New 3GPP Security Features in 5G Phase 1

Andreas Kunz[1], Xiaowei Zhang[2]

Lenovo, Oberursel, Germany[1]
Detecon International, Cologne, Germany[2]

Email: akunz@lenovo.com, xiaowei.zhang@detecon.com

Abstract — The Third Generation Partnership Project 3GPP finished the normative specifications of 5th Generation Wireless System 5G Phase 1 in 3GPP Release 15. While many new ideas and approaches were discussed and evaluated in the study phase for security aspects, the final specification is often different due to the consensus process of all stakeholders. This paper provides an overview of the new security features compared to the Evolved Packet System, which have passed the conclusions of the study and the final step into the normative specification in 3GPP for 5G Phase 1.

Index Terms – 5G, NextGen, Security, 3GPP, Standards,.

I. INTRODUCTION

5G became a synonym for a new network that is integrating different technologies from different disciplines, and is not limited only to the mobile network infrastructure. Still the mobile network operators are driving these technology developments for new services and business opportunities so that the official standard for 5G is specified in 3GPP.

In [1], we already provided a preview on what the 5G security aspects of the 5G standard in 3GPP TS 33.501 [2] would look like, but standardization is a constant process of change so that some of those decisions were revised due to various reasons. This paper is explaining the latest agreements just before the normative specification is going to be closed for 3GPP Release 15.

The paper is structured further as follows: in section II, we provide an overview of the 5G security architecture and in section III the new authentication variants for primary authentication. Section IV is explaining the key hierarchy and V the new feature of multiple NAS connections. The new decisions with respect to user plane security are shown in section VI and the 5G privacy enhancements compared to EPS are explained in section VII. Further, the new secondary authentication is described in section VIII and the security aspects of the Service Based Architecture in section IX. In Section X we draw the conclusions and give an outlook to the security aspects of 5G Phase 2.

The abbreviations known from 3GPP specifications are also used in the rest of this paper and are listed in the following Table 1.

Table 1: List of Abbreviations

3GPP	Third Generation Partnership Project
5G	5th Generation Wireless System
5GC	5G core network
AAA	Authentication, Authorization, Accounting
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
ARPF	Authentication credential Repository and Processing Function
AUSF	Authentication Server Function
AV	Authentication Vector
DRB	Data Radio Bearers
EAP	Extensible Authentication Protocol
EPS	Evolved Packet System
gNB	Next generation NodeB
GUTI	Globally Unique Temporary Identifier
IMSI	International Mobile Subscriber Identity
MCC	Mobile Country Code
MNC	Mobile Network Code
NAS	Non Access Stratum
NDS	Network Domain Security
NF	Network functions
NR	New Radio
NRF	Network Repository Function
PDU	Protocol Data Unit
(R)AN	(Radio) Access Network
RRC	Radio Resource Control
SBA	Service Based Architecture
SEAF	SEcurity Anchor Function
SMF	Session Management Function
SUCI	SUbscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
UDM	Unified Data Management
UE	User Equipment
UP	User Plane
USIM	Universal Subscriber Identity Module

II. 5G SECURITY ARCHITECTURE

The preliminary 5G network architecture and new features were introduced in [1]. In this paper, we describe the final defined security architecture by 3GPP [2]. Figure 1 below

shows the different security domains that are subject to the security work within 3GPP.

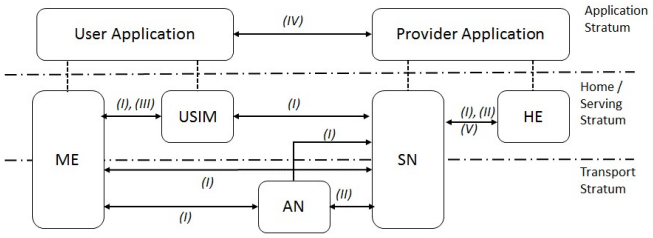

Figure 1: Security Domains in 3GPP

There are six security domains defined, which are (I). Network access security, (including both 3GPP and non-3GPP access) (II): Network domain security, (III). User domain security, (IV). Application domain security, (V). SBA domain security, (newly defined in 5G, including network element registration, discovery, and authorization, and service-based interface protection), and (VI). Visibility and configurability of security.

The high-level security architecture for the non-roaming case is shown in Figure 2, and the complete 5G system architecture can be found in 3GPP TS 23.501 [3].

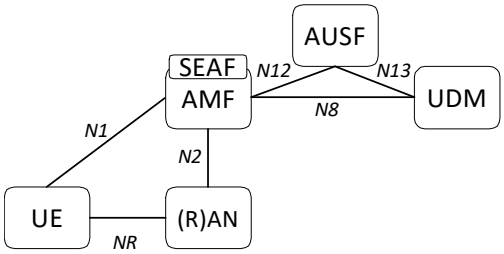

Figure 2: High-Level Security Architecture

The UDM stores the subscription information and generates the 3GPP authentication credentials. The AUSF handles the authentication requests for 3GPP access and non-3GPP access. The SEAF is co-located with the AMF in Release 15, but this may change in Phase 2 within Release 16. The AMF is terminating the 5G-NAS protocol between UE and AMF for session management and mobility management, which is carrying the authentication related messages. The (R)AN is the 5G base station. In the roaming architecture, a new network element named Security Edge Protection Proxy was introduced, which is responsible for exchanging Control Plane messages in inter-PLMN signalling between the two edge proxies of the PLMNs. The security for this case is still under discussion.

III. Primary Authentication and Key Agreement

The primary authentication and key agreement procedure is similar to the AKA procedure in the 4G network, which is to enable the mutual authentication and to share key materials between UE and the network. The key materials can be used in subsequent procedures between UE and the serving network.

With primary authentication, an anchor key called the K_{SEAF} is generated and shared between SEAF and UE. From which the K_{AMF} (part of 5G security context) is generated and shared between AMF and User Equipment UE.

The generated K_{SEAF} binds to the serving network with serving network name, such that it prevents the serving network from claiming to be a different one. This also enables valid authentication via both 3GPP and non-3GPP.

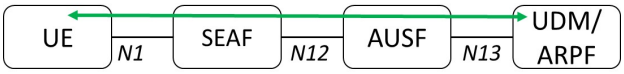

Figure 3: High-Level Architecture for 5G AKA

The primary authentication is initiated by SEAF during any procedure establishing a signalling connection between network and the UE (Figure 3). The SEAF will send an authentication request to the AUSF to initiate the authentication, containing the SUCI or 5G-GUTI received from UE. Once the AUSF verified that the SEAF is an authorized serving network, it will forward the request to UDM/ARPF. The UDM/ARPF will select a method for authentication, and generate the 5G AV with the necessary keys. Two methods were specified for primary authentication: EAP-AKA' as specified in RFC 5448 [4] as well as 5G AKA. 5G AKA is built on top of EPS AKA [5] in order to provide a proof of successful authentication of the UE in the visited network towards the home network. For private networks in isolated deployments, i.e. without roaming or interworking with public 5G networks, other authentication methods can be used and EAP-TLS [6] is specified for information as an example method.

The 5G AV contains the parameters RAND, AUTN, XRES*, in which the RAND and AUTN are sent to the UE. The UE will compute a RES*, which is verified by the AUSF against XRES*. The AUSF shall consider the authentication as successful from the home network point of view, only when they are equal.

Both AMF and SEAF at network side should support the primary authentication using SUCI, which is explained in detail in section VII. The 5G authentication protocols provide increased home control compared to 4G networks, i.e. the AUSF in the home network obtains a confirmation that the UE has been successfully authenticated in the serving network, e.g. a visited network.

IV. Key Hierarchy

The key hierarchy for 5G defines the derivation of keys within the different functional entities in the security architecture. Figure 4 below shows a key hierarchy, in which the K, CK/IK are related to authentication.

The long term key K is 128 bits or 256 bits long, which is stored in ARPF in the network and USIM in the UE

separately. The network interfaces shall be prepared to support 256 bit keys for future use (currently under study).

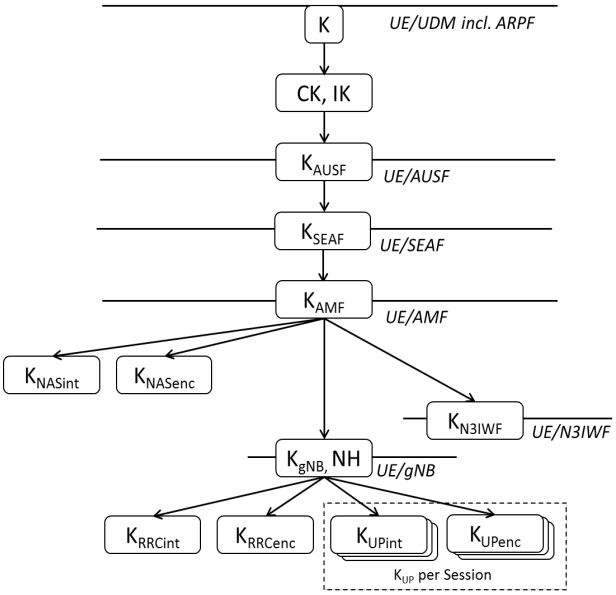

Figure 4: Key Hierarchy in 5G

The following keys are derived from K at UE and network element separately according to the key derivation function with the corresponding additional inputs for freshness and uniqueness as specified in 3GPP TS33.501 ([2]). The anchor key K_{SEAF} is derived from K_{AUSF} during authentication procedure by ME and AUSF and sent to SEAF. This anchor key is used for derivation of subsequent security keys including the K_{AMF}, and keys for NAS and RAN protection. The SUPI (see clause VII.) as input to the KDF for the K_{AMF} ensures that only the UE that has the secret identifier can derive the correct keys. Such that it provides additional home control in case of roaming. NAS signaling keys (K_{NASenc}, K_{NASint}) and K_{gNB} for NR are derived from K_{AMF}.

From K_{gNB}, the keys for RAN signaling and RAN UP traffic are further derived. The K_{RRCenc} and K_{RRCint} are for confidentiality and integrity protection of RRC signaling. The K_{UPenc} and K_{UPint} are for confidentiality and integrity protection of UP traffic. Furthermore,UE and AMF also can derive the K_{N3IWF} from K_{AMF} for non-3GPP access.

V. Multiple NAS Connections

In 3GPP SA2 group it defined a scenario that UE can register to multiple serving networks within the same PLMN or different PLMNs [3].

When a UE is registered to different PLMNs (Figure 5), it shall maintain two independent security context, one per PLMN serving network. The security contexts are generated from the primary authentication procedure separately. Both security contexts should be stored at UE side either in the USIM or the ME.

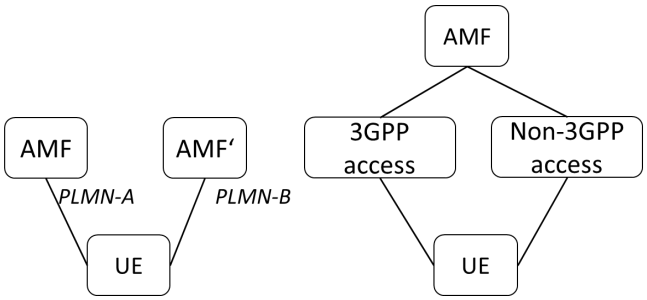

Figure 5: Multiple NAS-connection

When an UE is registered to the same PLMN but via both 3GPP and non-3GPP access (Figure 5), it will establish two NAS connections with the same AMF. In this case, AMF will verify whether UE has already been authenticated to the network and decide whether a new authentication procedure is needed. When the UE has already authenticated the network, the common security context can be used to protect the registration via non-3GPP access. Such common security context can be established at the first registration via any access. Such common NAS security-context shall have parameters specific to each NAS connection to enable cryptographic separation and replay protection. This feature enables now in difference to previous Releases in 3GPP that the UE can register with NAS signalling to the 5G core network via non-3GPP access.

VI. User Plane Security Enhancements

Within the EPS, there was only mandatory integrity protection of the RRC and NAS signaling, but confidentiality protection for signaling and user plane data was optional.

Integrity protection for UP data in EPS was only available between Relay Node and Donor eNB but not between UE and eNB. Due to recent man in the middle attacks on LTE networks with rogue eNBs, there are new thoughts in 3GPP to introduce also UP integrity protection in EPS.

UP integrity protection is now a new configurable security feature in 5G and implemented the following way in the specifications:

A new UP security policy is provided from the SMF to the gNB for a PDU session of an UE at the time of the PDU session establishment. This UP security policy provides the information whether UP confidentiality and/or UP integrity shall be activated. The policy is valid for all DRB that belongs to the same PDU session. Integrity protection is performed in the Packet Data Convergence Protocol layer.

There may be a conflict of support of the UP security policy in the gNB with the requested policy sent by the SMF: for the case that the gNB cannot activate the requested UP confidentiality and/or UP integrity for the DRBs of a PDU session, then gNB will reject the establishment of resources in the gNB and informs the SMF about it.

The same principle applies also for handover scenario via the Xn interface between two gNBs: if the target gNB cannot fulfill the UP security policy of the source gNB for a PDU session, it will reject the corresponding PDU session and informs the AMF about it.

The UP security is activated by the gNB with a RRC Connection Reconfiguration message to the UE with an indication for UP integrity and UP ciphering for each DRB. The UE verifies the RRC message and if UP integrity protection and/or UP ciphering is activated, it generates a key K_{UPint} and/or a key K_{UPenc} respectively for those DRBs. The UE then sends a confirmation back to the gNB in a RRC Connection Reconfiguration Complete message.

It could be also the case that neither integrity nor ciphering is activated by the gNB. Then the UE shall not include a Message Authentication Code for Integrity in order to avoid unnecessary padding bits set to 0, so that the packet size can be minimized.

The currently standardized data rate for integrity protection is up to 64 kbit/s or up to the max data rate supported by the UE based on UE capability that was indicated to the gNB. The integrity protection in current chipset implementations is done in software and performed by the modem processor so that in reality for the first 5G devices the integrity protection for user plane data is also not exceeding the 64 kbit/s data rate. For that reason, mobiles operators raised the concern that the new feature may not be available for normal broadband end user devices. Further solutions and discussions are required in order to provide UP integrity protection also for higher data rates.

VII. 5G PRIVACY

Privacy is one of the new key features in 5G security, which addresses an issue in the previous generations of the mobile network. The unique binding parameter of a subscription, the IMSI, is transmitted in clear text over the air interface in certain events. Some examples of such events are: initial attach to the mobile network, first attach at a roaming network, and response to identity request by an eNB before NAS security was setup. This issue of privacy can be now minimized, but it depends on the home network operator whether the feature is used or not. The successor of the IMSI is SUPI, which is pointing to the subscription information in the UDM function, a kind of successor of the Home Subscription Server in EPS.

The SUPI can be based on two different formats, either on the traditional IMSI for "normal" 3GPP access or on a private network-specific identifier for non-3GPP access or private networks. For both cases, the SUPI could have the form of a Network Access Identifier using RFC 7542 [7]. In case of interworking with EPC, the SUPI must be based on IMSI and for enabling roaming scenarios, the address of the home network (for IMSI based SUPI the MCC and the MNC) must be included in the SUPI.

The new privacy feature now allows the UE to conceal the SUPI, i.e. it generates a SUCI, which is used in the NAS signaling instead of the SUPI or before the IMSI. The UE uses a securely pre-provisioned public key from the home network and only the Subscription Identifier De-concealing Function in the UDM of the home network is able to de-conceal the SUPI from the SUCI. Also not the whole SUPI is concealed, since the MNC, MCC or home network address is required as non-concealed information for routing to the home network in case of roaming.

The USIM stores the home network public key and an indication whether the SUCI calculation is performed by the USIM or by the ME. Different protection schemes could be used e.g. the specified one in TS 33.501 [2] on Elliptic Curve Integrated Encryption Scheme, but it depends on the home operator which one to choose. In order to calculate the SUCI, the following parameters are required: the home network public key, the home network public key identifier, protection scheme profile and the protection scheme identifier. The home network operator can provide priority to certain protection schemes based on the order in the list on the USIM.

The UE only sends the SUCI in the initial registration request to the network when it does not have a 5G-GUTI or later onwards when it used the 5G-GUTI and received an identity request to send a fresh SUCI. The selected protection scheme is taking care of the freshness and randomness aspects of the SUCI.

It can also happen that the UE is not able to calculate a SUCI and under these circumstances, the UE will use a "null-scheme" to generate a SUCI, which is equal to the SUPI. This could happen due to three different scenarios:

- The home network configured the UE that the "null-scheme" shall be used;
- The home network did not provision a public key;
- The UE attempts an unauthenticated emergency session and it does not have a 5G-GUTI.

Of course, if SUCI equal to SUPI is used, then there is no privacy anymore. Pre-5G USIMs could be used also for authentication in 5G. However in order to enable the privacy feature, the pre-5G USIM is required to be able to store at least the parameters for the calculation of the SUCI. The calculation could be done in the ME, if the USIM is not capable of it.

VIII. SECONDARY AUTHENTICATION

The secondary authentication is an optional EAP (RFC 3748 [8]) procedure between the UE and an AAA server in an external data network via the 5GC. The exchange of the EAP messages are realized with Session Management NAS messages to the SMF, via the AMF at the time of the PDU

session establishment request from the UE. This request must contain authorization/ authentication information for the specific DN-AAA server, so that the SMF can determine whether it should forward this information to the DN-AAA. The SMF typically communicates with the DN-AAA via the UPF. In case the DN-AAA is located in the 5GC, it may exchange messages directly without UPF. A high-level architecture for the non-roaming scenario is shown in Figure 6 with the communication path between UE and DN-AAA.

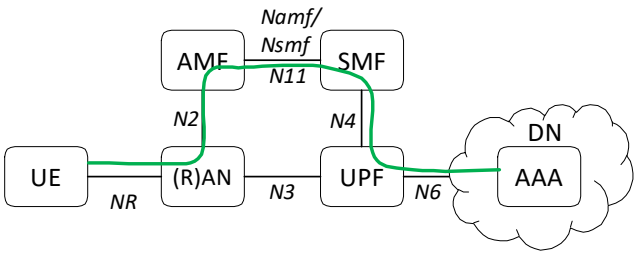

Figure 6: High-Level Architecture for Secondary Authentication

The EAP Authenticator role is in the SMF, i.e. the SMF trigger the EAP authentication to the UE with an EAP-Request/Identity to the UE. The UE then sends the EAP-Response/Identity message back to the SMF including its DN-specific identity in Network Access Identifier -format in a "DN request container". The SMF can based on the information from the UE or based on configuration identify the DN-AAA and forwards the DN request container to the DN-AAA. As specified in the EAP method, the DN-AAA will exchange EAP messages within the DN request container until the authentication and authorization is completed.

When the SMF receives the EAP success message from the DN-AAA, the SMF may save the UE ID/DNN combination in a list or update the UDM. Then the PDU session establishment will continue following the normal procedure in TS 23.502 [9].

IX. Service Based Architecture

SBA is a new concept for 3GPP although it is already well established in the area of internet based platforms and applications. SBA is adopting the Service-Oriented Architecture where a Service Provider registers its service at a Service Registry and a Service Consumer can query the registry to find a corresponding Service Producer, which can be then directly contacted to request the service. In the new 5G architecture all NFs of the control plane can act as Service Producer and/or Service Consumer. The implementation of Service-Oriented Architecture-based systems is achieved using Representational State Transfer due to its data independent nature.

The main benefits of such new architecture are the flexibility and possibilities for virtualization with new business opportunities in the mobile industry. This leads to new security challenges within 3GPP that are partly address already in other standardization bodies for service-based systems and virtual environments.

Authentication of two NFs in the same 5GC depends on the mobile operator policy and could be performed explicitly with TLS [10] between the entities or implicitly in case security is already provided, e.g. by use of NDS. The authorization of two NFs is performed together with the authentication in the NRF when it receives an access token request from a Service Consumer NF. The authorization procedure is based on OAuth, which is the state of the art protocol for granting authorizations to HTTP-services. Currently the roaming scenario for SBA security is still under discussion due to special requirements of interconnection service providers, which are required to change specific parameters and fields in the signaling messages.

X. Conclusions

The 5G Phase 1 security enhancements provide new features in comparison to the previous generations of the mobile network. Due to the lack of trust to the roaming partner, full home control is designed in the authentication schemes and key derivation such that the home network can verify that the UE is really in this roaming network. Privacy protection of the permanent subscriber identifier is a strong enhancement as well as user plane integrity protection mechanism. There are still many possibilities to circumvent those features in real deployments. For example, the mobile operator can switch off privacy or simply does not provide future proof SIM cards to the customers that cannot store the home network public key. In addition, integrity protection of the user plane traffic is available but it is limited to the capabilities of the UE's chipset that current available chipsets are not able to provide integrity protection more than the lowest possible rate of 64kbit/s. This may not suit the Mobile Broadband use cases of 5G and could only fit to certain Internet of Things traffic. New features like device authentication or USIM profile provisioning could be possible for the next 5G Phase 2.

Some earlier 5G security study in 3GPP TR 33.899 [11] contains many features that were not prioritized for 3GPP Release 15, but may be considered for Release 16 after studying the applicability to the finally defined system. Further new service requirements are coming up for 5G Phase 2 (3GPP TS 22.261 [12]), which will lead to respective studies of their security impacts within the 3GPP security group.

References

[1] X. Zhang, A. Kunz, S. Schröder "Overview of 5G Security in 3GPP", IEEE Conference on Standards for Communications and Networking (CSCN), September 2017

[2] 3GPP TS 33.501, Security architecture and procedures for 5G System, v.15.0.0

[3] 3GPP TS 23.501, System Architecture for the 5G System, v.15.1.0
[4] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')"
[5] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".
[6] IETF RFC 5216: "The EAP-TLS Authentication Protocol"
[7] IETF RFC 7542: “The Network Access Identifier”
[8] IETF RFC 3748: “Extensible Authentication Protocol (EAP)”
[9] 3GPP TS 23.502, Procedures for the 5G System, v.15.1.0
[10] IETF RFC 5246 “The Transport Layer Security (TLS) Protocol, Version 1.2”
[11] 3GPP TR 33.899, Study on the security aspects of the next generation system, v.1.1.0
[12] 3GPP TS 22.261 “Service requirements for the 5G system; Stage 1”, Release 16, v16.3.0