of control plane data and user data over N2/Xn could be affected	gNB	TS 33.501/9.2 and 9.4 Security mechanisms for N2 and Xn interfaces	In order to protect the reference points, it is required to implement IPsec ESP and IKEv2 certificates-based authentication. IPsec is mandatory to implement on the gNB and the ng-eNB. In addition to IPsec, DTLS shall be supported to provide integrity protection, replay protection and confidentiality protection.	Tampering data, Denial of Service. (NAAx, EIH4)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.17
Improper or missing replay protection of RRC-signalling	gNB must provide replay protection by dropping/ignoring replayed packets. If the gNB does not provide adequate integrity protection for RRC packets on, the control plane packets risk being exposed and modified. The intruder manipulations on control plane packets can lead to denial of service to legitimate users.	gNB, UE	TS 33.501/5.3.3 User data and signalling data integrity	The gNB shall support integrity protection and replay protection of RRC-signalling	Tampering data, Denial of Service (NAA2, NAA5)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.9
Improper ciphering of User data between UE and gNB	User data sent between UE and gNB over the NG RAN is not encrypted or encrypted using a non-compliant ciphering algorithm	gNB	TS 33.501/5.3.2 User data and signalling data confidentiality	The gNB shall activate ciphering of user data based on the security policy sent by the SMF. The gNB shall implement the following ciphering algorithms: - NEA0, 128-NEA1, 128-NEA2, 128-NEA3	Tampering data, Information Disclosure (NAA2, NAA3, NAA4)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.7
Improper integrity protection of user data between the UE and the gNB	If the gNB does not handle integrity protection for user plane packets for the NG RA interface then all the uplink/downlink user plane packets can be attacked and/or manipulated by intruders to launch Denial of Service attack.	gNB	TS 33.501/5.3.3 User data and signalling data integrity	The gNB shall implement the following ciphering algorithms: - NEA0, 128-NEA1, 128-NEA2, 128-NEA3	Information Disclosure, Rogue base station (NAAx, EIH4)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
User plane integrity check failure	Failure to ensure proper managing of PDCP PDU with faulty or missing MAC-I	gNB, UE	TS 33.501/6.6.4 UP integrity mechanisms	If the gNB or the UE receives a PDCP PDU which fails integrity check with faulty or missing MAC-I after the start of integrity protection, the PDU shall be discarded	Tampering data, Denial of Service. (NAAx)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.5
Missing of improper replay protection mechanisms of user data over NG RAN interface	gNB must provide replay protection by dropping/ignoring replayed packets. If the gNB does not provide such protection for user plane packets user plane packets can be manipulated by intruders to launch Denial of Service attack.	gNB, UE	TS 33.501/5.3.3 User data and signalling data integrity	The gNB shall support integrity protection and replay protection of user data between the UE and the gNB.	Tampering data, Denial of Service (NAA2, NAA5)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.8
Improper procedures for AS algorithm selection	If AS does not use the highest priority algorithm to protect AS layer, i.e. RRC and PDCP, data on the AS layer risks being exposed and/or modified, or denial of service.	gNB	TS 33.501/6.7.3. Procedures for AS algorithm selection	Each gNB/ng-eNB shall be configured via network management with lists of algorithms which are allowed for usage. When AS security context is to be established in the gNB/ng-eNB, the AMF shall send the UE 5G security capabilities to the gNB/ng-eNB. The gNB/ng-eNB shall choose the ciphering algorithm which has the highest priority from its configured list and is also present in the UE 5G security capabilities.	Tampering data, Information Disclosure, Denial of Service (NAAx, EIH4)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.12, 15
Lack of /improper mechanisms for prevention of bidding down at Xn-handover	If the gNB does not send the UE 5G security capabilities, the AMF cannot verify 5G security capabilities are the same as the UE security capabilities that the AMF has stored, the attacker (e.g. gNB) may force the system to accept a weaker security algorithm than the system is allowed forcing the system into a lowered security level making the system easily attacked and/or compromised	gNB, AMF	TS 33.501/6.7.3.1 Xn-handover	The AMF shall verify that the UE's 5G security capabilities received from the target gNB are the same as the UE's 5G security capabilities that the AMF has locally stored. If there is a mismatch, the AMF shall send its locally stored 5G security capabilities of the UE to the target gNB in the Path-Switch Acknowledge message. The AMF shall support logging capabilities for this event and may take additional measures, such as raising an alarm	Tampering Data, Information Disclosure, Denial of Service.	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Failure to refresh keys by gNB	If AS keys are not refreshed by the gNB when PDCP COUNTs is about to be re-used with the same Radio Bearer identity and with the same KgNB, key stream reuse is possible. This can result in information disclosure of AS signalling and user plane data.	gNB	TS 33.501/6.9.4. Key-change-on-the-fly	Key change on-the-fly consists of key refresh or key re-keying. Complete requirements are described in TS 33.501/6.9.4.	Information Disclosure (NAA4, EIH4)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.13
Failure to update key at the gNB on Dual Connectivity	Failure to update key at the gNB on Dual Connectivity may lead to key stream reuse. This can result in information disclosure of AS signalling and user plane data.	gNB	TS 33.501 / 6.10.2.1	When executing the procedure for adding subsequent radio bearer(s) to the same SN, the MN shall, for each new radio bearer, assign a radio bearer identity that has not previously been used since the last KSN change. If the MN cannot allocate an unused radio bearer identity for a new radio bearer in the SN, due to radio bearer identity space exhaustion, the MN shall increment the SN Counter and compute a fresh KSN, and then shall perform a SN Modification procedure to update the KSN"	Information Disclosure (NAA4, EIH4)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 3GPP TS 33.512 84.2.2.1.8
Failure to apply SMF-sent ciphering and integrity policy	If gNB does not apply security controls based on security policy provided by SMF, this can lead to no security or reduced security provided to the UE user plane	gNB	TS 33.501/5.3.2 User data and signalling data confidentiality TS 33.501/5.3.3 User data and signalling data integrity	The gNB shall activate ciphering of user data based on the security policy sent by the SMF.	Tampering data, Information Disclosure, Denial of Service (NAAx, EIH4)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.511, 4.2.2.1.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper protection of Data and Information of gNB Components							
System functions revealing confidential data	Presence of active system function(s) that reveal confidential system internal data in the clear to users and administrators. Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).	gNB	TS 33.117 / 4.2.3.2.2 Protecting data and information – Confidential System Internal Data	When the system is not under maintenance, there shall be no system function that reveals confidential system internal data in the clear to users and administrators. Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).	Elevation of Privilege, Information Disclosure, Tampering NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.2.2
Improper protection of data and information in storage	For sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of a system that are needed for the functionality shall be protected against manipulation. In addition, the following rules apply for: - Systems that need access to identification and authentication data in the clear, e.g. in order to perform an authentication. Such systems shall not store this data in the clear, but scramble or encrypt it by implementation-specific means. - Systems that do not need access to sensitive data (e.g. user passwords) in the clear. Such systems shall hash this sensitive data - Stored files on the network product: examples for protection against manipulation are the use of checksum or cryptographic methods.]	gNB	TS 33.117 / 4.2.3.2.3 Protecting data and information in storage	For sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of a system that are needed for the functionality shall be protected against manipulation.	Elevation of Privilege, Information Disclosure, Tampering NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.2.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Lack of or improper cryptographic protection of data in transfer	The transmission of data is done without proper protection (industry standard network protocols with sufficient security measures and industry accepted cryptographic algorithms), as defined in TS33.310/33.210	gNB	TS 33.117 / 4.2.3.2.4 Protecting data and information in transfer	Usage of cryptographically protected network protocols is required. The transmission of data with a need of protection shall use industry standard network protocols with sufficient security measures and industry accepted algorithms. In particular, a protocol version without known vulnerabilities or a secure alternative shall be used.	Spoofing, Information disclosure NAA3, NAA4, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.2.4
No traceability of access to personal data	In some cases, access to personal data in clear text might be required. If such access is required, access to this data shall be logged, and the log shall contain who accessed what data without revealing personal data in clear text. When for practical purposes such logging is not available, a coarser grain logging is allowed. In some cases, the personal data stored in the log files may allow the direct identification of a subscriber. In such cases, the revealed personal information may not expose the subscriber to any kind of privacy violation	gNB	TS 33.117 / 4.2.3.2.5 Logging access to personal data	In some cases, access to personal data in clear text might be required. If such access is required, access to this data shall be logged, and the log shall contain who accessed what data without revealing personal data in clear text. When for practical purposes such logging is not available, a coarser grain logging is allowed. In some cases, the personal data stored in the log files may allow the direct identification of a subscriber. In such cases, the revealed personal information may not expose the subscriber to any kind of privacy violation.	Information disclosure NAA4, LEG	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.2.5
Improper protection of availability and integrity of gNB Components							
Failure to address overload situation	Overload situation could appear in the case of DoS attack or increased traffic. Lack to deal with such events affects availability of information or security functionalities	gNB	TS 33.117 / 4.2.3.3.1 System handling during overload situations TS 33.117 /4.2.3.3.3 System handling during excessive overload situations	The system shall provide security measures to deal with overload situations which may occur as a result of a denial of service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided. In the situation where the security measures are no longer sufficient., it shall be ensured that the system cannot reach an undefined and thus potentially insecure state. In an extreme case this means that a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.	Denial of service attacks NAA5, UD5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.3.1, 4.2.3.3.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Boot from unauthorized memory devices	The network product can boot only from the memory devices intended for this purpose	gNB	TS 33.117 / 4.2.3.3.2 Boot from intended memory devices only	The network product can boot only from the memory devices intended for this purpose	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure (NAAx)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.3.2
Improper handling of unexpected input	The following typical implementation errors open relevant vulnerabilities: - No validation on the lengths of transferred data - Incorrect assumptions about data formats - No validation that received data complies with the specification - Insufficient handling of protocol errors in received data - Insufficient restriction on recursion when parsing complex data formats - White listing or escaping for inputs outside the values margin	gNB	TS 33.117 / 4.2.3.3.4 System robustness against unexpected input	During transmission of data to a system it is necessary to validate input to the network product before processing. This includes all data which is sent to the system. Examples of this are user input, values in arrays and content in protocols.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure (NAAx)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.3.4
Insufficient assurance of software package integrity	Lack of software package integrity could affect CIA of data, services, hardware and policies during installation or upgrade phases for the envisioned product/system. Missing information regarding software package integrity checks, including details of how the integrity check is carried out. Missing authentication and access control mechanisms for software package installation.	gNB	TS 33.117 / 4.2.3.3.5 Network Product software package integrity validation	1) Software package integrity shall be validated in the installation/upgrade stage; 2) Network product shall support software package integrity validation via cryptographic means, e.g. digital signature. To this end, the network product has a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software update is originated from only these sources; 3) Tampered software shall not be executed or installed if integrity check fails; 4) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software update, and modify the list mentioned in bullet 2.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.3.5

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
***Vulnerable* mechanisms for authentication and authorisation of gNB Components**							
Unauthenticated access to system functions	The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) opens the opportunity of exploitation and limits accountability. This includes M2M communication	gNB	TS 33.117 / 4.2.3.4.1.1 System functions shall not be used without successful authentication and authorisation.	The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.1.1
Improper authentication mechanisms	Depending of information sensitivity different level of strong authentication mechanisms are required. Fail to identify the proper correspondence between levels of protection and authentication mechanisms implemented creates the possibility to allow unauthorized entities to access unallocated resources	gNB	TS 33.117 / 4.2.3.4.1.2 Accounts shall allow unambiguous identification of the user TS 33.117 / 4.2.3.4.2.1 Account protection by at least one authentication attribute	The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.1.2, 4.2.3.4.2.1 4.2.3.4.3.
Predefined/ default accounts and/or authentication attributes	All predefined or default accounts and/or or default authentication attributes shall be deleted or disabled	gNB	TS 33.117 / 4.2.3.4.2.2 Predefined accounts shall be deleted or disabled TS 33.117 / 4.2.3.4.2.3 Predefined or default authentication attributes shall be deleted or disabled	All predefined or default accounts shall be deleted or disabled. Should this measure not be possible the accounts shall be locked for remote login. Preconfigured authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the vendor provides instructions on how to manually change it	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.2.2 4.2.3.4.2.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Weak or missing password policy	A password policy shall address the password structure, password change, hiding password display capabilities, consecutive failed login attempts. A week password structure and/or a long validity password period could lead to a successful brute force attack. Password display is vulnerable to eavesdropping attack. Password policy is a security policy component.	gNB	TS 33.117 / 4.2.3.4.3 Password policy	Password policy requirements include requirements regarding Password complexity, password change, Protection against brute force and dictionary attacks, hiding password display	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.3.
Lack of mutual authentication of entities for management interfaces	The network product management shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means	gNB	TS 33.117 / 4.2.3.4.4.1 Authentication on Network Product Management and Maintenance interfaces	The network product management shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.4.1
Improper authorisation and access control policy	The authorisations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.	gNB	TS 33.117 / 4.2.3.4.6 Authorisation and access control	The authorisations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform. Authorisations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.4.6

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper session protection mechanisms of gNB Components							
Improper / missing functionality for session protection	The system should have a function that allows a signed in user to logout at any time. All processes under the logged in user ID should be terminated on log out. A permanently exposed session increases the vulnerability of the system as an entry point for unauthorized person. OAM user interactive session should be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period	gNB	TS 33.117 / 4.2.3.5 Protecting sessions	The system shall have a function that allows a signed in user to logout at any time. All processes under the logged in user ID shall be terminated on log out. The network product shall be able to continue to operate without interactive sessions. An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.5.
Insufficient or improper monitoring mechanisms of gNB Components							
lack of security event logging	lack of security events logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred do not allow a correct and rapid audit in case of security incident occurrence. Security restauration is delayed.	gNB	TS 33.117 / 4.2.3.6.1 Security event logging	Security events shall be logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred. For each security event, the log entry shall include user name and/or timestamp and/or performed action and/or result and/or length of session and/or values exceeded and/or value reached. IETF RFC 3871, section 2.11.10 specifies the minimum set of security events.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.6.1
Vulnerabilities in Operating Systems supporting gNB Components							
Improper / missing controls for protection of security event log files	Security event logs should be forwarded or uploaded to a central location or external systems. Security event log files shall be protected in storage and transfer states, too. Availability and integrity of security event log files could conduct to delays, wrong audit results, delays in security restauration, threats persistence.	gNB	TS 33.117 / 4.2.3.6.2 Log transfer to centralized storage TS 33.117 / 4.2.3.6.3 Protection of security event log files	Log functions should upload securely of log files to a central location or to an external system for the Network Product that is logging. Secure transport protocols shall be used. The security event log shall be access controlled (file access rights) so only privileged users have access to the log files.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.3.6.2 4.2.3.6.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper handling of growing content by file system	Growing or dynamic content (e.g. log files, uploads) could influence system functions. A file system that reaches its maximum capacity could stop a system from operating properly.	gNB	TS 33.117 / 4.2.4.1.1.1 Handling of growing content	Growing or dynamic content (e.g. log files, uploads) shall not influence system functions. A file system that reaches its maximum capacity shall not stop a system from operating properly. Therefore, countermeasures shall be taken such as usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring to ensure that this scenario is avoided.	Denial of service attacks, equipment / software errors, growing dynamic content NAA5, UD5, FM5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.4.1.1.1
Processing of ICMP packets not required for operation	Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the network product. In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk.	gNB	TS 33.117 / 4.2.4.1.1.2 Processing of ICMPv4 and ICMPv6 packets TS 33.511 / 4.2.4.1.1.2 Processing of ICMPv4 and ICMPv6 packets	Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the network product. In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk. Permitted, forbidden and optional ICMP packets are detailed in TS 33.117 clause 4.2.4.1.1.2, with the specific additions in TS 33.511: Echo Reply can be sent by default and, in case of remote base station auto deployment, Router Advertisement can be processed	Denial of service attacks, equipment / software errors, misconfigurations NAA5, UD5, FM5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.4.1.1.2
Processing of IP packets with unnecessary options or extensions	IP packets with unnecessary options or extension headers could be used by attackers to get unauthorized access to system resources.	gNB	TS 33.117 / 4.2.4.1.1.2 Processing of ICMPv4 and ICMPv6 packets	IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g. source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.4.1.1.3
Privilege Escalation allowed without re-authentication	Authenticated Privilege Escalation allowed without re-authentication could permit to an authorized user to gain unallocated higher rights to resources, violating security policy	gNB	TS 33.117 / 4.2.4.1.2.1 Authenticated Privilege Escalation only	There shall not be a privilege escalation method in interactive sessions (CLI or GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication. Implementation example: Disable insecure privilege escalation methods so that users are required to (re-)login directly into the account with the required permissions.	Privilege escalation NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.4.1.2.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Recurrent UIDs for UNIX System accounts	Each system account in UNIX shall have a unique UID, to provide for system account accountability	gNB	TS 33.117 / 4.2.4.2.2 System account identification	Each system account in UNIX shall have a unique UID. The term 'UNIX' includes all major derivatives, including Linux.	Authorisation attacks NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.4.2.2
Vulnerabilities in Web Servers supporting gNB Components							
Unsecure Https connection to web servers	The communication between Web client and Web server shall be protected using TLS. TLS profile should be defined in compliance Annex E of TS 33.310, with the following additional requirement: cipher suites with NULL encryption shall not be supported	gNB	TS 33.117 / 4.2.5.1 HTTPS	The communication between Web client and Web server shall be protected using TLS. Cipher suites with NULL encryption shall not be supported	Spoofing identity, Tampering of Data, Information Disclosure NAA2, NAA3, NAA4, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.5.1
Lack of / improper logging of access to the webserver	When logging information lacks completeness, integrity or timeliness it is impossible to detect, analyse and respond to system faults and relevant security events.	gNB	TS 33.117 / 4.2.5.2 Webserver logging	Access to the webserver shall be logged. The web server log shall contain the following information: Access timestamp / Source (IP address) / (Optional) Account (if known) / (Optional) Attempted login name (if the associated account does not exist) / Relevant fields in http request. The URL should be included whenever possible / Status code of web server response	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.5.2
Lack of / improper http user session protection	Improper session protection mechanisms may lead to session hijacking, disclosure of confidential information, including authentication attributes	gNB	TS 33.117 / 4.2.5.3 HTTP User sessions	To protect user sessions the Network Product shall support comprehensive session ID and session cookie protection mechanisms	Session hijacking NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.5.3
Improper validation of HTTP input	The Network Product shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.	gNB	TS 33.117 / 4.2.5.4 HTTP input validation	The Network Product shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.	Injection, cross-site scripting NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.5.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerabilities of network devices running gNB Components							
Lack of packet filtering functionality	Lack of, or improper mechanisms to filter incoming IP packets on any IP interface according to defined and manageable rules leaves the network device vulnerable to denial-of-service attacks, service degradation or attack aimed at leading the device to an exception state.	gNB	TS 33.117 / 4.2.6.2.1 Packet filtering	The Network Product shall provide a mechanism to filter incoming IP packets on any IP interface, as defined in RFC 3871 and TS 33.117 clause 4.2.6.2.1	Denial of service, packet flooding NAA5, FM5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.6.2.1
Lack of robustness against unexpected input	If a network device does not have the capability to detect and drop by incoming packets, from other network element, that are manipulated or differing the norm, it can lead to an impairment of availability.	gNB	TS 33.117 / 4.2.6.2.2 Interface robustness requirements	All incoming packets, from other network element, that are manipulated or differing the norm shall be detected as invalid and be discarded. The process shall not be affecting the performance of the network device. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets.	Malware, denial-of-service, packet flood NAA5, FM5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.6.2.2
Improper or absent GTPU Filtering	In the absence of effective GTP-U filtering mechanisms, the network is exposed to malformed GTP packets, denial of service attacks, and out-of-state GTP messages, and also vectors such as spoofed IP packets.	gNB	TS 33.117 / 4.2.6.2.4 GTP-U Filtering	For each message of a GTP-U-based protocol, it shall be possible to check whether the sender of this message is authorized to send a message pertaining to this protocol.	Authorisation attacks, man-in-the-middle attacks NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.2.6.2.4
Improper hardening of gNB Components							
Unnecessary or insecure services / protocols	Should the network product run protocol handlers and services which are not needed for its operation, or which have known security vulnerabilities, they may be manipulated to gain unauthorized access to the system, impair its availability or other forms of manipulation.	gNB	TS 33.117 / 4.3.2.1 No unnecessary or insecure services / protocols	The network product shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Software errors NAAx, FMx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Unrestricted reachability of services	The network product shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. The absence of appropriate mechanisms expose the services to risk of exploitation of known or unknown vulnerabilities by malicious parties or technical faults.	gNB	TS 33.117 / 4.3.2.2 Restricted reachability of services	The network product shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. On interfaces were services are active, the reachability should be limited to legitimate communication peers. This limitation shall be realized on the network product itself (without measures (e.g. firewall) at network side) according to the requirement detailed in clause 4.2.6.2.1 Packet Filtering.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.2
Unused software components	Unused software components or parts of software which are not needed for operation or functionality of the network product create an unnecessary attack surface. Such unused software components have a high susceptibility of falling outside patching and vulnerability management processes and therefore are increasingly exposed to malicious attacks and technical faults.	gNB	TS 33.117 / 4.3.2.3 No unused software	Unused software components or parts of software which are not needed for operation or functionality of the network product shall not be installed or shall be deleted after installation. This includes also parts of a software, which will be installed as examples but typically not be used (e.g. default web pages, example databases, test data).	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.3
Unused software or hardware functions	During installation of software and hardware functions that are not required for operation or function of the system will be often activated. Such hardware and software functions increase the IT attack surface and their exposure is increased by their susceptibility of falling outside access control policies.	gNB	TS 33.117 / 4.3.2.4 No unused functions	During installation of software and hardware often functions will be activated that are not required for operation or function of the system. If unused functions of software cannot be deleted or deinstalled individually, such functions shall be deactivated in the configuration of the network product permanently. Also, hardware functions which are not required for operation or function of the system (e.g. unused interfaces) shall be permanently deactivated. Permanently means that they shall not be reactivated again after network product reboot.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Unsupported components	Unsupported components incur a high risk of unmitigated vulnerabilities that can be exploited by malicious actors or technical faults.	gNB	TS 33.117 / 4.3.2.5 No unsupported components	The network product shall not contain software and hardware components that are no longer supported by their vendor, producer or developer, such as components that have reached end-of-life or end-of-support. Excluded are components that have a special support contract. This contract shall guarantee the correction of vulnerabilities over components' lifetime.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Component malfunctions NAAx, FMx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.5
Remote login of privileged users	Unrestricted remote login for privileged users expose the network element to increased risk of unauthorized access and manipulation.	gNB	TS 33.117 / 4.3.2.6 Remote login restrictions for privileged users	Description: Direct login as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to the system remotely.	Authorisation attacks, elevation of privilege NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.6
Excessive file system Authorisation privileges	In the presence of excessive file system authorisation privileges, application and configuration data is exposed to risks of unauthorised disclosure, tampering, or destruction.	gNB	TS 33.117 / 4.3.2.7 file system Authorisation privileges	The system shall be designed to ensure that only users that are authorized to modify files, data, directories or file systems have the necessary privileges to do so.	Unauthorised / erroneous data element modification / deletion NAA1, NAA2, NAA3, UD1, UD2	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.2.7
Lack of protection against IP-Source address spoofing	IP address spoofing involving the use of a trusted IP address can be used by network intruders to overcome network security measures, such as authentication based on IP addresses. IP address spoofing is most frequently used in denial-of-service attacks, where the objective is to flood the target with an overwhelming volume of traffic, and the attacker does not care about receiving responses to the attack packets.	gNB	TS 33.117 / 4.3.3.1.1 IP-Source address spoofing mitigation	Systems shall not process IP packets if their source address is not reachable via the incoming interface.	Packet flood NAA5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Unneeded kernel network functions	Kernel based network functions not needed for the operation of the network element offer an unnecessary attack surface. Particularly vulnerable services are: IP Packet Forwarding between different interfaces of the same equipment, Proxy ARP (resource exhaustion attacks and man-in-the-middle attacks), Directed broadcast (Smurf, Denial of Service attack), IPv4 Multicast handling (smurf and fraggle attacks), gratuitous ARP messages (ARP Cache Poisoning attack)	gNB	TS 33.117 / 4.3.3.1.2 Minimized kernel network functions	Kernel based network functions not needed for the operation of the network element shall be deactivated	Exploitation of vulnerable kernel functions NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.2
automatic launch of removable media	Automatic launch of removable media provides a potential vector for unauthorized or malicious payloads	gNB	TS 33.117 / 4.3.3.1.3 No automatic launch of removable media	The network product shall not automatically launch any application when removable media device such as CD-, DVD-, USB-Sticks or USB-Storage drive is connected. If the operating system supports an automatic launch, it shall be deactivated unless it is required to support availability requirements.	Malware, bypassing of security controls, running unauthorised operating system NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.3
No SYN Flood Prevention	A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic	gNB	TS 33.117 / 4.3.3.1.4 SYN Flood Prevention ; RFC 4987	The network product shall support a mechanism to prevent Syn Flood attacks (e.g. implement the TCP Syn Cookie technique in the TCP stack by setting net.ipv4.tcp_syncookies = 1 in the linux sysctl.conf file). This feature shall be enabled by default.	Syn Flood attacks NAA5	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
No protection against buffer overflows	Exploiting the behaviour of a buffer overflow is a well-known security exploit. By sending in data designed to cause a buffer overflow, it is possible to write into memory areas known to hold executable code and replace it with malicious code, or to selectively overwrite data pertaining to the program's state, therefore causing behaviour that was not intended by the original programmer. Buffers are widespread in operating system (OS) code, so it is possible to make attacks that perform privilege escalation and gain unlimited access to the computer's resources.	gNB	TS 33.117 / 4.3.3.1.5 Protection from buffer overflows	The system shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided.	Buffer overflow attacks NAA2, NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.5
No/improper external file system mount restrictions	In the absence of effective external file systems mount restrictions, the system is exposed to privilege escalation and excessive access permissions due to the contents of the mounted file systems.	gNB	TS 33.117 / 4.3.3.1.6 External file system mount restrictions	If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.	Malware, bypassing of security controls, unauthorised operating system NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.3.1.6
Directory listings	Web servers can be configured to automatically list the contents of directories that do not have an index page present. This can aid an attacker by enabling them to quickly identify the resources at a given path, and proceed directly to analysing and attacking those resources. It particularly increases the exposure of sensitive files within the directory that are not intended to be accessible to users, such as temporary files and crash dumps.	gNB	TS 33.117 / 4.3.4.10 No directory listings	Directory listings (indexing) / "Directory browsing" shall be deactivated.	Scanning of vulnerable resources NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.10
Web server information in HTTP headers	The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version and languages used by the web server.	gNB	TS 33.117 / 4.3.4.11 Web server information in HTTP headers	The HTTP header shall not include information on the version of the web server and the modules/add-ons used.	Exploitation of vulnerable components NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.11

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Web server information in error pages	The error page sent by the web server discloses information that can aid an attacker, such as the server version, modules/add-ons used or information revealing inner workings such as internal server names, error codes, etc.	gNB	TS 33.117 / 4.3.4.12 Web server information in error pages	User-defined error pages shall not include version information about the web server and the modules/add-ons used. Error messages shall not include internal information such as internal server names, error codes, etc. Default error pages of the web server shall be replaced by error pages defined by the vendor.	Exploitation of vulnerable components NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.12
Unused file type- or script-mappings	Unused File type- or script-mappings can be used in attacks based on delivery of malicious payloads, such as code-injection attacks.	gNB	TS 33.117 / 4.3.4.13 Minimized file type mappings	File type- or script-mappings that are not required shall be deleted, e.g. php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs	Code injection NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.13
Unrestricted access to files	Improperly restricted file access rights may lead to unauthorized delivery of files which are not meant to be delivered, and to path traversal attacks.	gNB	TS 33.117 / 4.3.4.14 Restricted file access	Restrictive access rights shall be assigned to all files which are directly or indirectly (e.g. via links or in virtual directories) in the web server's document directory. In particular, the web server shall not be able to access files which are not meant to be delivered.	Direct access to restricted data from public domain NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.14
Execution rights outside CGI/Scripting directory	Improper restriction of execute rights may lead to Remote Command Execution by unauthorized delivery of malicious payload through various vectors.	gNB	TS 33.117 / 4.3.4.15 Execute rights exclusive for CGI/Scripting directory	If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights	Code injection NAAx	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.15
System privileges for web server processes	If the web server runs under privileged accounts, web server compromise caused by malicious action or technical fault has an increased chance to compromise the host operating system's integrity and availability.	gNB	TS 33.117 /4.3.4.2 No system privileges for web server	No web server processes shall run with system privileges. This is best achieved if the web server runs under an account that has minimum privileges. If a process is started by a user with system privileges, execution shall be transferred to a different user without system privileges after the start.	Elevation of privileges NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Active and unused HTTP methods	Unused http methods provide an unnecessary attack surface that can lead to security compromise of the system	gNB	TS 33.117 / 4.3.4.3 No unused HTTP methods	HTTP methods that are not required shall be deactivated. Standard requests to web servers only use GET, HEAD, and POST. If other methods are required, they shall not introduce security leaks such as TRACK or TRACE.	Abuse of unused vulnerable methods NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.3
Unused web server add-ons	Unused server add-ons provide an unnecessary attack surface that can lead to security compromise of the system	gNB	TS 33.117 / 4.3.4.4 No unused add-ons	All optional add-ons and components of the web server shall be deactivated if they are not required. In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.	Code injection NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.4
Access to compiler, interpreter, or shell via CGI or other server-side scripting	CGI and other server-side scripting specifications provide opportunities to read files, acquire shell access, and corrupt file systems on server machines and their attached hosts. Means of gaining access include: exploiting assumptions of the script, exploiting weaknesses in the server environment, and exploiting weaknesses in other programs and system calls. Presence in the scripting directory of compilers, interpreters or operating system shells renders the system particularly vulnerable.	gNB	TS 33.117 / 4.3.4.5 No compiler, interpreter, or shell via CGI or other server-side scripting	If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory - or other corresponding scripting directory - shall not include compilers or interpreters (e.g. PERL interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells).	Code injection NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.5
Common directory for uploads and CGI/Scripting	In upload is permitted in the CGI/Scripting, the system is vulnerable to code injection / shell upload attacks.	gNB	TS 33.117 / 4.3.4.6 No CGI or other scripting for uploads	If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.	Code injection NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.6

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Execution of system commands with server side includes (SSI)	SSIs are directives present on Web applications used to feed an HTML page with dynamic contents. The Server-Side Includes attack allows the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary codes remotely. It can be exploited through manipulation of SSI in use in the application or force its use through user input fields.	gNB	TS 33.117 / 4.3.4.7 No execution of system commands with SSI	If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.	Code injection NAA2, NAA3, NAA4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.7
Excessive / improper access rights for web server configuration files	Improper setting of access rights for web server configuration files may lead to unauthorized disclosure or modification of configuration information.	gNB	TS 33.117 / 4.3.4.8 Access rights for web server configuration	Access rights for web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges. Implementation example: Delete "read" and "write" access rights for "others." Only grant "write" access to the user who configures the web server	Manipulation of server configuration files NAA2, NAA3	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.8
Presence of default content	Presence of default content may disclose information on the web server version, add-ons and configuration or information/file structure, and thus facilitate information gathering for a malicious party. Also, default content may include known vulnerabilities (such as the case of IIS Default Page).	gNB	TS 33.117 / 4.3.4.9 No default content	Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the web server shall be removed.	Abuse of vulnerable content, collection of system information (NAA2, NAA3, NAA4)	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.4.9
Inadequate traffic separation of traffic belonging to different network domains	Unsegregated traffic belonging to different planes (data, control, management) increases the risk that unauthorized individuals will be able to observe management traffic and/or compromise the device.	gNB	TS 33.117 / 4.3.5.1 Traffic Separation RFC 3871 / 2.3.5. Support Separate Management Plane IP Interfaces	The network product shall support physical or logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See RFC 3871 [3] for further information.	Lateral movement, elevation of privileges, eavesdropping NAA2, NAA3, NAA4, EIH4	Vendor, SECAM Accreditation Body, Accredited Test Lab	3GPP TS 33.117 3GPP TS 33.511-519 4.3.5.1

F ANNEX: DETAILED VULNERABILITIES IN NETWORK FUNCTION VIRTUALIZATION – MANO

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Service-Based Vulnerabilities of NFV components							
Improper message and session integrity checks on internal interfaces	The transmitter of a message should provide means to allow for the determination whether any modification, deletion, insertion, or replay has occurred. The receiver should have corresponding verification mechanisms. Lack of or improper such measures facilitate abuse and modification of sessions and messages.	NFV MANO	Message integrity checks	Detection of any changes, deletions, insertions or replays.	Abuse and modification of sessions and messages (NAA2, NAA5)	MNO	ETSI GS NFV-SEC 014 / 6
Improper confidentiality protection of data transferred over internal interfaces to MANO	Lack of appropriate confidentiality protection of data transferred over any internal interface of MANO.	NFV MANO, VNF	Use of secure communication protocols	Provide confidentiality of internal transfers using an encrypted mode of well-known network protocols.	Data leakage (NAA4, EIH4)	MNO	ETSI GS NFV-SEC 014 / 5
Improper API Access implementation	TLS not implemented for API communication, or implementation shortcomings such as lack of TLS-based authentication: client and authorisation servers are not mutually authenticated or client does not authenticate the resource server.	Os-Ma-nfvo	Secure API	The confidentiality and data integrity of all messages shall be ensured by using TLS on each interface. The client and authorisation servers shall mutually authenticate. The client shall authenticate the resource server.	Unauthorized access (NAAx)	MNO	ETSI GS NFV-SEC 022 / 4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Use of legacy PNF	Vulnerabilities of a PNF could be used as a starting point for an attack against VNFs, potentially taking advantage of legacy security used by PNFs and not provided by the virtualisation layer.	Control plane	Enforce security policies to protect mixed PNF-VNF deployments	The 5GC should be configured so that NFs can only communicate with NFs which they are specifically authorised to communicate with.	Attackers using insecure interfaces as injection points and for reverse attack. (NAAx)	MNO	3GPP TR 33.848 / 5.17
Improper verification of identity and location of transmitting party on internal interfaces	If an internal interface allows any actions from received data without successfully identifying and verifying the identity and location of the transmitting party, it enables masquerading of the Orchestrator and other forms of privilege escalation that in turn can lead to abuse of VIM or VNFM functions by unauthorized parties.	NFV MANO	Identity validation	Successful identification and verification of the identity and location of the transmitting party	Abuse of VIM or VNFM functions by unauthorized parties (NAAx)	MNO	ETSI GS NFV-SEC 014 / 6
Improper protection of Data and Information of NFV components							
Inability to provide proof of integrity of the data stores used for VM images	Poor monitoring of stored images to determine if any unauthorized modification, deletion or insertion has occurred renders VIM unable to ensure integrity of VM images and of data transfers.	VIM	VIM shall monitor stored images	The VIM shall monitor stored images to determine if any unauthorized modification, deletion or insertion has occurred	Unauthorized modification, deletion or insertion of the data stores used for VM images (NAAx)	MNO	ETSI GS NFV-SEC 014 / 5.2-c.1.1.4
Lack of encryption of control plane data	An attacker could read data in transit if control plane data in transit between hosts is not sent over an encrypted and authenticated channel.	Control plane	Encrypt control plane data	All control plane data in transit between hosts should be sent over an encrypted and authenticated channel using non-proprietary protocols.	An attacker could read data in transit. (NAA4, EIH4)	MNO	3GPP TR 33.848 / 5.15

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper hardening of NFV components							
Improper patch management	Once identified, vulnerabilities in software can be fixed through security patches whereas hardware vulnerabilities are much more costly to fix. Security patches may require a reboot and could cause service disruption, particularly if many commodity servers have to be rebooted over a short period. Security patches are not always in time. Failure to apply necessary patches leave the systems open to exploitation of known vulnerabilities.	VNF	System patching	Regular and effective patch management program	Malware Denial of service Unauthorized access (NAAx, FMx)	MNO	ETSI GS NFV-SEC 001 / 7.2.2
Mis-configuration	Complexity brought by virtualisation increases probability for errors and misconfiguration remaining undetected. Accidental misconfigurations or failure to follow security standards and practices can cause service problems directly, or leave open unintended vulnerabilities, which will cause service problems if exploited.	VNF	Hardening standards and procedures	Careful planning, detailed documentation, configuration review, testing before production, periodic security configuration checks	Human error (UDx)	MNO	ETSI GS NFV-SEC 001 / 7.1
No mechanism to enforce geo-restrictions	The MANO system should allow instantiation of MANO components and managed entities, the NFVIs, only at explicit geographic locations. Failure to do so may leave the system vulnerable to legal and licensing risks.	NFV MANO	Implementing mechanisms to allow geo-restrictions	Attribute-based access control and attribute-based or multi-factor authentication - where location is one of the attributes or behavioural factors	Unknown geographic jurisdiction (e.g. for legal and policy compliance) (LEG)	MNO	ETSI GS NFV-SEC 014 / 6
Time Manipulation	The VNFs must synchronize with trusted time servers. Failure to do so, leaves the system vulnerable to an attack that manipulates the network timing source or VNF clock, thus causing the network to be compromised.	VNF	The system should provide a protected and trusted network time source	The VNFs shall synchronize with trusted time servers.	Time manipulation attacks. (NAAx)	MNO	3GPP TR 33.848 / 5.20

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Virtualisation platform vulnerabilities							
Inadequate access privileges in virtualized environments	Administrative models that enable an admin/root/super user account type has full access to system resources allow visibility and modification of cryptographic keys, passwords in memory, configuration files, intellectual property and other resources within the NFV. The hypervisor is fully aware of the current state of each guest OS it controls. Hypervisor introspection can enable the ability to view, inject, and/or modify operational state information associated with NFV through direct or indirect methods. Access to state information can result in the ability to arbitrarily read and/or write the contents of memory, storage, key storage and other NFV operational aspects.	Virtualised Resources	Hardening of virtualized environments	Granting access based on the "lowest privilege" principle	Human error (NAAx)	MNO	ETSI GS NFV-SEC 003 / 4.4.2.1.2
Improper key management system	The host system shall provide cryptographically separated secure environments to different applications. In the absence of these conditions, the virtualised environment can be abused to compromise sensitive functions from less protected ones.	NSM	Core HBRT hardware requirements	The host system shall implement a key management system which includes key generation, key storage, key deletion and cryptographic processing.	Manipulation of VNFs (NAAx)	MNO, Vendor	ETSI GS NFV-SEC 012 / 5.1.2
Lack of a proper mechanism for ensuring a Hardware-Based Root of Trust (HBRT)	A Hardware-Based Root of Trust (HBRT) should act as Initial Root of Trust to ensure a safe environment for running sensitive virtualised components.	NFVI	Core HBRT hardware requirements	The host system shall implement a Hardware-Based Root of Trust (HBRT) based on core hardware requirements	Manipulation of VNFs (NAAx)	MNO, Vendor	ETSI GS NFV-SEC 012 / 5.1.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Software Vulnerabilities in NFV implementation	The risks from software vulnerabilities could be higher with NFV than with traditional bespoke appliances because VNFs are expected to run on commodity software and hardware and because NFV is built on cloud technology with standard security level. Virtualisation technology will need to be re-assessed before it can be considered suitable for protecting critical network infrastructure.	VNF	Vulnerability assessment	Regular and effective vulnerability management program	Malware Denial of service Unauthorized access (NAAx, UDx, FMx)	MNO	ETSI GS NFV-SEC 001 / 7.2.2
Vulnerable mechanisms for authentication and authorisation of NFV components							
Improper VNF on-boarding	Improper procedures for signing and management of associated cryptographic key may enable manipulation and integrity compromise of VNF Packages.	VNF Manager	Cryptographic signature of VNF Package	Verification of VNF Package during instantiation; Handling of confidentiality protected of VNF Package during instantiation	Manipulation of VNFs (NAA2)	MNO	ETSI GS NFV-SEC 021 / 5.1
Improper VNF instantiation	Lack of or improper mechanisms to prevent instantiation of VNF Packages unless their signature is verified may enable manipulation and integrity compromise of VN Functions	Ve-Vnfm-em Ve-Vnfm-vnf	Signature of VNF Package	Signing of VNF Package; Handling of confidentiality protected for VNF Package during on-boarding	Manipulation of VNFs (NAA2)	MNO	ETSI GS NFV-SEC 021 / 5.2
Improper authentication policy	Unauthenticated access to system functions of NFV Management and Orchestration The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) opens the opportunity of exploitation and limits accountability. This includes M2M communication.	NFV-MANO, VSF, ISF, PSF,	System functions shall not be used without proper authentication and authorisation.	The usage of a system function without proper authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure (NAAx)	Vendor	3GPP TS 33.117 4.2.3.4.1.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Insecure / insufficient authentication attributes	Failure to protect accounts by at least one authentication attribute, active predefined authentication attributes. Depending on information sensitivity, different level of strong authentication mechanisms are required. Fail to identify the proper correspondence between levels of protection and authentication mechanisms implemented creates the possibility to allow unauthorized entities to access unallocated resources.	NFV-MANO, VSF, ISF, PSF,	Secure procedures for authentication and authorisation	The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user. All predefined or default accounts and/or or default authentication attributes shall be deleted or disabled.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure (NAAx, Udx)	Vendor	3GPP TS 33.117 4.2.3.4.1.2, 4.2.3.4.2.1 4.2.3.4.3.
Insecure password policy	A password policy shall address the password structure, password change, hiding password display capabilities, consecutive failed login attempts. A week password structure and/or a long validity password period could lead to a successful brute force attack. Failure to block consecutive failed login attempts may lead to password guess.	NFV-MANO, VSF, ISF, PSF,	Password policy	Password policy requirements include requirements regarding Password complexity, password change, Protection against brute force and dictionary attacks, hiding password display	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure	Vendor	3GPP TS 33.117 4.2.3.4.3.
Insecure authentication mechanisms to management / maintenance interfaces	The network product management shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means.	NFV-MANO, VSF, ISF, PSF,	Protect management interfaces	Protect devices used for administration. Reduce the exposure of management interfaces. Ensuring there's a trail of breadcrumbs.	Unauthorised access at system, theft of data	Vendor	3GPP TS 33.117 4.2.3.4.4.1
Insecure authorisation and access control mechanisms	The authorisations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.	NFV-MANO, VSF, ISF, PSF,	Authorisation and access control	The authorisations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform. Authorisations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error	Vendor	3GPP TS 33.117, 4.2.3.4.6

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Insufficient or improper monitoring mechanisms of NFV							
Insufficient / inadequate logging of security events for MANO and NFVI	Lack of security events logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred do not allow a correct and rapid audit in case of security incident occurrence.	NFV-MANO, NFVI	Security event logging	Security events shall be logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred. For each security event, the log entry shall include user name and/or timestamp and/or performed action and/or result and/or length of session and/or values exceeded and/or value reached. IETF RFC 3871, section 2.11.10 specifies the minimum set of security events.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error	Vendor	3GPP TS 33.117, 4.2.3.6.1
Logs not transferred to centralized storage	Security event logs should be forwarded or uploaded to a central location or external systems. Security event log files shall be protected in storage and transfer states, too.	NFV-MANO, NFVI	Transfer security logs to a centralized storage	Log functions should upload securely of log files to a central location or to an external system for the Network Product that is logging. Secure transport protocols shall be used.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error	Vendor	3GPP TS 33.117, 4.2.3.6.2 4.2.3.6.3
Improper protection of security event log files	Availability and integrity of security event log files could conduct to delays, wrong audit results, delays in security restauration, threats persistence.	NFV-MANO, NFVI	Protection of security event log files	The security event log shall be access controlled (file access rights) so only privileged users have access to the log files.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error	Vendor	3GPP TS 33.117,

G ANNEX: DETAILED VULNERABILITIES IN SOFTWARE DEFINED NETWORKS

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerabilities in implementation of SDN functionalities							
Improper mechanisms for preventing flow rules confliction	Lack of functionality in the SDN control layer to support preventing flow rules confliction in order to avoid mandatory network policies from being bypassed.	SDN Controller	Prevention of flow rules confliction	It is required to provide a functionality in the SDN control layer to support preventing flow rules confliction in order to avoid mandatory network policies from being bypassed.	Flow rules confliction, Fake flow rule insertion (NAA2, UD2, FM2)	MNO, Vendor	Rec. ITU-T X.1038 (10/2016) / R15
SBA/SBI vulnerabilities of SDN components							
Insecure APIs	Like any software, APIs can be compromised and data can be intercepted. The 10 most known APIs vulnerabilities are those presented by OWASP foundation in the "OWASP API Security Project". API exploitation may relate to all the different types of APIs that may be found in an SDN: Northbound API exploitation, Southbound API exploitation, Eastbound-Westbound API exploitation.	Northbound Interface, Southbound Interface, Eastbound-Westbound Interface	Secure APIs	Network providers should consider deploying encryption and authentication techniques to all SDN APIs.	Interception, Eavesdrop, Availability Attacks, TCP Attack (NAAx)	MNO	ENISA Threat Landscape and Good Practice Guide for Software Defined Networks/5G / 8.1
Improper mechanisms to protect integrity and confidentiality of configuration data	Inadequate security of configuration data (including security policies and QoS policies) while being transported from SDN applications to the SDN controller over the application-control interface.	SDN Controller	Data integrity	Implement security mechanisms for integrity protection of configuration data stored in the SDN controller and configuration interfaces. Holistic Support for Security policies	Unauthorized access, Denial of service, eavesdropping, Manipulation attacks. (NAAx, EIH4)	MNO	Rec. ITU-T X.1038 (10/2016) / R-18, R-22

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerable mechanisms for authentication and authorisation of SDN components							
Improper authentication and authorisation	Improper authentication and/or authorisation mechanism for SDN controller or defective implementations of these mechanisms,	SDN Controller	Authentication and authorisation	It is required to provide a functionality in the SDN resource layer to authenticate the SDN controller. It is required to provide a functionality in the SDN control layer to authenticate the SDN switch.	Unauthorized access, Denial of service, eavesdropping, repudiation attacks, information disclosure (NAAx, EIH4)	MNO	Rec. ITU-T X.1038 (10/2016) / R-10, R-11, R-12, R-13, R-14
Improper hardening of SDN components							
Multiple vulnerabilities in operating system	An attacker may exploit vulnerabilities of the operating system such as default passwords, back-door accounts, open ports, unprotected services, unsecure protocols.	SDN Controller	Operating system hardening	Disable unused services; close unused ports, activate firewall, update software package, monitor integrity of file system.	Spoofing (NAAx)	MNO	Rec. ITU-T X.1038 (10/2016) / R-24
Software vulnerabilities	SDN controllers operate as a software platform. Vulnerabilities of general software become vulnerabilities for the SDN controller. A software vulnerability is a flaw, defect in software construction, weakness or even an error, which could be exploited by attackers to alter the normal behaviour of the SDN network or to reconfigure the whole network to make further attacks.	SDN Controller	Vulnerability assessment	Regular and effective vulnerability management program	Authentication and authorisation attacks, denial of service, eavesdropping, repudiation attacks, information disclosure (NAAx, FMx)	MNO	Rec. ITU-T X.1038 (10/2016) / R-25
Improper cryptographic key management mechanisms	Improper mechanisms to manage cryptographic key, including use of weak algorithms, undermine trust in integrity and confidentiality protection mechanisms	SDN Controller	Cryptographic controls	It is required to provide a functionality in the SDN controller layer to perform key/certificate management.	Spoofing, Repudiation, Information Disclosure (NAAx)	MNO	Rec. ITU-T X.1038 (10/2016) /R19
Lack of, or improper DoS protection mechanisms	Lack of DoS mechanisms lays all SDN applications and resources potentially uncontrollable in case of an attack	SDN Controller	DoS protection mechanisms	It is required to provide a functionality in the SDN control layer to support anti-DoS protection.	DoS attacks (NAA5)	MNO, Vendor	Rec. ITU-T X.1038 (10/2016) /R16

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Insufficient or improper monitoring mechanisms of SDN components							
Improper log and audit mechanisms	Improper monitoring may lead to attacks or failures going undetected and therefore not mitigated	SDN Controller	Log and audit management	It is required to provide a functionality in the SDN control layer to support log and audit.	Undetected nefarious activities Undetected malware Undetected failures of malfunctions (NAAx, FMx)	MNO	Rec. ITU-T X.1038 (10/2016) /R-17
Lack of, or improper hardware monitoring mechanisms	Improper monitoring and management of hardware resources may lead to the operator not being able to prevent or to mitigate hardware failures in a timely manner. Hardware failures may in turn compromise network security or bring down the SDN network.	SDN Controller	Hardware monitoring mechanisms	It is recommended to provide a functionality in the SDN control layer to support hardware management to discover hardware failure automatically and recover from such a failure as soon as possible.	Hardware failure (FMx)	MNO	Rec. ITU-T X.1038 (10/2016) /R26
Virtualisation vulnerabilities of relevant SDN components							
Vulnerabilities in virtualization layer	SDN offers a high level of abstraction to the programmers. When applications are developed caution is required to protect the network operation against application misbehaviour and bugs.	SDN Application, SDN Resources	Application Isolation	Sandboxing, application-Kernel isolation, application permission policy enforcement	Eavesdropping, Interception, Hijacking (NAAx, EIH4)	Developers, Administrators, System configuration	ENISA Threat Landscape and Good Practice Guide for Software Defined Networks/5G / 8.1
Physical and environmental vulnerabilities of relevant SDN components							
Data centre vulnerabilities	Many SDN systems are deployed within data centres. Security vulnerabilities of data centres should be considered. Data servers are using Data Centre Interconnect (DCI) protocols, which may lack authentication and encryption to secure the packet contents.	SDN Infrastructure layer	Traffic encryption	Encrypt the interconnection traffic between Data Centres.	Eavesdropping, Interception, Hijacking (NAAx, EIH4)	Administrators, System configuration	ENISA Threat Landscape and Good Practice Guide for Software Defined Networks/5G / 5.3

H ANNEX: DETAILED VULNERABILITIES IN MULTI-ACCESS EDGE COMPUTING

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerabilities in implementation of MEC security functionalities							
Improper mechanisms for collection, secure storage and transmission of charging-related information	The mobile edge system shall allow the collection of charging-related information, log it in a secure way and make it available for further processing.	Application Data Traffic, MEC Host	Collection of charging related information	The mobile edge system shall allow the collection of charging-related information, log it in a secure way and make it available for further processing.	"Unauthorised access to data, Fraud NAA2"	MNO, Edge Computing Service Provider	ETSI GS MEC 002 V2.1.1 (2018-10) / 8.3. [Charging-01]
Improper mechanisms for Lawful Interception at Edge level	The mobile edge system shall comply with regulatory requirements for lawful interception.	Multi-edge computing	Compliance with lawful interception requirements	The mobile edge system shall comply with regulatory requirements for lawful interception.	Inability to respond to lawful interception mandates LEG	MNO, Edge Computing Service Provider	8.2. [Lawful-01] ETSI GS MEC 002 V2.1.1 (2018-10)
SBA/SBI vulnerabilities of MEC components							
Improper implementation of APIs	CAPIF main purpose is to have a unified north bound API framework across several 3GPP functions. Like any software, APIs can be compromised and your data can be stolen. Since APIs serve as conduits that reveal applications for third-party integration, they are susceptible to attacks.	3GPP SA6 interfaces, ETSI MEC interfaces	Secure APIs	The confidentiality and data integrity of all messages shall be ensured by using TLS on each interface. The client and authorisation servers shall mutually authenticate. The client shall authenticate the resource server.	Unauthorized access, Interception, Eavesdrop, Availability Attacks, TCP Attack NAAx, EIH4	MNO, Edge Computing Service Provider	ETSI White Paper #36 - Harmonizing standards for edge computing

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper traffic path update for mobility support	MEC system is able to flexibly choose UPF(s) and the corresponding DN according to MEC operators' and/or MEC application providers' operation policy or unstable physical conditions. If traffic path is not updated appropriately, user context may not be transferred to the application instance.	Application Data Traffic	5GC control plane solution	Obtaining the mandatory input parameters and use high level message flow to influence traffic path.	Service unavailability FM5	MNO, Edge Computing Service Provider	ETSI GR MEC 031 V2.0.20 (2020-08) / 5.1
Improper protection of Data and Information							
Improper access control to information	The mobile edge platform shall only provide a mobile edge application with the information for which the application is authorized.	MEC platform, MEC Application, EAS	Information access controls	The mobile edge platform shall only provide a mobile edge application with the information for which the application is authorized. Authentication of access to the MEC services has to be performed according to CAPIF	Unauthorised access to data, malicious modification of configuration data, elevation of privileges NAAx	MNO, Edge Computing Service Provider	ETSI GS MEC 002 V2.1.1 (2018-10) / 8.1. [Security-02]
Virtualisation vulnerabilities of relevant MEC components							
Vulnerable virtualisation / container / micro-service environment	Security risks and concerns around virtual IT systems can be broadly classified into three types: 1. Architectural: The layer of abstraction between physical hardware and virtualized systems running IT services is a potential target for attack. A VM or group of VMs connected to the same network can be the target of attacks from other VMs on the network. 2. Hypervisor software: The most important software in a virtual IT system is the hypervisor. Any security vulnerability in the hypervisor and associated infrastructure and management software / tools puts VMs at risk. 3. Configuration: Given the ease of cloning and copying images in a virtual environment, a new infrastructure can be deployed very easily. This introduces configuration drift. As a result, controlling and accounting for rapidly deployed environments becomes a critical task.	Virtual infrastr., Virtual Infrastr. manager (VIM)	Best Practices for Mitigating Risks in Virtualized Environments	The design should take into account the appropriate logical segregation of instances that contain sensitive data. During implementation, extensive assessment of the vulnerability of the virtualization components is mandatory. The underlying virtualization platform should be hardened using vendor-provided guidelines and/or third-party tools. In a virtualized environment, robust key management is essential to access control and proof of ownership for both data and keys. Role-based access policies should be enforced to enable segregation of duties and data. Proper VM encryption is required to significantly reduce the risk associated with user access to physical servers and storage containing sensitive data.	Unauthorised access, eavesdropping, modification of security parameters, lateral movements, denial of services NAAx, FMx	MNO, Edge Computing Service Provider	Cloud Security Alliance - Best practices for mitigating risks in virtualized environments

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper hardening of MEC Components							
Lack of / improper DDoS Protection	Due to the distributed nature of edge computing deployments, appropriate DDoS mechanisms may be impractical to deploy. Alternative protection mechanisms need to be implemented in order to deter attacks.	Customer facing service (CFS) portal	Response to DoS/DDoS attacks	Although specific measures required depend upon the type of DoS/DDoS attacks, telecommunications organizations should take account of the following countermeasures: a) filtering of packets heading for the target site under attacks; b) restriction of communication port used for DoS/DDoS attacks; c) reduction or suspension of operation of target telecommunications facilities.	Denial of Service NAA5	MNO, Edge Computing Service Provider	ISO/IEC 27011 - ITU x.1205 / TEL.13.1.6
MEC Application Vulnerabilities							
Vulnerabilities in MEC applications	Vulnerabilities in MEC Applications may be used as an entry point for attacks aiming at exploiting the virtualisation environments, unauthorised access to data, elevation of privileges or denial of service.	MEC applications, Edge Application Server (EAS)	Security Testing of MEC Applications	A regular security testing program should be implemented to provide assurance that application vulnerabilities are identified and mitigated in a timely manner.	Exploitation of application security vulnerabilities	Edge Computing Application Provider	ISO/IEC 27001 / A.18.2.3
Vulnerabilities of the MEC virtualization platform							
Improper isolation of resources	Physical and logical resources should not be shared with components which have not the same criticality. This constraint requires the right level of isolation around the service to prevent regulation pollution to its own components and infrastructures	Virtualisation infra-structure, MEC host, MEC Platform	Resource isolation	Network segmentation, resource separation, data segregation.	Unauthorized access, Interception, Eavesdrop NAAx	MNO, Edge Computing Service Provider	NIS Directive

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Physical and environmental vulnerabilities of relevant MEC components							
Improper Physical and environmental security of edge computing facilities	Edge computing facilities are, by their nature, seated in locations distributed geographically. Normally, the first choice will be communications shelters already operated by MNO. While communications shelters have physical security controls in place, these are calibrated to risks associated with communication equipment. An additional risk assessment is needed to assess suitability in the context of additional risks incurred by presence of computing facilities.	MEC Host	Improper physical security of equipment in remote locations	To protect physically isolated operating areas (e.g., mobile base stations) in which telecommunications facilities are located for providing telecom business, the following controls should be considered: a) earthquake-proofing; b) automatic fire control equipment; c) monitoring by a remote office for the purpose of detecting facility failures, power failures, fire, humidity and temperature and so on; d) physically secure perimeters, including an automatic alert function.	Destruction of edge computing facilities, unauthorised access at system level as an entry point to all hosted resources, theft of data on local storage. Vandalism, Sabotage Natural Disaster PAx, DIS	MNO, Edge Computing Service Provider	ISO/IEC 27011 - ITU x.1205 / TEL.11.1.8, TEL 11.3
Improper security monitoring of edge computing facilities	Mobile-edge computing have to be integrated in the network-wide Security Incident and Monitoring System, but with additional considerations: development of use-case specific alert rules, integration and correlation of data at all levels (network, application), integration and correlation with service provider -level monitoring mechanisms. Failure to do so may leave advanced or sustained threats undetected, as well as technical failures or malfunctions of local resources.	MEC Host	Security Incident and event monitoring	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. Additional considerations: development of use-case specific alert rules, integration and correlation of data at all levels (network, application), integration and correlation with service provider -level monitoring mechanisms.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Unauthorised access, Elevation of privileges. Technical failures NAAx, FMx	MNO, Edge Computing Service Provider	ISO/IEC 27011 - ITU x.1205 / A.12.4.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Insecure service environment	The mobile edge system shall provide a secure environment for running services for the following actors: the user, the network operator, the third-party application provider, the application developer, the content provider, and the platform vendor.	MEC Host	Secure environment	The mobile edge system shall provide a secure environment for running services for the following actors: the user, the network operator, the third-party application provider, the application developer, the content provider, and the platform vendor.	Unauthorised access, eavesdropping, modification of security parameters, lateral movements, denial of services PAx, DIS, NAAx, FMx	MNO, Edge Computing Service Provider	ETSI GS MEC 002 V2.1.1 (2018-10) / 8.1. [Security-01]
Vulnerable mechanisms for authentication and authorisation of MEC components							
Improper authentication policy, such as unauthenticated access to system functions, use of generic accounts	The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) opens the opportunity of exploitation and limits accountability. This includes M2M communication.	LCM Proxy, MEC Orchestrator	System functions shall not be used without proper authentication and authorisation.	The usage of a system function without proper authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure	MNO, Edge Computing Service Provider	3GPP TS 33.117 4.2.3.4.1.1
Insecure / insufficient authentication attributes, such as failure to protect accounts by at least one authentication attribute, active predefined authentication attributes.	Depending on information sensitivity different level of strong authentication mechanisms are required. Fail to identify the proper correspondence between levels of protection and authentication mechanisms implemented creates the possibility to allow unauthorized entities to access unallocated resources.	LCM Proxy, MEC Orchestrator	Secure procedures for authentication and authorisation	The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user. All predefined or default accounts and/or or default authentication attributes shall be deleted or disabled.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure	MNO, Edge Computing Service Provider	3GPP TS 33.117 4.2.3.4.1.2, 4.2.3.4.2.1 4.2.3.4.3.

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Weak or missing password policy	A password policy shall address the password structure, password change, hiding password display capabilities, consecutive failed login attempts. A week password structure and/or a long validity password period could lead to a successful brute force attack. Failure to block consecutive failed login attempts may lead to password guess.	LCM Proxy, MEC Orchestrator	Password policy	Password policy requirements include requirements regarding Password complexity, password change, Protection against brute force and dictionary attacks, hiding password display	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure	MNO, Edge Computing Service Provider	3GPP TS 33.117 4.2.3.4.3.
Insecure authentication mechanisms to management / maintenance interfaces	The network product management shall support mutual authentication mechanisms, the mutual authentication mechanism can rely on the protocol used for the interface itself or other means.	LCM Proxy, MEC Orchestrator	Protect management interfaces	Protect devices used for administration. Reduce the exposure of management interfaces. Ensuring there's a trail of breadcrumbs.	Unauthorised access at system, theft of data	MNO, Edge Computing Service Provider	3GPP TS 33.117 4.2.3.4.4.1
Insecure authorisation and access control mechanisms	The authorisations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.	LCM Proxy, MEC Orchestrator	Authorisation and access control	The authorisations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform. Authorisations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error	MNO, Edge Computing Service Provider	3GPP TS 33.117 4.2.3.4.6
Insufficient or improper monitoring mechanisms of MEC components							
Insufficient / inadequate logging of security events for MEC App and MEC host	Lack of security events logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred do not allow a correct and rapid audit in case of security incident occurrence.	MEC platform, MEC Host, MEC Application, VIM	Security event logging	Security events shall be logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred. For each security event, the log entry shall include user name and/or timestamp and/or performed action and/or result and/or length of session and/or values exceeded and/or value reached. IETF RFC 3871, section 2.11.10 specifies the minimum set of security events.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error	MNO, Edge Computing Service Provider	3GPP TS 33.117 4.2.3.6.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Logs not transferred to centralized storage	Security event logs should be forwarded or uploaded to a central location or external systems. Security event log files shall be protected in storage and transfer states, too.	MEC platform, MEC Host, MEC Application, VIM	Transfer security logs to a centralized storage	Log functions should upload securely of log files to a central location or to an external system for the Network Product that is logging. Secure transport protocols shall be used.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error	MNO, Edge Computing Service Provider	3GPP TS 33.117 4.2.3.6.2 4.2.3.6.3
Improper protection of security event log files	Availability and integrity of security event log files could conduct to delays, wrong audit results, delays in security restauration, threats persistence.	MEC platform, MEC Host, MEC Application, VIM	Protection of security event log files	The security event log shall be access controlled (file access rights) so only privileged users have access to the log files.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error	MNO, Edge Computing Service Provider	3GPP TS 33.117 4.2.3.6.2 4.2.3.6.3

I ANNEX: DETAILED VULNERABILITIES IN THE PHYSICAL INFRASTRUCTURE

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stake-holder	Source Ref
Vulnerabilities of Data centre and telecommunication facilities							
Improper physical security of communication centres	Communication centres should provide a full set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters. Failure to do so may lead to unauthorised access, destruction of assets and impairment of operations.	Physical asset, Cloud Data Centre	Securing communication centres	Physical security of communication centres, where telecommunications facilities such as switching facilities for providing telecommunications business are housed, should be designed, developed and applied.	Destruction of assets, unauthorised access, theft of data on local storage, vandalism, sabotage Natural Disasters (PAx, DIS)	MNO	ISO/IEC 27011 - ITU x.1205 / TEL.11.1.7, TEL 11.3
Improper physical security of telecommunications equipment room	Telecom equipment rooms should provide a risk-calibrated set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters. Failure to do so may lead to unauthorised access, destruction of assets and impairment of operations.	Physical asset, Light Data Centre	Securing telecommunications equipment room	Physical security of equipment room, where telecommunications facilities are set for providing telecommunications business, should be designed, developed and applied.	Destruction of assets, unauthorised access, theft of data on local storage, vandalism, sabotage Natural Disasters (PAx, DIS)	MNO	ISO/IEC 27011 - ITU x.1205 / TEL.11.1.8, TEL 11.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stake-holder	Source Ref
Improper physical security of physically isolated operation areas	Remote equipment facilities should provide a set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters, taking into account its remoteness and lack of human presence. Failure to do so may lead to unauthorised access, destruction of assets and impairment of operations.	Physical asset, Light Data Centre	Securing physically isolated operation areas	For physically isolated operating areas, where telecommunications facilities are located for providing telecom business, physical security controls should be designed, developed and implemented.	Destruction of assets, unauthorised access, theft of data on local storage, vandalism, sabotage Natural Disasters (PAx, DIS)	MNO	ISO/IEC 27011 - ITU x.1205 / TEL.11.1.9, TEL 11.3
Improper physical security equipment sited in other carrier's or partner's premises	Equipment located in third party facilities rooms should be protected using a risk-calibrated set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters. Failure to do so may lead to unauthorised access, destruction of assets and impairment of operations.	Physical asset, Light Data Centre	Protection of equipment sited in other carrier's premises	When telecommunications organizations install equipment outside of their own premises, the equipment should be sited in a protected area so that any risks from environmental threats or dangers and from the possibility of unauthorized access are reduced.	Destruction of assets, unauthorised access, theft of data on local storage, vandalism, sabotage Natural Disasters (PAx, DIS)	MNO, Partner	ISO/IEC 27011 - ITU x.1205 / TEL.11.1.8, TEL 11.3.1
Improper protection to Power Outages	Lack of a power supply continuity strategy that includes multiple power supplies to avoid a single point of supply failure.	Physical asset	Continuity of power supplies	Power supply facilities in the isolated area such as mobile base stations should preferably provide an uninterruptible power supply with capacity for all loading and capable of withstanding primary power supply failures for the duration of likely outages. If that is impossible, a mechanism to provide uninterruptible power to critical equipment should be installed. Batteries may need to be augmented with a private electric generator, especially in isolated areas.	Unavailability of resources (OUT)	MNO, Vendor	ISO/IEC 27011 / 11.2.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stake-holder	Source Ref
Improper protection against environmental disasters	Environmental conditions, such as temperature and humidity, should be monitored for conditions, which could adversely affect the operation of information processing facilities. If the systems of several organizations are sited in the same data centre as telecommunications facilities, the telecommunications organization should implement appropriate measures to protect customers' information stored in their systems.	Physical asset	Equipment siting and protection	Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Destruction of assets, natural disasters (FM5, DIS)	MNO, Partner	ISO/IEC 27011 / 11.2.1
Improper capacity planning	Lack of capacity for mission critical telecommunication systems and facilities.	Physical asset	Capacity management	The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Unavailability of services (OUT)	MNO	ISO/IEC 27011 / 12.1.3
Improper maintenance	Improper maintenance of equipment in the data centre can lead to failures.	Physical asset	Maintenance program	Equipment should be maintained in accordance with the supplier's recommended service intervals and specifications. Only authorized maintenance personnel should carry out repairs and service equipment.	Destruction of assets, unavailability of services (UD4, OUT)	MNO	ISO/IEC 27011 / 12.1.4
Improper monitoring of hardware parameters	The lack of monitoring of the hardware parameters means that the preventive alerts given by the equipment are not included in the operative maintenance. Thus, preventive maintenance is not done in time and defects can occur, creating incidents and making equipment unavailable. The cost of corrective maintenance is much higher than the cost of preventive maintenance	Physical asset	Monitoring program	Develop a program to monitor critical hardware resources	Destruction of assets, unavailability of services (UD4, OUT)	MNO	ISO/IEC 27011 / 12.1.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stake-holder	Source Ref
Hardware vulnerabilities							
Firmware vulnerabilities	Firmware could be hacked and embedded with malware. Firmware producers usually do not design their firmware with security in mind. Firmware malware will exploit this lack of security by attaching their code to the firmware's code.	Hardware	Secure firmware	The firmware must be secured by a cryptographic signature (hash) in order to be able to detect infiltration. Update firmware periodically. Buy hardware with built-in protections against malicious firmware.	Firmware malware (NAAx)	Vendor	
Side-channel vulnerabilities	A side-channel vulnerability bypasses a computer's account permissions, virtualization boundaries and protected memory regions and exposes sensitive device information. Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited. Notable side-channel vulnerabilities include: Spectre / Meltdown, Foreshadow, TLBleed, PortSmash, NetSpectre.	Hardware	TEMPEST-resistant standards	Shielding of devices from EMR is achieved by a number of methods. The most sophisticated devices use advanced micro-components that have been designed from scratch to minimize Tempest emanations. Generally, shielding involves encompassing the device in a Faraday cage that does not permit stray emanations, along with special modifications to the power source. Tempest shielding also involves such issues as the design of a room and placement of equipment within it, to ensure that no information can escape.	Unauthorised access at system, theft of data (PAx)	Vendor	
Hardware Backdoor	A hardware backdoor might easily be installed through re-flashing BIOS. A hardware backdoor typically has full access to the device it runs on. The backdoors may be directly implemented as hardware Trojans in the integrated circuit.	Hardware	Firmware upgrade	Hardware backdoor might be removed by replacing the hardware or re-flashing BIOS, or firmware for net devices.	Recovered keys could be used to compromise the operating system and encrypted data. (NAAx)	Vendor	
Semiconductor Doping	Adding impurities to silicon-based semi-conductors change or control their electrical properties. It is possible to 'dope' transistors of a chip to change function behaviour. This was done successfully to change the random number generator of Ivy Bridge Intel processors.	Hardware	Product testing	Purchase and use of tested and certified hardware equipment.	Rogue designer /developer / admin (NAAx)	Vendor	

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stake-holder	Source Ref
Unprotected management interfaces and consoles	Management interfaces are written in software, and like all software, can contain vulnerabilities.	Hardware	Protect management interfaces	Protect devices used for administration. Reduce the exposure of management interfaces. Ensuring there is a trail of breadcrumbs.	Unauthorised access at system, theft of data (NAA4, EIH4)	MNO, Vendor	
TPM-FAIL vulnerabilities	TPM-FAIL vulnerabilities allow attackers to steal cryptographic keys protected inside of Trusted Platform Modules (TPMs).	Hardware	Monitor hardware vulnerabilities	Buy only tested and certified hardware. Replace vulnerable hardware immediately.	Recovered keys could be used to compromise the operating system and encrypted data. (NAA4, EIH4)	Vendor	
Cabling vulnerabilities							
Unprotected cables	Fibres routed between pieces of equipment without proper protection are susceptible to damage, which can critically affect network reliability. The fibre cable management system should therefore ensure that every fibre is protected from physical damage.	Cables	Compliance with cable standards	Raceway / conduit, is one of the easiest ways to protect any cable, fibre optic included. These hollow pieces of plastic act like a protective outer shell.	Destruction of assets, unauthorised access, vandalism, sabotage (UD4, OUT)	MNO	TIA-569-E
Unprotected junction boxes	Lack of protection of junction boxes / splice closures. Improper cable routing also causes increased congestion in the termination panel and the cableways, increasing the possibility of bend radius violations and long-term failure.	Cables	Secure junction boxes	Optical fibre junction boxes / splice closures shall be accessible to maintenance personnel and maintenance vehicles. A closure should be located away from high traffic or conditions that could cause damage to the closure or injury to personnel.	Destruction, unauthorised access, vandalism, sabotage (UD4, OUT)	MNO	TIA-569-E
Vulnerabilities related to virtualisation technologies							
Improper protection of access to management interfaces	Management interfaces are written in software, and like all software, may contain vulnerabilities. Avoiding exposure of management interfaces can reduce attack surface.	Virtualisation assets	Secure management interfaces	Reducing the exposure of management interfaces.	Improper protection of access to management interfaces	MNO,	Cloud Security Alliance

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stake-holder	Source Ref
Vulnerable mechanisms for Hardware-Based Root of Trust (HBRT)	A Hardware-Based Root of Trust (HBRT) should act as Initial Root of Trust to ensure a safe environment for running sensitive virtualised components.	Virtualisation assets	Core HBRT hardware requirements	The host system shall implement a Hardware-Based Root of Trust (HBRT) based on core hardware requirements	Hardware manipulation	MNO, Vendor	NA
Hypervisor vulnerabilities conduct to cross-contamination of shared resources	A hypervisor-based attack is an exploit in which an intruder takes advantage of vulnerabilities in the program used to allow multiple operating systems to share a single hardware processor. A compromised hypervisor can allow the hacker to attack each virtual machine on a virtual host.	Virtualisation assets	Hardening hypervisor	Secure access can become compromised due to VM sprawl and other issues. Ensure that authentication procedures, identity management, and logging are enforced	Hypervisor-based attacks	MNO, Vendor	NA
Improper availability arrangements for hardware infrastructure	Denial of service attacks exploit many hypervisor platforms and range from flooding a network with traffic to sophisticated leveraging of a host's own resources. The availability of botnets continues to make it easier for attackers to carry out campaigns against specific servers and applications with the goal of derailing the target's online services.	Virtualisation assets	VM traffic monitoring	The ability to monitor VM backbone network traffic is critical. Conventional methods will not detect VM traffic because it is controlled by internal soft switches. However, hypervisors have effective monitoring tools that should be enabled and tested.	Denial of service	MNO, Vendor	NA
Shared resource contamination	VM guest OS may escapes from its VM encapsulation to interact directly with the hypervisor. This gives the attacker access to all VMs and, if guest privileges are high enough, the host machine as well. Although few if any instances are known, experts consider VM escape to be the most serious threat to VM security.	Virtualisation assets	VM segregation	In addition to normal isolation, strengthen VM security through functional segregation.	VM image attacks, VM-based attack	MNO, Vendor	NA

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stake-holder	Source Ref
Vulnerability to Radio Jamming Attacks							
Vulnerability to radio jamming attacks	As any wireless cellular networks, 5G networks are built upon open sharing in which the communication medium is three space making them prone to interference. This weakness can be used by some adversary nodes to cause intentional interference and hinder legitimate user's communication over specific wireless channels. 5G improves resilience against jamming attacks over the 4G LTE but remains vulnerable to customised attacks. Jamming attacks are a special concern for mission-critical applications.	Base stations	Implement Anti-Jamming Technologies	Jam-resistance designs. Use hardware-based real-time encryption and decryption.	Eavesdropping, Interception, Hijacking, Denial of service, information disclosure (EIH4)	Vendor	NA

J ANNEX: DETAILED VULNERABILITIES IN IMPLEMENTATION OPTIONS

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerabilities of legacy technologies							
Inadequate integrity protection of over-the-air User Plane traffic	Should the Access Stratum (AS) over-the-air User Plane traffic not be adequately protected by Integrity Protection security algorithms, a scenario is possible where a customer's message and/or communication flow could be intercepted in the middle between the UE and the server. An adversary could then manipulate the customer's message and/or communication flow between the UE and the server.	UE, eNB, MME	Integrity protection of AS User Plane Traffic	User data and signalling data integrity, 3GPP 33.401 / 5.1.4	Tampering of Data, Information Disclosure NAAx, EIH4	MNO	3GPP 33.401 / 5.1.4
Exposure of international mobile subscriber identities (IMSI)	Exposure of IMSI may occur due to clear text transmission of IMSI during Authentication Procedures, or by means of insecure IMS Emergency Session Handling	UE, eNB, MME	Encryption of authentication procedures	Security Aspects of IMS Emergency Session Handling 3GPP 33.401 / 15 Authentication and key agreement3GPP 33.401 / 6.1	Tampering of Data, Information Disclosure NAAx, EIH4	MNO	3GPP 33.401 / 15 3GPP 33.401 / 6.1
Roaming vulnerabilities							
SS7 Vulnerabilities	Extensive research of SS7 and Diameter vulnerabilities is available in the ENISA - Signalling Security in Telecom SS7/Diameter/5G," Report, https:// www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g/at_download/fullReport.	LTE Visiting PLMN	Compensating controls	Compensating controls are detailed in the referred report	Tampering of Data, Information Disclosure NAAx, EIH4	MNO, Roaming partners	Signalling Security in Telecom SS7/Diameter /5G / Section 3.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Diameter vulnerabilities	Extensive research of SS7 and Diameter vulnerabilities is available in the ENISA - Signalling Security in Telecom SS7/Diameter/5G," Report, https:// www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g/at_download/fullReport.	LTE Visiting PLMN	Compensating controls	Compensating controls are detailed in the referred report	Tampering of Data, Information Disclosure NAAx, EIH4	MNO, Roaming partners	Signalling Security in Telecom SS7/Diameter /5G / Section 3.3
VoLTE vulnerabilities	Vulnerability to ReVOLTE attack: Adding a PDCP entity for the VoLTE data-bearer in the same radio connection resets packet counts fora second time, which introduces the keystream reuse for a subsequent call along with reusing the same bearer identity[96]	LTE Visiting PLMN	Increase bearer identities; derive new key with an intra-cell handover; mandatory media encryption and integrity protection	Using different radio bearer identities mitigates the threat of keystream reuse, as a separate input parameter changes the output keystream for the subsequent call. However, the radio bearer identity is only defined as a 5-bit field, which means that incrementing it only works for 32 new bearers. An inter-cell handover allows transferring a phone from one cell to another while the phone stays connected. Using an intracell handover as mitigation works, as the handover procedure has a built-in key reuse avoidance. A successful REVOLTE attack requires that no additional media encryption is active. Even though the adversary can attack and decrypt the radio layer encryption, such additional encryption via SRTP prevents access to any voice data	Tampering of Data, Information Disclosure NAAx, EIH4	MNO, Roaming partners	See reference

[96] David Rupprecht and Katharina Kohls and Thorsten Holz and Christina Popper, Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE, 29th USENIX Security Symposium Proceedings, 2020. isbn 978-1-939133-17-5, pages 73-88, accessed October 2020

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper implementation of updated security functions							
Vulnerabilities in MME implementation	Improper or not updated configuration and implementation of MME to comply with updated security requirements as defined by Release 16 versions of applicable 3GPP requirements	MME	MME security functionalities and configurations as defined by 3GPP updated specification	Relevant security requirements include: - User data and signalling data confidentiality and integrity - Integrity-, confidentiality- and replay-protection of control plane data over S1-MME and X2-C interfaces - Compliant Security Procedures between UE and EPC / EPS - Secure key derivation and management requirements - NAS Integrity mechanisms - Network Domain Control Plane protection - Secure IMS Emergency Session Handling	Tampering Data, Information Disclosure, Denial of Service NAAx, EIH4	MNO, Vendor	3GPP TS 33.401 v.16.3.0 / eNB / 5.1, 5.3, 6, 7, 8.1, 9,11, 14.1, 14.3, 15
Vulnerabilities in evolved Node B (eNB) implementation	Improper or not updated configuration and implementation of eNB to comply with updated security requirements as defined by Release 16 versions of applicable 3GPP requirements	eNB	User-to-network security; Security visibility and configurability; Security requirements for eNB	User-to-network security requirements include: - User identity and device confidentiality - Entity authentication - User data and signalling data confidentiality - User data and signalling data integrity Security requirements for eNB include: - Requirements for eNB setup and configuration - Requirements for key management inside eNB - Requirements for handling User plane data for the eNB - Requirements for handling Control plane data for the eNB - Requirements for secure environment of the eNB	Tampering Data, Information Disclosure, Denial of Service NAAx, EIH4	MNO, Vendor	3GPP TS 33.401 v.16.3.0 / eNB / 5.1, 5.2, 5.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerabilities in the technical baseline of EPC+ functions							
Improper protection of Data and Information of EPC+ components	Inadequate security measures for protecting sensitive data, such as: - System functions revealing confidential data - Improper protection of data and information in storage - Lack of or improper cryptographic protection of data in transfer - No traceability of access to personal data	EPC+ functions	3GPP TS 33.117 / 4.2.3.2 Protecting data and information	EPC+ components should be secured on a similar level to 5G Core components. Detailed description of security requirements in the technical baseline is presented in the corresponding 5G Core detailed vulnerabilities section.	Elevation of Privilege, Information Disclosure, Tampering NAA2, NAA3, NAA4	MNO, Vendor	3GPP TS 33.117, 116, 216 / 4.2.3.2.
Improper protection of availability and integrity of EPC+ components	Inadequate security measures for protecting availability and integrity, such as: - Failure to address overload situation - Boot from unauthorized memory devices - Improper handling of unexpected input - Insufficient assurance of software package integrity	EPC+ functions	3GPP TS 33.117 / 4.2.3.3 Protecting availability and integrity	EPC+ components should be secured on a similar level to 5G Core components. Detailed description of security requirements in the technical baseline is presented in the corresponding 5G Core detailed vulnerabilities section.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	MNO, Vendor	3GPP TS 33.117, 116, 216 / 4.2.3.3.
Vulnerable mechanisms for authentication and authorisation of EPC+ components	Inadequate mechanisms for authentication and authorisation, such as: - Unauthenticated access to system functions - Improper authentication mechanisms - Predefined/ default accounts and/or authentication attributes - Weak or missing password policy - Lack of mutual authentication of entities for management interfaces - Improper authorisation and access control policy	EPC+ functions	3GPP TS 33.117 / 4.2.3.4 Authentication and authorisation	EPC+ components should be secured on a similar level to 5G Core components. Detailed description of security requirements in the technical baseline is presented in the corresponding 5G Core detailed vulnerabilities section.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure NAAx	MNO, Vendor	3GPP TS 33.117, 116, 216 / 4.2.3.4.

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper session protection mechanisms of EPC+ components	The system shall have a function that allows a signed in user to logout at any time. All processes under the logged in user ID shall be terminated on log out. A permanent exposed session increases the exposure of the system as an entry point for unauthorized person. OAM user interactive session shall be terminated automatically after a specified period of inactivity.	EPC+ functions	3GPP TS 33.117 / 4.2.3.5 Protecting sessions	EPC+ components should be secured on a similar level to 5G Core components. Detailed description of security requirements in the technical baseline is presented in the corresponding 5G Core detailed vulnerabilities section.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx"	MNO, Vendor	3GPP TS 33.117, 116, 216 / 4.2.3.5.
Insufficient or improper monitoring mechanisms of EPC+ components	Lack of security events logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred hinder a correct and rapid audit in case of security incident occurrence. Security restauration is delayed.	EPC+ functions	3GPP TS 33.117 / 4.2.3.6 Logging	EPC+ components should be secured on a similar level to 5G Core components. Detailed description of security requirements in the technical baseline is presented in the corresponding 5G Core detailed vulnerabilities section.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error NAAx, Udx	MNO, Vendor	3GPP TS 33.117, 116, 216 / 4.2.3.6.
Vulnerabilities in Operating Systems supporting EPC+ components	Inadequate or missing security measures at O.S. level, such as: - Improper / missing controls for protection of security event log files - Improper handling of growing content by file system - Processing of ICMP packets not required for operation - Processing of IP packets with unnecessary options or extensions - Privilege Escalation allowed without re-authentication - Recurrent UIDs for UNIX System accounts	EPC+ functions	3GPP TS 33.117 / 4.2.4. Operating Systems	EPC+ components should be secured on a similar level to 5G Core components. Detailed description of security requirements in the technical baseline is presented in the corresponding 5G Core detailed vulnerabilities section.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Operator Error, equipment / software errors, growing dynamic content r NAAx, Udx, FMx	MNO, Vendor	3GPP TS 33.117, 116, 216 / 4.2.4.
Vulnerabilities in Web Servers supporting EPC+ components	Inadequate or missing measures to secure web servers, such as: - Unsecure Https connection to web servers - Lack of / improper logging of access to the webserver - Lack of / improper http user session protection - Improper validation of HTTP input	EPC+ functions	3GPP TS 33.117 / 4.2.5. Web Servers	EPC+ components should be secured on a similar level to 5G Core components. Detailed description of security requirements in the technical baseline is presented in the corresponding 5G Core detailed vulnerabilities section.	Spoofing identity, Tampering of Data, Information Disclosure, Denial of Service, Session hijacking Injection, cross-site scripting, NAAx, EIH4	MNO, Vendor	3GPP TS 33.117, 116, 216 / 4.2.5.

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Vulnerabilities of network devices running EPC+ components	Inadequate or missing security in network devices, such as: - Lack of packet filtering functionality - Lack of robustness against unexpected input - Improper or absent GTP-C Filtering - Improper or absent GTPU Filtering	EPC+ functions	3GPP TS 33.117 / 4.2.6. Network Devices	EPC+ components should be secured on a similar level to 5G Core components. Detailed description of security requirements in the technical baseline is presented in the corresponding 5G Core detailed vulnerabilities section.	Denial of service, packet flooding, malware, authorisation attacks, man-in-the-middle attacks NAAx, FM5	MNO, Vendor	3GPP TS 33.117, 116, 216 / 4.2.6.
Improper hardening of EPC+ components	Failure to implement hardening baseline controls, such as: - Unnecessary or insecure services / protocols - Unrestricted reachability of services - Unused software components - Unused software or hardware functions - Unsupported components - Remote login of privileged users - Excessive Filesystem Authorisation privileges - Lack of protection against IP-Source address spoofing - Unneeded kernel network functions - automatic launch of removable media - No SYN Flood Prevention - No protection against buffer overflows - No/improper external file system mount restrictions - Directory listings - Web server information in HTTP headers - Web server information in error pages - Unused file type- or script-mappings - Unrestricted access to files - Execution rights outside CGI/Scripting directory - System privileges for web server processes - Active and unused HTTP methods - Unused web server addons - Access to compiler, interpreter, or shell via CGI or other server-side scripting - Common directory for uploads and CGI/Scripting	EPC+ functions	3GPP TS 33.117 / 4.3. Security requirements related to hardening	EPC+ components should be secured on a similar level to 5G Core components. Detailed description of security requirements in the technical baseline is presented in the corresponding 5G Core detailed vulnerabilities section.	Denial of Service, Spoofing identity, Tampering of Data, Information Disclosure, Component malfunctions, Authorisation attacks, elevation of privilege, Unauthorised / erroneous data element modification / deletion, Packet flood, Exploitation of vulnerable kernel functions, malware, bypassing of security controls, running unauthorised operating system, Syn Flood attacks, Buffer overflow attacks, Exploitation of vulnerable components, Code injection, Elevation of privileges, Abuse of unused vulnerable methods NAAx, UDx,FMx	MNO, Vendor	3GPP TS 33.117, 116, 216 / 4.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
	- Execution of system commands with server side includes (SSI) - Excessive / improper access rights for web server configuration files - Presence of default content - Inadequate traffic separation of traffic belonging to different network domains - Code execution or inclusion of external resources by JSON parsers - JSON Parser not robust						

K ANNEX: DETAILED VULNERABILITIES IN MNO PROCESSES

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper Resource Capability Delivery Processes							
Improper processes to map and analyse resource requirements	The Map & Analyse Resource Requirements processes define the detailed resource infrastructure requirements and the associated performance requirements. The high complexity of the 5G system demands well-structured analysis of such requirements. Failure to do so may lead to inability to deliver on planned operational and security parameters.	5G system architecture Operational processes	Map & Analyse Resources Requirements for end-to-end 5G network lifecycle using as a reference the applicable requirements, such as 3*GPP 33.501 and 23.501 and corporate / service-level security requirements.*	Implement sound processes to define the detailed resource infrastructure requirements to support the service capabilities required by new technological arrangements in the context of 5G. Such requirements should be based on detailed analysis of new resource requirements and should include detailed performance requirements – current and forecast.	Design errors; network complexity; new technology; lack of competences (NAAx, EIH4, Pax, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.5.2.1
Failure to adapt resource support and operations	The Enable Resource Support & Operations processes manage the design of any improvements or changes required to the operational support processes to support the new capabilities and infrastructure brought by the new technology. Improper functioning of these processes leads to operational support shortfalls which impair the ability to achieve, preserve or restore operational and security attributes.	Resource support and operations processes	Enable Resource Support & Operations - eTOM process type	Operator examines the network product; the compliance reports and the test laboratories accreditation published by the SECAM Accreditation Body and decides if the results are sufficient according to its internal policies	Faults or vulnerabilities in equipment FMx, OUT	MNO, Vendor, Accreditation Body	eTOM 20 / 1.5.2.5

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Inability to capture resource capability shortfalls	Processes must be in place to identify specific or imminent resource capacity, resource performance and/or resource operational support shortfalls. These processes must be adapted to the new technological and operational challenges of the 5G System. Failure to do so may lead to failure to foresee otherwise preventable operational and security incidents triggered by resource failure or limitations.	Resource capability delivery processes	Capture Resource Capability Shortfalls process - eTOM process type	Sound analysis to identify specific or imminent resource capacity, resource performance and/or resource operational support shortfalls. Special attention needs to be given to foreseen impact to connected systems, such as business support, billing, customer interfaces and common infrastructure, and adequate mechanisms have to be enabled for monitoring Tolerance (Survivability, Disruption Tolerance, Traffic Tolerance)	Network complexity; new/untested technology; new/untested business models; lack of competences (UDx, FMx)	MNO	eTOM 20 / 1.5.2.2
Improper Resource Capabilities design	Resource capabilities design processes must ensure a sound integration between the existing legacy resource infrastructure and the new resource infrastructure. Care must be given that resource analysis references relevant standards and best practices as well as security functionalities and controls. Failure to do so expose the system to degradation of operational and security attributes.	Resource capability delivery processes	Design Resource Capabilities process - eTOM process type	Sound management of resource infrastructure management to ensure that requirements of the migration projects include relevant standards and best practices as well as security functionalities and controls.	Network complexity; new/untested technology; new/untested business models; lack of competences (UDx, FMx)	MNO	eTOM 20 / 1.5.2.4
Improper management of Resource Capability Delivery	Adequate processes must be in place to manage the provision, implementation, commissioning and roll-out of the new resource capabilities and their associated operational support processes. Improper management and co-ordination of the delivery of individual resource infrastructure components lead to inability to deliver the overall resource capability and therefore inability to deliver the planned operational and security parameters	Resource capability delivery processes	Manage Resource Capability Delivery process - eTOM process type	Implement sound processes to manage the provision, implementation, commissioning and roll-out of the new or enhanced resource capability and associated operational support processes, aligned with the relevant eTOM reference and industry best practices. Such processes should include management of suppliers/partners responsible for the resource delivery, installation, and construction, and may include audits on operators and on implementation projects.	Exploitation of 5G networks triggered by improper management and co-ordination of the delivery of individual resource infrastructure component; nefarious activity/abuse (NAAx)	MNO	eTOM 20 / 1.5.2.6

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper processes to manage Handover to Resource Operations	Adequate processes must be in place to ensure that all relevant requirements have been met, and prerequisites for successful operation are in place at the prior to new resource infrastructure is handed over to operations. Failure to do so may lead to loss of operational control over the newly deployed resources.	Resource capability delivery processes Resource Management & Operations Processes	Manage Handover to Resource Operations process	Implement sound processes to manage the handover new resource infrastructure to operational control, aligned with the relevant eTOM reference and industry best practices. Such processes should ensure that all relevant requirements are met by the new resource infrastructure, and prerequisites for successful operation are in place, including skills, equipment and support processes and include coordination of all stakeholders involved in the approval and acceptance of handover to operational control.	Lack of available skills and competences (UDx)	MNO	eTOM 20 / 1.5.2.7
Improper Resource Development & Retirement Processes							
Improper control of Detailed Resource Specifications development	Adequate processes must be in place to develop and document detailed technical, performance and operational specifications for the components of the new 5G System. Failure to ensure adequate control on specification development may lead to significant security and operational exposure, especially so in the context of emerging technologies such as 5G System components.	Resource Development & Retirement Process	Develop Detailed Resource Specifications - eTOM process type	Implement sound processes to manage the develop and document detailed technical, performance and operational specifications, aligned with the relevant eTOM reference and industry best practices. Such processes must have as mandatory input security requirements and adherence to 3GPP specifications.	Network complexity; new/untested technology; lack of competences (UDx, FMx)	MNO	eTOM 20 / 1.5.3.4
Inadequate coordination of resource development	Adequate processes must be in place to ensure that all resources needed to support new resource classes/components are identified and developed. These might include new operational processes and procedures, IT / network changes and operational/service level agreements. Failure to do so impairs the ability to deliver the required resource capability and the associated operational and security attributes.	Resource Development & Retirement Process SLAs OLAs	Manage Resource Development - eTOM process type	Processes to ensure that the required service level agreements and operational level agreements are developed and agreed for each resource class deployed, and that any supplier/partner operational support has been identified and agreed, aligned with the relevant eTOM reference and industry best practices.	Legal Threats, Loss of Quality (LEG, FMx)	MNO	eTOM 20 / 1.5.3.5

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper management of resource deployment	Adequate processes must be in place to ensure the co-coordinated deployment of new resources aligned with the approved 5G business cases and to ensure that all resources needed to support new resource classes/components are implemented. These might include new operational processes and procedures, IT / network changes and operational/service level agreements. Failure to do so impairs the ability to deliver the required resource capability and the associated operational and security attributes.	Resource Development & Retirement Process	Manage Resource Deployment - eTOM process type	Implement sound processes to ensure the co-coordinated deployment of new resources aligned with the approved 5G business cases and to ensure that all resources needed to support new resource classes/components are implemented, aligned with the relevant eTOM reference and industry best practices.	Flawed products / resources, flawed processes, unreliable processes, lack of competences, unreliable partners (UDx, FMx)	MNO	eTOM 20 / 1.5.3.6
Improper storage media sanitisation	Reuse of data storage media without properly deleting previous data could lead to confidentiality loss of various types of data (management, operation, personnel) and subsequently to major security, commercial or judicial issues	Decommissioning processes Network Elements	Manage Resource Exit - eTOM process type	Resource exit procedures should include clear risk-based rules for media sanitisation upon decommissioning of network elements.	Unauthorised access to information (NAA1, NAA4)	MNO	ISO/IEC 27001 /A.8.3.2
Improper management of resource exit	Appropriate processes must be in place to develop specific exit or migration strategies, develop resource infrastructure transition and/or replacement strategies, and manage the operational aspects of the exit process. Failure to do so leaves open gateways for security threats, information leaks and operational failures.	Decommissioning processes Network Elements	Manage Resource Exit - eTOM process type	Implement sound processes to ensure the controlled of resource exit, aligned with the relevant eTOM reference and industry best practices. Such processes should ensure that specific exit, migration, resource infrastructure transition and/or replacement strategies are developed, and that the operational aspects of the exit process are managed. It is key that these processes include cross-enterprise co-ordination to ensure that the needs of all stakeholders are identified and managed.	Nefarious activity / abuse of vulnerable components, information leaks, operational failures (NAAx)	MNO	eTOM 20 / 1.5.3.7

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper Party Tender Management Processes							
Inadequate definition of sourcing requirements	Sourcing requirements take into account the required functional, technical and/or operational specifications. Such requirements must include security relevant requirements, must be aligned with industry standards, and must be aligned with the risk level of the purchased component. Failure to do so may lead to inability to deliver on security and operational attributes of the system.	Tender and purchasing processes	Determine the Sourcing Requirements - eTOM process type Indispensable baseline security requirements for the procurement of secure ICT products and services	Implement sound processes to determine sourcing requirements, aligned with the relevant eTOM reference. Such requirements should include technical, operational, training, and specific supplier support requirements. Security requirements, with regard for the entire supply chain must be taken into consideration. Industry standards and applicable regulatory requirements provide an essential input for this process.	Scarcity of potential and existing industry suppliers and partners, limited interoperability between different suppliers' equipment, high-risk suppliers (NAAx, FMx, UDx, LEG)	MNO	eTOM 20 /1.6.2.1
Improper process to determine Potential Suppliers/Partners	Potential S/P selection process must leverage information available from the Gather & Analyse Supply Chain Information processes, as well as other specific inputs available from within the enterprise, or from external supplier research organizations at the specific time the need arises. Failure to do so may lead to selection of suppliers whose risk profile is inadequate for the purchased product / service.	Tender and purchasing processes	Determine Potential Parties - eTOM Process Type Indispensable baseline security requirements for the procurement of secure ICT products and services	Implement sound processes to determine Potential Suppliers/Partners, aligned with the relevant eTOM reference. Such processes should shortlist suppliers that meet specific enterprise and industry standard requirements. Also, such processes should provide detailed analysis of potential partners/suppliers, leveraging information available from internal and external sources, such as dependency risks, espionage by state or state-backed actors using malware to abuse poor quality network components or unintentional vulnerabilities affecting sensitive elements in the network.	Scarcity of potential and existing industry suppliers and partners, limited interoperability between different suppliers' equipment, high-risk suppliers (NAAx, FMx, UDx, LEG)	MNO	eTOM 20 / 1.6.2.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Manage the Tender Process	In absence of sound tender management process, delays, and errors in selecting the appropriate vendors and solutions may result in deteriorating the security and availability of the 5G system, and failure to comply with applicable regulation.	Tender and purchasing processes	Manage the Tender Process	Implement sound processes to manage and administer the mechanics of the tender process, aligned with the relevant eTOM reference. Such processes should ensure coordination and control of engagement interactions with potential parties, timing of the process, inclusion of relevant commercial and functional requirements and tender analysis mechanisms, procedures, and approach.	Scarcity of potential and existing industry suppliers and partners, limited interoperability between different suppliers' equipment, high-risk suppliers (NAAx, FMx, UDx, LEG)	MNO	eTOM 20 / 1.6.2.3
Improper Resource management and operation Support & Readiness processes							
Improper processes to support resource provisioning	Improper processes for supporting Resource Provisioning processes may lead to ineffective and uncontrolled resource provisioning processes, leading availability issues and wrong configurations due to inappropriate information or emergency handling	Resource management and operation processes	Enable Resource Provisioning - eTOM process type	Implement sound processes to ensure availability and adequacy of support infrastructure for Resource Provisioning processes, and ensure that these processes are adequately managed, monitored, and reported on, aligned with the relevant eTOM reference and industry best practices. Key objectives of these processes in the context of 5GS migration include: - creation and deployment of support tools for resource deployment, and of adequate processes for newly modified resource infrastructure; - scheduling, management, and monitoring of the roll-out of new resource infrastructure -·monitoring of newly deployed infrastructure to provide early detection of potential shortfalls;	Network complexity; new/untested technology; lack of competences; flawed design/ equipment / system integration (UDx, FMx, OUT)	MNO	eTOM 20 / 1.5.4.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper processes to support resource performance management	Sound processes should be in place to monitor and assess resource infrastructure performance, as well as ensuring the capability of the Resource Performance Management processes. Soundness of such processes increases in importance with the increase in complexity and performance requirements of 5G networks	Resource management and operation processes	Enable Resource Performance Management - eTOM process type	Implement sound processes to monitor and assess resource infrastructure performance, and to monitor, manage and report on the capability of the Resource Performance Management processes, aligned with the relevant eTOM reference and industry best practices.	Network complexity; new/untested technology; lack of competences; flawed design/ equipment / system integration (UDx, FMx, OUT)	MNO	eTOM 20 / 1.5.4.2
Improper processes to support resource trouble management	Proper processes to conduct resource infrastructure maintenance and repair activities will be key to prevent performance degradation caused by unforeseen corelations and dependencies, and to proactively identify and remediate flaws that can affect confidentiality, integrity, availability of systems and data.	Resource management and operation processes	Support Resource Trouble Management - eTOM process type	Implement sound support processes for Resource Trouble Management, such as statistically driven preventative and scheduled maintenance and repair activities, and monitoring, management and reporting on Resource Trouble Management processes, aligned with the relevant eTOM reference and industry best practices.	Network complexity; new/untested technology; lack of competences; flawed design/ equipment / system integration (UDx, FMx, OUT)	MNO	eTOM 20 / 1.5.4.3
Improper management of resource inventory	Improper processes to establish and manage the enterprise Resource Inventory Database may lead to uncontrolled access to the resource inventory and poor data quality, which in turn opens the path to risks such as resource misconfiguration, loss of confidentiality for security-sensitive data and inefficient resource allocation and incident response	Resource management and operation processes	Manage Resource Inventory - eTOM process type	Implement sound support processes for resource inventory management, aligned with the relevant eTOM reference and industry best practices. Key objectives of these processes in the context of 5GS migration include: - updating of processes and tools for resource inventory management and information capture; - management of registration and access control processes - accuracy, completeness, and validation of resource inventory;	System heterogeneity (UDx, FMx, OUT)	MNO	eTOM 20 / 1.5.4.5

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper Party Agreement processes							
Insufficient / improper definition of relevant operational and security clauses in agreements with suppliers and partners	Improper processes for party agreement management may lead to Insufficient / improper definition of relevant operational and security clauses in agreements with suppliers and partners	Party Agreement processes	Prepare Party Agreement	Define and maintain a sound process to prepare agreements or a template agreement that can be used as the basis for party-specific agreements. Agreements should define the commercial terms and conditions and requirements to ensure compliance with the technical / operational reference specifications. All agreements should include relevant security clauses	Nefarious activities, Improper performance, Improper definition of security responsibilities and parameters, System misconfiguration, Lack of responsibility (NAAx, UDx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.5.1
Improper management of contract variations	Improper management of contract variations may lead to improper updating of security-relevant clauses and parameters, thus imperilling the overall security of the system	Party Agreement processes	Manage Party Agreement Variation	Define and maintain a sound process to manage changes to the terms/conditions of an agreement during its term of agreement.	Nefarious activities, Improper performance, Improper definition of security responsibilities and parameters, System misconfiguration, Lack of responsibility (NAAx, UDx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.5.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper Party Support processes							
Support Party Requisition Management	In the absence of sound processes to manage engagement with parties who own and manage outsourced infrastructure, and to ensure that the Party Requisition Management processes are operating effectively, a variety of risks affecting resource integrity and availability may ensue. Also, as these processes manage access authorisation, unauthorized access may result from faulty processes	Party Support processes	Support Party Requisition Management	Define and maintain sound Support Party Requisition Management processes to: - arrange and manage external party access to infrastructure deployment support tools and processes; - oversee roll-out of the new infrastructure; - track and monitor infrastructure deployment undertaken by contractors; - continuously update relevant inventories;	High-risk suppliers, supplier dependency, resource scarcity (UDx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.6.1
Support Party Performance Management	In the absence of sound processes to manage performance restoration activity with outsourced infrastructure providers, and to ensure that the Contractor Performance Management processes can operate effectively, resource and service availability issues may affect the performance and security of the system	Party Support processes	Support Party Performance Management	Define and maintain sound Support Party Performance Management processes, aligned with the relevant eTOM reference and industry best practices.	High-risk suppliers, supplier dependency, resource scarcity (UDx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.6.3
Support Party Interface Management	These processes are responsible for implementing generic and specific changes to supplier/partner interfaces, and to keep up to date all information concerning suppliers and partners. Inability to do so may lead to wrong allocation of resources, inability to liaise to S/P resources for resolution of operational / security incidents or allowing/maintaining unauthorized access rights due to obsolete contact data.	Party Support processes	Support Party Interface Management	Define and maintain sound processes to ensure that there is adequate capability to support effective operation of the S/P Interface Management processes, aligned with the relevant eTOM reference and industry best practices.	High-risk suppliers, supplier dependency, resource scarcity (UDx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.6.5

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper resource provisioning processes							
Improper processes for resource allocation and installation	Improper processes for allocation, installation, configuration, activation and testing of specific resources to meet the service requirements, or in response to requests from other processes may lead to resource capacity shortfalls, availability concerns or failure conditions, as well as misconfiguration-related security risks	Resource provisioning processes	Allocate & Install Resource - eTOM process type	Define and maintain sound processes to allocate & deliver specific resources required to support new services, and to ensure that sufficient information is supplied with the resource requisition orders regarding resource installation and configuration, aligned with the relevant eTOM reference and industry best practices.	Network complexity; new/untested technology; lack of competences; flawed design/ equipment / system integration	MNO	eTOM 20 / 1.5.6.1
Improper / obsolete processes to Configure & Activate Resources	The objective of the Configure & Activate Resource Processes is to configure and activate the specific resources allocated to fulfil resource orders. Improper processes or obsolete data used in process may lead to insecure configuration of equipment as well as lack of visibility over the systems' active resources.	Resource provisioning processes	Configure & Activate Resource - eTOM process type	Define and maintain sound processes to configure and activate the specific resources allocated against issued resource orders, aligned with the relevant eTOM reference and industry best practices. Key control objectives in the context of 5GS migration include: - configuration and activation approach and planning; - resource inventory update with the configuration of new resources and their status.	Network complexity; new/untested technology; lack of competences; flawed design/ equipment / system integration (UDx, FMx, OUT, LEG)	MNO	eTOM 20 / 1.5.6.2
Improper tracking & management of resource provisioning	Inefficient processes for tracking and management fail to provide guarantee that all provisioning tasks are finished at the appropriate time and in the appropriate sequence. An aggravating circumstance is reliance on provisioning activities when that have been outsourced or contracted to external parties.	Resource provisioning processes	Track & Manage Resource Provisioning - eTOM process type	Define and maintain sound processes to ensure resource provisioning activities are assigned, managed, and tracked efficiently, aligned with the relevant eTOM reference and industry best practices. Key control objectives in the context of 5GS migration include: - resource provisioning scheduling, allocation and coordination; - tracking of the execution process; - including all relevant information to resource orders, such as use case-specific security or operational requirements;· - Monitoring resource orders' status, and escalating resource orders as necessary; - engaging external suppliers when necessary	Network complexity; new/untested technology; lack of competences; flawed design/ equipment / system integration (UDx, FMx, OUT, LEG)	MNO	eTOM 20 / 1.5.6.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Resource Trouble Management							
Improper survey and analysis of resource trouble	Improper resource alarm event notification collection, filtering and correlation impairs the ability of the operator to detect and respond to service impacting condition, either by failing to respond to a relevant event, or by allocating resources to deal with false-positives, such as events triggered by planned outages. In the case of security event notifications, improper correlation and analysis may lead to significant losses of security attributes.	Resource Trouble Management processes	Survey & Analyse Resource Trouble	Define and maintain sound processes and tools to: - detect, collect, record, and manage resource alarm events; - perform alarm event notification analysis, correlation, and filtering; - report alarm events to relevant processes.	Network complexity; new/untested technology; lack of competences; flawed design/ equipment / system integration (UDx, FMx, OUT, LEG)	MNO	eTOM 20 / 1.5.8.1
Improper processes for localisation of resource trouble	Improper procedures for root-cause analysis and problem isolation, or failure to abide by such procedures may lead to significant delays in incident analysis and response and degradation of operational and security attributes	Resource Trouble Management processes	Localize Resource Trouble - eTOM process type	Define and maintain sound processes and tools to: - verify resource configuration and validate fitness for the relevant service features; - schedule and perform diagnose, test, and audit of resources in order to localise resource trouble events	Network complexity; new/untested technology; lack of competences; flawed design/ equipment / system integration (UDx, FMx, OUT, LEG)	MNO	eTOM 20 / 1.5.8.2
Improper processes for correction and resolution of resource trouble	Improper procedures, or deficient resource allocation for correction and resolution activities, as well as improper communication of correction & resolution results to other relevant processes may lead to significant losses of operational and security attributes.	Resource Trouble Management processes	Correct & Resolve Resource Trouble - eTOM process type	Define and maintain sound processes and tools to restore or replace resources that have failed as efficiently as possible, aligned with the relevant eTOM reference and industry best practices.	Network complexity; new/untested technology; lack of competences; flawed design/ equipment / system integration (UDx, FMx, OUT, LEG)	MNO	eTOM 20 / 1.5.8.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Resource data collection & distribution							
Incomplete / untimely / inaccurate Management and Security Information & Data	Processes and mechanisms for collection of management and security information and data records from resource and service instances and from relevant processes produces produce incomplete / untimely / inaccurate or otherwise inadequate management and security information and data	Security Data	Collect Management and Security Information & Data - eTOM process type	Define and maintain sound processes and tools to collect management and security information and data records from resource and service instances and relevant enterprise processes, aligned with the relevant eTOM reference and industry best practices. Key control objectives in the context of operation of 5GS include: - collection of security information and data from networks, systems, and security sensors - collection of usage, network, security, and information technology events and, performance and other management information - distribution of relevant information to other corporate processes or to resource and service instances.	Network complexity, evolving threat landscape (NAAx, EIH4, Pax, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.5.7.1
Improper processing of management and Security Information & Data	Processing of management and security information and/or data that does not output a form suitable for the intended recipient processes, resource or service instances renders such data unusable and hinders action upon it.	Security Data	Process Management and Security Information & Data - eTOM process type	Define and maintain sound processes and tools for processing of management and security information & data, aligned with the relevant eTOM reference and industry best practices.	Network complexity, evolving threat landscape (NAAx, EIH4, Pax, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.5.7.2
Inadequate processes for Audit of Management and Security Data Collection & Distribution	Audit and analysis of information & data collection, processing and distribution activities is not executed on a consistent basis to identify possible anomalies and to preserve audit data for future forensic use.	Security Data	Audit and Security Data Collection & Distribution - eTOM process type	Define and maintain sound processes and tools to audit information & data collection activities, aligned with the relevant eTOM reference and industry best practices.	Network complexity, evolving threat landscape (NAAx, EIH4, Pax, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.5.7.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper Resource Performance Management Processes							
Improper monitoring of resource performance	Improper processing of resource performance data, or improper setting of performance thresholds and standards, as well as failure to notify relevant resource trouble or resource performance management processes may lead to failure to detect and adequately respond to security-relevant events.	Performance data	Monitor Resource Performance - eTOM process type	Define and maintain sound processes and tools to monitor received resource performance information and perform direct detection of security-relevant events, aligned with the relevant eTOM reference and industry best practices. Key control objectives in the context of operation of 5GS include: - first in detection of security relevant events by monitoring specific resource performance data; - detection of performance threshold violations that signal resource failures; - detect performance degradation that provides early warning of potential issues; - log resource performance degradation and violation details to ensure historical records are available for other relevant processes.	Network complexity, evolving threat landscape (NAAx, EIH4, Pax, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.5.9.1
Improper processes for controlling resource performance	Control Resource Performance processes are designed to optimize resource performance by restoring failed resource instances, or normal operation thereof. Improper control plans, or improper decision making on necessary controls may lead to exposure to security risks or degradation of security attributes. This is especially relevant due to the highly interdependent nature of 5G systems	Performance data	Control Resource Performance - eTOM process type	Define and maintain sound processes and tools for timely and effective restoration of failed resource instances, or normal operation thereof, aligned with the relevant eTOM reference and industry best practices.	Network complexity, evolving threat landscape (NAAx, EIH4, Pax, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.5.9.3

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper Party Interaction Management Processes							
Track and Manage Party Interaction	In the absence of sound processes to ensure that Party Interactions are managed and tracked efficiently to meet applicable interaction policies and SLA requirements, performance and security deviations may appear	Party Interaction Management Processes	Track and Manage Party Interaction	Define and maintain sound processes and tools to track and manage interactions with relevant parties, aligned with the relevant eTOM reference and industry best practices. Key control objectives in the context of operation of 5GS include: - track and manage timely completion and closure of all interactions - monitoring and notifying situation when applicable SLAs are endangered; - measure, analyse and communicate KPIs to improve efficiency of interactions.	Network complexity, evolving threat landscape (NAAx, EIH4, Pax, UDx, FMx, OUT, DIS, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.9.3
Handle Party Interaction (Including Self Service)	The purpose of this process is to manage all requests. Improper management of interactions may leave unresolved security or operational events that involve external parties in analysis, response, and mitigation.	Party Interaction Management Processes	Handle Party Interaction (Including Self Service)	Define and maintain sound processes and tools to fulfil all inbound and outbound requests from/to external parties, aligned with the relevant eTOM reference and industry best practices.	Loss of quality, legal threats, supplier interface complexity (FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.9.4
Improper Party Problem Handling Processes							
Receive Party Problem	In the absence of sound processes to receive party-originated problems, problems may get unnoticed and unmanaged.	Party Problem Handling Processes	Receive Party Problem	Define and maintain sound processes and tools to manage problem raised by, or related to external parties, aligned with the relevant eTOM reference and industry best practices.	Loss of quality, security incidents, legal threats (NAAx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.10.1
Assess Party Problem	In the absence of sound processes to analyse party problems, solutions are not properly identified and implemented	Party Problem Handling Processes	Assess Party Problem	Define and maintain sound processes and tools to manage problem raised by, or related to external parties, aligned with the relevant eTOM reference and industry best practices.	Loss of quality, security incidents, legal threats (NAAx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.10.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Track Party Problem	In the absence of sound processes to track party problems, problems may stay unsolved	Party Problem Handling Processes	Track Party Problem	Define and maintain sound processes and tools to manage problem raised by, or related to external parties, aligned with the relevant eTOM reference and industry best practices.	Loss of quality, security incidents, legal threats (NAAx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.10.4
Analyse Party Problem Trend	In the absence of sound processes to analyse party problem trends, availability and integrity of critical systems and services may be imperilled	Party Problem Handling Processes	Analyse Party Problem Trend	Define sound processes to conduct and report trend analysis on party problems. These should include security parameters	Loss of quality, security incidents, legal threats (NAAx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.10.9
Improper Party Performance Management Processes							
Monitor & Control Party Performance	Improper processes to monitor & control performance of services, processes or resources delivered by external parties open significant operational risks due to the high availability objectives of the 5G system and attack path via forcing of emergency arrangements due to Supplier-side performance degradation.	Party Performance Management Processes	Monitor & Control Party Performance	Improper processes to monitor & control performance of services, processes or resources delivered by external parties open significant operational risks due to the high availability objectives of the 5G system and attack path via forcing of emergency arrangements due to Supplier-side performance degradation.	Loss of quality, security incidents, legal threats (NAAx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.11.1
Track & Manage Party Performance Resolution	The objective of the track & manage party performance resolution processes is to ensure improvement and restoration activities are being assigned, coordinated, and tracked efficiently, and that corrective actions are initiated for any relevant performance degradation reports. Failure to do so may lead to degradation of operational and security attributes.	Party Performance Management Processes	Track & Manage Party Performance Resolution	The objective of the track & manage party performance resolution processes is to ensure improvement and restoration activities are being assigned, coordinated, and tracked efficiently, and that corrective actions are initiated for any relevant performance degradation reports. Failure to do so may lead to degradation of operational and security attributes.	Loss of quality, security incidents, legal threats (NAAx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.11.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Manage and Administer Party Inventory	Improper management of Supplier inventory may lead to availability, integrity, and confidentiality risks on supplier data, including capabilities, resources, and contact data. These in turn may lead to operational and security risks of unauthorized access, inability to respond to operational or security events, or resource misallocation.	Party Inventory Management Processes	Manage and Administer Party Inventory	Improper management of Supplier inventory may lead to availability, integrity, and confidentiality risks on supplier data, including capabilities, resources, and contact data. These in turn may lead to operational and security risks of unauthorized access, inability to respond to operational or security events, or resource misallocation.	Loss of quality, security incidents, legal threats (NAAx, FMx, OUT, LEG)	MNO, Vendor, Service Provider	eTOM 20 / 1.6.21.2
Business Continuity Management							
Inadequate / obsolete business continuity plans	Business continuity plans must be updated to take into consideration the changed operational and risk landscape. Failure to do so may lead to inability to respond to major disruptive events.	BCM Process	Plan Business Continuity - eTOM process type	Business continuity must be carefully planned and operational procedures that support business continuity must be proactively tested, in line with the relevant eTOM specifications and industry best practices.	Disasters, outages (OUT, DIS)	MNO	eTOM 20 / 1.7.2.1.2
Inadequate / obsolete Infrastructure Recovery plans	Infrastructure recovery plans must be updated to take into consideration the changed operational and risk landscape. Failure to do so may lead to inability to respond to major disruptive events,	BCM Process	Plan Infrastructure Recovery - eTOM process type	Proactive determination and implementation of recovery procedures and backup planning for all key 5G infrastructure capabilities and their regular testing, in line with the relevant eTOM specifications and industry best practices.	Disasters, outages (OUT, DIS)	MNO	eTOM 20 / 1.7.2.1.3
Inadequate / obsolete incident management plans	Incident management plans must be updated to take into consideration the changed operational and risk landscape. Failure to do so may lead to inability to respond to major disruptive events,	BCM Process	Plan Serious Incident Management - eTOM process type	Plan and implement sound processes and for Serious incident management, including roles and responsibilities, operational procedures, and escalation criteria.	Disasters, outages (OUT, DIS)	MNO	eTOM 20 / 1.7.2.1.4
Fraud Management							
Failure to adapt fraud management policies and controls	Practices and processes for detection, investigation, ongoing education, tool uses, feedback of identified frauds, external interactions (partners, LEAs) must be adapted to the risks of 5G operations and technology. Failure to do so may lead to inability to prevent, detect, and respond to fraud,	Fraud Management	Fraud Policy Management - eTOM process type	Manage and maintain sound policies for fraud prevention and management, aligned with the relevant eTOM specifications and industry best practices.	Disasters, outages (OUT, DIS)	MNO	eTOM 20 / 1.7.2.3.1

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Insurance management							
Failure to identify insurable risks	With the introduction of the 5G systems, areas, and activities within the enterprise where risk aspects are insurable must be updated. Failure to identify insurable risks may lead to unnecessary risk exposure.	Insurance management	Identify Insurable Risks - eTOM process type	The risk management process must ensure that all risks that are insurable are identified, assessed, and appropriately mitigated.	Outages, failures and malfunctions, denial of service attacks, privacy threats (OUT, DIS, NAA5)	MNO	eTOM 20 / 1.7.2.5.1
Regulatory management							
Failure to identify and comply with updated compliance requirements	5G system with its verticals will involve significant changes in applicable compliance requirements, including but not limited to security, privacy, consumer protection. Failure to identify applicable requirements for implementation scenarios and verticals may lead to significant regulatory actions	Regulatory management	Ensure regulatory compliance - eTOM process type	Ensure that the enterprise complies with all existing government regulations.	Evolving and complex regulatory landscape, outages, failures and malfunctions, denial of service attacks, privacy threats (NAAx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.6.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Security management							
Non-proactive Security Management	Security management processes should proactively identify areas of threat and support the categorization and prioritization of threat and deal with exposure to loss of value or reputation. Failure to ensure a systematic risk analysis framework based on information collection and exchange leaves the organisation exposed in the context of implementing 5G technology in which the threats and vulnerabilities landscape is in ongoing exploration.	Security management	Manage Proactive Security Management - eTOM process type ENISA Threat Landscape	Identify internal and external sources of threat. Areas of threat can be physical or logical. Set up a sound framework for security risk analysis. Connect to information exchange sources and communities.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.1
Failure to monitor Industry Trends for Security Management	Monitoring of industry trends and best practice approaches is essential to ensure the 5G operator is on top of security challenges. Failure to do so is especially damaging in the context of 5G technology in which the threats and vulnerabilities landscape is in ongoing exploration.	Security management	Monitor Industry Trends for Security Management - eTOM process type ETSI, GSMA, 3GPP, ITU Standards ENISA Threat Landscape	Security management threat minimization through monitoring of industry trends and best practice approaches.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.2

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Inadequate / obsolete Security Management Policies & Procedures	Security Management corporate policies, guidelines, best practices, and auditing processes need to be updated to adapt to the new challenges posed by the new technologies and subsequently changed operations, services, and business models.	Security management	Define Security Management Policies & Procedures - eTOM process type ISO 27011 / ITU 1051	Define and follow corporate policies, procedures, guidelines, best practices. Audit processes are needed to provide assurance that the necessary control structures are in place and provide assurance that the procedures are followed and are effective.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.3
Failure to involve security management functions in Deployment of adequate security controls	Security management functions should assist operational areas in deploying appropriate infrastructure, procedures, and monitoring capabilities. Security management functions should be involved in all phases of the system lifecycle. Failure will be translated in poorly deployed or inadequate security controls	Security management	Assist with Security Management Deployment - eTOM process type	Deploy appropriate physical infrastructure, procedures, and monitoring capabilities to support relevant operational areas. Security Management processes are implemented at many levels of the enterprise.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.4

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper data collection capabilities	Improper definition and deployment of updated processes and tools to capture relevant operational and security date may generate significant blind spots that may impede security management and fraud prevention activities.	Security management	Manage Reactive Security Management - eTOM process type	Implementation of tools and capabilities for data collection on operational activity. Incorporate in the operational infrastructure the procedures and facilities for security monitoring, control, and management in the areas of the SIP process and Operations. Integration of these processes with relevant fraud management processes.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.5
Improper detection capabilities of Potential Security Threats & Violations	Failure to adapt analysis and correlation algorithms and procedures to the new technologies and changed threat landscape may leave the operator unable to detect potential threats, security violations, fraud, or other security-relevant events.	Security management	Detect Potential Security Threats & Violations - eTOM process type	Up to date data analysis and correlation tools and rulesets to detect potential threats, security violations, fraud, or other security-relevant events.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.6

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Investigate Potential Security Threats & Violations	Forensic procedures must be adapted to new technologies. Failure to do so may impede investigations and fitness of forensic evidence.	Security management	Investigate Potential Security Threats & Violations - eTOM process type	Update tools, processes, and rulesets for forensic investigations to provide capabilities adequate to the new technologies.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.7
Improper security risk treatment	Improper process to select, design and specify a baseline set of security controls may leave the system unprotected by ignoring relevant areas or failing to identify adequate sizing and prioritisation of preventive measures.	Security management	Define Security Management Prevention - eTOM process type ISO/IEC 27011 / ITU X.1051 EU 5G Toolbox Implementation Plan	Implementation of risk management plans that take into account in addition to technical options and the value of assets to be protected, as well as the probability of threats. The technical specifications of security controls, operational procedures such as vulnerability management, risk assessment and secure configuration procedures must be considered. Catalogues of best practices such as EU 5G Toolbox Implementation Plan and ISO 27011/ITU x.1051 provide frameworks to check for completeness and consistency of prevention measures.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.8

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper Monitoring of Security	Failure to define updated policy-based tools and processes for collection, filtering, aggregation, distribution, and retention of relevant data may lead to several alternative risk scenarios: monitoring blind spots, excessive resource consumption, data overload, inability to process data for relevant decisions.	Security management	Define Monitoring to Facilitate Security Management - eTOM process type	Development of security monitoring procedures as part of prevention process, which define rules for collecting and storing relevant data that come from or are associated with a certain set of managed resources and services. Tools and mechanisms for collection, filtering, aggregation, distribution, and retention of relevant data will be implemented.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.9
Improper Security Management Analysis	Failure to adapt tools and procedures for assessment of collected/correlated data for events or trends of interest may lead to inability to form complete and accurate picture of events and conditions and in turn to failure to adapt preventive measures to changed threat and vulnerability environment.	Security management	Define Security Management Analysis - eTOM process type	Update and maintain sound processes and tools for collecting, assessing, and correlating relevant data into statistical models to detect patterns and trends, in line with industry best practices and newly implemented technologies.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.10

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Improper Security policies & procedures to facilitate detection of incidents	Failure to adapt policies and procedures for anomaly detection may lead to operator unable to define automated policy-based remediation controls. Increased complexity of systems and operations may render current correlation & analysis tools unable to generate meaningful and accurate predictions and alerts.	Security management	Define Security Management policies & procedures to facilitate detection incidents - eTOM process type	Update and maintain sound implement policies and procedures for incident detection, in line with industry best practices and newly implemented technologies.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.11
Improper Incident Management policies and procedures	Incident management processes need to be adapted to take into account changed technologies and processes and updated incident response ecosystem and responsibilities.	Security management	Define Incident Management policies and procedures - eTOM process type ISO 27011 / ITU X.1051	Implement ITSM-based or ISO 27011 incident management policies and procedures to identify and undertake necessary response and recovery actions that may be conducted by Business Continuity Management processes or within Operations or Assurance.	Evolving threat landscape, network complexity, resource scarcity, lack of competences, advanced threats, fraud, abuse (NAAx, EIH4, PAx, UDx, FMx, OUT, DIS, LEG)	MNO	eTOM 20 / 1.7.2.2.12

L ANNEX: DETAILED VULNERABILITIES IN VENDOR PROCESSES

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stake-holder	Source Ref
Design							
Failure to apply security architectural and security design principles throughout the development lifecycle.	Security-by-design ensures vulnerabilities can be mitigated by a secure design of the Network Product. Failure to apply security architectural and security design principles and follow them throughout the entire development lifecycle leads to structural security problems that imperil the security of the components and of the 5G system	Vendor Development Processes, 5G System Components	Security by design	The Network Product shall implement security by design throughout the whole development and product lifecycles. Therefore, architecture and design decisions shall be made based on a set of security principles that are tracked throughout the development and product lifecycles. Security principles must be considered and applied when appropriate. In the design phases, a threat analysis process for the Network Product shall be undertaken to identify the potential threats and related mitigation measure	Design Flaws, Exploitation of vulnerabilities. (NAAx, UDx)	Vendor, Auditor	GSMA FS.16 /7.2.1.
Coding							
Lack of or improper code review	Failure to apply consistent code review in line with specification and security best practices elevates the risk of risk of accidental occurrence of vulnerabilities.	Vendor Development Processes, 5G System Components	Source code review process; application of coding best practices; use of static and dynamic code review tools; external code review process	The Equipment Vendor shall ensure that new and changed source code dedicated for a Network Product is appropriately reviewed in accordance with an appropriate coding standard. If feasible, the review should also be implemented by means of using a Source Code Analysis Tool and automation where appropriate	Insecure Code (Source code dedicated for use in the Network Product leads to a vulnerability) (NAAx, UDx)	Vendor, Auditor	GSMA FS.16 /7.3.1.

Ineffective code governance	In absence of effective mechanisms for code governance source code changes are not controlled, and it is impossible to trace reasons and requirements for code changes	Vendor Development Processes, 5G System Components	Robust change management processes; independent lines of control for any changes	The Equipment Vendor shall ensure that no changes are introduced into the Network Product without appropriate governance	Rogue developer (secretly introduces a vulnerability into source code dedicated for use in the Network Product) (NAAx, UDx)	Vendor, Auditor	GSMA FS.16 /7.3.1.
Compilation							
Vulnerabilities in Build process and environment	Compilation and build processes and environment must protected from tampering, to ensure that builds are reproducible, deterministic and cover the security procedures defined by the Equipment Vendor. Manipulated build tools or parameters may introduce vulnerabilities to the Network Product through the compilation environment.	Vendor Development Processes, 5G System Components	Automated Build Process; Build Environment Control	The Equipment vendor shall apply an automated build tool with a minimum of manual intervention to compile the source code and store the build log. All the data (including source code, building scripts, compilation tools, and compilation environment) of the compilation build environment shall come directly from a version control system.	Malicious attacker, Tampering with build tools (NAAx, UDx)	Vendor, Auditor	GSMA FS.16 /7.4.1, 7.4.2
Testing							
Lack of or improper security testing	Failure to ensure proper testing leaves the network products exposed to vulnerabilities and unexpected and unspecified behaviour.	Vendor Development Processes, 5G System Components	Security testing	Security testing should include the validation of security functionality, both positive and negative testing, as well as vulnerability testing of the Network Product. Network Products are to be tested from a security perspective within a fair representation of the operational environment. Vulnerability testing shall test for the robustness of the Network Product against undefined/unexpected input.	Rogue developer, Poor Design, Erroneous / Insecure Code (NAAx, UDx)	Vendor, Auditor	GSMA FS.16 /7.5.1.
Release							
Improper verification of software integrity	Software integrity verification methods are not implemented or not effective. In their absence, maliciously or unintentionally tampered software loads may be accidentally installed.	Vendor Development Processes, 5G System Components	Software Integrity Protection	The Equipment Vendor shall establish and maintain methods to ensure that the delivery of Network Products is carried out under controlled conditions. The mobile network operator shall be provided with appropriate means to identify whether a received software package is genuine	Intentional or unintentional use of non-genuine release (NAAx, UDx)	Vendor, Auditor	GSMA FS.16 /7.6.1.

Ambiguous software release identifiers	Failure to ensure that software versions are uniquely identified may lead to old versions of software being accidentally installed and old vulnerabilities being re-introduced in networks.	Vendor Development Processes, 5G System Components	Strict release mechanisms including allocation of unique identifiers to software versions	All released software package versions shall bear a unique identifier that maps to a specific build version	Intentional or unintentional use of outdated, vulnerable release (NAAx, UDx)	Vendor, Auditor	GSMA FS.16 /7.6.2.
Inaccurate / obsolete documentation	Failure to ensure that product documentation is updated in all security relevant aspects and properly reflects the current functionality. This may in turn impair operation, protection and maintenance of network products.	Vendor Development Processes, 5G System Components	Change management processes. Strict release mechanisms. Documentation management.	Customer documentation shall be up to date in all security related aspects and reflect the current functionality of the Network Product at the time when both the Network Product, or software upgrades of it, and the customer documentation are shipped to the customer. The documentation delivered with the Network Products contains all up-to-date information necessary to securely configure and run the Network Product.	Intentional or unintentional impairing of system operation or security (NAAx, UDx, FMx)	Vendor, Auditor	GSMA FS.16 /7.6.3., 7.6.4.
Operation							
Failure to provide a security contact	For all security inquiries the customer should know who to approach in the Equipment Vendor organisation. In absence of a clear communication from the Equipment Vendor to let clients know who to contact for any security inquiries or incidents, incident response and resolution are impaired.	Vendor Development Processes, 5G System Components	Security Point of Contact	The Equipment Vendor shall provide a point of contact for security questions/issues and communicate this point of contact to its customers and 3rdparty vulnerability disclosers. This point of contact shall be able to find the right person/department inside the Equipment Vendor organisation to deal with security concerns raised by a customer/3rd party vulnerability discloser	Security incidents (NAAx, UDx, FMx)	Vendor, Auditor	GSMA FS.16 /7.7.1.
Insufficient vulnerability awareness	Failure to collect and process updated information with regard to vulnerabilities in 3rd party components may lead to situations in which vulnerabilities go undetected although they may be publicly known and are therefore not mitigated.	Vendor Development Processes, 5G System Components	Threat and vulnerability intelligence	The Equipment Vendor shall have reliable processes in place to ensure it can become aware of newly revealed potential vulnerabilities in used 3rd party components and to evaluate whether they result in vulnerabilities in the Network Product	Exploitation of unfixed vulnerabilities (NAAx, UDx)	Vendor, Auditor	GSMA FS.16 /7.7.2.
Ineffective vulnerability remedy process	In absence of a reliable process to deal with vulnerabilities found in, or in relation to, released Network Products it cannot be ensured that known vulnerabilities are addressed appropriately and timely. Failure to deploy security patches independently	Vendor Development Processes, 5G System Components	Vulnerability Remedy Process and mechanisms	The Equipment Vendor shall establish a process to deal with vulnerabilities found in, or in relation to, released Network Products. Vulnerabilities shall be dealt with appropriately and, if applicable, patches/software upgrades shall be distributed to all affected mobile network	Exploitation of unfixed vulnerabilities (NAAx, UDx)	Vendor, Auditor	GSMA FS.16 /7.7.3, 7.7.4

	from regular functional updates increases the time window of exposure.			operators, in order to honour existing maintenance contracts within an agreed schedule. Equipment Vendor shall have the facility to provide patches/software upgrades that close security vulnerabilities independently from unrelated patches/software upgrades that modify functionality of the Network Product			
Unreliable communication of software fixes	Absence of reliable processes and mechanisms to inform network operators that security fixes are available, unnecessarily extends the window of vulnerability within their networks.	Vendor Development Processes, 5G System Components	Vulnerability Remedy Process and mechanisms	A reliable process shall ensure that information regarding available security related fixes is communicated to mobile network operators that have maintenance agreements in place at the time the fix is released	Exploitation of unfixed vulnerabilities (NAAx, UDx)	Vendor, Auditor	GSMA FS.16 /7.7.5.
Entire lifecycle							
Improper version control system	The version control system should cover all relevant components of the network product, and it should ensure accountability, authorisation and integrity of all changes. Otherwise, the changes in components cannot be controlled, and vulnerabilities may find their way in to the finished product, unintentionally or on purpose.	Vendor Development Processes, 5G System Components	Version control system	During the entire lifetime of a Network Product, the Equipment Vendor shall utilise a version control system on hardware, source code, build tools and environment, binary software, 3rd party components, and customer documentation ensuring accountability, authorisation and integrity of all changes	Rogue developer (NAAx)	Vendor, Auditor	GSMA FS.16 /7.8.1.
Improper change management process	Properly controlled change management is essential to ensure that changes are appropriate, effective, properly authorised and carried out in such a manner as to minimise the opportunity for either malicious or accidental compromise. Failure to do so may lead to uncontrolled	Vendor Development Processes, 5G System Components	Change tracking	The Equipment Vendor shall establish a comprehensive, documented and cross Network Product line procedure to ensure that all requirements and design changes, which may arise at any time during the development and product lifecycles and which impact the Network Product(s), are managed and tracked in a systematic and timely manner appropriate to the life cycle stage of all affected product components in all Network Products.	Rogue developer (NAAx)	Vendor, Auditor	GSMA FS.16 /7.8.2. ISO/IEC 27001 /A.12.1.2.
Insufficient security education and awareness of staff	Staff involved in design, engineering, development, implementation, and maintenance is insufficiently aware of IT/network security matters.	Vendor Development Processes, 5G System Components	Staff education	Continuous education of all staff involved in Network Product design, engineering, development, implementation, testing and maintenance shall be provided to ensure knowledge and awareness on security matters, relevant to their roles are up-to-date	Insecure Code (NAAx, UDx)	Vendor, Auditor	GSMA FS.16 /7.8.3. ISO/IEC 27001 /A.7.2.2

Ineffective Information Security Management System	In the absence of an effective ISMS, reliable identification and mitigation of risks and achievement of relevant security objectives cannot be demonstrated.	Vendor Development Processes, 5G System Components	Information Security Management Continual Improvement Process	In the entire lifecycle, the Equipment Vendor shall employ an information classification and handling scheme to avoid sensitive information, such as security flaws, signing keys, etc., being leaked The Equipment vendor must have a continual improvement process for its development and product lifecycle and this process must include a root cause analysis of the security flaws. The resulting improvements shall be incorporated into the relevant design or processes.	Information Leakage (NAA4)	Vendor, Auditor	GSMA FS.16 /7.8.3 ISO/IEC 27001 /4-10

M ANNEX: DETAILED VULNERABILITIES IN SECURITY ASSURANCE PROCESSES

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Standardisation Processes							
Obsolescence of standards	As 5G technology is rapidly advancing and new security risks and requirements are identified, standards need to be updated constantly. Slow response of standardisation activities to technological advances and security research may leave the systems exposed.	Assurance processes, 5GS components	Standardisation Harmonisation	{NA}	{NA}	ENISA, Standardisation Bodies, Industry Associations	CSA Regulation
Alignment of standards	As several organisation are working on standardisation in the 5G sector, alignment of standards is paramount to ensure consistency and usability of developed references	Assurance processes, 5GS components	Standardisation Harmonisation	{NA}	{NA}	ENISA, Standardisation Bodies, Industry Associations	CSA Regulation
Missing security requirements reference for verticals	While security assurance specifications exist for the building blocks of the 5G system, no security assurance criteria and processes are defined for 5G verticals. This may leave relevant security considerations not covered or reference security requirements unfit for specific use cases.	Assurance processes, Communication services	Standardisation Harmonisation	{NA}	{NA}	ENISA, Standardisation Bodies, Industry Associations	CSA Regulation

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Accreditation Processes							
Recognition of accreditation scheme	While GSMA accreditation body and the accreditation scheme are internationally agreed by all technology providers, no mechanisms such as peer review are in place to ensure recognition of the accreditation scheme by all relevant stakeholders.	Assurance processes	EU 5G CSA Scheme	[Scheme to be developed given pending decision from Member States (NIS CG, ECCG)]	Lack of EU-wide security certification	ENISA, European Commission, ECCG	CSA Regulation
No alignment with internationally recognized standards for accreditation and conformity assessment	Accreditation and conformity assessment processes should be aligned with the internationally recognized conformity assessment standards - the ISO 17xxx series. Failure to do so may cast doubt on the soundness of conformity assessment processes.	Assurance processes	EU 5G CSA Scheme	[Scheme to be developed given pending decision from Member States (NIS CG, ECCG)]	Lack of EU-wide security certification	ENISA, European Commission, ECCG	CSA Regulation
Lack of control by regulatory and supervisory bodies	While the existing assurance scheme - NESAS/SCAS- is accepted by manufacturers and operators, it defines no oversight mechanisms from regulatory and supervisory bodies.	Assurance processes	EU 5G CSA Scheme	[Scheme to be developed given pending decision from Member States (NIS CG, ECCG)]	Lack of EU-wide security certification	ENISA, European Commission, ECCG	CSA Regulation
Conformity Assessment Processes							
No security evaluation of the operational environment	While SECAM / SCAS scheme provides that accredited security test laboratories (vendors or third party) evaluate network product according to SCAS. Conformity and security evaluation is performed on individual network products in a vendor-documented configuration for SECAM testing, without due consideration on the environment for specific deployments.	Assurance processes, 5G components	EU 5G CSA Scheme	[Scheme to be developed given pending decision from Member States (NIS CG, ECCG)]	Lack of EU-wide security certification	ENISA, European Commission, ECCG	CSA Regulation

Name of Vulnerability	Description	Associated Assets Category	Security Controls	Security Requirements /Description of security controls	Threats (Threat Taxonomy)	Stakeholder	Source Ref
Insufficient assurance of environmental assumptions	The logic of the SECAM/SCAS scheme is that environmental assumptions taken into consideration at product testing time are upheld and tested at deployment by the Operator. This validation of environmental assumptions can only be performed during deployment and is needed for security, but at present no framework exists to provide sufficient assurance for a third-party certification	Assurance processes, 5G components	EU 5G CSA Scheme	[Scheme to be developed given pending decision from Member States (NIS CG, ECCG)]	Lack of EU-wide security certification	ENISA, European Commission, ECCG	CSA Regulation
Certification overhead and relevance	Certification must not be a barrier to entry or to innovation. Any certification scheme needs to add value and go beyond a box ticking exercise	Assurance processes	EU 5G CSA Scheme	[Scheme to be developed given pending decision from Member States (NIS CG, ECCG)]	Lack of EU-wide security certification	ENISA, European Commission, ECCG	CSA Regulation
No assessment scheme for evaluation of virtualized products	No agreed assessment/certification scheme for virtualised products.	Assurance processes, Virtualised Network Products	EU 5G CSA Scheme	[Scheme to be developed given pending decision from Member States (NIS CG, ECCG)]	Lack of EU-wide security certification	ENISA, European Commission, ECCG	CSA Regulation
Insufficient security assurance level	Once the operator received the evaluation report, the operator then decides if the results are sufficient according to its internal policies and whether to accept the security assurance level of the network product or not. The operator's acceptance decision may depend on external forces such as regulatory requirements.	Assurance processes, Legal Requirements	EU 5G CSA Scheme	[Scheme to be developed given pending decision from Member States (NIS CG, ECCG)]	Lack of EU-wide security certification	ENISA, European Commission, ECCG	CSA Regulation
Re-use of evidence created by conformity assessment bodies	In the absence of a recognized assessment scheme of conformity assessment bodies, re-use of evidence produced by auditors and laboratories to support certification processes or regulatory compliance statements is limited.	Assurance processes, Legal Requirements	EU 5G CSA Scheme	[Scheme to be developed given pending decision from Member States (NIS CG, ECCG)]	Lack of EU-wide security certification	ENISA, European Commission, ECCG	CSA Regulation

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-445-9
DOI: 10.2824/802229