Overview on the Security in 5G Phase 2

Noamen Ben Henda

Ericsson, Torshamnsgatan 23, 164 40 Stockholm, Sweden
E-mail: noamen.ben.henda@ericsson.com

Received 26 October 2019; Accepted 28 November 2019;
Publication 04 January 2020

Abstract

During the early development stages of the 5G specifications by 3GPP, it was quickly identified that it is not possible to address all the use cases of the 5G System within the normal Release timeframe. Therefore, it was decided to split the work in two phases. The 5G Phase 1 work focused on the foundation of the new system while 5G Phase 2 focused more on the needed enhancements to address the use cases. The work on the security in 5G Phase 1 was ample enough to deliver all the needed mechanisms not only to secure the communication between the different entities but also to protect the privacy of the user. Therefore, it is expected that the work on 5G Phase 2 will unlikely have impact on the security mechanisms. Nevertheless, some of the new features in 5G Phase 2 give rise to subtle security challenges which may require enhancements to the existing mechanisms. In this article, we consider some of the 5G Phase 2 features and shed light on such security aspects.

Keywords: 3GPP, 5G, security, privacy.

1 Introduction

5G is the most recent standard developed by the 3rd Generation Partnership Project (3GPP) [1] for the next generation of mobile networks, a.k.a. 5G Systems. 5G integrates both the Long-Term Evolution (LTE) and the New

Journal of ICT, Vol. 8_1, 1–14. *River Publishers*
doi: 10.13052/jicts2245-800X.811

Radio (NR) technologies, and focuses on three important uses cases, namely, enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communication (URLLC) and massive Machine Type Communication (mMTC).

5G Systems are expected to create an ecosystem involving vertical markets such as agriculture, healthcare, energy, automotive, manufacturing and public safety which takes mobile networks one step further beyond the normal use cases of providing telephony and internet access services [2]. This resulted in a large variety of requirements ranging from high bandwidth and ultra-low latency to reliability and security, the latter being increasingly at focus nowadays.

This focus is not only due to the amplitude and media coverage of the recent attacks [3] but also due to the general public increasing awareness of aspects such as end user privacy on which we cite the latest large-scale initiative and effort by the EU law makers that led to the adoption of the General Data Protection Regulation (GDPR) [4].

In mobile communication systems, security, has been continuously evolving throughout the different generations from the point where no security at all was provided for the traffic over the air interface in GSM to a multi layered security in LTE. The trend continues with 5G. In fact, 5G builds on top of the security features of LTE and further enhances them with the introduction of for example the support of the Extensible Authentication Protocol (EAP) [5], user plane integrity, the Subscription Permanent Identifier (SUPI) privacy, etc.

Now during the early development stages of the 5G specifications by 3GPP, it was quickly identified that it was not possible to address all the requirements and features expected in 5G Systems within the normal Release timeframe of 15 to 24 months. Therefore, it was decided to split the work in two phases. 5G Phase 1 work was performed in Release 15 which was frozen, i.e. finalized in 3GPP terminology, in August 2018. The work on 5G Phase 2 is currently ongoing and is planned to be completed in March 2020.

In this article, we consider some of the most anticipated features covered in the work on 5G Phase 2 and we provide an outlook of the corresponding security aspects studied by 3GPP but first, we give an overview of the security in 5G Systems as defined during the Phase 1 work.

2 Overview of 5G Security in Phase 1

Figure 1 below illustrates a simplified architecture of the 5G System including only the security related functions. In general, a 5G System consists of

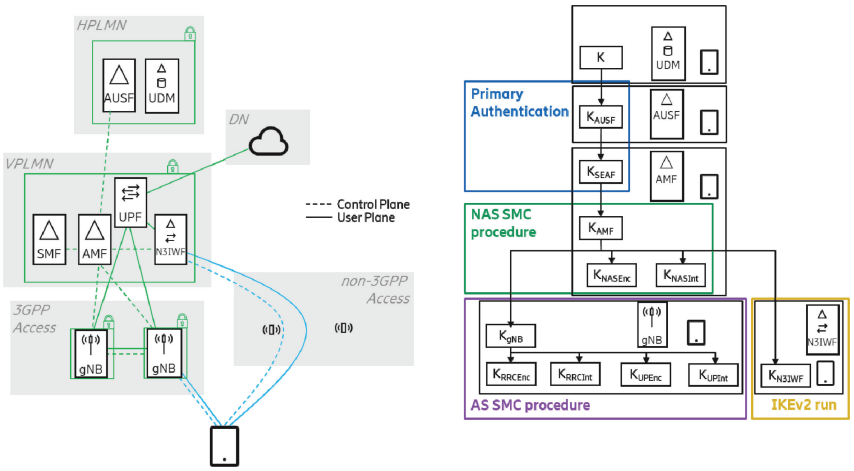

Figure 1 5G security architecture and key hierarchy [6].

the access network and the core network. The access network comprises the Next Generation Node B's (gNB) which are the 5G base stations. The core network is at the heart of the operator network and contains the functions for the management and delivery of the different services to the User Equipment (UE), terminal or device in 3GPP specifications. The core functions include the Authentication Server Function (AUSF), the Access and Mobility Function (AMF), a.k.a. MME in LTE, the Unified Data Management function (UDM) where the user subscription profiles are stored, etc. Whenever the user is roaming, both core networks of the home and the roaming operators are involved.

The security features of the 5G System can be partitioned in two groups. First, there is the group of all the features necessary to secure the communication between the UE and the network over the air interface, i.e. between the UE and the base station. Then, there is the group of non-UE-specific features needed to secure the communication between the different network functions such as between the access and the core network, i.e. the backhaul network interfaces (see Figure 1).

Between the UE and the network, security is provided at two levels or strata. The first level is the Access Stratum (AS) for the protection of the control and user planes between the UE and the gNB carried over the Packet Data Convergence Protocol (PDCP). The second level is the Non-Access Stratum (NAS) for the protection of the control plane between the UE and the core network carried over the NAS protocol.

The bootstrapping of the security starts in the initial registration, or what used to be called initial attachment in LTE. During initial registration mutual authentication between the UE and the network is achieved by a run of the Primary Authentication procedure [6]. 5G supports two variants of this authentication procedure. The first one is an enhanced version of the Authentication and Key Agreement procedure (AKA) developed for earlier generations, called 5G-AKA. The second one is an EAP-based procedure called EAP-AKA′ specified in [12] and developed for LTE for authentication of UEs over non-3GPP type of access networks such as WLAN.

5G mandates the use of different session keys for specific protocols and purposes between the UE, and the network entities. Those keys are organized in a hierarchy (see Figure 1). At the root of the hierarchy is a key that is shared between the UDM in the home network and the UE where it is securely kept in a smart card.

This level of granularity in the key hierarchy was deemed necessary to meet the stringent requirements for isolation and key separation. Mobility of the UE incurs mobility of the security anchor points within the network, i.e. change of the gNB or the AMF serving the UE. Therefore, it is important to adhere to the principle of compartmentalization so that a compromise of one key in one network entity does not spread to the other entities.

The Primary Authentication is based on the root key. The other keys are subsequently derived from keys higher in the hierarchy during other dedicated procedures. Each key in the hierarchy is shared between the UE and a particular entity, now called function, in the network. For example, the $\mathrm{K_{AUSF}}$ key is shared with the AUSF; the $\mathrm{K_{SEAF}}$ and $\mathrm{K_{AMF}}$ keys are shared with the AMF; the $\mathrm{K_{gNB}}$ key is shared with the gNB.

The 5G specifications define specific procedures for the establishment of each key in the hierarchy. For instance, the $\mathrm{K_{AUSF}}$ and $\mathrm{K_{SEAF}}$ keys are established by the Primary Authentication procedure which runs between the UE and the AUSF. While the $\mathrm{K_{AUSF}}$ key remains in the AUSF, the $\mathrm{K_{SEAF}}$ is sent to the target AMF serving the UE and later used for the derivation of the $\mathrm{K_{AMF}}$ key.

The $\mathrm{K_{gNB}}$ is initially established by a combination of procedures involving the AMF, the gNB, and the UE. The UE and AMF use the $\mathrm{K_{AMF}}$ to agree on a $\mathrm{K_{gNB}}$. The AMF then provides this key to the gNB, through which the UE is connected to the network, and which finally activates the security over the air interface between the UE and the base station based on the $\mathrm{K_{gNB}}$.

More details on 5G security could be found in [6, 7].

3 Security in 5G Phase 2

In this section we consider some of the features introduced in 5G Phase 2 and present their most relevant security aspects. Typically, in 3GPP, the work on a new feature goes through two cycles. First, there is the study cycle in which issues and solutions are discussed and documented in a Technical Report (TR). Then, there is the normative cycle during which few of the study solutions are selected and described in a Technical Specification (TS).

For a given feature, there might be several aspects that must be taken into consideration. These different aspects are typically in the remit of separate Working Groups (WG) in 3GPP. For example, security aspects are covered by the security working group (WG3 or SA3) while architectural aspects are covered by (WG2 or SA2).

All the security mechanisms and issues mentioned in this section are described in detail in various SA3 TRs.

3.1 Authentication and Key Management for Applications

The Authentication and Key Management for Applications (AKMA) framework [8, 9] is a new feature being developed by SA3 similar to the Generic Bootstrapping Architecture (GBA) [10] feature specified for earlier generations. The goal is to leverage an operator authentication infrastructure in order to bootstrap security between the UE and an Application Function (AF). In fact, since the UE has already a subscription to access the network and thus shares security key with a given operator, such keys can as well be used to establish a secure channel for other purposes such as to secure communication with an application service provider, e.g. bank, taxes office, social security services, etc.

The earlier feature, i.e. GBA, was intended to be access agnostic and hence the requirement was that the UE has only IP connectivity. Therefore, the GBA was shipped with a new Bootstrapping Server Function (BSF) for the sole purpose of authenticating the UE and maintaining the security context intended to be used to derive further keys for applications. In this regard, the key difference in the 5G System is that a UE can be registered in, or attached to, the network both over 3GPP or non-3GPP access. More precisely, in 5G, a UE can still be authenticated and reachable by the network, e.g. over Wi-Fi. In addition, the key hierarchy in the 5G System includes a new key K_{AUSF} shared between the UE and the home network.

Following these observations, several questions arise (see Figure 2). Is it still required for AKMA to introduce a new *anchor* function such as the BSF

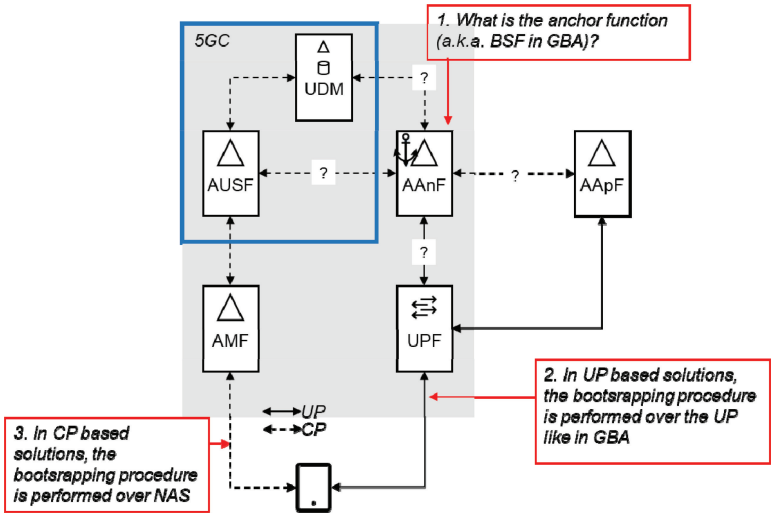

Figure 2 AKMA architecture.

in GBA? Is it also still required to support a separate authentication procedure for AKMA purposes knowing that there is always already a key, i.e. K_{AUSF}, that can be used for registered UEs? If such authentication procedure is needed, would it then be supported over the User Plane like for GBA (HTTP Digest AKA [11]) or the Control Plane? etc.

3.2 Integrated Access Backhaul

The Integrated Access Backhaul (IAB) is a new feature developed by the RAN groups in 3GPP and for which SA3 is currently studying the security aspects [13]. This feature is intended to enhance the coverage and boost the performance over the New Radio (NR) technology of 5G. This is related to the so-called split architecture introduced already in 5G Phase 1 and where a gNB can be split into a Central Unit (CU) and a Distributed Unit (DU) with a new interface called F1 in between. The goal is to allow deploying lower protocol layer devices such as antennas further away in the field to provide a better coverage and cater for the limitation, in terms of range, of the NR technology.

The IAB feature builds further on the split by including additional nodes on the "access path" namely IAB-donor nodes and IAB nodes connected over a wireless backhaul in contrast to the more conventional wired one (see Figure 3). This would further enhance coverage and also would allow

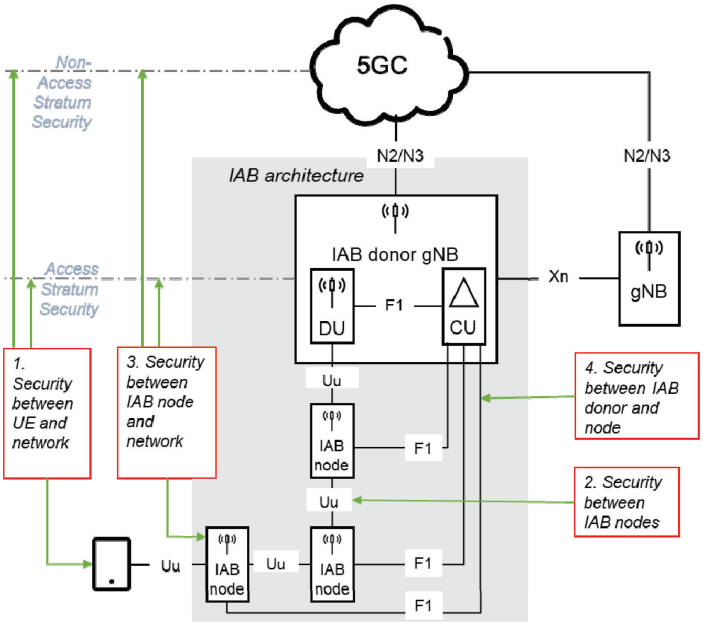

Figure 3 IAB architecture.

a certain type of dynamicity so that such IAB nodes can be deployed and enrolled on demand, e.g. to allow better service quality during large events, e.g. festivals or tournaments.

For IAB nodes it was quickly decided in 3GPP that they will support some of the UE capabilities for authorization and configuration aspects. More precisely, IAB nodes are expected to be authenticated by the networks, to establish NAS and AS security and to be provisioned by the necessary parameters in order to establish a backhaul connection with the IAB donor nodes. This backhaul connection is not only expected to carry the signalling traffic between the IAB node and the CU, it is also expected to carry all the signalling and user data traffic pertaining to UEs attached to the network through the IAB node in question.

For this purpose, SA3 is currently studying the following aspects: How is security established between an IAB node and the network? Is there impact on the UE security procedures, should they register through IAB nodes? What are the required security mechanisms for the protection of the backhaul traffic which is conventionally realized by IPsec and DTLS protocols? Finally, are there any security issues related to the signalling traffic between IAB nodes?

3.3 Study on Security Aspects of 3GPP Support for Advanced V2X Services

For vehicular communications, 3GPP has undertaken the effort to enhance the 5G System in order to support the so-called vehicle-to-everything (V2X) services. Such communication is to be supported not only over the usual air interface Uu between the UE and the network, but also over the PC5 interface a.k.a. the side channel (See Figure 4). The security study carried by SA3 is recorded in [14].

While for V2X communication over Uu not much security impact is expected since the existing mechanisms for UE to secure that link could be used, for the sidelink the situation is more challenging. In fact, for V2X, PC5 will support broadcast, groupcast and unicast communication. In addition, sidelink communication is expected to work off coverage and even between UEs that have subscriptions with different operators. Such requirements then automatically apply to any security solution for protecting the sidelink communication.

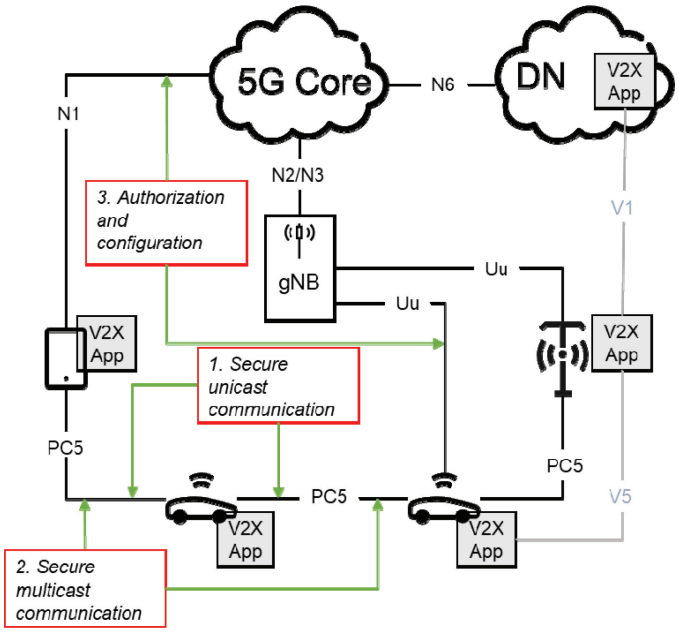

Figure 4 V2X architecture in 5G.

Moreover, the sidelink is expected to carry both signalling (RRC/PDCP) and user data massages (e.g. IP/PDCP) like over the Uu interface. For the Uu interface the K_{gNB} key which is shared between the UE and the network is used, but for the PC5 interface, it is not clear how can such key be established especially between UEs potentially out of network coverage.

Furthermore, SA3 is also studying the privacy issue related to the fact that vehicle UEs will expose various source and destination identifiers (layer 2, IP, application layer) while engaging in sidelink communication. For example, if not changed regularly and in an unpredictable manner, the source identifiers can be used by an eavesdropper to track UEs.

3.4 Enhancements of 5GS for Vertical and Local Area Network (LAN) Services

The work on enhancements to the 5G System for the support of verticals and Local Area Network, a.k.a. Vertical_LAN together with the CIoT and URLLC is targeting the so called "factory case". This is to allow verticals to deploy their own 5G System and to provide services to their devices either in a standalone manner or with the help of an operator in an integrated manner.

One of the key aspects to facilitate the integration of the 5G System in the Vertical legacy environment is the credentials, both management and use, for the various devices and users of the system. In IT environment this is typically realized by an Authentication, Authorization and Accounting infrastructure (AAA) using protocols like Radius and Diameter. This is one of the issues that SA3 is currently studying [15] and in fact it is not clear yet whether any enhancement would be needed since the 5G System already supports the EAP protocol for the primary authentication (Section 2) and EAP integrates well with AAA protocols (See Figure 5).

Another security issue arises for the LAN services. More precisely, the new group communication feature which allows UEs attached to the network over 3GPP radio to establish LAN groups and communicate with each other similarly to how it is done in conventional IT networks. The difference here is that the UEs will not communicate directly with each other but indirectly through the network each over a separate user data connection with the network. The challenge is due to the introduction of the User Plane (UP) Security Policy in Release 15, a concept which allow the network to negotiate and activate the security features separately for each user data connection [6]. Such UP Security Policy amounts to whether integrity or/and confidentiality protection is to be activated or not.

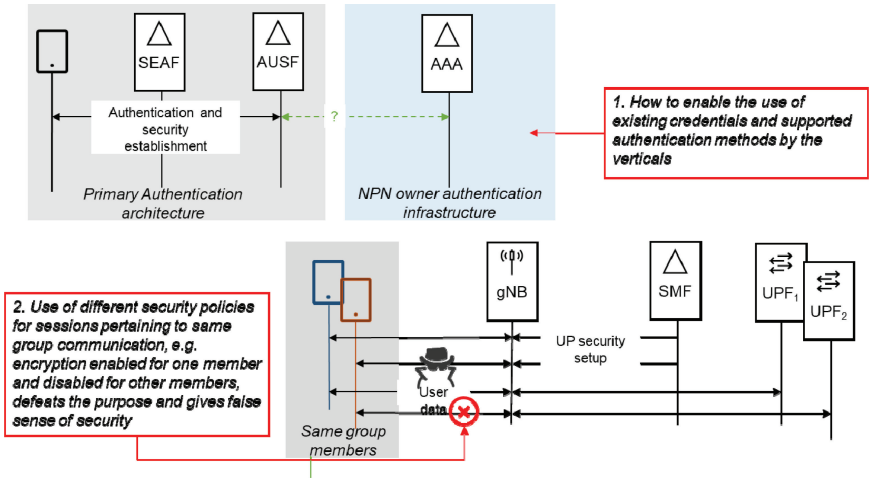

Figure 5 Security aspects in Vertical_LAN.

The observation now is that for the LAN group communication, if different policies are applied to the user data connections of all the UEs pertaining to the same group, then there is a risk that the group traffic could be confidentiality protected on some of communication links but in clear on other links. This would compromise and hence defeat the purpose of the protection.

3.5 Ultra-Reliable Low Latency Communication

The work on Ultra Reliable and Low Latency Communication is targeting one of the most important use cases of the 5G System. This is in order to meet the requirement of certain mission critical applications. For applications requiring a high degree of reliability, it was decided by 3GPP to leverage the Dual Connectivity (DC) architecture to realize the support of two parallel paths for the redundant transmission of such application data.

Dual Connectivity is a feature introduced already in LTE and which enables a UE to establish parallel user data connections over two base stations one of them endorsing the role of the Master Node (MN) and the other the Secondary Node (SN). Since DC was also adopted in 5G Phase 1, it was then straightforward to use it to provide the needed support for redundant user data paths for certain applications.

Now there are few subtle security aspects [16] related to redundant transmission of the same user data from the same UE simultaneously. The

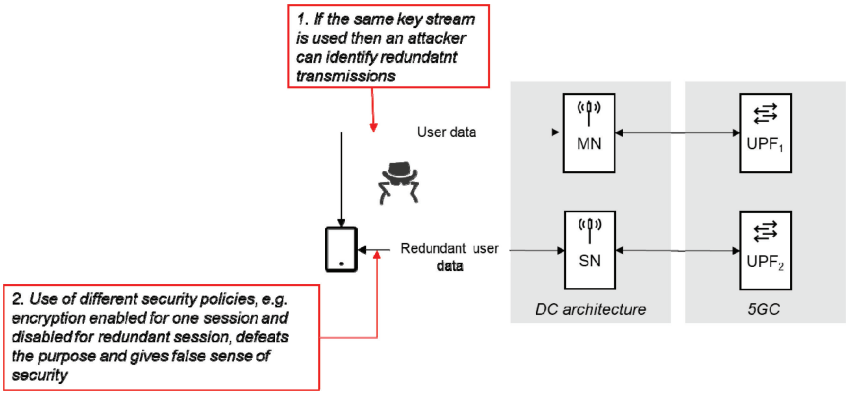

Figure 6 Security aspects in URLLC.

first is that in case the same key stream is used then an eavesdropper can identify redundant transmission and target the attack to whatever critical application making use of the feature. The second aspect is related to the UP Security Policy concept and is similar to the LAN group communication issue described in Section 3.4. The use of different security policies for each of the user data connection pertaining to the same data transmission may compromise the overall protection, e.g. it may lead to confidentiality protection being activated for one connection but not for the redundant one.

3.6 Security Assurance Specifications for 5G

The work on the Security Assurance Specification (SCAS) for 5G network functions is a continuation of the work started already for LTE nodes. In fact, back during the development of LTE, 3GPP in collaboration with GSMA undertook a big effort to define procedures for not only the certification of network products but also accreditation of security testing laboratories. In this process, 3GPP has the responsibility to develop test specifications (SCASes) for the different network products. For LTE, 3GPP developed SCASes for the eNB, MME and PDN-GW nodes.

Figure 7 below shows the different SCASes developed for the 5G System. There is a total of 9 SCAS specifications, one for every 5G network function that has some security functionality. Furthermore, SA3 has also two ongoing studies related to virtualization. One is focusing on the security impact of virtualization [17] while the other on how to adapt the security assurance methodology and procedures for virtualized network products [18].

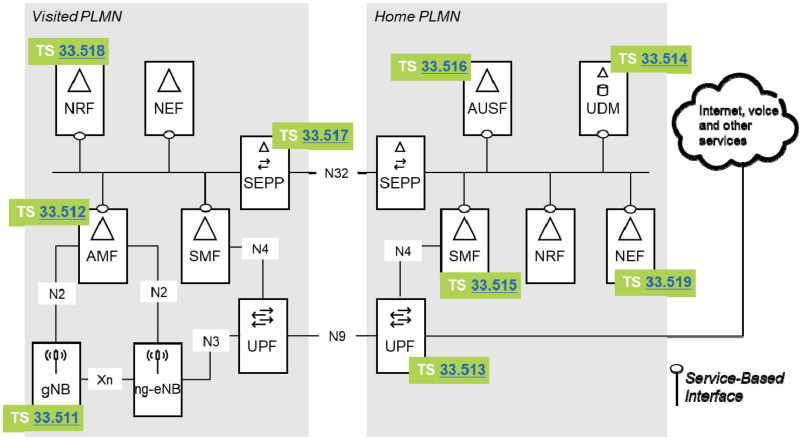

Figure 7 Security assurance specifications for 5G network functions.

4 Conclusion

In this article, we provided a quick overview of the security in 5G Phase 1. Then we considered some of the new features being developed in 5G Phase 2 and described some of the corresponding security aspects studied in SA3. Currently, there are many other ongoing security studies in SA3 among which we can site, e.g., the study on 5G security enhancements against false base stations [19], the study on authentication enhancements in the 5G System [20], the study key issues and potential solutions for Integrity protection of the User Plane [21], etc. In fact, for 5G Phase 2, SA3 had a record breaking number of topics to cover. Therefore, as future work, it would be interesting to provide an overview of the other Release 16 security topics not covered in this article. Another possibility is to provide an assessment of the outcome of the security studies and the actual security mechanisms and enhancement that ended up in the specifications.

References

[1] https://www.3gpp.org/
[2] 3GPP TS 22.261: “Service requirements for next generation new services and markets”.
[3] D. Rupprecht, K. Kohls, T. Holz, C. Pöpper: “Breaking LTE on Layer Two” ‘Designing power-efficient WDM ring networks’, 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, 2019.

[4] https://edpb.europa.eu/edpb_en
[5] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz: [RFC3748] "Extensible Authentication Protocol (EAP)", IETF, June 2004.
[6] 3GPP TS 33.501: "Security architecture and procedures for 5G System".
[7] A. R. Prasad, S. Arumugam, B. Sheeba, A. Zugenmaier: "3GPP 5G Security", Journal of ICT, Vol. 6 1&2, 137–158. River Publishers, May 2018.
[8] 3GPP TR 33.835: "Study on authentication and key management for applications based on 3GPP credential in 5G".
[9] 3GPP TS 33.535: "Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)".
[10] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".
[11] A. Niemi, J. Arkko, V. Torvinen: [RFC3310] "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", IETF, September 2002.
[12] J. Arkko, V. Lehtovirta, P. Eronen: [RFC5448] "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", IETF, May 2009.
[13] 3GPP TR 33.824: "Study on security aspects of Integrated Access and Backhaul (IAB) for Next Radio (NR)".
[14] 3GPP TR 33.836: "Study on security aspects of 3GPP support for advanced V2X services".
[15] 3GPP TR 33.819: "Study on security enhancements of 5GS for vertical and Local Area Network (LAN) services".
[16] 3GPP TR 33.825: "Study on the security of Ultra-Reliable Low-Latency Communication (URLLC) for the 5G System (5GS)".
[17] 3GPP TR 33.848: "Study on security impacts of virtualisation".
[18] 3GPP TR 33.818: "Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products".
[19] 3GPP TR 33.809: "Study on 5G security enhancements against false base stations".
[20] 3GPP TR 33.846: "Study on authentication enhancements in the 5G System (5GS)"
[21] 3GPP TR 33.853: "key issues and potential solutions for Integrity protection of the User Plane".

Biography

Noamen Ben Henda is currently the chairman of SA3, the security working group of 3GPP. He was elected for the position in May 2019. Within Ericsson, Noamen Ben Henda holds the title of Master Researcher Security in the global Ericsson Research organization. His responsibilities include driving 3GPP security standardization and related research. After a Bachelor degree in fundamental sciences, Noamen obtained a Master of Science degree in Information Technology in 2002 and a Ph.D. in theoretical computer science in 2008 from Uppsala University in Sweden. When he joined Ericsson in 2013, Noamen's main interest was in software security. More specifically, he has been driving research activities related to the formal verification of security protocols. Noamen joined the Ericsson SA3 team in 2015 and has since been contributing to several studies and work items. Notably, Noamen has been heavily involved in the development of the 5G security standards. In 2018, Noamen assumed the role of Ericsson's technical coordinator for SA3 and head of the delegation. Before joining Ericsson, Noamen worked as an application engineer for safety-critical systems.