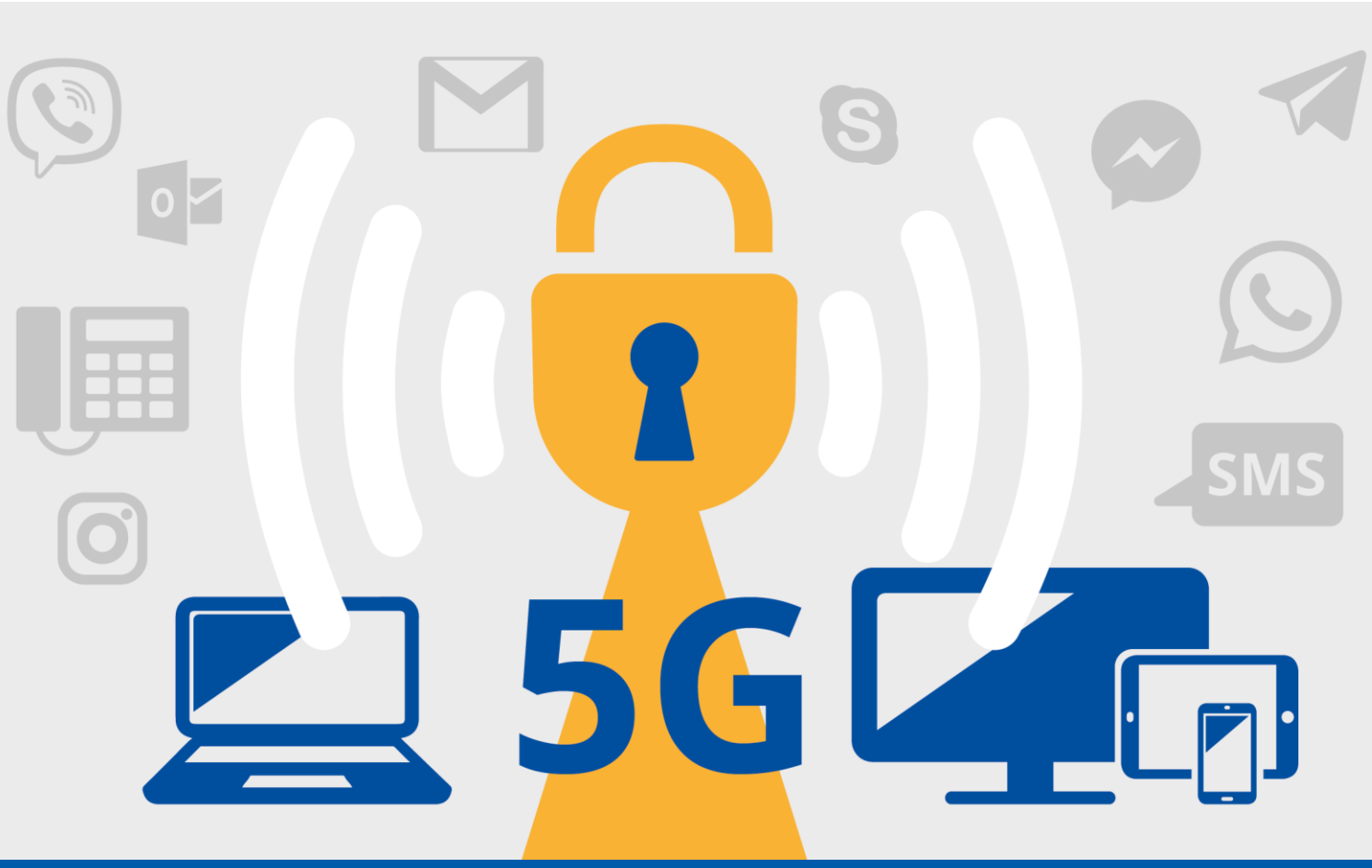
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



SECURITY IN 5G SPECIFICATIONS

Controls in 3GPP Security Specifications (5G SA)

FEBRUARY 2021

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 here: www.enisa.europa.eu.

CONTACTS

For technical queries about this paper, please email resilience@enisa.europa.eu
For media enquires about this paper, please email press@enisa.europa.eu

AUTHORS

Goran Milenkovic, Dr. Marnix Dekker – European Union Agency for Cybersecurity (ENISA)

ACKNOWLEDGEMENTS

We are grateful for the review and valuable input received from the experts from national authorities in the NIS Cooperation group, and particularly those experts contributing to NIS CG Work Stream on 5G cybersecurity and those involved in the sub-group on standardisation and certification. We are in particular thankful to colleagues from Swedish PTS, Austrian RTR and French ANSSI for further help and cooperation during the validation phase and for their useful suggestions and comments. In addition, we would also like to thank members of the ENISA ad-hoc 5G Expert Group, Pascal Bisson and Jean-Philippe Wary, as well as the member of the ENISA Advisory Group, Dr. Silke Holtmanns, all acting on an ad personam basis, for their support in the expert review of technical elements of the report and for useful suggestions and remarks.

In the preparation of the material for the report we have conducted an analysis of publically available information on security in 5G specifications in collaboration with Plum Consulting, under the tender ENISA S-COD-20-T14.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-472-5, DOI: 10.2824/30076

TABLE OF CONTENTS

LIST OF ACRONYMS

Acronym	Meaning
5GC	5G Core Network
5G-RAN	5G Radio Access Network
5G SA	5G Standalone
5G NSA	5G Non-Standalone
ABBA	Anti-Bidding down Between Architectures
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
AMF	Authentication Management Field
AI	Artificial Intelligence
API	Application Programming Interface
AUSF	Authentication Server Function
CAPIF	Common API Framework
CI/CD	Continuous integration (CI) and continuous delivery (CD)
CTR	Counter (mode)
DDoS	Distributed Denial of Service (attack)
EAP	Extensible Authentication Protocol
EAP-AKA	Extensible Authentication Protocol - Authentication and Key Agreement
eNB	Evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
gNB	NR Node B
GPS	Global Positioning by Satellite
GSMA	Global System for Mobile Communications Association
GTP	GPRS Tunnelling Protocol
GUTI	Globally Unique Temporary UE Identity
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
JSON	JavaScript Object Notation
LI	Lawful Intercept
MEC	Multi-access Edge Computing
ML	Machine Learning

MME	Mobility Management Entity
MTD	Moving Target Defence
NAI	Network Access Identifier
NAS	Non Access Stratum
NDS	Network Domain Security
NEA	New radio Encryption Algorithm
NEF	Network Exposure Function
NFV	Network Function Virtualisation
NGMN	Next Generation Mobile Networks (Alliance)
ng-eNB	Next Generation Evolved Node-B
NIA	New radio Integrity Algorithm
NR	New Radio
NRF	Network Repository Function
NSI	Network Slice Instance
NSSAAF	Network Slice Specific Authentication and Authorisation
N3IWF	Non-3GPP access InterWorking Function
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
PEI	Permanent Equipment Identifier
PKI	Public key infrastructure
PLMN	Public Land Mobile Networks
RFC	Request for Comments
RRC	Radio Resource Control
SBA	Service Based Architecture
SCT	Security Competence Team
SDN	Software Defined Networking
SDR	Software Defined Radio
SDSec	Software Defined Security
SEAF	SEcurity Anchor Function
SECOP	Service Communication Proxy
SEPP	Security Edge Protection Proxy
SIDF	Subscription Identifier De-concealing Function
SME	Subject Matter Expert
SMF	Session Management Function
SMS	Short message service
SRB	Signalling Radio Bearer
SRVCC	Single Radio Voice Call Continuity
S-TMSI	Serving Temporary Mobile Subscriber Identity
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier

TLS	Transport Layer Security
TEE	Trusted Execution Environment
TSC	Time Sensitive Communication
UE	User Equipment
UEA	Universal Mobile Telecommunications System Encryption Algorithm
UDM	Unified Data Management
UICC	Universal Integrated Circuit Card
URLLC	Ultra-Reliable Low-Latency Communication
UP	User Plane
UPF	User Plane Function
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VPLMN	Visited Public Land Mobile Network
VPN	Virtual Private Network
ZSM	Zero-touch Network Secure Management
ZUC	Zu Chongzhi 祖冲之 (Algorithm)

1. INTRODUCTION

The 3rd Generation Partnership Project, or 3GPP, is the main body developing technical specifications for 5G networks, including security specifications. These specifications bring a number of security enhancements in comparison to previous generations of mobile networks. At the same time, however, some of these security controls are defined as optional or there is a degree of flexibility left to suppliers on how to implement and for operators on how to interpret and utilise the controls. Having a good understanding of these security controls is important for vendors, system integrators and operators in order to build, deploy and manage resilient 5G networks, but it is equally important for cybersecurity and national regulatory authorities in charge of cybersecurity policy development and implementation.

In addition to 3GPP, other standardization bodies and industry groups have been working on developing related technical specifications and standards. Some of these standards, such as those related to authentication and encryption, form the basic building blocks of the mechanisms incorporated in 3GPP security specifications. Others have been developing specifications in specialised domains and for specific technologies that 5G will heavily rely upon, such as virtualization. Work in these institutions is supported by industry organisations, such as GSMA, and in collaboration with academia, for example through 5G PPP research projects.

1.1 BACKGROUND AND POLICY CONTEXT

Following on the European Commission's Recommendation on the cybersecurity of 5G networks[1] (hereafter 'The Recommendation') published on 26 March, 2019, and based on the individual national risk assessments, the Commission and the Member States, with the support of ENISA, developed a single EU Coordinated Risk Assessment on Cybersecurity in 5G Networks[2] (hereafter 'Coordinated risk assessment'). This coordinated risk assessment identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities and the main risks. Subsequently, on 29 January 2020, the NIS Cooperation Group published the EU toolbox of risk mitigating measures[3] (hereafter 'the Toolbox') addressing the risks identified in the coordinated risk assessment.

The Toolbox identifies two groups of measures MS can take: *strategic* and *technical measures*. In addition, it identifies a number of *supporting actions* that can assist, enable or support the implementation of strategic and technical measures.

In December 2018, the EU adopted a new set of telecom rules, the European Electronic Communications Code (EECC)[4]. An important part of the EECC is consumer protection and security of electronic communications. Article 40 of the EECC contains specific security requirements for electronic communication providers. The EECC replaces the 2009 Framework directive (Directive 2009/140/EC). ENISA has been supporting EU Member States for over a decade with supervision of security measures in telecom sector, among others, by maintaining ENISA Technical Guideline on Security Measures (hereafter 'the Guideline')[5].

[1] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154, accessed October 2020
[2] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security, accessed October 2020
[3] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures, accessed October 2020
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN, accessed October 2020
[5] The new, updated technical guideline, version 3.0, that will substitute the existing guideline, version 2.0, available at the following URL: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures, accessed October 2020

1.2 DOCUMENT PURPOSE AND OBJECTIVES

One of the technical measures, TM02, calls relevant authorities in EU Member States to ensure and evaluate the implementation of security measures in existing 5G standards (3GPP specifically) by operators and their suppliers.

For convenience, we give the full text of the TM02, directly as stated in the Toolbox:

"Ensure that MNOs and their suppliers implement the existing security measures in the relevant 5G technology standards (e.g. 3GPP) and use it as a minimum security baseline for MNOs, so as to ensure that also the optional parts of these standards, relevant for security, are adequately implemented".

To support implementation of this technical measure, the Toolbox also defines the supporting action SA04, asking for development of guidance on implementation of security measures in these standards, identifying ENISA and MS relevant authorities as relevant actors for this action.

This report is directly driven by the objectives set in the supporting action SA04 and is intended to help MS implementing the technical measure TM02.

The report is also intended to help national competent and regulatory authorities get a better picture of the standardisation environment pertaining to 5G security and to improve understanding of 3GPP security specifications and its main elements and security controls. With this, competent authorities will be in a better position to understand what the key security controls that operators have to implement are and what the role of such controls is for achieving the overall security of 5G networks.

Remark: It is important to emphasize that implementation of security controls defined in 3GPP or any other 5G related standards, does not, on its own, guarantee the overall security of 5G networks. This is partially because there are many aspects that are not covered by standards and specifications. Further reflections on this are given in Section 4 of this document. This is also in line with 5G Toolbox, where the corresponding technical measure TM02 is categorized in the sub-category of baseline network security measures and is only one of the 11 technical measures defined overall.

1.3 DOCUMENT SCOPE AND INTENDED AUDIENCE

1.3.1 In scope

This document focuses primarily on the 3GPP technical specification TS 33.501[6], which is the central security technical specification for 5G networks. Other technical specifications and technical reports, from 3GPP and from other standardisation bodies and groups, are covered on informative/reference level.

In regards of the coverage of the measures defined in the Toolbox, the scope of this document targets primarily the technical measure TM02.

1.3.2 Out of scope

Security measures for previous generations of mobile networks (3G, 4G)[7] are not discussed in great detail and the focus is on new security mechanisms for 5G, hence considering primarily the 5G stand-alone deployment option.

[6] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169
[7] It is acknowledged that legacy network elements based on previous generations of mobile and wireless communications technology such 4G or 3G are also stipulated in the Commission Recommendation on 5G and further referred to in the Coordinated risk assessment. The priority in this report, however, has been put on the aspects pertaining to the new 5G architecture networks. The issues of legacy networks, related migration paths and associated threats and vulnerabilities is discussed in ENISA 5G Threat Landscape 2020 and may further be assessed in more details from the specifications point of view in the follow-up to this report, depending on the interest of relevant stakeholders.

Activities such as a gap analysis of telecommunication standardisation are out of the scope of this document. In addition, deeper analysis of standardisation of security controls pertaining to NFV, SDN, MEC, IoT, Cloud Computing, Artificial Intelligence, Lawful Interception are currently not in the scope of this report.

In regards of the coverage of the measures defined in the Toolbox, this document does not directly address technical measures other than TM02 or any of the strategic measures SM01-SM08.

1.3.3 Intended audience

The document is intended primarily for the representatives of relevant national ministries and national cybersecurity agencies who are members of the NIS Cooperation group and who are engaged in the work stream on 5G cybersecurity and for national regulatory authorities in charge of supervision of security measures under the European Electronic Communications Code ("The Article 13 Expert Group"), but it may be useful for other stakeholders as well.

1.4 DOCUMENT STRUCTURE

The document is structured as follows:

- In **Section 2** we give a high-level overview of the specification and standardization landscape for 5G networks security and list main activities by various standardisation organisations and industrial groups in this domain.
- In **Section 3** we take a close look at the main 3GPP security technical specification for 5G networks. We look at the security architecture and we identify key security areas. For each of the identified areas we provide explanations and include the analysis of optional elements – from the point of view of coverage, security implications and possible recommendations of good security practices.
- In **Section 4** we reflect of the role of technical specifications and standards for security of 5G networks and we briefly discuss security aspects not (fully) covered in these specifications.
- In **Section 5** we provide a summary of key findings and list identified good security practices for consideration.

In addition, the document also contains an annex:

- **Annex A** contains a detailed map of the main 3GPP security technical specification 33.501 with a section-by-section guide.

2. OVERVIEW OF 5G SECURITY STANDARDISATION EFFORTS

There are many standards bodies and working groups working on the 5G specifications. In this section we give an overview of the main ones.

Figure 1: Standardisation organisations of relevance for 5G security

2.1 THE THIRD GENERATION PARTNERSHIP PROJECT (3GPP)

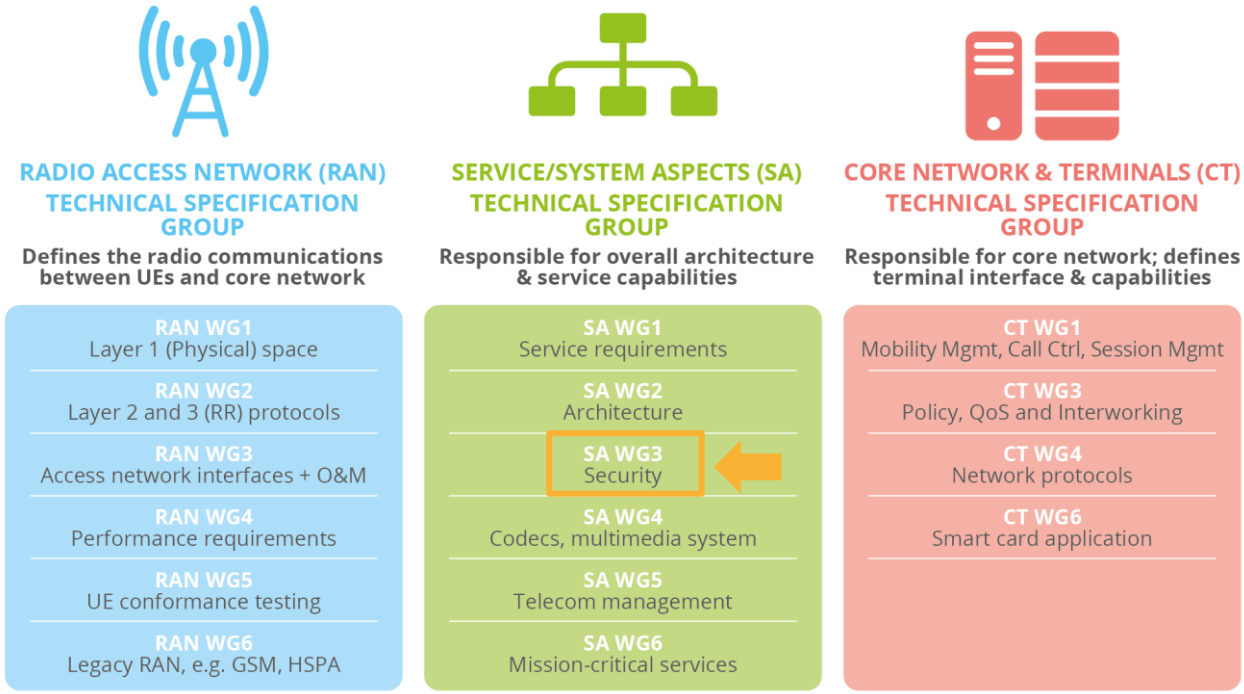
3GPP stands for 3rd Generation Partnership Project. It unites various regional standard development organizations in the domain of telecommunications in order to develop and maintain global technical specifications[8]. Areas in the scope include cellular telecommunications technologies, including radio access, core network and services, as well as for non-radio access to the core network and interworking with non-3GPP networks[9].

3GPP specifications and studies are contribution-driven, by organizational partners[10], in Working Groups and at the Technical Specification Group level.

3GPP is made up of different groups, most important of which for the technical work are working groups. Working groups meet periodically to discuss contributions to the development of technical specifications. The overall structure with all working groups depicted is given at the following diagram.

[8] https://www.ericsson.com/en/blog/2020/5/3gpp-security-standards-5g-future, accessed October 2020
[9] https://www.3gpp.org/about-3gpp, accessed October 2020
[10] The 3GPP consists of 7 organizational partners. These partners can invite market representatives to advise them.

Figure 2 - 3GPP distributed organization structure (source: Qualcomm[11])



The main active working group addressing 5G security and privacy issues is 3GPP SA3[12]. The group is responsible for identifying the security and privacy requirements and defining the security architectures and associated protocols to address these requirements. 3GPP SA3 also ensures that cryptographic algorithms which need to be part of the 5G security specifications are available.

The 3GPP SA3 work on 5G security started in 2016 and the first version of 5G security Technical Specification 3GPP TS 33.501 Version 15.1.0[13] was published in June 2018. The subsequent work on security has been undertaken over two releases (Release 15 and 16). This document is based mainly on the version 16.4.0 (September 2020). The latest work has been concentrated on developing security enhancements and features to support use cases including cellular IoT, connected vehicles, private networks and low latency applications[14][15].

3GPP has also published several other security related specifications as shown in the following figure.

[11] https://www.qualcomm.com/news/onq/2017/08/02/understanding-3gpp-starting-basics, accessed November 2020
[12] https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security, accessed October 2020
[13] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169
[14] These aspects are not covered in great details ion this document. Rather, the focus is on essential security elements of access and core network as introduced with Release 15.
[15] https://www.ericsson.com/en/blog/2020/5/3gpp-security-standards-5g-future, accessed October 2020

Figure 3: Main 3GPP security specifications

SECURITY ARCHITECTURE AND PROCEDURES

- ✓ Security architecture and procedures for 5G system (TS 33.501)

SECURITY ASSURANCE

- ✓ Catalogue of general security assurance requirements (TS 33.117)
- ✓ SCAS for the next generation Node B (gNodeB) network product class (TS 33.511)
- ✓ 5G SCAS; Access and Mobility management Function (AMF) (TS 33.512)
- ✓ 5G SCAS; User Plane Function (UPF) (TS 33.513)
- ✓ 5G SCAS for the Unified Data Management (UDM) network product class (TS 33.514)
- ✓ 5G SCAS for the Session Management Function (SMF) network product class (TS 33.515)
- ✓ 5G SCAS for the Authentication Server Function (AUSF) network product class (TS 33.516)
- ✓ 5G SCAS for the Security Edge Protection Proxy (SEPP) network product class (TS 33.517)
- ✓ 5G SCAS for the Network Repository Function (NRF) network product class (TS 33.518)
- ✓ 5G SCAS for the Network Exposure Function (NEF) network product class (TS 33.519)
- ✓ 5G SCAS; Non-3GPP InterWorking Function (N3IWF) (TS 33.520)
- ✓ 5G SCAS; Network Data Analytics Function (NWDAF) (TS 33.521)
- ✓ 5G SCAS; Service Communication Proxy (SECOP) (TS 33.522)

OTHER SECURITY SPECIFICATIONS, STUDIES AND REPORT

- ✓ Study on Lawful Interception (LI) service in 5G (TR 33.842)
- ✓ Lawful Interception requirements (TS 33.126)
- ✓ Lawful Interception (LI) architecture and functions (TS 33.127)
- ✓ Security; Protocol and procedures for Lawful Interception (LI); Stage 3 (TS 33.128)
- ✓ Study on security aspects of 5G network slicing management (TR 33.811)
- ✓ Study on security aspects of enhancement of support for edge computing in 5GC (TR 33.839)
- ✓ Study on security enhancements of 5G System (5GS) for vertical and LAN services (TR 33.819)
- ✓ Study on 5G security enhancements against False Base Stations (FBS) (TR 33.809)
- ✓ Key issues and potential solutions for integrity protection of the User Plane (UP) (TR 33.853)
- ✓ Study on authentication enhancements in the 5G System (5GS) (TR 33.846)
- ✓ SECAM and SCAS for 3GPP virtualized network products (TS 33.818)

REQUIREMENTS FOR USE-CASES

- ✓ Security aspects of MTC and other mobile data applications communications enhancements (TS 33.187)
- ✓ Proximity-based Services (ProSe); Security aspects (TS 33.303)
- ✓ Security aspects of 3GPP support for advanced V2X services (TS 33.536)

OTHERS

- ✓ Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in 5GS (TS 33.535)
- ✓ Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs (TS 33.122)

Of the publications listed here, we'll discuss the main one (TS 33.501) in great detail in section 3 and we'll come back to specifications pertaining to security assurance scheme SCAS in section 4. Other documents will be referred to where applicable.

The complete list of specifications is available at the 3GPP website[16].

2.2 THE EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI)

ETSI has several subgroups addressing various elements related to 5G system security[17].

Figure 4: ETSI working groups

2.2.1 Network Function Virtualisation Security (NFV SEC) working group

The NFV SEC working group has been advising the ETSI Industry Specification Group NFV (ETSI ISG NFV)[18] on NFV security issues. The group participants include network, computer and cloud security experts representing operators, vendors and law enforcement agencies[19]. The group has produced sixteen specifications[20] which include 'system architecture specification for execution of sensitive NFV components' (ETSI GS NFV-SEC 012) and 'security management and monitoring specification' (ETSI GS NFV-SEC 013). The main focus in the group's recent activities has been defining access token specifications for Application Programming Interface (API) access.

2.2.2 Technical Committee for Cybersecurity (TC CYBER)

ETSI TC CYBER has been developing specifications for the protection of the internet[21]. The committee published a whitepaper in 2016 providing an overview of ETSI's up-to-date work related to cybersecurity together with their future targets[22]. A more recent whitepaper (published in July 2018) addressed issues on implementation of security for quantum cryptography[23].

ETSI TC CYBER has produced a number of standards, technical reports and specifications addressing the security of infrastructures, devices, services and protocols[24]. Their recent work has been related to 'cybersecurity for consumer Internet of Things', 'global cybersecurity ecosystem' and 'techniques for assurance of digital material used in legal proceedings'.

[16] https://www.3gpp.org/DynaReport/33-series.htm, accessed October 2020
[17] https://www.etsi.org/technologies/5g, accessed October 2020
[18] https://www.etsi.org/technologies/nfv, accessed October 2020
[19] https://www.iotglobalnetwork.com/iotdir/2018/06/28/facing-the-nfv-security-challenge-12796/ , accessed October 2020
[20] https://www.etsi.org/standards-search#page=1&search=NFV-SEC&title=0&etsiNumber=1&content=0&version=1&onApproval=0&published=1&historical=0&startDate=1988-01-15&endDate=2020-06-08&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1, accessed October 2020
[21] https://www.etsi.org/technologies/cyber-security, accessed October 2020
[22] https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp18_CyberSecurity_Ed1_FINAL.pdf, accessed October 2020
[23] https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf, accessed October 2020
[24] https://www.etsi.org/standards-search#page=1&search=&title=1&etsiNumber=1&content=1&version=1&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2020-06-08&harmonized=0&keyword=&TB=824,,856&stdType=&frequency=&mandate=&collection=&sort=2, accessed October 2020

2.2.3 Technical Committee for Lawful Interception (TC LI)

ETSI TC LI has been developing standards to support the technical requirements of law enforcement. The lawful interception and retention of the communications-related data of electronic communications are key areas of their work[25]. The committee has produced numerous specifications since 2003 and their recent specifications address 'handover for messaging services over HTTP/XML', 'interface for warrant information' and 'handover interface for the request and delivery of retained data'[26].

2.2.4 Technical Committee for Intelligent Transport Systems (TC ITS)

The ETSI TC ITS Working Group 5 (WG5) has been focussing on the security aspects of Cooperative ITS (C-ITS) where the vehicles communicate with each other and/or with the transport infrastructure. The design and implementation of a security management infrastructure for C-ITS has been the key element of the security framework[27]. The group has produced a number of technical specifications and the recent work has been related to 'interoperability test specifications for security' and 'conformance test specifications for ITS PKI (public key infrastructure) management'[28].

2.2.5 Industry Specification Group on Securing Artificial Intelligence (ISG SAI)

The ETSI ISG SAI is a relatively new group (first meeting held in October 2019)[29] and aims to produce technical standards to improve the security of AI. Key areas of work include securing AI from attacks, mitigation against malicious AI and the use of AI to enhance security measures[30].

2.2.6 Security Algorithms Group of Experts (SAGE)

ETSI SAGE has been developing cryptographic algorithms and protocols specific to fraud prevention, unauthorized access to public and private telecommunications networks and user data privacy[31]. The group has developed encryption, authentication and key generation algorithms for various mobile technologies including 2G/3G/4G[32]. More recently, the group has been collaborating with 3GPP in the development of cryptographic algorithms for 5G, for example the support provided for 3GPP TR 33.841 V16.1.0 'Study on the support of 256-bit algorithms for 5G'[33].

2.3 ITU TELECOMMUNICATION STANDARDIZATION SECTOR (ITU-T)

ITU-T standardization work is undertaken by various technical Study Groups (SGs) where ITU-T member representatives develop consensus-based Recommendations (standards). ITU-T X-series Recommendations address security issues associated with OSI, information and network, cyberspace, cloud computing and data[34].

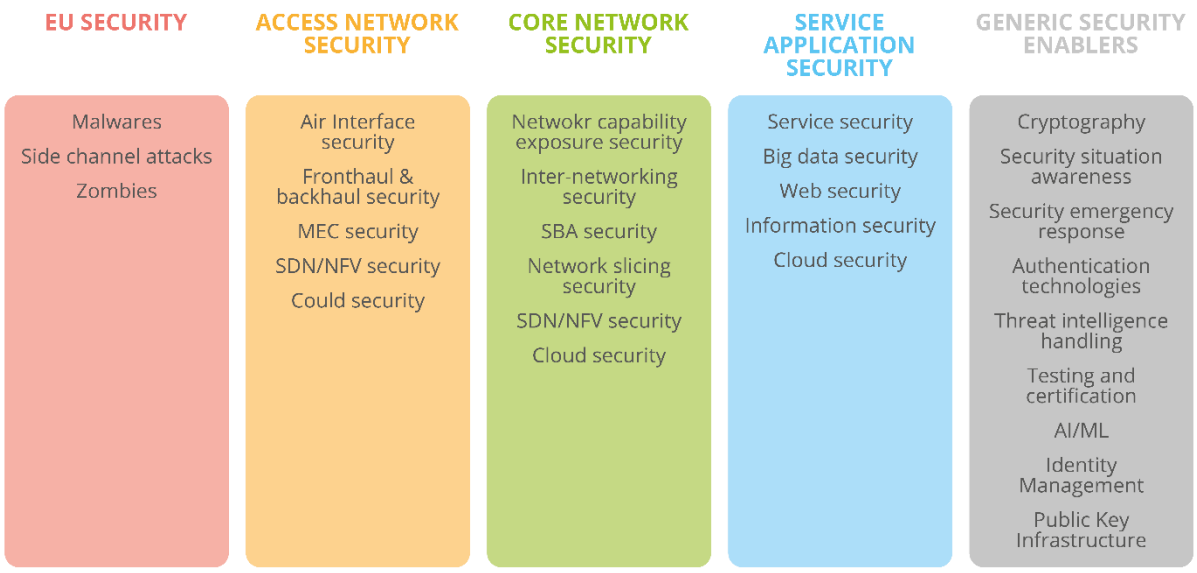
ITU-T SG 17 is responsible for addressing 5G system security[35]. The group's activities related to 5G security include development of X-series Recommendations on the following topics[36].

- Software Defined Network (SDN);
- Network Function Virtualisation (NFV);
- Internet of Things (IoT);
- Big data analytics in mobile internet services;
- Cloud computing; and
- Cryptographic profiles.

[25] https://www.etsi.org/committee/1403-li, accessed October 2020
[26] https://www.etsi.org/standards-search#page=5&search=&title=1&etsiNumber=1&content=1&version=1&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2020-06-08&harmonized=0&keyword=&TB=608&stdType=&frequency=&mandate=&collection=&sort=3, accessed August 2020
[27] https://www.etsi.org/technologies/automotive-intelligent-transport , accessed August 2020
[28] https://www.etsi.org/standards-search#page=1&search=&title=1&etsiNumber=1&content=1&version=1&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2020-06-08&harmonized=0&keyword=&TB=711&stdType=&frequency=&mandate=&collection=&sort=3, accessed August 2020
[29] https://www.etsi.org/committee-activity/activity-report-sai, accessed August 2020
[30] https://www.etsi.org/technologies/securing-artificial-intelligence, accessed August 2020
[31] https://www.etsi.org/technologies/security-algorithms, accessed August 2020
[32] https://portal.etsi.org/TB-SiteMap/Sage/Activity-Report, accessed August 2020
[33] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3422, accessed August 2020
[34] https://www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=17, accessed August 2020
[35] https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx, accessed August 2020
[36] https://docbox.etsi.org/Workshop/2018/201806_ETSISECURITYWEEK/5G/S01_INPUT_TO_5G/ACTIVITIES_ACTION_PLAN_5G-SEC_ITUT_YANG.pdf , accessed August 2020

It is also noted that the study item 'Security guidelines for applying quantum-safe algorithms in 5G systems' was established in March 2018[37]. The group's 5G end-to-end security framework is shown below.

Figure 5: ITU-T 5G end-to-end security framework[38]

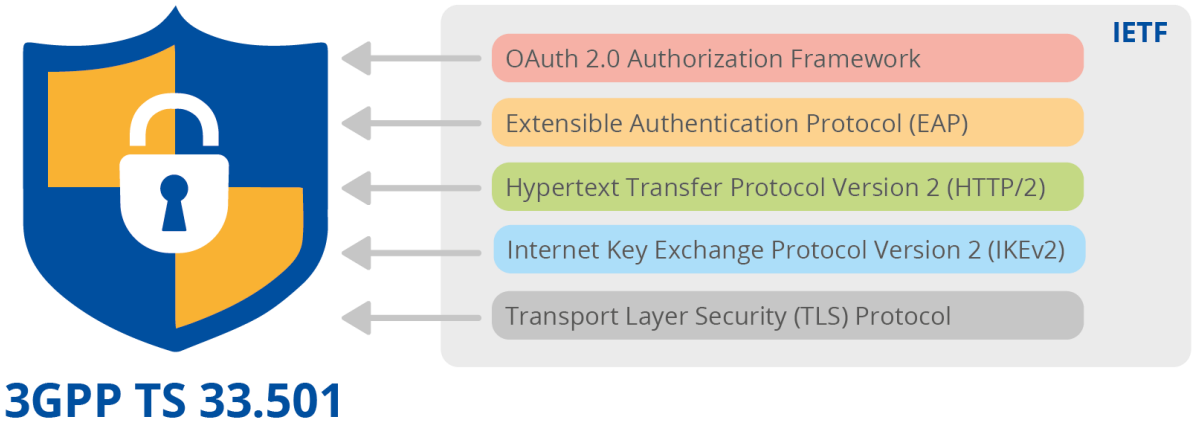


2.4 THE INTERNET ENGINEERING TASK FORCE (IETF)

The Internet Engineering Task Force (IETF) is an internet standards body and addresses technical areas covering protocols and architectures designed to support delay-sensitive and delay-tolerant applications, IP layer, network management, routing, end-to-end data transport in the internet and security[39].

The IETF has been cooperating with 3GPP in the development of 5G security specifications[40]. A number of IETF defined security mechanisms are incorporated into 3GPP TS 33.501 as shown below.

Figure 6: IETF security mechanisms incorporated into 3GPP TS 33.501



[37] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201807/Documents/Heung_Youl_Youm_Remote.pdf , accessed August 2020
[38] Source: 5G Security in ITU-T SG17, Presentation by Xiaoya Yang, ETSI Security Week, June 2018, accessed October 2020
[39] https://ietf.org/topics/areas/, accessed October 2020
[40] https://www.3gpp.org/news-events/1869-ietf_cooper, accessed October 2020

2.5 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE) is a professional association for electronic engineering and electrical engineering. IEEE describes itself as a "leading developer of industry standards in a broad range of technologies that drive the functionality, capabilities, and interoperability of products and services, transforming how people live, work, and communicate."[41] The unit within IEEE that develop standards is the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA).

In the context of 5G networks, the most relevant standards developed by IEEE are those in the 802.11 series on Wireless LAN[42], being one of the key non-3GPP protocol for 5G networks access.

2.6 OTHER STAKEHOLDERS

One of the most relevant stakeholders in the domain of mobile communications is the GSM Association, or the **GSMA**. This is an industry association that, according to the own description,

"*represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors.*"[43]

GSMA has a security team supporting its member's ability to protect mobile systems[44]. The team works collaboratively with the GSMA Fraud and Security Group (FASG) which is the GSMA's main group addressing fraud and security matters related to 5G[45]. Other GSMA groups supporting security aspects of 5G networks include[46]

- The Future Network Programme[47] which supports the industry with 5G implementation guidance.
- The GSMA Coordinated Vulnerability Disclosure (CVD) programme[48] which manages disclosures into the 5G standards by cooperating with 3GPP.
- The GSMA IoT Security Project[49] which develops resources specifically targeted at addressing IoT security risks.
- The Networks Group (NG)[50] which defines network architecture guidance and functionality.

The recent publications of GSMA on security matters include the following[51]

- *Mobile Telecommunications Security Threat Landscape* report (Jan 2020)[52] – gives insights into the threat landscape of the mobile telecommunications ecosystem, details key dimensions of consideration, and offers guidance to mitigate and tackle such threats.
- *Baseline Security Controls* report FS.31 (Feb 2020)[53] – outlines a specific set of security controls that the mobile telecommunications industry should consider deploying.

GSMA has also been active in the domain of the eSIM/eUICC specification, including the work on the eUICC security assurance scheme[54].

[41] https://www.ieee.org/standards/index.html, accessed December 2020
[42] https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/5G.pdf, accessed December 2020
[43] https://www.gsma.com/aboutus/, accessed December 2020
[44] https://www.gsma.com/security/, accessed August 2020
[45] https://www.gsma.com/aboutus/workinggroups/fraud-security-group, accessed August 2020
[46] https://www.gsma.com/security/securing-the-5g-era/, accessed August 2020
[47] https://www.gsma.com/futurenetworks/, accessed August 2020
[48] https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/, accessed August 2020
[49] https://www.gsma.com/iot/iot-security/, accessed August 2020
[50] https://www.gsma.com/aboutus/workinggroups/networks-group , accessed August 2020
[51] https://www.gsma.com/security/publications/, accessed August 2020
[52] https://www.gsma.com/security/wp-content/uploads/2020/02/2020-SECURITY-THREAT-LANDSCAPE-REPORT-FINAL.pdf
[53] https://www.gsma.com/security/wp-content/uploads/2020/02/FS.31-v2.0.pdf, accessed August 2020
[54] https://www.gsma.com/esim/esim-specification/, accessed November 2020

- *NESAS Development and Lifecycle Assessment Methodology*[55] - defines audit and assessment process for vendor development and product lifecycle process under the GSMA Network Equipment Security Assurance Scheme (NESAS)[56]
- *NESAS Development and Lifecycle Security Requirements*[57] - defines security requirements for vendor development and product lifecycle process under the GSMA Network Equipment Security Assurance Scheme (NESAS)[58]

It is worth mentioning that the GSMA as a closed group in which not all technical documents are publically available to non-members and where national authorities may not have the ability to have an influence to the work of the group.

A number of other groups and forums have been or are currently active, mainly in the realm of pre-standardization consensus building. This includes, for example, the Next Generation Mobile Networks (**NGMN**) Alliance, which is an industry organisation of telecom operators, vendors and research institutes with the aim to ensure that the standards for next generation network infrastructure, service platforms and devices meet the requirements of operators[59]. NGMN Security Competence Team (SCT) is responsible for 5G security issues[60]. The NGMN SCT's activities cover 5G end-to-end architecture framework; security and privacy aspects of cellular V2X; securing network capabilities exposure to 3rd parties; security of new interfaces associated with 5G RAN functional decomposition; and trial and testing of security functions[61].

Another initiative worth mentioning is the **5G PPP[62],** as a joint initiative involving the European Commission and stakeholders from the ICT industry (manufacturers, operators, service providers, SMEs and research organisations). A number of research projects in the domain of 5G security have been undertaken under this initiative, such as *5G ENSURE*[63] (a two-year study investigating 5G security topics including authentication, authorisation and accounting; privacy; trust; security monitoring; and network management and virtualisation), *CHARISMA*[64] (a 30-months study which proposed a hierarchical routing and para-virtualised architecture using two concepts: devolved offload with shortest path nearest to end-users and an end-to-end security service chain via virtualized open access physical layer security). Contributions from these two projects together with a number of other Phase 1 projects have also resulted in a whitepaper describing the 5G PPP security landscape[65].

Work engaged on 5G Security through Phase 1 projects led to the creation of 5G IA Security WG co-chaired by Thales and Orange and encompassing all 5G Projects addressing security topics. This work was continued through Phase 2 project active on the field, namely NRG-5[66] (Enabling Smart Energy as a Service via 5G Mobile Network advances the project has been active for what concerns security on NRG-5 architecture, as well as 5G slicing security and on authentication and authorization mechanism via blockchain) and the work is now further pursued through Phase 3 projects among which INSPIRE-5G plus[67] [68] (a three year project investigating Smart, Trustworthy and Liability-aware 5G security platform for future connected systems while promoting adoption of a set of emerging trends and technologies, such as zero-touch network and service management (ETSI ZSM),[69] SDSec models, AI/ML techniques, MTD and TEE).

[55] https://www.gsma.com/security/resources/fs-15-network-equipment-security-assurance-scheme-vendor-development-and-product-lifecycle-requirements-and-accreditation-process/ , accessed November 2020
[56] https://www.gsma.com/security/network-equipment-security-assurance-scheme/, accessed November 2020
[57] https://www.gsma.com/security/resources/fs-16-network-equipment-security-assurance-scheme-dispute-resolution-process/, accessed November 2020
[58] https://www.gsma.com/security/network-equipment-security-assurance-scheme/, accessed November 2020
[59] https://www.ngmn.org/about-us/organisation.html, accessed August 2020
[60] https://www.ngmn.org/wp-content/uploads/Publications/2020/200316-NGMN-LS-on-Security-consideration-of-Low-Layer-Split-in-O-RAN.pdf, accessed August 2020
[61] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180319/Documents/1_Min_Zuo.pdf, accessed August 2020
[62] https://5g-ppp.eu/, accessed November 2020
[63] https://5g-ppp.eu/5g-ensure/, accessed August 2020
[64] https://5g-ppp.eu/charisma/, accessed August 2020
[65] https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf, accessed August 2020
[66] https://5g-ppp.eu/NRG-5, accessed January 2021
[67] https://5g-ppp.eu/inspire-5gplus/, accessed January 2021
[68] https://www.inspire-5gplus.eu/, accessed January 2021
[69] https://www.etsi.org/technologies/zero-touch-network-service-management, accessed January 2021

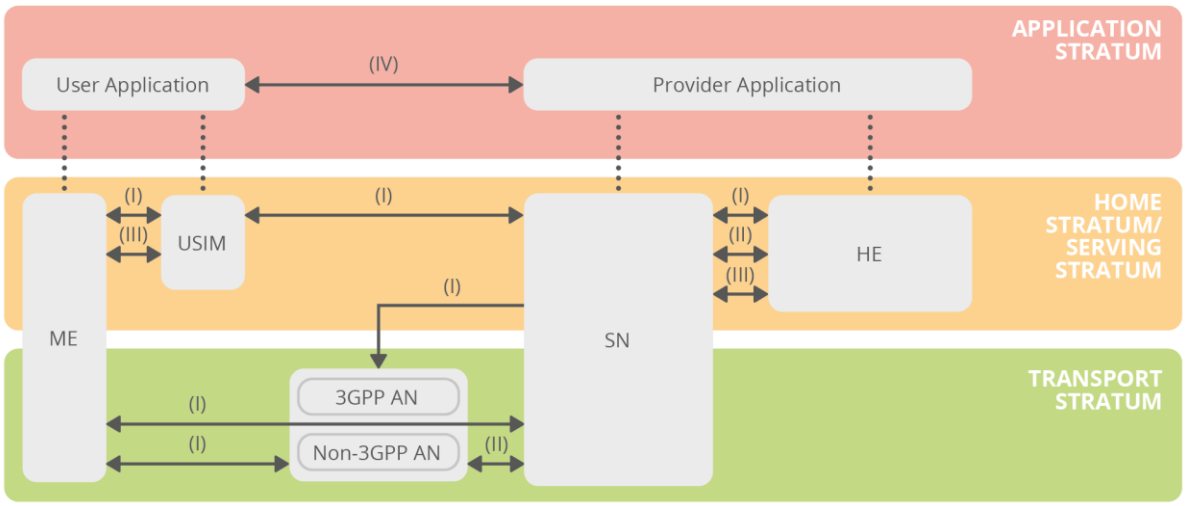
3. 3GPP SECURITY SPECIFICATIONS FOR 5G

3.1 SECURITY ARCHITECTURE AND PROCEDURES FOR 5G SYSTEM

3GPP TS 33.501 is the key document providing a detailed description of 'security architecture and procedures for 5G system'. This document is based mainly on the version 16.4.0 (September 2020) which is associated with Release 16[70]. This technical specification forms the basis for discussion and analysis in this report.

The specification defines a model of a security architecture, consisting of six security domains.

Figure 7: Security architecture model as defined in TS 33.501[71]



- **Network access security (I)** – security features that enable a user terminal to authenticate and access the network by providing protection on the radio interfaces.
- **Network domain security (II)** - security features that enable network nodes to exchange signalling and user data securely.
- **User domain security (III)** - security features that enable the secure user access to mobile devices.
- **Application domain security (IV)** - security features that enable user and provider domain applications to exchange messages securely. 33.501 specifications do not cover application domain security.
- **Service Based Architecture (SBA) domain security (V)** - a new set of security features that enable network functions of the SBA to communicate securely within serving and other network domains.
- **Visibility and configurability of security (VI)** - security features that enable the user to be informed regarding which security features are in operation or not.

The acronyms used on the above image are as follows: ME=Mobile Equipment, SE=Serving Network, HE=Home environment.

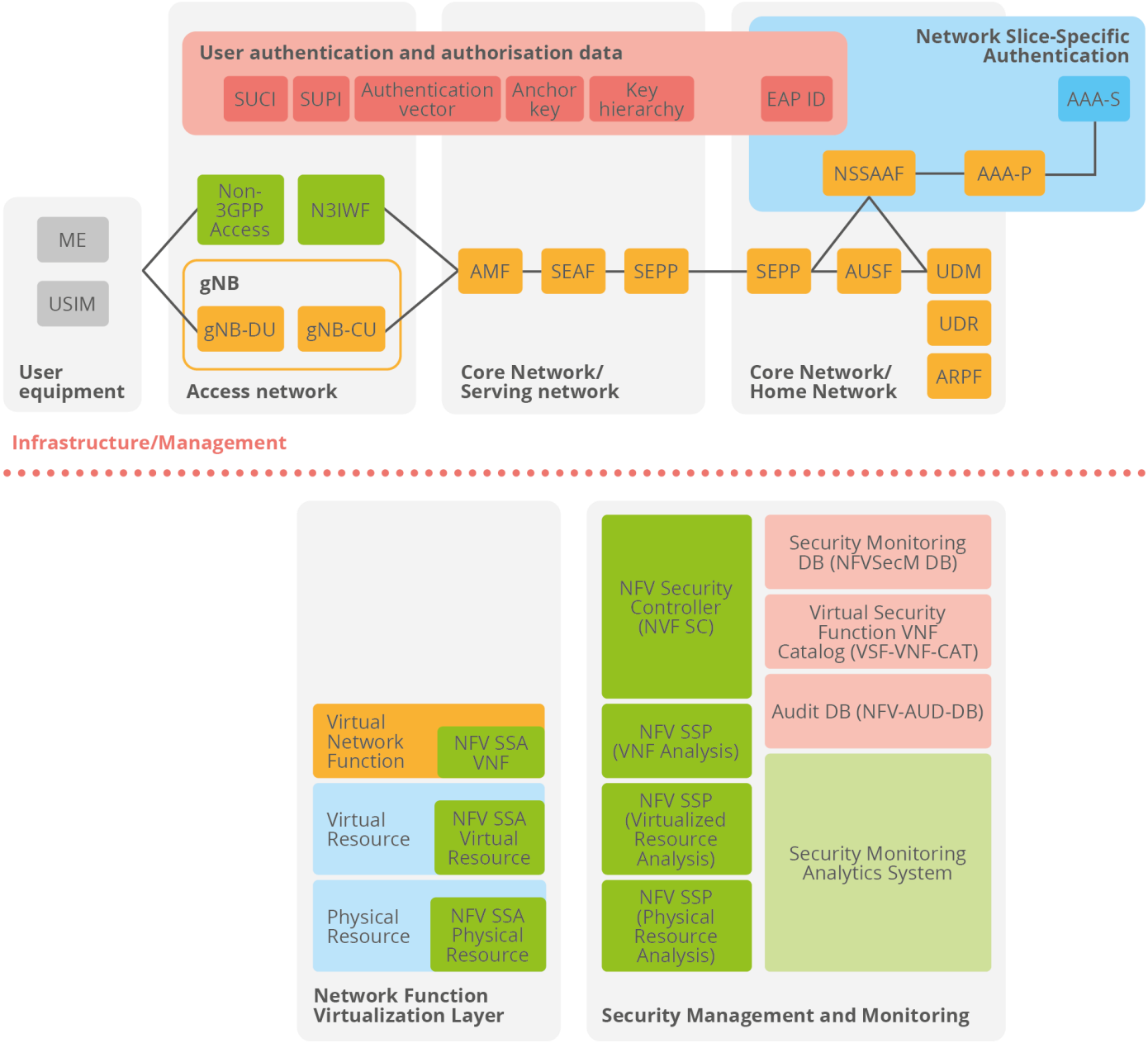
The above described security architecture model could be seen as a high-level composition of different security domains distributed across different system layers. However, the model does not show the key security elements of

[70] http://www.3gpp.org/ftp//Specs/archive/33_series/33.501/33501-g30.zip, accessed October 2020
[71] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169, accessed November 2020

the actual system security architecture or their relationship with other architectural components. It is worth noticing that this high-level architectural model is not extensively used or referred to in the specification itself.

Another view of the 5G security architecture is presented and described in details in the **ENISA Threat Landscape for 5G networks**[72] (hereinafter '**ETL5G'**). For completeness and ease of reference, we include the full security architectural diagram, with a remark that the scope of this report mostly pertains to the architectural elements above the 'infrastructure/management' layer, whilst the network function virtualization and security management and monitoring layers are not extensively covered in this report.

Figure 8: Security architecture zoom-in from the ENISA 5G Threat Landscape 2020



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

For further technical details about this architectural mode, including a detailed description of each of the architectural elements depicted, we refer reader to the full ETL5G. In addition, the most relevant security elements are further explained and described in this report, in the context of describing related security controls.

In following sections we analyse each of these improvements, with references to the 3GPP technical specification.

3.2 KEY SECURITY FEATURES

5G specifications bring significant security improvements in comparison to previous generations of networks[73]. In the following sections we list and explain some of the most relevant security features, making references to specific sections of the mentioned technical specification TS 33.501 and, where applicable, to other related technical specifications from 3GPP or other bodies. Note that the list is not exhaustive and that the features listed are only carefully selected security features believed to be of high relevance and in the focus of attention of experts from both industry and academia.

Certain important security features, however, including some of the newly introduced ones, are defined as optional, or there is a degree of flexibility for interpretation and implementation of some controls. This could potentially introduce vulnerabilities in what theoretically is a solid and robust security architecture, if trade-offs are made for the sake of performance, cost or time-to-market, at expense of security. Experts warn about this risk[74], reminding that similar has already happened earlier with 4G, claiming that some operators even have ignored some mandatory security features when implementation was expensive[75].

Therefore, for each of the highlighted security features we also identify potential optional elements, we include a brief analysis of possible security implications and we provide recommended good practice to be considered.

Remark: Some descriptions of technical details and underlying architectural elements in this section, both graphical and in narrative, are intentionally simplified, for convenience and simplicity. For a more complete technical information readers are referred to ETL5G and other technical documents detailing 5G general and security architecture and related technical aspects, including to the original 3GPP technical specification itself.

3.2.1 Subscriber Privacy

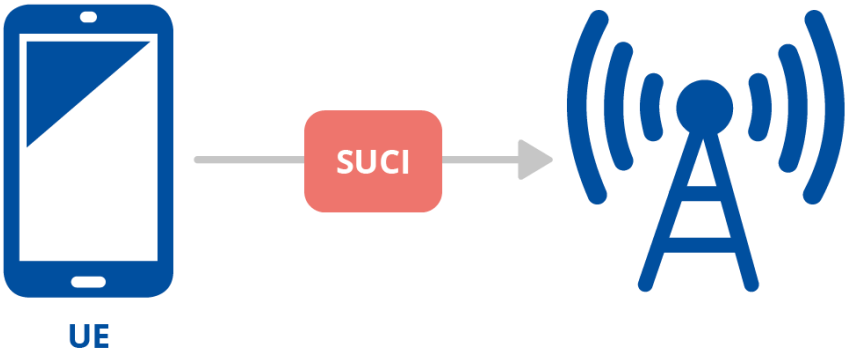
One of the typical problems with previous generations of mobile networks were false base stations or Stingrays, also called IMSI catchers, used by attackers to conduct man-in-the-middle and eavesdropping attacks[76] [77]. One of the key vulnerabilities that contributed to such attacks possible was that the subscriber identifier, IMSI, was sent in a clear text, unprotected. This vulnerability is addressed in 5G by various means, the most important of which is the introduction of the concealed subscriber identifier.

3.2.1.1 Protection of subscriber identifiers

In the 3GPP security specifications (TS 33.501), mechanisms used for subscription identifier privacy are defined in Clause 6.12. These include the use of permanent, concealed and temporary subscription identifiers. The globally unique 5G subscription permanent identifier is called Subscription Permanent Identifier (SUPI). The SUPI is privacy protected over-the-air by **identifier concealment**, using the Subscription Concealed Identifier (SUCI). SUCI does not provide privacy protection when it uses 'null scheme'. The user equipment generates SUCI using a protection scheme with the raw public key that was securely provisioned in control of the home network[78].

[73] A. R. Prasad, .A. Zugenmaier, A. Escott. M.C, Soveri, 3GPP 5G Security, https://www.3gpp.org/news-events/1975-sec_5g, accessed October 2020
[74] B. Schneier, "China isn't the only problem with 5G", Foreign Policy, January 2020, https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/, accessed September 2020
[75] L.N. Newman, "5G Is More Secure Than 4G and 3G—Except When It's Not", Wired, December 2019 https://www.wired.com/story/5g-more-secure-4g-except-when-not/, accessed October 2020
[76] K. Shubber, "Tracking devices hidden in London's recycling bins are stalking your smartphone", Wired, August 2013, https://www.wired.co.uk/article/recycling-bins-are-watching-you, accessed October 2020
[77] "Cellphone surveillance detected near the White House, DHS says", CNN, June 2018, https://edition.cnn.com/2018/06/01/politics/cell-phone-spying-dhs-wyden-study/index.html, accessed October 2020
[78] 3GPP TS 33.501 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169, accessed October 2020

Figure 9: Transmission of a Subscriber Concealed Identifier between UE and gNB (simplified scheme)



The subscription temporary identifier is called Globally Unique Temporary UE Identity (GUTI) which is sent to a user equipment after a successful activation of non-access stratum security. The Subscription Identifier De-Concealing Function (SIDF) is responsible for de-concealing the SUPI from the SUCI. Only a network element of the home network can request SIDF.

Valid SUPI types include the International Mobile Subscriber Identity (IMSI) and Network Access Identifier (NAI). It is never disclosed when user equipment is establishing a connection. Instead, SUCI is used. This prevents IMSI catchers from intercepting the subscriber identity. Note that in case of an unauthenticated emergency call, privacy protection for SUPI is not required.

The user equipment sends measurement reports to the network in accordance with the measurement configuration provided by the network (RRC_CONNECTED mode). These measurement reports have security values which can be used for detection of false base stations or SUPI/5G-GUTI catchers. Depending on implementation, the network could choose user equipment, tracking areas or duration for which the measurement reports are to be analysed for detection of false base stations. Examples of how this method can be used for detection of false base stations are given in the (informative) Annex E of the TS 33.501.

The actual requirement for SUPI is contained in the clause 5.2.5, which explicitly states that "*SUPI should not be transferred in clear text over NG-RAN*". The only exception explicitly listed here is for unauthenticated emergency calls, for which privacy protection for SUPI is not required.

Looking at the possible optionality for the implementation of this security feature, there are three cases listed in the clause 6.12.2 where SUCI is generated using 'null scheme' (i.e. no privacy protection and so the SUPI and SUCI are essentially the same identifier). One of them mirrors the exception stated in 5.2.5 (for unauthenticated emergency session). The other two cases refer to cases when the home network has configured 'null-scheme' to be used, or when the home network has not provisioned the public key needed to generate a SUCI.

When it comes to the choice of actual encryption scheme to be used, the same clause makes references to Annex C, where the details of a specific protection scheme ECIES, based on elliptic curve cryptography, are specified. However, it is stated that "the protection schemes shall be the ones specified in Annex C of this document *or the ones specified by the HPLMN*", hence leaving some flexibility for the choice of the scheme to be used.

Another important element that could be of high relevance for ensuring the robustness and resilience of the applied protection scheme is a requirement within the NOTE 2 in the same clause related to *freshness and randomness* of SUCI, which has to be taken care of by the corresponding SUPI protection scheme[79]. This is important as overlooking this requirement may significantly weaken the scheme and open space for various types of attacks against the scheme. Protection scheme described in Annex C.3 (ECIES) already contains elements to fulfil this requirement, by including a new, unique ephemeral key generated by UE at every connection request, ensuring that SUCI always changes and cannot be easily tracked over multiple connections. Any other protection scheme that could be used in

[79] H. Khan, B. Dowling, K.M. Martin, "Identity Confidentiality in 5G Mobile Telephony Systems", https://eprint.iacr.org/2018/876.pdf, accessed October 2020

lieu of the suggested ECIES scheme would have to take care of implementing this requirement and, essentially, ensuring the same or higher level of resilience.

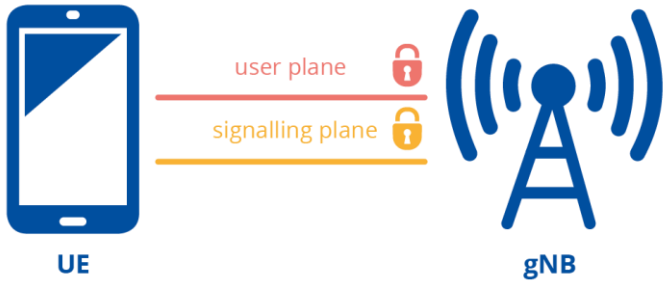
Additional security mechanism of relevance for protection of subscriber privacy is GUTI refreshment. This is defined in the clause 6.12.3 of the TS 33.501, which defines several mandatory cases when GUTI has to be refreshed (initial registration, mobility registration, periodic registration update and network triggered service request) and provides optionality to operators to implement more frequent re-assignments. Strict GUTI refreshment is important for prevention of attacks in which attackers are trying to identify or trace subscribers based on 5G-GUTI, impractical[80].

Security implications in the case of not implementing appropriate protection of subscribed identifier include compromise of subscriber privacy, allowing attackers to observe and capture subscriber's information and to mount an IMSI catcher and similar types of attacks.

3.2.2 Protection of user and signalling data

Using strong encryption for protection of radio path between the UE and the base station is not new. In the current 4G networks, encryption of traffic between mobile station and eNodeB can be implemented for protection of confidentiality and integrity of data exchanged between UE and Mobility Management Entity (MME). In 5G networks similar requirements apply. Like it was the case in 4G, some of these requirements are optional. The novelty coming with 5G is protection of integrity of the user plane data, but this is also optional.

Figure 10: Transmission of user and signalling data between UE and gNB (simplified scheme)



3.2.2.1 Confidentiality protection

Requirements for user and signalling data confidentiality protection to be employed on the UE are set out in the clause 5.2.2. These same requirements are effectively mirrored for the gNB, in respect of user data and RRC signalling (clause 5.3.2) and for the AMF, in respect of NAS signalling (clause 5.5.1).

In all cases, confidentiality protection of both user and signalling data is indicated as optional.

Four ciphering algorithms are indicated that can be used for such confidentiality protection, which are further explained in the specification Annex D. Those algorithms are:

- NEA0 – plaintext with no encryption (therefore offering no protection)
- 128-NEA1 – SNOW 3G cipher permitting backwards compatibility with 3G networks
- 128-NEA2 - AES-128 CTR cipher permitting backwards compatibility with 4g-LTE networks
- 128-NEA3 – based on the ZUC stream cipher which is specific to 5G implementations

As per the specification, the UE has to implement support for the first three algorithms (NEA0, 128-NEA1 and 128-NEA2), whilst implementation of support for the fourth algorithm (128-NEA3) is optional.

The specification states that confidentiality protection should be used wherever regulations in the operating territory permit. In other words, the default position for security is always on unless explicit local conditions prevent this.

[80] H. Khan, K.M. Martiny, "A survey of subscription privacy on the 5G radio interface - The past, present and future", Journal of Information Security and Applications, Vol. 53, August 2020

In terms of security implications, the lack of confidentiality protection of user data makes data vulnerable to interception. Likewise, lack of confidentiality protection of signalling data may result in interception of status and authorisation data between the UE and gNB/AMF giving opportunities for attackers to track user location and conduct other passive or active attacks[81].

3.2.2.2 Integrity protection

Requirements for user and signalling data integrity and replay protection to be employed on the UE are set out in the clause 5.2.3. These same requirements are effectively mirrored for the gNB, in respect of user data and RRC signalling (clause 5.3.3) and for the AMF, in respect of NAS signalling (clause 5.5.2).

Based on these requirements, integrity protection is mandatory[82] for signalling plane only (RRC-signalling and NAS-signalling), whilst it is optional for the user plane.

Four integrity protection algorithms are listed that can be used for such integrity protection, which are further explained in the specification Annex D. Those algorithms are:

- NIA0 – plaintext with no encryption (therefore offering no protection)
- 128-NIA1 – based on SNOW 3G
- 128-NIA2 – based on AES-128 in CMAC mode
- 128-NIA3 – based on 128-bit ZUC

As per the specification, the UE has to implement support for the first three algorithms (NIA0, 128-NIA1 and 128-NIA2), whilst implementation of support for the fourth algorithm (128-NIA3) is optional.

Lack of integrity and reply protection of signalling data traffic between UE and the gNB or AMF could lead to compromise and alteration of data and may facilitate various man-in-the-middle attacks. Moreover, possibility to also have user plane integrity protection, as a new feature added to 5G specification, is important to prevent malicious alteration of user data. Such alteration, as researches have shown[83], may have a major impact, such as redirecting of DNS request from UE to malicious server.

Remark: Integrity protection is considered to be a resource expensive operation and hence not all devices may be able to always support it or can only support it at certain rates[84]. Further issues may arise in 5G NSA scenarios, when legacy equipment without support for user plane integrity protection are used. Some of these issues and proposed solutions are analysed in details in the 3GPP technical report TR 33.853[85].

There is also an optional procedure for PDCP COUNT defined in the TS 33.501, section 6.13, that can be used by the gNB to periodically perform a local authentication and checking the amount of data sent between the gNB and UE both up- and down-stream. The check may be used to detect any tampering or intervention between the two devices as any mismatch in the count tally will reveal maliciously inserted packets. In the environment where integrity protection is on, such additional count check is redundant. In other cases, when there is no integrity protection active, using such a counter may offer some level of integrity protection with a relatively low overhead to the operator and user, but such control is not considered to be a sufficiently secure alternative for above described cryptographic integrity protection.

3.2.3 Protection of gNB setup and configuration

Clause 5.3.4 defines requirements for gNB setup and configuration which includes requirements for how gNB should be securely set up and configured by Operations and management (O&M) systems. Essentially, these requirements mandate usage of integrity confidentiality and replay protection for interfaces between O&M system and gNB, as well

[81] X. Hu et. al, "A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security", IEEE Access, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8817957, accessed November 2020
[82] With some exceptions, defined in TS 24.501 and TS 38.331
[83] D. Rupprecht, K.Kohls, T. Holz, C. Popper, “Breaking LTE on layer Two”, 2019 IEEE Symposium on Security and Privacy, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8835335, with a detailed explanation of the aLTEr attack available at https://alter-attack.net/ , accessed October 2020
[84] N. B. Henda, M. Wifvesson, C. Jost, “An overview of the 3GPP 5G security standard”, July 2019, https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview, accessed September 2020
[85] 3GPP TR 33.853, “Key issues and potential solutions for integrity protection of the user plane”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3571, accessed November 2020

as the requirements for gNB to ensure that software and data changes are authorized before installation and use[86].

The same clause also indicates that the certificate enrolment mechanism (as specified in TS 33.310) should be supported by gNB, however the decision on the actual use of this enrolment mechanism is left to operators and can hence be considered optional.

Finally, the same clause mandates the boot-up process to be performed in a secure environment, which is essential for protection of its sensitive elements[87].

The risk in the case of not implementing these requirement is related to potential modification of gNB settings and software configurations by attackers.

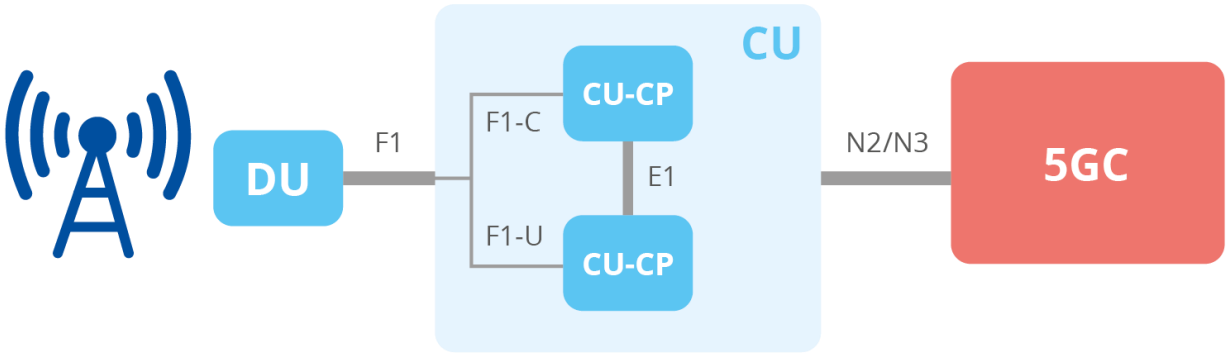
3.2.4 Protection of RAN Interfaces

3.2.4.1 CU-DU interfaces

5G brings the concept of a split or disintegrated RAN, where RAN is separated into: Distributed Units (DU) and Central Units (CU). Typically, DU does not have any access to customer communications and hence they are suitable to be deployed in unsupervised sites. On the other hand, CU performs security functions, it terminates the AS security and is typically deployed in sites with restricted access to maintenance personnel. Together DU and CU form the gNB.

Communication between DU and CU is established using the F1 interface. Moreover, CUs communicate with each other via E1 interface. Traffic transmitted through these interfaces may carry sensitive data and hence is a target for attackers. Hence, the specification mandates confidentiality, integrity and reply protection for control plane data exchanged over these interfaces, though some choices are left to operators, which we analyse further below.

Figure 11: Interfaces between components of the split RAN and 5G Core (simplified scheme)



In the 3GPP security specifications (TS 33.501), requirements for protection of base station (gNB) internal interfaces supporting the split architecture are set in clause 5.3.9 and 5.3.10 and further security mechanisms are detailed in Clauses 9.8.1 and sub-clause 9.8.2, for both F1 and E1 interfaces. In both cases, support of IPSec is mandated[88]. Concrete implementation requirements are provided in the Clause 9.1, sub-clause 9.1.2, specifying that the IPSec ESP protocol according to IETF RFC 4303 as profiled by TS 33.210[89] and IKEv2 certificate-based authentication (according to the profile described by TS 33.310[90]) shall be used[91].

Looking at the potential optionality/flexibility defined in the specification, there is a difference between control and user plane data. The clause 5.3.9 sets the requirements for confidentiality, integrity and replay protection as mandatory for the control plane interface (F1-C). However, when it comes to the user plane (F1-U) interface, the situation is somewhat different. Although there is a requirement that says that “The gNB shall support confidentiality, integrity and

[86] https://www.sdxcentral.com/5g/definitions/5g-security-standards/, accessed December 2020
[87] https://www.sdxcentral.com/5g/definitions/5g-security-standards/, accessed December 2020
[88] In addition to IPsec, for the F1-C interface, DTLS shall be supported as specified in RFC 6083 [58]
[89] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279, accessed October 2020
[90] https://www.etsi.org/deliver/etsi_ts/133300_133399/133310/12.02.00_60/ts_133310v120200p.pdf, accessed November 2020
[91] It is relevant to highlight that the mentioned mandatory nature of usage of IPSec and IKEv2 mainly pertains to the implementation part, as to be compliant with the 3GPP standards. In order to actually benefit from these security controls, they have to be actually used.

replay protection on the gNB DU-CU F1-U interface for user plane", there is also a NOTE which says: "The above requirements allow to have F1-U protected differently (*including turning integrity and/or encryption off or on for F1-U*) from all other traffic on the CU-DU (e.g. the traffic over F1-C)".

Regarding the E1 interface protection, used for signalling data transfer, the requirement simply states that "the E1 interface between CU-CP and CU-UP shall be confidentiality, integrity and replay protected." without explicitly listing any further remarks or exclusions.

From this we can conclude that the specification requires mandatory confidentiality, integrity and replay protection for the F1 signalling plane and for the E1 interface, while leaving it optional for the F1 user plane interface.

3.2.4.2 N2 and N3 interfaces

Interfaces N2 and N3 (also shown on the above figure) are interfaces that connect 5G-AN with AMF (Access and Mobility Function) and with the UPF (User Plane Function), respectively. They carry sensitive signalling and user plane data between access network and the core, meaning that they can be target for attackers. Hence, In the 3GPP security specification (TS 33.501) the requirements for confidentiality, integrity and replay-protection of all transport of both control and user plane data over N2 and N3 interfaces are defined in clauses 9.2 and 9.3, respectively.

In both cases there is also a requirement to implement IPsec ESP and IKEv2 certificate-based authentication, as specified in sub-clause 9.1.2 of the specification[92]. In addition, clause 9.2 also requires support of DTLS (as specified in RFC 6083) and refers to security profiles for DTLS implementation and usage as defined in the clause 6.2 of TS 33.210, clarifying also that the use of DTLS for transport layer security does not rule out usage of other network layer protection, emphasizing the advantage of IPSec in terms of providing topology hiding.

Having said all that, it is worth pointing out that in both cases, for N2 and for N3 interface, there are notes within the respective clauses that say that the use of cryptographic solutions to protect N2/N3 is an *operator's decision*. This introduces a degree of flexibility, if not optionality.

Security implications: Data transmitted through RAN interfaces includes sensitive data, both on user and control data plane and its protection is essential to prevent information disclosure, data tampering or denial of service attacks. DU-CU split allows flexibility in deployment options, but relies on appropriate securing of the interface between DU and CU, as otherwise sensitive data could be left vulnerable to attacks.

3.2.5 SBA protection

The 5G core network is based on a new architectural model[93], called SBA (Service Based Architecture). It is essentially a framework where the 5G network control plane functionality and data repositories are implemented by a set of interconnected Network Functions (NFs)[94] [95].

SBA is based on network entity functionalities which are refactored into services exposed and offered to other network entities. These network functions expose their functionality through Service Based Interfaces (SBI) through an SBI message bus that implements RESTful APIs over HTTP/2[96].

Essentially, all NFs can communicate with each other using either a request/response or subscribe/notify interactions between NF service consumers and producers. From the security point of view, such communication requires protection of confidentiality and integrity of the messages exchanged, as well as strong authentication and

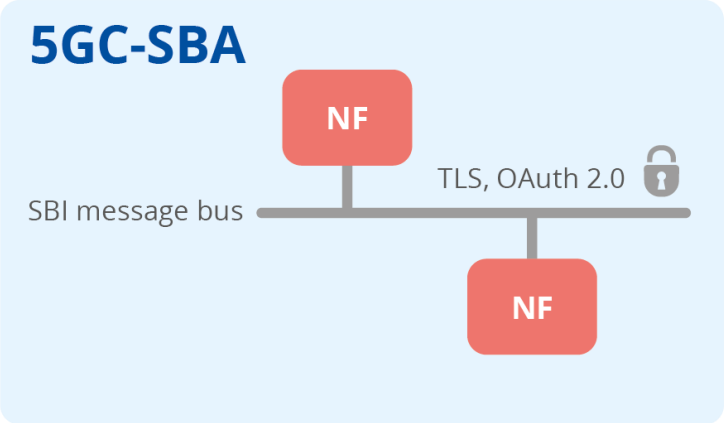
[92] The specification also says that it is mandatory to implement IPsec on the gNB side and that on the core side, a SEG (Security Gateway) may be used to terminate the IPsec tunnel.
[93] It may be worth clarifying that this concept is new only in the world of mobile networks architecture, whilst it is a known and mature concept applied for years in other ICT domains.
[94] "What is the 5G Service-Based Architecture (SBA)?", https://www.metaswitch.com/knowledge-center/reference/what-is-the-5g-service-based-architecture-sba, accessed October 2020
[95] G. Mayer, "RESTful APIs for the 5G Service Based Architecture", River Publishers, 2018, https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_617.pdf, accessed October 2020
[96] "What is the 5G Session Management Function (SMF)?", https://www.metaswitch.com/knowledge-center/reference/what-is-the-5g-session-management-function-smf

authorization mechanism[97].

In the 3GPP security specifications (TS 33.501), requirements for core network security are defined in clause 5.9. Further description of procedures and security aspects are given in section 13 of the technical specification and referred to in sections below.

Another specification document that is important is TS 33.122[98], defining security aspects of common API framework (CAPIF) for 3GPP northbound APIs. CAPIF is introduced for the purpose of standardising functionality exposed through northbound APIs[99]. This specification defines several common security requirements, related mainly to authentication and authorization, but also related to topology hiding.

Figure 12: Secure communication between network functions in 5G core SBA (simplified scheme)



3.2.5.1 Protection at the network or transport layer

Description of requirements for protection mechanisms at the transport layer is provided under the Clause 13.1. In short, NFs shall support client and server certificates and TLS, which is envisaged to be used for transport protection, whilst NDS/IP can still be used for network layer protection.

Looking at the possible optionality from the request for using TLS, it may be worth noticing that although the clause 13.1.0 explicitly states that “all NFs shall support TLS”, the actual *usage of TLS for transport protection* seems not to be as strictly defined. Instead, the clause specifies that “TLS shall be used for transport protection within a PLMN *unless network security is provided by other means.*” This may create space for introducing vulnerabilities if “by other means” would include weaker protection than the one provided by TLS.

Moreover, there is also an exception that in the case of trusted (e.g. physically protected) interfaces, it is up to an operator to decide whether to use cryptographic protection or not. This may increase the risk to confidentiality of data, depending on the actual level of such physical protection offered.

Security implications of improper transport layer protection of service-based interfaces (SBI) may include sensitive information/data being disclosed and eventually tampered[100].

3.2.5.2 Authentication

Description of requirements for authentication and static authorization for direct communication between NF and NRF[101] and between NFs is provided under the Clauses 13.3.1 and 13.3.2, respectively. In short, mutual

[97] "Security for 5G Service-Based Architecture: What you need to know", Ericsson, https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture, accessed October 2020
[98] Technical Specification Group Services and System Aspects; Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs (Release 16), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3420, accessed November 2020
[99] https://www.mpirical.com/glossary/capif-common-api-framework-for-3gpp-northbound-apis, accessed November 2020
[100] ETL5G, 2020
[101] NRF (Network Repository Function) can be seen as the authorization server that issues access tokens to other NFs that want to communicate to each other.

authentication between these functions communication is mandatory and for NF-NRF communication it shall be done during discovery, registration and access token request. The actual authentication mechanism would depend on the protection mechanism used under the clause 13.1. In other words, if it is the TLS, then the authentication provided by TLS shall be used. Likewise, any exceptions from using the TLS (as discussed above in section 2.3.2.1) would directly translate to the exceptions in the authentication mechanism utilised.

Security implications of improper mutual authentication are similar to those described above in section 2.3.2.1[102].

3.2.5.3 Authorization

Description of requirements for authorization of NF service access is given in section 13.4. The authorization framework specified (in the clauses 13.4.1 and 13.4.1.0) is 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.

Security implications of incorrect verification of access tokens may include: (1) 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; (2) 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[103].

3.2.5.4 Topology hiding

Topology hiding is important security feature that secures the address of the network elements and can prevent the attacks intended for unauthorized access to network element or for interruption of the network service.[104]

Clause 5.9.2.1 of the TS 33.501 includes several requirements for SBA service registration, discovery and authorization, one of which states that “NF service based discovery and registration shall be able to hide the topology of the available / supported NF's”[105] between different trust domains, for example between NFs in home and NF in visited network. Further requirements related to topology hiding for topology hiding for exposed APIs are also defined in the section 4.2. of the TS 33.122.

3.2.6 Authentication Framework

Mutual authentication between users and the mobile network is one of the fundamental elements of security in any network and is of particular importance in networks based on zero-trust model. Equally important is the generation, derivation and distribution of cryptographic keys necessary to protect signalling and user data (as discussed above). In this section we look at the fundamental aspects of the authentication and key management mechanism for 5G networks, as defined in the 3GPP technical specification.

In addition to primary and secondary authentication discussed below in more details, authentication for network slicing is also defined in TS 33.501. Clause 16.3 defines requirements for network slice specific authentication and authorization (NSSAA) between UE and external AAA server[106]. These requirements specify that EAP framework is to be used for this purpose with SEAF/AMF as the EAP authenticator. The whole NSSAA is defined as optional to use.[107]

3.2.6.1 Primary Authentication

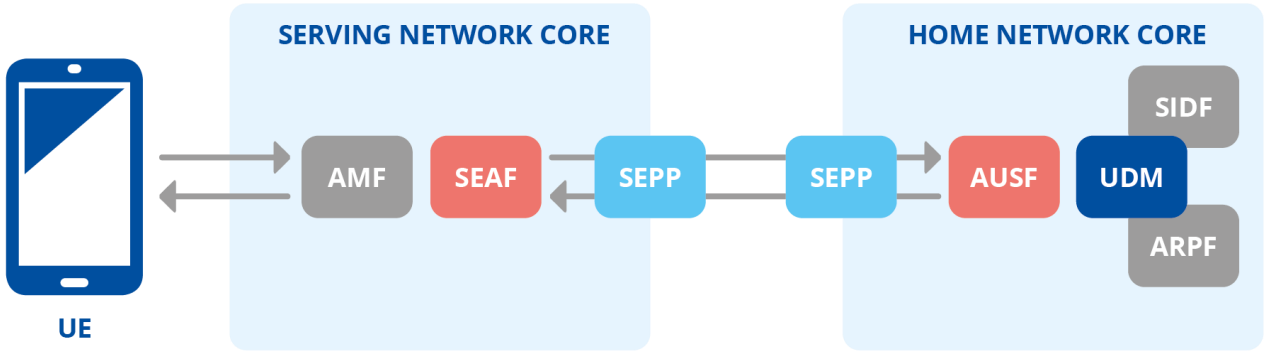
5G introduces a new, flexible and strong authentication framework. The objective is mutual authentication between user equipment and the network and provision of keying material that can be used in subsequent security procedures between the user equipment and the serving network. In the 3GPP security specifications (TS 33.501) this is

[102] ETL5G, 2020
[103] ETL5G, 2020
[104] Jha, Divya & Shahi, Bimlendu & .D, Dushyanth.N., “Topology Hiding of Connected Network Elements Using Diameter Protocol”, Innovations in Computer Science and Engineering (pp.87-93) January 2019
[105] 3GPP TS 33.501, https://www.3gpp.org/DynaReport/33501.htm, accessed November 2020
[106] Procedure is also defined in TS 23.502, section 4.2.9, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3145, accessed November 2020
[107] Another authentication framework worth mentioning in the context of future applications, is Authentication and Key management for Applications (AKMA), defined in TS 33.535. Under this framework, subscriber credentials can be used for authentication and key management at the application layer, for 3rd party applications. This may be particularly be relevant for IoT applications.

described in the Clause 6.1.

The main authentication protocol is 5G-AKA (Authentication and Key Agreement Scheme), depicted in a simplified form at the diagram below.

Figure 13: Authentication and key Agreement Scheme in 5G (simplified scheme)



The main task accomplished by this procedure is mutual authentication between the UE and the network. On the side of the core network, the key element that effectively performs authentication with the UE is AUSF (Authentication Server Function). It uses services of UDM (Unified Data Management) and ARPF (Authentication Credential Repository and Processing Function), which are responsible for hosting functions related to data management and for selecting authentication methods and computing data and keyring material that AUSF needs[108]. At the same time, SIDF (Subscriber Identifier De-concealing Function) comes into play to recover SUPI from SUCI. All this is happening in the home network core.

On the side of the serving network, the key function is SEAF (Security Anchor Function), which could be seen as a kind of proxy during the authentication process, as it relies on the information received form AUSF from the home network.

The result of the primary authentication and key agreement procedure is an anchor key (K_{SEAF}) provided by the AUSF of the home network to the SEAF of the serving network. Keys for more than one security context can then be derived from the K_{SEAF} without the need of a new authentication run. For example, keys obtained from an authentication run over a 3GPP access network can be used to establish security between the user equipment and a Non-3GPP access InterWorking Function (N3IWF) used in untrusted non-3GPP access. The primary authentication and key agreement procedures bind the anchor key K_{SEAF} to the serving network which provides implicit serving network authentication, regardless of the access network technology, to the user equipment.

Described framework allows home network to be in charge of authentication instead of the visiting/roaming network. This is a difference from 4G networks, where although the home network is consulted during the authentication process (for the purpose of generating authentication vectors), it is not the home network that makes the decision on the authentication results[109].

5G networks support Extensible Authentication Protocol (EAP) framework defined in IETF RFC 3748 which defines the roles peer, pass-through authenticator and back-end authentication server. EAP provides flexibility for authenticating 3GPP and non-3GPP access networks.

3.2.6.2 Secondary Authentication

EAP supports both primary (typically implemented during initial registration for example when a device is turned on for the first time) and secondary (executed for authorisation during the set-up of user plane connections, for example, to surf the web or to establish a call) authentication. The secondary authentication allows the operator to delegate the

[108] Cable Labs, "A Comparative Introduction to 4G and 5G Authentication" https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication, accessed October 2020
[109] Ibid.

authorisation to a third party. It is meant for authentication between UE and external data networks (DN), residing outside the operator's domain. Similar service was also possible in 4G, but it is now integrated in 5G architecture[110].

In the 3GPP security specifications (TS 33.501), provisions for EAP based secondary authentication by an external DN authentication server are specified in the clause 11.1, within the section 11, defining general security procedures between UE and external data networks. Secondary authentication as defined in this clause is optional to use.

Some operators[111] are using the described mechanism to expand this as to allow external network operators to perform independent authentication and authorization before UE is allowed to connect to that external network using EAP to request secondary authentication by the external network.

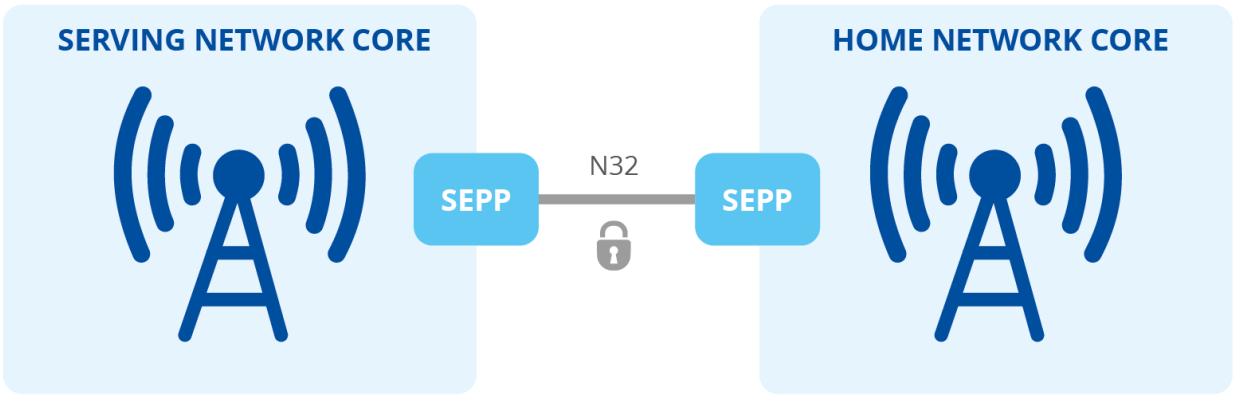
3.2.7 Roaming Security

Security issues in roaming and inter-operator interfaces have been affecting earlier generations of mobile networks for years, both for the older SS7[112] and SIGTRAN, as well as for the newer Diameter protocol[113]. In 2018 ENISA also published a technical report[114] containing a deep dive analysis of these matters. 5G comes with a new stack of a new generation of protocols and introduces new dedicated security elements for ensuring inter-operator security.

3.2.7.1 SEPP for inter-operator security

In 5G security architecture model, a new architecture element is introduced: the Security Edge Protection Proxy (SEPP). SEPP acts as the security gateway on interconnections between the home network and visited networks. Functions supported by SEPPs include end-to-end authentication, integrity and confidentiality protection via signatures and encryption of all HTTP/2 roaming messages; and key management mechanisms for setting the required cryptographic keys and performing the security capability negotiation procedures[115]. SEPPs also support prevention of bidding down attacks[116] and also provides topology hiding[117].

Figure 14: Secure communication between two SEPPs (simplified scheme)



Underlying requirements defined in the 3GPP security specifications (TS 33.501) are those in the clause 5.9.3, related to requirements for e2e core network interconnection security and those in the clause 5.9.3.2, containing specific requirements for SEPP.

Further details are specified in section 13. Essentially, the specification says that TLS shall be used between SEPPs

[110] A. R. Prasad, .A. Zugenmaier, A. Escott. M.C, Soveri, 3GPP 5G Security, https://www.3gpp.org/news-events/1975-sec_5g, accessed October 2020
[111] Verizon, "The security of Verizon's 5G Network, Network Security Planning Version 1.0", August 2020, https://www.verizon.com/about/sites/default/files/2020-09/200574_Schulz_07242020.pdf, accessed October 2020
[112] S. Gibbs, "SS7 hack explained: what can you do about it?", Guardian, 2016, https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls, accessed October 2020
[113] C. Cimpanu, "Newer Diameter Telephony Protocol Just As Vulnerable As SS7", https://www.bleepingcomputer.com/news/security/newer-diameter-telephony-protocol-just-as-vulnerable-as-ss7/ , accessed September 2020
[114] Signalling Security in Telecom SS7/Diameter/5G, ENISA, 2018, https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g, accessed September 2020
[115] "Securing the 5G era", GSMA, https://www.gsma.com/security/securing-the-5g-era/, accessed October 2020
[116] where the user equipment and the network entities falsely believe that the other side does not support a security feature
[117] See section 3.2.4.5

in scenarios where there are no IPX entities between them and otherwise an application layer security protocol over N32 layer called PRINS shall be used (clause 13.1.2).

Details of PRINS are provided under Clause 13.2. SEPPs allow secure communication between service-consuming and a service-producing Network Functions in different public land mobile networks. Security Edge Protection Proxies use JSON Web Encryption described in IETF RFC 7516 (JSON Web Encryption (JWE)) for protecting messages on the N32 interface against eavesdropping and replay attacks and IP exchange service providers use JSON Web Signatures defined in IETF RFC 7515 (JSON Web Signature (JWS)) for signing their modifications needed for their mediation services. The application layer security protocol for the N32 interface is called PRINS and described in detail (procedures for key agreement, parameter exchange, error detection, error handling and context). N32 application layer protection policies including data-type encryption policy (specifying which data types need to be confidentiality protected) and modification policy (specifying which Information Elements (IEs) are modifiable by IP exchange service providers) are also described in detail.

This is followed by the detailed descriptions of authentication and authorisation methods involving NFs and SEPPs in Clause 13.3 – 13.5. In particular, an extensive explanation of OAuth 2.0 authorisation framework (specified in IETF RFC 6749) is provided in Clause 13.4 in the context of authorisation for Network Function (NF) service access within the Public Land Mobile network (PLMN) and roaming scenarios.

It is important to note that the use of an IP-based protocol stack instead of proprietary protocols allows interoperability with a wide number of services and technologies[118]. As mentioned above, these include HTTP/2 over N32 and TLS. All network functions are required to support TLS in the context of service-based interfaces and HTTP/2 request/response messages from Network Functions are used for SEPP connections over N32.

Recently, there have been discussions on practicability of using PRINS due to the apparent difficulties of implementing and maintaining it[119]. For these reasons, GSMA has recently established a dedicated task force to reconsider solutions for securing 5G roaming as to define “a scalable, usable and secure solution for 5G mobile roaming”, possibly revisiting the current recommendations described above[120].

Looking at the potential optionality/flexibility defined in the specification, there are no explicit options or exceptions defined when it comes to the requirements or the technologies to be used. Potential vulnerabilities that could be introduced in implementing these requirements would more likely come from specific implementation aspects and may include issues related to certificate and key management. We’ll mention this in section 4 of this document, but for more detailed technical information about specific vulnerabilities, related threats and possible security controls we refer the reader to the ETL5G, 2020.

3.2.8 Secure Storage

Many of the security mechanisms listed above are based on secure protocols and underlying cryptographic algorithms that all rest upon the ability of the system to securely store secret keys. Moreover, critical operations that use these keys should, ideally, always be executed within a secure hardware environment.

3.2.8.1 Secure storage requirements for UE

For the **UE**, in the 3GPP security specifications (TS 33.501), requirements for secure storage and processing of subscription credentials are defined in the clause 5.2.4. They are related to integrity and confidentiality protection of subscription credentials and long term keys of subscription credentials, for which the usage of tamper resistant secure hardware component is mandated.

Further on, in the section 6.2, procedures related to key hierarchy, key derivation and distribution scheme are given. Within that section, there is a clause 6.2.2.2 that includes procedures for handling keys. For example, for the Home Network Public Key that is used for concealing the SUPI, it is specified that it shall be stored in the USIM. However, storing of K_{AUSF} in the USIM is optional and a possibility for this key to also be stored in non-volatile memory

[118] “Securing the 5G era”, GSMA, https://www.gsma.com/security/securing-the-5g-era/, accessed October 2020
[119] https://ibasis.com/5g-security-when-roaming/, accessed December 2020
[120] P. Veenstra, Reasons for the GSMA to reconsider the solutions for 5G Roaming, NetNumber, https://www.netnumber.com/reasons-for-the-gsma-to-reconsider-the-solutions-for-5g-roaming/ , accessed December 2020

(depending on the UE capability) is also defined. Given the importance of this key[121], in the latter case there is a security dependency on whether protection and/or encryption is in place on the memory locations to ensure that these cannot be accessed through unauthorised attempts.

3.2.8.2 Secure storage requirements for gNB

For **gNB**, requirements for handling keys are defined in the clause 5.3.5. The clause emphasizes the importance of protecting keys held in gNB, such as session keyring material that also contains long term keys used for authentication and security association setup. These requirements specify that any part of gNB deployment that stores or processes keys in clear text has to be protected from *physical* attacks. No specificities are given, however, in regards of a type and required level of such protection. The stated alternative is that the whole entity is placed in a *physically* secure location and that keys are processed in a *secure requirement*, which is defined in the clause 5.3.8. This includes requirements for supporting of secure storage of sensitive data, secure execution of sensitive functions and execution of sensitive parts of the boot process, as well as for access control to such environment.

3.2.8.3 Secure storage requirements for 5GC

Clause 5.8.1 defines generic requirements on the Unified Data Management (UDM), which include requirements for the long-term keys used for authentication and security association setup processes. It is said that these keys shall be protected from *physical* attacks and shall never leave security environment of the UDM/Authentication credential Repository and Processing Function (ARPF) unprotected. At the same time, however, the clause does not go into the details of security mechanisms for protection of subscription credentials in ARPF or Unified Data Repository (UDR), nor for the transfer of such credentials between the ARPF and UDR, stating that these are "*left to implementation*".

When it comes to protection of the Home Network Private Key, which is the critical element for de-concealment of SUCI, clause 5.8.2 (Subscriber privacy related requirements to UDM and SIDF) includes the requirement that the key has to be protected from *physical* attacks in the UDM. At the same time, however, the clause 6.2.2 (Key derivation and distribution scheme) and its sub-clause 6.2.2.1 (keys in network entities) also include the following provision: "The ARPF holds the Home Network Private Key that is used by the SIDF to de-conceal the SUCI and reconstruct the SUPI. *The generation and storage of this key material is out of scope of the present document.*"

In summary: 5G security depends on keeping security-critical data (e.g. subscriber credentials, decryption keys) secret. Some key storage requirements exist (e.g. for UE), but some details are unspecified or left to implementation

[121] KAUSF is one of the primary elements of the key hierarchy and is used to decrypt messages between the AUSF and UE, unauthorised capture of which would permit unauthorised decryption of authentication message traffic, and be potentially used to generate false messages and/or authenticate unauthorised devices.

4. OTHER SECURITY ASPECTS

Security technical specifications and standards define controls that make a foundation for development and implementation of secure networks and for development of related security assurance and certification schemes. However, experts[122] agree that "security posture of a deployed network cannot be realized through standardization alone". Based on standards and specifications, suppliers develop network equipment and operators design the overall network, procure, configure and deploy network equipment and manage and operate the network[123].

Figure 15: Beyond standards and specifications

In this section we list some of the possible additional security considerations related to above listed technical areas and conclude with a brief discussion on general aspects.

4.1 TECHNICAL ASPECTS

For more detailed information on processes and respective security responsibilities for both suppliers and operators, it is worth looking at their respective security lifecycle processes, related to product development and network design, deployment and operation. Readers are referred to the updated ENISA Threat Landscape for 5G Networks (ETL5G 2020) report[124], section "Process Map", section 3.13, where related security considerations are discussed in detail. Here we briefly discuss some of the most relevant areas, highlighting also the aspect that are not covered, or only partially covered, in the technical specification discussed in section 3.

4.1.1 Security Testing and Assurance

To ensure that security controls have been correctly implemented, it is necessary to conduct appropriate tests. A basic set of predefined test-cases is identified and explained in a series of 3GPP documents that form the SCAS (Security Assurance Specifications) scheme.

Operators can also use the scheme as part of a methodological security assurance process. In the above mentioned new section "Process map" in the ETL5G 2020 report there is more detailed guidance on security assurance process. For completeness, here we reproduce an introduction part containing the high-level description of the related methodology and we refer the reader to the original report for more details:

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 3GPP TR 33.916[125] and TR 33.818[126] for virtualized network products .

[122] Security standards and their role in 5G, Ericsson, https://www.ericsson.com/en/blog/2020/6/security-standards-role-in-5g, accessed October 2020
[123] Security standards and their role in 5G, Ericsson, https://www.ericsson.com/en/blog/2020/6/security-standards-role-in-5g, accessed October 2020
[124] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks, accessed December 2020
[125] Security Assurance Methodology (SCAS) for 3GPP network products, https://www.3gpp.org/DynaReport/33916.htm, accessed November 2020
[126] Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products, https://www.3gpp.org/DynaReport/33818.htm, accessed November 2020

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

- *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)*

Remark: It is important to highlight that the above described testing based on predefined security assurance test cases, many of which could be seen as functional tests, is not sufficient for ensuring the high level of overall security of products or for a comprehensive security assessment of a network as a whole. Additional testing should be considered, which could involve negative tests and fuzzing of individual components, integrated systems and the network as a whole. Regular vulnerability scanning using specialised third party vulnerability scanning tools is highly recommended, in addition to periodic penetration testing by third parties.

4.1.2 Product development

To ensure high level of security and resilience for end-products, suppliers need to have a secure product development process and to have security by design as a basic principle, systematically and verifiably applied. In the case of 5G networks, where key elements will be software-based, this process have to take particular care of matters such as secure software development, security assessment and testing, version control, secure software update and alike. This would typically also include systematic source code review process, application of coding best practices, using of static and dynamic code analysis, external code review process and individual product vulnerability scanning. Moreover, due to the prominence of supply-chain risks for security of 5G networks, suppliers also need to have adequate measures in place to adequately manage such security risks.

The role of authorities in ensuring the adequate level of security for products and equipment that will be built in the 5G networks deployed nationally depends on specific legal framework adopted and the related regulatory powers. Some of the strategic measures from the Toolbox directly or indirectly address the matter of security of supplier's products. Moreover, the "*overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices*" is one of the three suggested factors for assessment of risk profiles of suppliers, identified in the Coordinated risk assessment.

Competent authorities responsible for supervision of security measures defined in the EECC Article 40 may also consider setting specific requirements for operators to ensure security of third party assets deployed in their networks. ENISA guideline and its 5G supplement[127] contain specific measures and additional checks that regulatory authorities may consider in this regard under the security objective SO4: security of third party assets. In addition, authorities may refer to other available industry standards and good practices[128].

4.1.3 Network Design

Despite the fact that security specifications include set of security requirements, procedures and considerations related to the design and implementation, the actual network design is typically in the hands of operators and the number of permutations and ways in which this could be done is large and typically not something that is prescribed in standards and technical specifications. When designing the overall network, however, operators may want to use of the security architecture concepts and philosophy that is built in the 5G specifications to improve network resilience.

[127] In preparation, draft available for MS on CIRCABC, final version will be published on ENISA website by the end of 2020
[128] E.g. NESAS Development and Lifecycle Security Requirements v.1.1, https://www.gsma.com/security/resources/fs-16-network-equipment-security-assurance-scheme-dispute-resolution-process/ , accessed November 2020

For example, some large operators are building 5G network security plans in which network design concepts are put in place which leverage disaggregated nature of 5G NF[129], such as:

- Reducing the blast radius in the case of an outage or compromise of a NF, by isolating critical NFs at network and/or compute/storage level;
- Configuring level of redundancy based on NF criticality (e.g. using 2N redundancy for critical NFs and N+1 redundancy for other NFs);
- Tailoring network-based security protections based on NF criticality (e.g. deploying sophisticated IDS, anti-DDoS protection and advanced monitoring for critical NFs);
- Having an on-demand tailoring of redundancy and network-based security depending on the changing network and threat conditions.

Additional considerations that should ideally be addressed early may also include design of secure communication between management systems to the network, additional network security controls for protection of internet facing functions (e.g. N6 interface connecting UPF to external data network), additional network security controls for protection of important internal interfaces (e.g. protection from DDoS flood from IoT devices over N3 interface), procedures for secure auto-provisioning and secure boot-up and alike. These are just some of the possible additional controls to be considered that are already been implemented by some operators.[130] [131]

Moreover, a recent research study[132] analysing security of the 5G Standalone (5G SA) core has highlighted several possible attack scenarios on N4 interface between user and control plane that may result in denial of service or redirection of data. This underlies the importance of adequately configuring internal network interfaces (such as N4) in order to prevent external access to them.

4.1.4 Network Configuration and Deployment

Whilst 3GPP specifications define key functional elements, interfaces and related security requirements, there are multiple security considerations when it comes to deployment scenarios for a full 5G system, which are sometimes categorized into horizontal (e.g. security at the network level, slicing, application level security, confidentiality and integrity protection, interconnect-SBA) and vertical security considerations (e.g. NFV, distributed clouds)[133].

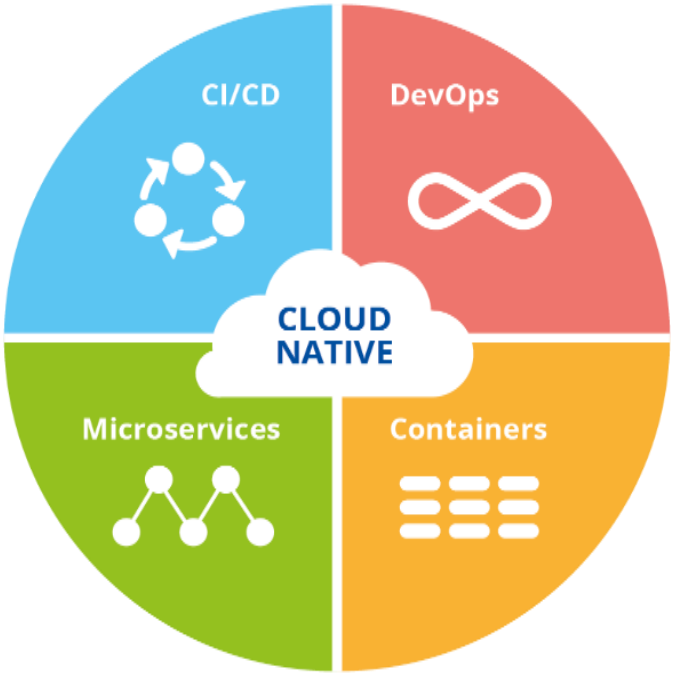
One of the key considerations is how the network functions in the new 5G core are to be deployed and here **virtualization** is a key technology for enabling flexible deployments. As discussed in section 2, standardisation on NFV is mostly done in ETSI ISG NFV, who are looking at NFV security "from a more general network management and orchestration point of view" while, on the other hand, 3GPP security experts are looking at virtualization security aspects from mobile a network architecture point of view." [134] Experts also warn that not all virtualization aspects can be standardized, as some are a matter of implementation, deployment, configuration and operation, highlighting that "it is important to find the right balance between standardized and non-standardized aspects to allow for freedom for innovation and differentiation." [135]

At the same time, there is a trend of shifting both the core and access of 5G to **cloud-native** architectures[136]. According to the definition by the Cloud Native Computing Foundation (CNCF)[137], "*cloud-native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach. These techniques enable loosely coupled systems that are resilient, manageable, and*

[129] Verizon, "The security of Verizon's 5G Network, Network Security Planning Version 1.0", August 2020, https://www.verizon.com/about/sites/default/files/2020-09/200574_Schulz_07242020.pdf, accessed October 2020
[130] Verizon, "The security of Verizon's 5G Network, Network Security Planning Version 1.0", August 2020, https://www.verizon.com/about/sites/default/files/2020-09/200574_Schulz_07242020.pdf, accessed October 2020
[131] The controls listed here are given as examples and for illustration only and are by no means meant to represent a full and exhaustive set of controls. Many more network design good security practises may be used by operators to achieve adequate level of resilience.
[132] https://positive-tech.com/knowledge-base/research/5g-sa-core-security-research/, accessed January 2021
[133] Ericsson, "A guide to 5G network security", https://www.ericsson.com/en/security/a-guide-to-5g-network-security, accessed November 2020
[134] Security standards and their role in 5G, Ericsson, https://www.ericsson.com/en/blog/2020/6/security-standards-role-in-5g, accessed October 2020
[135] Ibid.
[136] 5G Americas, Security Considerations of 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 November 2020
[137] https://www.cncf.io/, accessed December 2020

observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil."[138]

Figure 16: Cloud-native essential elements[139]



Moreover, the entire area of **microservices** is not directly covered by existing specification. Microservices are key building blocks if the cloud-native system and are essentially "*small, independent services that interact through a shared fabric*"[140]. One of the important security aspects is certificate management for microservices. More generally speaking, secure communication and authentication between microservices within a given NF[141] is highly relevant. These aspects do not appear to be standardized in 3GPP so far[142].

Cloud as the infrastructural choice on its own brings a new set of important security considerations and dilemmas to be solved, such as whether to build/utilize a private cloud infrastructure or to make use of external could service providers, how to ensure secure communication in cloud, how to leverage cloud high availability and resilience etc.

Another important consideration is related to **PKI** and **certificate management**. Key security mechanisms for protection of SBA rely on Public-Key Infrastructure (PKI). In the core of the PKI are certificates, typically issued and signed by Certificate Authority (CA) which bind certain identities with corresponding public/private key pairs which are then used for accomplishment of asymmetric cryptographic operations that are necessary for mutual authentication, TLS and OAuth 2.0. In static and pre-configured environments, establishment of PKI and issuance and distribution of certificates is relatively straightforward. However, experts warn that environment such as SBA, that rely on virtualised network functions, likely implemented using microservice architecture, with continuous deployment and fast-paced updates, it will not be feasible to perform certificate issuance manually and that high automation is needed.[143]

[138] https://github.com/cncf/foundation/blob/master/charter.md, accessed December 2020
[139] Source: https://dzone.com/articles/cloud-native-seeing-through-the-hype, accessed January 2021
[140] https://docs.microsoft.com/en-us/dotnet/architecture/cloud-native/definition, accessed December 2020
[141] 5G Americas, Security Considerations of 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 November 2020
[142] Ericsson, Security for 5G Service-Based Architecture: What you need to know, https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture, accessed December 2020
[143] Security standards and their role in 5G, Ericsson, https://www.ericsson.com/en/blog/2020/6/security-standards-role-in-5g, accessed October 2020

4.1.5 Network Operation and Management

Once the network is deployed, operators have to manage and operate the network in a secure manner. This includes application of standard baseline security measures for network security and resilience and appropriate reinforcement of technical measures that are of particular relevance for risks in the 5G environment. Competent authorities may refer to industry standards[144] or to ENISA guideline for best practices on implementation of baseline security measures in telecom sector[145]. This guideline contains ~150 measures, at three levels of sophistication, organised in 29 security objectives across following 8 security domains:

- D1: Governance and risk management
- D2: Human resources security
- D3: Security of systems and facilities
- D4: Operations management
- D5: Incident management
- D6: Business continuity management
- D7: Monitoring, auditing and testing
- D8: Threat awareness

In addition to this guideline, ENISA has developed a supplement related to 5G networks[146], which contains a set of additional checks that regulators may take in consideration when assessing the implementation and reinforcement of security measures by operators providing 5G networks and services.

Operators should strive to reinforce those security measures and controls that address the most important risks identified for 5G networks, taking also as guidance the set of technical measures identified in the 5G Toolbox. These reinforcements may span across all security domains, but should in any case consider strengthened access control, resilience and monitoring capabilities.

Considering the likely increased volume of monitoring data points, a use of integrated monitoring solutions with automation and, where applicable, machine learning supported data analytics, may also be considered[147].

It is also important to adapt operational processes to new, software-based environments. Experts recommend reinforcing of **Operational capabilities** that are needed so as to[148]:

- *Embrace software pipelines (Continuous integration (CI) and continuous delivery (CD)) and DevSecOps to make development and deployment more efficient, secure and with drastically reduced lead times.*
- *Upgrade IT skills so that the workforce can evolve with the technologies.*
- *Enable a data driven predictive environment, to proactively address issues before they arise and become detrimental.*

4.2 GENERAL ASPECTS

Standards and specifications in the area of 5G are complex, as is the underlying technology. Moreover, they are fluid and still under development. Not all aspects are fully covered and some gaps are yet to be filled.

For the EU MS and their respective relevant national authorities it is important to be aware of the key security aspects of technical standards and specifications, to identify and to understand possible gaps that may exist in current specifications and to ensure their *increased level of engagement in relevant standardisation bodies, in particular*

[144] E.g. ISO/IEC 27011:2016 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations - https://www.iso.org/standard/64143.html, ; ITU x.1051 (Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations) - https://www.itu.int/rec/T-REC-X.1051 , eTOM Processes (see also section 3.13 in ETL5G)
[145] Guideline on Security Measures under the EECC, ENISA, 2020, https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc, accessed December 2020
[146] 5G Supplement - to the Guideline on Security Measures under the EECC, ENISA, December 2020, https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc, accessed December 2020
[147] Verizon, "The security of Verizon's 5G Network, Network Security Planning Version 1.0", August 2020, https://www.verizon.com/about/sites/default/files/2020-09/200574_Schulz_07242020.pdf, accessed October 2020
[148] H. Patil, "Your 5G - it's as easy as 1, 2, 3", Ericsson, July 2019, https://www.ericsson.com/en/blog/2019/7/your-5g---its-as-easy-as-1-2-3, Accessed November 2020

through reinforced coordination at EU level in order to increase ability to shape standardisation according to identified needs, as stipulated in the 5G Toolbox, supporting action SA03.

At the same time, as these specifications are evolving, in parallel new products are being developed, new networks are being deployed and the regulatory environment is being shaped. All this creates a complex and dynamic environment in which all relevant actors listed in the EU Toolbox - suppliers, operators, MS authorities, EC and ENISA have to navigate in real time. This underlines the importance of further collaboration between individual MS and between MS and private sector entities, so that complexities are better understood and that appropriate solutions are identified in a collaborative manner. ENISA, following on its mission *"to achieve a high common level of cybersecurity across the Union in cooperation with the wider community"* and its role in "*stimulating active cooperation between the cybersecurity stakeholders in Member States and the EU institutions and agencies*"[149] is ready to further explore the needs and modalities for boosting the mentioned collaboration and is looking forward to supporting such cooperation.

[149] "A Trusted and Cyber Secure Europe – ENISA strategy", June 2020, https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy, accessed October 2020

5. CONCLUSIONS AND NEXT STEPS

In this report we gave a brief overview of various standardisation efforts and related technical specifications for security of 5G networks and we took a closer look at the 3GPP security specification, analysing its key security features and discussing its optional elements. We also looked at some technical aspects not directly covered by specifications and analysed some of the main security considerations. Finally, we reflected on some general aspects related to possible further directions that MS authorities may take in consideration.

In this chapter we summarize the key findings and we propose a set of good security practices that may be considered to address the findings. These can be considered by EU MS competent authorities to assist the process of policy development and implementation in the area of cybersecurity of mobile networks and to support implementation of technical measures identified in the 5G toolbox and may be of relevance for both suppliers and MNOs. The findings and good practices listed in this chapter are directly derived from the analysis conducted in Chapters 3 and 4. For each good practice, a reference is provided to the underlying document section containing the corresponding analysis.

Good practices included in the following section do not represent a definite and exhaustive list and should not be understood and interpreted as an ultimate set of minimum security requirements or as a substitute for a full set of security controls as defined in the 3GPP technical specification itself. Rather, the list represents a selection of some prominent security features, including security enhancements introduced specifically for 5G networks, and some generally recognized good practices beyond specifications, which are worth taking into account[150].

The chapter concludes with a short section discussing the proposed directions of further work.

5.1 KEY FINDINGS AND CONSIDERATIONS

Finding 1: 3GPP technical specification on security architecture and procedures for 5G system (TS 33.501) comes with a set of security features and improvements. To ensure the expected security benefits are realized, it is important that security requirements defined in the specification are fully and correctly implemented and utilised, including relevant optional requirements.

To address this finding, the following **good security practices** should be considered:

1. Ensure that UEs by default encrypts subscriber identifier SUPI to derive SUCI, utilizing a non-null protection scheme and the home network public key securely provided by the home network, in combination with ephemeral keys generated by UE (or alternative mechanism) and ensure that there is no transmitting of subscriber identifier in clear text over the access network. The protection scheme used should be ECIES or an alternative scheme that provides the same or higher level of security.

[Related document section: 3.2.1]

2. To protect data from interception and alteration, apply by default a strong, not-NULL ciphering and integrity protection algorithms (e.g. 128-NEA1 or stronger and 128-NIA1 or stronger, respectively) for both user and signalling data exchanged between the UE and the network.

[Related document section: 3.2.2]

[150] At the same time, it is also worth pointing out that not all of the listed good practices may always be fully implementable (say due to regulatory or other constraints) or there may be alternative security controls that adequately fulfil the same security objectives. It is typically for the competent authorities of EU MS to define such objectives and requirements and to evaluate their implementation (in line with the Toolbox technical measure TM02 and with other relevant policy instruments, e.g. EECC).

3. Use a secure protocol on network or transport layer (IPSec or DTLS) to implement confidentiality, integrity and replay protection by default for both user and control plane data on RAN interfaces (F1-U, F1-C, E1, N2, N3).
[Related document section: 3.2.4]

4. Apply state-of-the-art mechanisms for transport protection and mutual authentication (e.g. TLS 1.2 or 1.3 with X.509 certificates), and for authorization (e.g. OAuth 2.0) between SBA network functions, by default.
[Related document section: 3.2.5]

5. Implement authentication framework defined in the specifications, consider use of EAP for secondary authentication whenever secure authentication and authorization with external networks is required and ensure that the keys generated and distributed are adequately protected and stored.
[Related document section: 3.2.6]

6. Ensure correct implementation of specification requirements for end-to-end core network interconnection security, including the usage of identified state-of-the-art security protocols for transport (TLS) or application layer security (PRINS) between SEPPs in different networks and ensure appropriate procedures for key and certificate management.
[Related document section: 3.2.7]

7. Ensure that secure, tamper resistant hardware is used for storing and/or processing of security critical data (e.g. subscriber credential and decryption keys), such as UICC (Universal Integrated Circuit Card) in UE or HSM (Hardware Security Module) in the network and that there is a strict access control policy regulating both logical and physical access to corresponding systems and/or network functions.
[Related document section: 3.2.8]

Finding 2: Technical specifications and standards are important elements for the overall security and resilience of mobile networks. However, they only make a foundation on which other elements build on. It is important that security features defined by technical specifications and standards are properly implemented in products that suppliers supply, securely deployed and configured in the networks that operators implement and operate and that their functioning and effectiveness is tested and assessed.

To address this finding, the following **good security practices** should be considered:

8. Network components and equipment should be subjected to rigorous **security testing**. In addition to testing against the predefined set of test cases according to a standard security assurance methodology (e.g. SECAM), this should include additional security tests and assessment (e.g. negative tests, fuzzing), regular vulnerability assessments using specialised vulnerability scanning tools and periodic 3rd party penetration tests.
[Related document section: 4.1.1]

Note: Similar objectives may fully or partially be achieved by ensuring adequate assurance levels under a (future) EU-wide certification scheme[151] for 5G network components, customer equipment and/or suppliers' processes, as defined in the Toolbox technical measure TM09.

9. Product development should ensure that mandatory and optional security features are built-in, using a robust, mature and secure product development process built with security and resilience in mind (e.g. source code review process, application of coding best practices, using of static and dynamic code analysis, external code review process etc.).
[Related document section: 4.1.2]

[151] Or an equivalent national-level certification scheme, where appropriate

10. Network design, configuration and deployment shall follow security best practices. This may include having defined processes for activation of security features, for secure provisioning, for establishment of PKI infrastructure and certificate management, for hardening of the virtualization and/or cloud environment and for secure admin infrastructures and would typically also include ensuring adequate network segmentation and protection of internal interfaces from external access.

[Related document sections: 4.1.3 and 4.1.4]

11. Robust **network operation and management** processes should be put in place according to security best practices. This may include robust processes for change management according to best practices for software-based environments, strengthened access control model for privileged accounts, integrated monitoring and usage of automation and machine learning where applicable.

[Related document section: 4.1.5]

Finding 3: Standards and specifications in the area of 5G are complex, as is the underlying technology, and they are still under development, as the technology is evolving. It is important to ensure continued collaboration between EU MS and with other relevant stakeholders, including relevant standardisation bodies and private sector, so that complexities are better understood and managed, gaps are identified and addressed and the overall standardisation process is shaped according to the identified needs.

To address this finding, the following **further steps** could be considered:

A. Continue EU-facilitated coordination between MS regarding standardisation matters, including gap analysis and increased engagement of EU MS in standardisation bodies, including through the subgroup on standardisation and certification, with support of ENISA.

[Related document section: 4.2]

B. Explore the needs and possible modalities for further strengthening of collaboration among relevant actors identified in the Toolbox (relevant authorities, operators, suppliers and critical infrastructure operators) for knowledge building, experience sharing and joint work in the area of implementation of technical security measures from 5G specifications.

[Related document section: 4.2]

5.2 FOLLOW-UP

In addition to this report, ENISA has also prepared several other reports in 2020 that directly or indirectly support MS and relevant stakeholders in implementing the measures from the Toolbox, in particular those related to technical security controls. We have referred of some of them in this document.

Moving forward, ENISA plans to continue its support to relevant authorities of EU MS and intends to work on preparation of a 5G Security Controls Matrix, as a consolidated, dynamic, online repository of security controls at various levels of abstractions, from various reports, documents and standards, as to provide “one-stop shop” repository that will also be able to better respond to the dynamic nature of specifications and standards in the area of 5G security. ENISA will cooperate closely with relevant stakeholders, in particular with experts from national competent cybersecurity and regulatory authorities in undertaking this activity.

ANNEX A: TS 33.501 SECTION-BY-SECTION

In this annex we give a full list of all groups of security requirements described in TS 33.501, going section-by-section and clause-by-clause and providing a brief description of the security requirements/controls defined therein.

A.1 GENERAL REQUIREMENTS

Clause	Title	Description
5.1	**General security requirements**	Clause 5.1 states that general security requirements relate to the prevention of bidding down attacks (where the user equipment and network entities falsely believe that the other side does not support a security feature); secure authentication and authorisation (including subscription, serving network and emergency service authentication; and user equipment, serving network and access network authorisations); and the use of keys for the protection of user plane, access and non-access stratums.
5.2	**Requirements on the UE**	Clause 5.2 define a range of user equipment security requirements. The key areas considered include user and signalling data confidentiality and integrity; subscriber privacy; secure storage and processing of subscription credentials.
5.3	**Requirements on the gNB**	Clause 5.3 define a range of base station (gNB) security requirements. The key areas considered include user and signalling data confidentiality and integrity; subscriber privacy; secure storage and processing of subscription credentials; and various gNB functions (setup and configuration, key management, handling user and control plane data, protection and secrecy of all sensitive information and operations, and confidentiality, integrity and replay protection for E1 and F1 interfaces interconnecting central and distributed units).
5.4	**Requirements on the ng-eNB**	Clause 5.4 states that requirements related to the Next Generation Evolved Node-B (ng-eNB) are the same as those specified for Evolved Node-B (eNB) in TS 33.401.
5.5	**Requirements on the AMF**	Clause 5.5 contains requirements for Access And Mobility Function (AMF). This includes requirements for signalling data confidentiality and integrity (sub-clauses 5.5.1 and 5.5.2 respectively) and for subscriber privacy (5.5.3) – which includes the requirement for triggering primary authentication using SUCI.
5.6	**Requirements on the SEAF**	Clause 5.6 contains requirements for the Security Anchor Function (SEAF). In reality, there is only a single requirement defined here, which is for SEAF to support primary authentication using SUCI.
5.8	**Requirements on the UDM**	Clause 5.8 contains requirements for Unified Data Management (UDM) function. This includes requirements for protection of long-term keys and subscription credentials and for subscriber privacy requirements for UDM and SIDF, including de-concealment of SUCI. In addition, requirements on AUSF are included in this clause in relation to its role in the authentication process.
5.9	**Core network security**	Core network security requirements covering service-based architecture and end to end interconnection security requirements are outlined in Clause 5.9. Service-based architecture requirements address service registration, discovery and authorisation involving Network Function (NF), Network Repository Function (NRF), Network Exposure Function (NEF) and Service Communication Proxy (SECOP). End to end core network interconnection security requirements are mainly related to ensuring end-to-end confidentiality and integrity between source and destination network for specific message elements. This is achieved through Security Edge Protection Proxy (SEPP) which is present at the edge of source and destination networks.
5.10	**Visibility and configurability**	Clause 5.10 focuses on security of visibility. Requirements are associated with access and non-access stratum confidentiality and integrity. In addition, a user configurability feature of granting or denying access to Universal Subscriber Identity Module (USIM) without authentication is required as described in TS 33.401

Clause	Title	Description
5.11	**Requirements for algorithms, and algorithm selection**	In Clause 5.11, requirements for ciphering and integrity algorithm identifier values and algorithm selection are described
5.12	**Requirements for 5G-RG**	Residential gateway security requirements are provided in Clause 5.12. All security requirements and features defined for user equipment are required to be supported by residential gateways.

A.2 SECURITY PROCEDURES BETWEEN USER EQUIPMENT AND 5G NETWORK FUNCTIONS

The user equipment is able to select and connect Evolved Packet (4G) or 5G core networks (EPC or 5GC). This procedure is described in Clause 4.8.4 in TS 24.501. If user equipment selects a 4G core network, associated security procedures are defined in 3GPP TS 33.401. This section provides a brief of security procedures associated with the 5G core network.

Clause	Title	Description
6.1	**Primary authentication and key agreement**	Clause 6.1 states that primary authentication and key agreement procedures are part of the overall user equipment and 5G network authentication framework. The objective is mutual authentication between user equipment and the network and provision of keying material that can be used in subsequent security procedures between the user equipment and the serving network. Authentication procedures which involve a range of security functions are described in detail. It is stated that the 5G authentication and key agreement protocols provide increased home control and this provides better security useful in preventing certain types of fraud (Clause 6.1.4).
6.2	**Key hierarchy, key derivation, and distribution scheme**	Clause 6.2 provides detailed description of key hierarchy and key derivation and distribution scheme. These include keys in network entities and user equipment. Procedures for key setting, identification and lifetimes are also included.
6.3	**Security contexts**	Clause 6.3 focuses on the security contexts and covers distribution of subscriber identities and security data within and between 5G serving network domains and between 5G and Evolved Packet System (EPS) serving domains. Scenarios addressing user equipment multiple registrations in the same and different Public Land Mobile Networks (PLMNs) are also included.
6.4	**NAS security mechanisms**	Clause 6.4 describes security mechanisms associated with integrity and confidentiality of non-access stratum (NAS) signalling and data between user equipment and the Access and Mobility Management Function (AMF). These mechanisms include securing multiple active non-access stratum connections in the same and with different Public Land Mobile Networks (PLMNs); integrity algorithm, activation and failure handling; and confidentiality algorithm and activation. Procedures relating to handling of NAS COUNTs, protection of initial NAS message and security of SMS over NAS are outlined.
6.5	**RRC security mechanisms**	Clause 6.5 explains Radio Resource Control (RRC) security mechanisms. RRC integrity and confidentiality protection is provided by the Packet Data Convergence Protocol (PDCP) layer between user equipment and base station (gNB).
6.6	**UP security mechanisms**	Clause 6.6 provides User Plane (UP) security activation mechanism together with confidentiality and integrity mechanisms. These are implemented to ensure that the user traffic is not modified during transit. The Session Management Function (SMF) provides user plane security policy for a Protocol Data Unit (PDU) session to the base station (ng-eNB/gNB) during the PDU session establishment procedure as specified in TS 23.502. The user plane security policy indicates whether user plane confidentiality and/or integrity protection will be activated or not for all dedicated radio bearers belonging to that PDU session. The user plane security policy is used to activate user plane confidentiality and/or integrity for all dedicated radio bearers belonging to the PDU session. The Packet Data Convergence Protocol (PDCP), as defined in TS 38.323, between the user equipment and the 5G radio access network (NG-RAN) is responsible for user plane data confidentiality and integrity protection.

Clause	Title	Description
6.7	**Security algorithm selection, key establishment and security mode command procedure**	Procedures for non-access stratum and access stratum algorithm selection (integrity protection and ciphering algorithms) are described in Clause 6.7.
6.8	**Security handling in state transitions**	Handling of security in state transitions is the topic covered in Clause 6.8 where very detailed descriptions of key handling at connection and registration state transitions and security handling at Radio Resource Control (RRC) state transitions are provided.
6.9	**Security handling in mobility**	Clause 6.9 addresses security handling procedures used in mobility. Key handling in handover and mobility registration update; key change on the fly; and rules associated with concurrently running of security procedures are described in detail.
6.10	**Dual connectivity**	Clause 6.10 describes the security functions required to control dual connectivity when a user equipment is connected to more than one radio access node. Dual connectivity protocol architecture is provided and security mechanisms and procedures including secondary node addition or modification; secondary node key update; establishing the security context and protection of traffic between the user equipment and secondary node; handover; signalling; and radio link failure recovery are described.
6.11	**Security handling for RRC connection re-establishment procedure**	Clause 6.11 describes how security handling of Radio Resource Control (RRC) connection re-establishment (e.g. in handover failure case) is implemented.
6.12	**Subscription identifier privacy**	Mechanisms used for subscription identifier privacy are defined in Clause 6.12. These include the use of permanent, concealed and temporary subscription identifiers. The globally unique 5G subscription permanent identifier is called Subscription Permanent Identifier (SUPI). The SUPI is privacy protected over-the-air by using the Subscription Concealed Identifier (SUCI).
6.13	**Signalling procedure for PDCP COUNT check**	Clause 6.13 describes the optional procedure to be used by a base station (gNB) to periodically perform a local authentication. In parallel, the amount of data sent during the access stratum connection is periodically checked by the gNB and the user equipment by exchanging Counter Check and Counter Check Response messages. The Packet Data Convergence Protocol (PDCP) COUNT check is used to detect maliciously inserted packets. Note that packet insertion is detected automatically in integrity protected dedicated radio bearers; therefore, the PDCP COUNT check procedure is unnecessary for integrity protected bearers.
6.14	**Steering of roaming security mechanism**	Clause 6.14 describes security procedures required to support steering of the user equipment in the Visited Public Land Mobile Network (VPLMN) during and after the registration procedure. The security functions are described in the context of the functions supporting the control plane solution for steering of roaming in 5G system. In essence, steering of roaming enables the home network operator to steer its roaming customers to its preferred Visited Public Land Mobile Networks (VPLMN) to enhance roaming customers' experience and reduce roaming charges[152]. The content of Steering Information List as well as the conditions for sending it to the user equipment are described in TS 23.122.
6.15	**UE parameters update via UDM control plane procedure security mechanism**	Security mechanisms for updating user equipment parameters by using the Unified Data Management (UDM) control plane procedure are provided in Clause 6.15. These mechanisms are applied after the user equipment is successfully registered to the 5G network
6.16	**Security handling in Cellular IoT**	This clause covers exclusively CIoT (Cellular Internet of Things) and is not discussed in the scope of this document.

[152] "The Evolution of Security in 5G", 5G Americas white paper, October 2018, https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_5G_Security_White_Paper_Final.pdf, accessed October 2020

A.3 SECURITY FOR NON-3GPP ACCESS TO THE 5G CORE NETWORK

Clause	Title	Description
7.1	**Primary authentication and key agreement**	Clause 7.1 states that the procedure used for non-3GPP access to the 5G core network is defined in IETF RFC 7296 (Internet Key Exchange Protocol Version 2, IKEv2). This is used to set up one or more IP Encapsulating Security Payload (ESP) security associations defined in IETF RFC 4303. Depending on the sufficiency of security feature groups provided by the non-3GPP access network, the home public land mobile network (HPLMN) operator decides if a non-3GPP access network is to be identified as trusted or untrusted non-3GPP access network.
7.1a	**Determining trust relationship in the UE**	According to Clause 7.1a, in determining the trust relationship in the user equipment, the non-3GPP access networks, which are trusted, can be pre-configured in the user equipment. Additionally, during primary authentication the user equipment may receive an indication whether the non-3GPP IP access is trusted or not. If no such indication is received and there is no pre-configured information, the user equipment considers the non-3GPP IP access as untrusted.
7.2	**Security procedures**	Clause 7.2 specifies how a user equipment is authenticated to 5G network via an untrusted non-3GPP access network. This is based on the use of a vendor-specific Extensible Authentication Protocol (EAP) method called EAP-5G.
7A	**Security for trusted non-3GPP access to the 5G core network**	Clause 7A defines security procedures for trusted non-3GPP access to the 5G core network which is achieved when the user equipment registers to the 5G core network via the trusted non-3GPP access network. The user equipment registers to 5G core network and, at the same time, it authenticates with the trusted non-3GPP access network by using the EAP-5G procedure, similar to the one used with the registration procedure for untrusted non-3GPP access.
7B	**Security for wireline access to the 5G core network**	Clause 7B states that 5G and fixed network residential gateway entities are introduced in the 5G architecture specification to accomplish secure wireline access to the 5G core network. Associated authentication procedures are described.

A.4 SECURITY OF INTERWORKING

Clause	Title	Description
8.1	**General**	Clause 8.1 notes that the user equipment can operate in single or dual registration mode. In dual registration mode, when the target system is Evolved Package System (EPS) (4G) all security mechanisms defined in 3GPP TS 33.401 are applicable. When the target system is 5G security mechanisms defined in 33.501 are applicable.
8.2	**Registration procedure for mobility from EPS to 5GS over N26**	The registration procedure to support mobility from EPS to 5G system over N26 interface (between Access and Mobility Management Function (AMF) and Mobility Management Entity (MME)) is explained in Clause 8.2.
8.3	**Handover procedure from 5GS to EPS over N26**	The detailed procedures explaining handover from 5G system to EPS and from EPS to 5G system over N26 interface are provided in Clause 8.3 and 8.4
8.4	**Handover from EPS to 5GS over N26**	
8.5	**Idle mode mobility from 5GS to EPS over N26**	Tracking Area Update (TAU) procedure to be used by the user equipment in idle mode mobility from 5G system to EPS over N26 interface is described in Clause 8.5.
8.6	**Mapping of security contexts**	This is followed by the explanation of mapping of security contexts between 5G and EPS in Clause 8.6.
8.7	**Interworking without N26 interface in single-registration mode**	References to support interworking without N26 interface in single registration mode are provided in Clause 8.7.

A.5 SECURITY PROCEDURES FOR NON-SERVICE-BASED INTERFACES

Clause	Title	Description
9.2	**Security mechanisms for the N2 interface**	Security mechanisms for several interfaces between different security entities are described. These include N2 (Clause 9.2), N3 (Clause 9.3) and Xn (Clause 9.4) interfaces as well as DIMETER and GTP-based interfaces between 5G core and other network entities (Clause 9.5).
9.3	**Security requirements and procedures on N3**	
9.4	**Security mechanisms for the Xn interface**	
9.5	**Interfaces based on DIAMETER or GTP**	
9.8	**Security mechanisms for protection of the gNB internal interfaces**	For the protection of base station (gNB) internal interfaces supporting the split architecture, security mechanisms for F1 and E1 interfaces are described in Clause 9.8.
9.9	**Security mechanisms for non-SBA interfaces internal to the 5GC and between PLMNs**	In addition, security mechanisms related to N2, N3, N4, N9 and N32 interfaces are defined in the context of non-service based 5G architecture and Wireline 5G Access Network (W-5GAN) under Clause 9.9 and 9.10.
9.10	**Security mechanisms for the interface between W-5GAN and 5GC**	

A.6 SECURITY ASPECTS OF IMS EMERGENCY SESSION HANDLING

Clause	Title	Description
10.2	**Security procedures and their applicability**	Security procedures for authenticated and unauthenticated emergency sessions are described in Clause 10.2. Scenarios where these sessions can be supported are defined together with the key generation and handover procedures associated with unauthenticated emergency sessions.

A.7 SECURITY PROCEDURES BETWEEN UE AND EXTERNAL DATA NETWORKS VIA THE 5G NETWORK

Clause	Title	Description
11.1	**EAP based secondary authentication by an external DN-AAA server**	Optional initial authentication and re-authentication procedures between the user equipment and external data network are defined in Clause 11.1. These are achieved through the implementation of Extensible Authentication Protocol (EAP) defined in IETF RFC 3748

A.8 SECURITY ASPECTS OF NETWORK EXPOSURE FUNCTION (NEF)

Clause	Title	Description
12.2	**Mutual authentication**	The Network Exposure Function (NEF) is used by Network Functions to securely expose capabilities to 3rd party Application Functions which are authenticated and authorised. Application Functions can also provide information within the network via NEF. References addressing the security aspects of NEF are provided in Clause 12.1 – 12.5. These include • 3GPP TS 33.210 (Clause 6.2) – certificate-based authentication profiles for mutual authentication and integrity protection, replay protection and confidentiality protection for the interface between the Network Exposure Function (NEF) and the Application Function. • IETF RFC 6749 – OAuth-based authorisation mechanism for authorising requests from the Application Function. • TS 33.122 (Clause 6.5.2) - mutual authentication and protection of the Network Exposure Function (NEF) – Application Function interface when NEF supports the Common Application Programming Interface Framework (CAPIF).
12.3	**Protection of the NEF-AF interface**	
12.4	**Authorization of Application Function's requests**	
12.5	**Support for CAPIF**	

A.9 SERVICE BASED INTERFACES (SBI)

Clause	Title	Description
13	**Service Based Interfaces (SBI)**	Under Clause 13, the detailed description of protection mechanisms at the transport layer is provided. It is stated that the transport layer security profile defined in 3GPP 33.210 is adopted. It is also required that the transport layer security profile needs to be complaint with the profile given by HTTP/2 defined in IETF RFC 7540 (Hypertext Transfer Protocol Version 2 (HTTP/2)).
13.1	**Protection at the network or transport layer**	Procedures for the transport layer security between Network Function and Security Edge Protection Proxy (SEPP) and between Security Edge Protection Proxies are explained in Clause 13.1.
13.2	**Application layer security on the N32 interface**	Clauses related to the application layer security on the N32 interface are provided under Clause 13.2. Security Edge Protection Proxies allow secure communication between service-consuming and a service-producing Network Functions in different public land mobile networks.
13.3	**Authentication and static authorization**	This is followed by the detailed descriptions of authentication and authorisation methods involving Network Functions and Security Edge Protection Proxies in Clause 13.3 – 13.5. In particular, an extensive explanation of OAuth 2.0 authorisation framework (specified in IETF RFC 6749) is provided in Clause 13.4 in the context of authorisation for Network Function (NF) service access within the Public Land Mobile network (PLMN) and roaming scenarios.
13.4	**Authorization of NF service access**	
13.5	**Security capability negotiation between SEPPs**	

A.10 SECURITY RELATED SERVICES

Clause	Title	Description
14.1	**Services provided by AUSF**	Services provided by Authentication Server Function (AUSF) are described under Clause 14.1. These include: • Nausf_UEAuthentication; • Nausf_SoRProtection; • Nausf_UPUProtection;
14.2	**Services provided by UDM**	Services provided by Unified Data Management (UDM) are described under Clause 14.2. These include: • Nudm_UEAuthentication_Get; • Nudm_UEAuthentication_ResultConfirmation
14.3	**Services provided by NRF**	Services provided by Network Repository Function (NRF) are described under Clause 14.3. These include: • Nnrf_AccessToken_Get.
14.4	**Services provided by NSSAAF**	Services provided by Network Slice Specific Authentication and Authorisation Function (NSSAAF) are described under Clause 14.4. These include: • Nnssaaf_NSSAA_Authenticate • Nnssaaf_NSSAA_Re-AuthenticationNotification • Nnssaaf_NSSAA_RevocationNotification

A.11 MANAGEMENT SECURITY FOR NETWORK SLICES

5G management systems provide management services that cover the creation, modification and termination of Network Slice Instance (NSI). In **Clause 15**, a brief explanation of mutual authentication and authorisation procedures associated with the security of network slices is provided by identifying reference 3GPP and IETF specifications. These include:

1. 3GPP TS 28.533 - standardised service interfaces for accessing a management service;
2. 3GPP TS 33.210 – transport layer security client and server certificates with the profiles;
3. IETF RFC 4279 and RFC 8446 - transport layer security pre-shared keys; and
4. IETF RFC 6749 – authorisation mechanism.

A.12 ANNEXES

Annex	Title	Description	Normative/ informative
Annex A	**Key derivation functions**	Specifies how to construct the input string and the input key for each distinct use of the Key Definition Function defined in 3GPP TS 33.220.	**normative**
Annex B	**Using additional EAP methods for primary authentication**	Describes an example of the usage of additional Extensible Authentication Protocol (EAP) methods for primary authentication in private networks using the 5G system as specified in 3GPP TS 22.261. More specifically, how the 5G authentication framework for primary authentication can be applied to Extensible Authentication Protocol methods other than Extensible Authentication Protocol - Authentication and Key Agreement (ESP-AKA) is provided.	**informative**
Annex C	**Protection schemes for concealing the subscription permanent identifier**	Defines the protection schemes used for concealing the subscription permanent identifier. These include 'Null-scheme' and 'Elliptic Curve Integrated Encryption Scheme'.	**normative**
Annex D	**Algorithms for ciphering and integrity protection**	Provides the algorithms used for confidentiality and integrity protection.	**normative**
Annex E	**UE-assisted network-based detection of false base station**	Gives brief examples of how measurement reports from user equipment could be used for the detection of false base stations and actions to be followed afterwards.	**informative**

Annex	Title	Description	Normative/ informative
Annex F	**3GPP 5G profile for EAP-AKA'**	Describes the 3GPP 5G profile for Extensible Authentication Protocol - Authentication and Key Agreement (ESP-AKA) described in IETF RFC 5448 and RFC 4187. Topics covered include subscriber privacy, subscriber identity and key derivation.	**normative**
Annex G	**Application layer security on the N32 interface**	Provides information related to the application layer security on the N32 interface which includes exchange of HTTP signalling messages among Access and Mobility Management Function (AMF), Authentication Server Function (AUSF) and Security Edge Protection Proxy (SEPP).	**informative**
Annex I	**Non-public networks**	Provides details on security for non-public networks by specifying exceptions to the normal procedures adopted for securing public networks.	**normative**
Annex J	**SRVCC from 5G to UTRAN**	Specifies the security aspect of supporting Single Radio Voice Call Continuity (SRVCC) session and emergency call in SRVCC from 5G to UTRAN. The keys used to protect the SRVCC session are based on security context mapping from 5G to E-UTRAN.	**normative**
Annex K	**Security for 5GLAN services**	Provides a brief note on authentication and authorisation of user equipment in 5G LAN services (described in 3GPP TS 23.501 and 502). This is based on the secondary authentication procedures between user equipment and external data networks described earlier.	**normative**
Annex L	**Security for TSC service**	Outlines the procedures for access security and protection of user plane data for 5G Time Sensitive Communication (TSC) service (described in 3GPP TS 23.501).	**normative**
Annex M	**Security for integrated access and Backhaul (IAB)**	Provides the security procedures applied to New Radio Integrated Access and Backhaul (NR IAB) architecture and functional entities for supporting wireless backhauling of NR base stations. These include IAB node integration, authentication and authorisation procedures. IAB architecture and functional entities are described in 3GPP TS 23.501 and 3GPP TS 38.401.	**normative**
Annex N	**Security for UTLLC services**	Describes the additional security features used for supporting Ultra-Reliable Low-Latency Communication (URLLC).	**normative**
Annex O	**Authentication for non-5G capable devices behind residential gateways**	Outlines the authentication procedure for Non-5G Capable (N5GC) devices behind Residential Gateways (RGs) in private networks or in isolated deployment scenarios (i.e. no roaming) with wireline access	**informative**
Annex P	**Security aspects of DNS and ICMP**	Specifies security measures to protect DNS and ICMP messages. These security measures are intended when integrity protection over the user plane cannot be used.	**informative**
Annex Q	**Security and privacy in 5G system location services**	This annex only states that for security and privacy in 5GS LCS (5G System Location Services), the mechanisms defined in TS 23.273 and TS 38.305 apply.	**informative**
Annex R	**Authorization aspects in communication models for NF/NF services interaction**	Includes a graphical overview of the authorization aspects in the different models that NF and NF services can use to interact with each other.	**informative**
Annex S	**Change history**	Provides the change history of 3GPP TS 33.501	**informative**

TP-09-21-009-EN-N

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 here: 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: 978-92-9204-472-5
DOI: 10.2824/30076