Non-3GPP Access Security in 5G

Andreas Kunz[1,*] and Apostolis Salkintzis[2]

[1]*Lenovo, Oberursel, Germany*
[2]*Motorola Mobility, Athens, Greece*
E-mail: akunz@lenovo.com; salki@motorola.com
[*]*Corresponding Author*

Received 16 October 2019; Accepted 28 November 2019;
Publication 04 January 2020

Abstract

Non-3GPP Access technologies such as WLAN technologies can be connected to the 3GPP core network like EPC (Evolved Packet Core) in various ways based on the operator's business models and architectural preferences. The desire to provide this access to the 5G core network, currently defined in 3GPP, requires the design of new protocols and procedures in order to fulfill all requirements. This paper describes the current status of the specification in Release 15 of the untrusted non-3GPP access where the mobile operator does not trust the access point and tunnels all traffic to a trusted gateway in the mobile network. Further, the paper provides an outlook of the new Release 16 feature for trusted non-3GPP access, i.e. the mobile operator trusts the access point, as well as the feature for 5G core network access from WLAN devices with 3GPP credentials that do not support the Non Access Stratum protocol.

Keywords: Non-3GPP Access, WLAN, 5G, 3GPP.

1 Introduction

The first Non-3GPP Access considered for interworking with the 3GPP system was WLAN [1] and got specified in the 3GPP Release 6 already in 2006. With the introduction of the EPC [2] and the new radio access

Journal of ICT, Vol. 8_1, 41–56. *River Publishers*
doi: 10.13052/jicts2245-800X.814

technology LTE (Long Term Evolution) in 3GPP Release-8, also other Non-3GPP technologies like CDMA200 and WiMAX were included in the procedures for interworking with the EPC [3]. The main focus was still remaining on WLAN, which got integrated even tighter in later releases with the 3GPP radio access with the features LTE-WLAN Aggregation (LWA), LTE-WLAN Radio Level Integration with IPsec Tunnel (LWIP) and RAN controlled LTE-WLAN interworking (RCLWI).

There are two basic principles for the Non-3GPP Access to the 3GPP core network:

Untrusted Access: The mobile operator does not trust the access point the User Equipment (UE), i.e. the device, is connected to. It could be a free WLAN from a coffee shop or the WLAN at home. Also, the encryption on the radio link is out of the scope of the mobile operator. The UE tunnels all traffic to a gateway in the network, which is trusted by the mobile operator. This is the most common deployed Non-3GPP Access for EPC (e.g. Voice over Wifi feature) and is standardized in Release 15 for 5G.

Trusted Access: the mobile operator trusts and operates the access points, i.e. the encryption of the radio link is also controlled by the operator and the credentials are derived from the security context in the UE and the network. The trusted access is agreed to be standardized in Release 16.

The following Figure 1 shows the 5G architecture for untrusted Non-3GPP Access via Y1 and Y2 reference points, including the 3GPP access via N1, N2 reference points.

The following network functions and functional entities are defined: The User Equipment (UE) connects via the New Radio (NR) on the radio interface to the Radio Access Network (RAN) and then further to the Access and Mobility Management Function (AMF) for the control plane signalling and for the user plane to the User Plane Function (UPF), which is the gateway to the Data Network (DN), e.g. internet. On the Non-3GPP Access, the UE connects first to the Non-3GPP Interworking function (N3IWF) and then to AMF and UPF respectively as for the 3GPP access. For the authentication procedures in the following, the Authentication Server Function (AUSF) and the Unified Data Management (UDM) are relevant to create the authentication vectors and perform the authentication. The Application Function (AF), Network Exposure Function (NEF), Network Slice Selection Function (NSSF), Network Repository Function (NRF) and the Policy Control Function (PCF) are just shown for completeness of the Service Based Architecture (SBA).

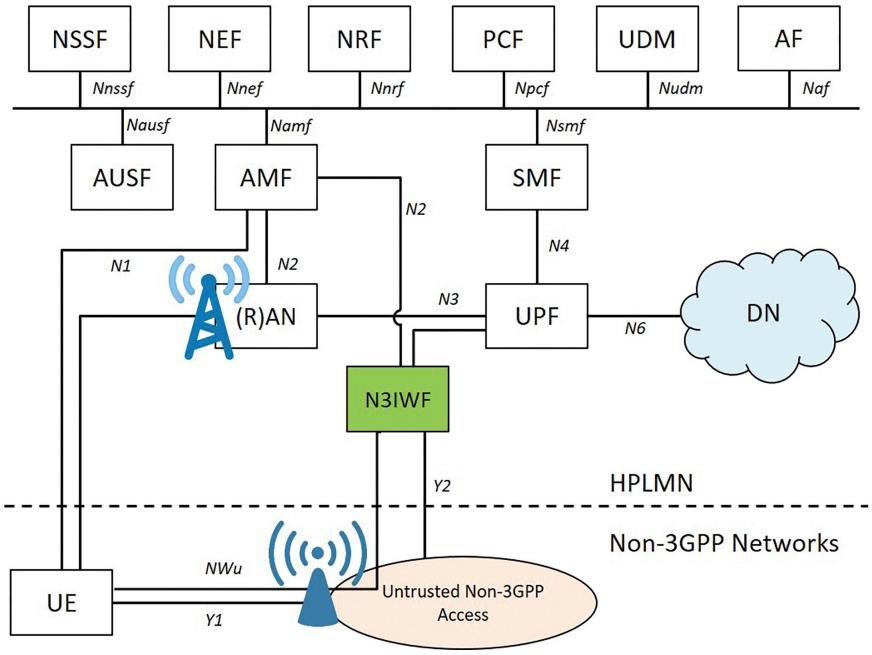

Figure 1 Untrusted Non-3GPP Access architecture.

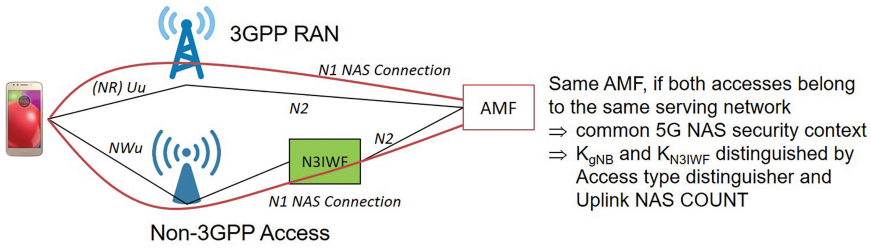

Figure 2 Multiple NAS connections.

5G is bringing a new principle to the Non-3GPP Access i.e. multiple Non Access Stratum (NAS) connections are now possible at the same time via 3GPP access and non-3GPP access. The idea behind is that the same authentication procedures EAP-AKA' and 5G-AKA for primary authentication can be reused also via the non-3GPP access. The following Figure 2 shows the scenario where the UE is connected via 3GPP and Non-3GPP Access at the same time, where both access networks belong to the same operator, i.e. the NAS signalling is terminated at the same AMF and the same

security context is reused. The distinguishing of the security keys takes place at lower layer for deriving the key K_{gNB} for 3GPP access and the key K_{N3IWF} for non-3GPP access.

Of the scenario that the Non-3GPP Access and the 3gpp access belong to different operators is also supported, but then the two NAS connections are very independent, i.e. authentication is performed per access with the credentials of the respective operator.

For 5G, there are two authentication procedures specified: EAP-AKA' as specified in RFC 5448 [4] and 5G AKA as specified in TS 33.501 [8]. Which procedure is used in the network is based on the decision of the mobile operator. Figure 3 shows the two procedures in one call flow. They could be triggered by an authentication request from the UE, i.e. with an initial

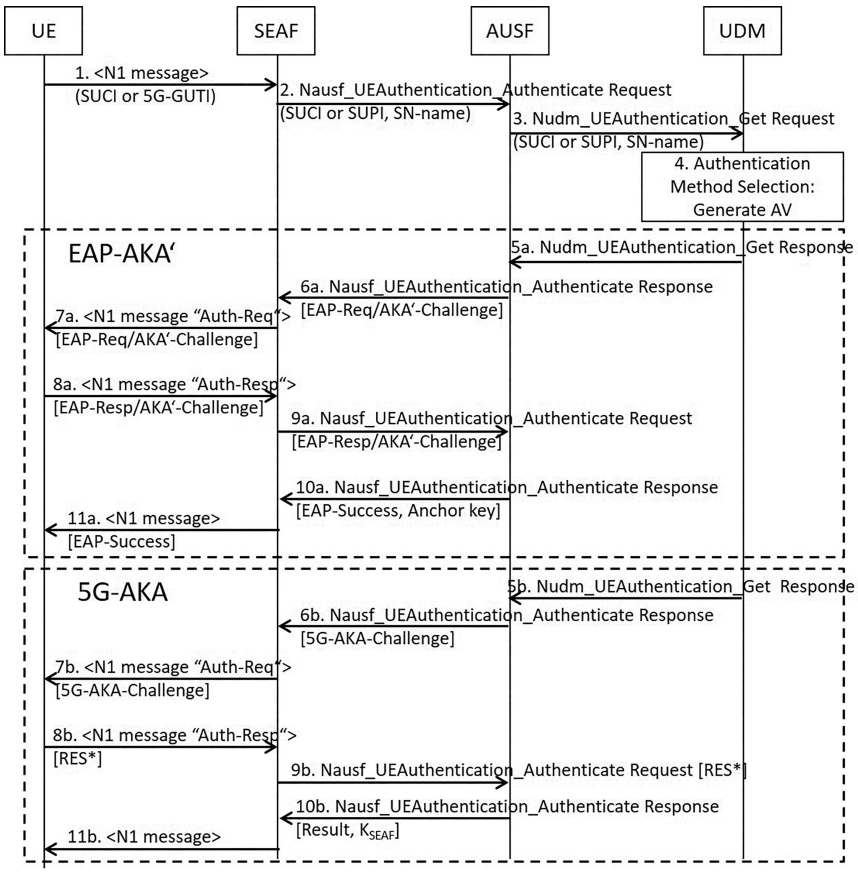

Figure 3 5G Authentication: EAP-AKA' and 5G-AKA.

registration (step 1–4), or at any time afterwards from the AUSF (step 5). The basic difference between the two procedures is that EAP-AKA' is based on the EAP framework and evaluates the response from the UE in the AUSF, i.e. always in the home network and not in the visited network as e.g. in 4G. The same procedure was applied also to the 5G-AKA as an extension of the EPS-AKA, specified for 4G, i.e. the result of the challenge, computed by the UE is verified first in the SEAF of the visited network and then in the AUSF in the home network. In terms of number of messages, there is no difference between EAP-AKA' and 5G-AKA. The main differences are more in the way the authentication vector is constructed, how the results are computed and how the keys for the visited network are derived. In some cases, the EAP-AKA' might have additional EAP messages compared to the minimum number of steps in Figure 3.

2 Release 15 Untrusted Non-3GPP Access

Since untrusted Non-3GPP Access is the most common deployed access mostly for WLAN access to the mobile operator core for offering additional services like Voice over Wifi, which is very useful e.g. in locations where the mobile network radio coverage is not sufficient. The principle of untrusted Non-3GPP Access is that the mobile operator has no influence on the WLAN access point and its deployment, e.g. at the subscriber's home or in a shopping mall. Since the operator does not trust the access point, the UE communicates with a node of trust, the Non-3GPP Interworking Function (N3IWF) which is the termination point of the IPsec tunnel between UE and N3IWF. Before establishment of the IPsec tunnel, the UE must be authenticated by the 5G home network which then provides the key to the N3IWF for the tunnel establishment. A new transport protocol EAP-5G was introduced in order to keep the IKEv2 between UE and the N3IWF open with EAP Request/Response pairs since an IKE_AUTH exchange without EAP is designed to support only one request/response between the UE and the network. EAP-AKA' or 5G-AKA in the NAS messages require more than one exchange and would result in an IKEv2 failure. The details of EAP-5G are explained in clause 3 of this document.

The UE connects to an untrusted Non-3GPP Access network and starts with the establishment of an IPsec Security Association (SA) with the selected N3IWF by initiating an IKE initial exchange according to RFC 7296 [10]. After step 2 all subsequent IKE messages are encrypted and integrity protected by using the IKE SA. The UE then sends an IKE_AUTH request

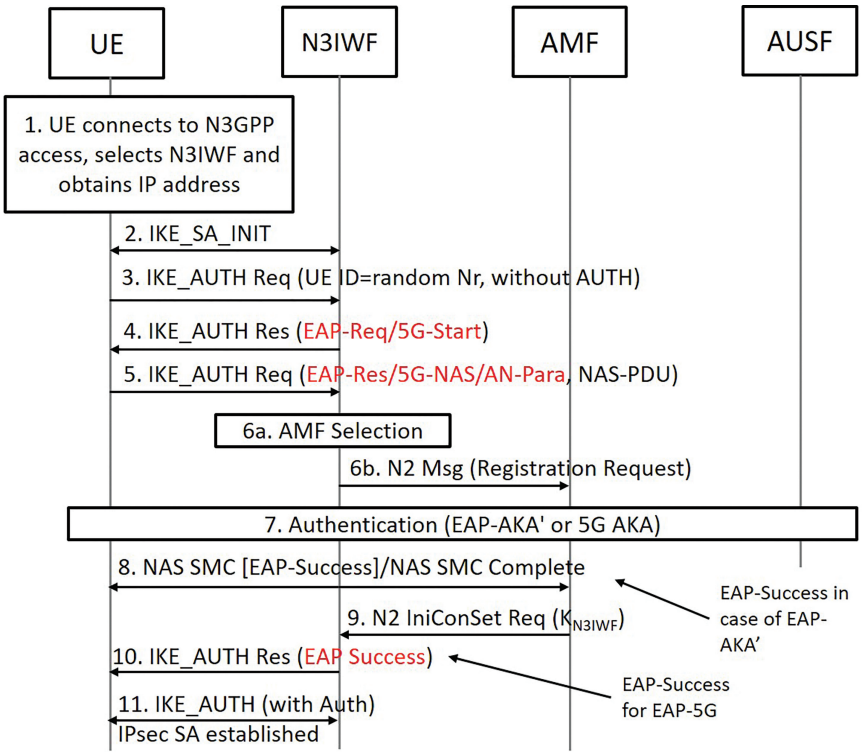

Figure 4 Untrusted Non-3GPP Access Registration & Authentication.

message without the AUTH payload, which indicates that the IKE_AUTH exchange shall use EAP signaling (in this case EAP-5G signaling). The UE shall set the UE Id field in this message equal to any random number. The UE shall not use its GUTI/SUCI/SUPI as the user Id. Now the EAP-5G exchange is started with the EAP-Request/5G-Start packet in step 4 to inform the UE to start sending NAS messages encapsulated within EAP-5G packets. The UE sends a NAS Registration Request encapsulated in EAP-5G and in an IKE_AUTH request to the N3IWF. The N3IWF then forwards the NAS message to the AMF after the selection process. Normal primary authentication (5G-AKA or EAP-AKA') is performed (step 7). The final authentication message from the AUSF contains the anchor key K_{SEAF} derived from K_{AUSF}. The SEAF (not shown in the call flow but is collocated with the AMF in Release 15) derives the K_{AMF} from K_{SEAF} and sends it to the AMF which is used by the AMF to derive NAS security keys and a

security key for N3IWF (K_{N3IWF}). The N3IWF key is used later by the UE and N3IWF for establishing the IPsec Security Association (in step 11). The AMF shall send a Security Mode Command (SMC) in step 8 to the UE in order to activate NAS security and may contain the EAP-Success in case of EAP-AKA'. The UE completes the authentication and creates a NAS security context and an N3IWF key K_{N3IWF}. The EAP-5G encapsulation is no longer required and the UE sends an EAP-Response/5G-Complete packet, which triggers the N3IWF to send an EAP-Success to UE in step 10, assuming the N3IWF has also received the N3IWF key from AMF. The common N3IWF key K_{N3IWF} is now used to create the IPsec SA in step 11. All further NAS messages between the UE and the N3IWF shall be sent over the established IPsec SA.

3 EAP-5G: The New Transport Method

EAP-5G is specified within 3GPP under its existing 3GPP Vendor-Id in [8] and [9] as a vendor-specific EAP method [4], utilizing the "Expanded" EAP type that is registered with IANA under the SMI Private Enterprise Code registry [5]. The "EAP-5G" method is used only for encapsulating NAS messages between the UE and the N3IWF.

The EAP-5G protocol runs only between the UE and N3IWF and its primary purpose is to transparently relay NAS messages between the UE (over NWu) and the AMF (over N2). In addition, it is enable AMF selection by the N3IWF.

Except the EAP-5G Start and Stop messages contain all EAP-5G messages a NAS message that is forwarded by the EAP-5G layer to the NAS layer. If the UE receives a NAS Registration Reject message, then the UE shall terminate the EAP-5G session by sending an EAP-5G Stop packet. After that, the N3IWF sends an EAP-Failure message to the UE and completes the EAP-5G session.

The EAP-5G session between the UE and N3IWF is successfully performed when the EAP-5G layer in the UE receives the N3IWF key from the NAS layer and the EAP-5G layer in the N3IWF receives the N3IWF key from AMF. The UE receives then from the N3IWF an EAP-Success message. After that, the EAP-5G layer in the UE and the EAP-5G layer in the N3IWF forward the common N3IWF key to the lower layer (IKEv2), which is further used for establishing an IPsec security association.

EAP-5G needs to support the following information elements:

- An EAP-5G Type field; and
- Three message identifiers for 5G-Start, 5G-NAS and 5G-Stop;
- Two attributes were defined: AN parameters and NAS-PDU.

3.1 EAP-5G Type Field

The Vendor-Type field is specified in 3GPP TS 33.402 [12] annex C and set to EAP-5G method identifier of 3 (decimal) in all EAP-5G messages.

3.2 EAP-5G Message Identifiers

The following message identifiers are considered:

5G-Start which is only sent by the N3IWF to signal the initiation of an EAP-5G session. An EAP-5G Start message does not include any other information (i.e. contains no attributes).

5G-Stop which is only sent by the UE to signal the completion of an EAP-5G session due to a NAS registration failure.

5G-NAS which is the transport message and send between UE and N3IWF to encapsulate the NAS messages.

3.3 EAP-5G Attributes

The following attributes are considered:

AN-Parameters attribute: This is included in an EAP-5G packet when the UE wants to send access network parameters (AN parameters) to N3IWF to be used for AMF selection. The use of AN parameters during a 5G registration is specified in TS 23.502 [7].

NAS-PDU attribute: This is included in an EAP-5G packet to encapsulate a NAS message.

An EAP-5G packet can include:

- No attributes: This is the case when the 5G-Start or 5G Stop message is sent.
- Both the AN-Parameters attribute and the NAS-PDU attribute: This is the case where the UE needs to send the first NAS message and the associated access network parameters, which are used by the N3IWF to perform AMF selection.

– Only a NAS-PDU attribute: This is the most common case where the EAP-5G packet carries only a NAS message that should be transparently relayed by N3IWF to the AMF.

4 Release 16 Enhancements

Two new features with respect to WLAN access were concluded to be included in the normative specifications in the ending Rel-16 study on the security of the wireless and wireline convergence for the 5G system architecture [11].

4.1 Trusted Non-3GPP Access

The trusted access is the corresponding deployment option of the untrusted access with the difference that the operator also trusts and controls the access point. For this reason, three new definitions were introduced:

Trusted Non-3GPP Access Network (TNAN): the TNAN consists of the Trusted Non-3GPP Access Point (TNAP) and the Trusted Non-3GPP Gateway Function (TNGF). The TNAN can connect to the 5GC by exposing north-bound interfaces compliant with N2/N3.

Trusted Non-3GPP Access Point (TNAP): The TNAP enables UEs to access the TNAN by using a non-3GPP wireless or wired access technology and corresponds to a WLAN access point.

Trusted Non-3GPP Gateway Function (TNGF): The TNGF exposes the N2/N3 interfaces and enables the UE to connect to 5GC over a Non-3GPP Access technology (TNAP).

The registration procedure and the authentication is shown in the following figure:

The UE registers to 5GC and, at the same time, it authenticates with the TNAN by using the EAP-based procedure, which is essentially the same with the registration procedure for untrusted non-3GPP access. The interface between the TNAP and Control Plane part of the TNGF is an AAA interface. The TNGF terminates the EAP-5G signalling and behaves as an authenticator when the UE attempts to register to 5GC via the TNAN.

EAP-5G is used like in the untrusted Non-3GPP Access to encapsulate the NAS messages, starting in step 3 of Figure 5. After the authentication, the UE derives the TNAP and TNGF keys. The AMF sends a NAS SMC to the TNGF

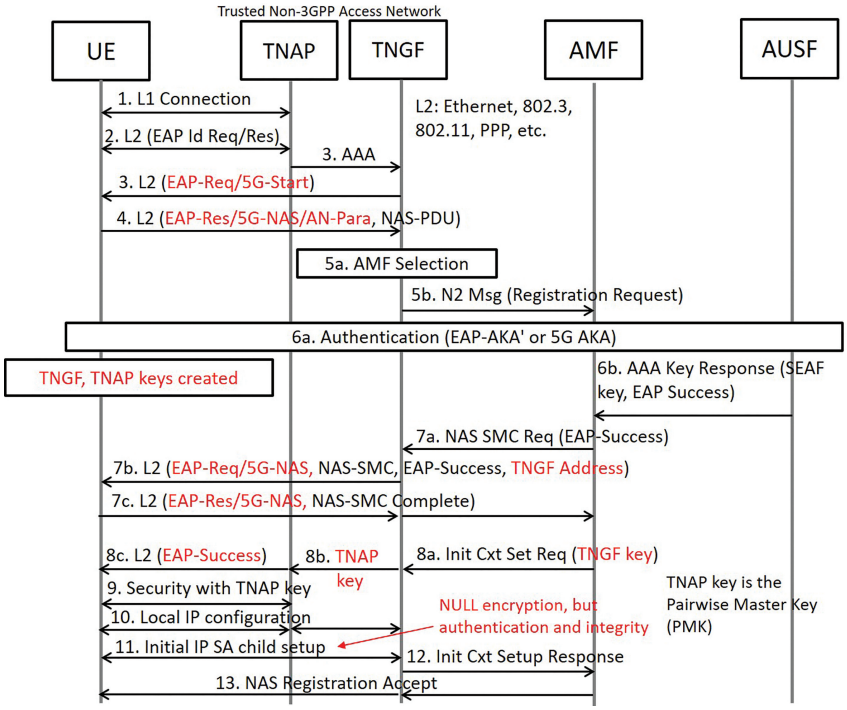

Figure 5 Trusted Non-3GPP Access Registration & Authentication.

with the EAP success flag of the primary authentication in step 6a. The TNGF includes its own IP address in the NAS SMC and forwards it to the UE. When the AMF receives the NAS SMC Complete message from the UE, it provides the TNGF key to the TNGF, which derives the TNAP key, which corresponds to the Pairwise Master Key (PMK) and provides it to the TNAP. Now the EAP-5G encapsulation can be terminated and the UE can use the TNAP key for encryption over the air interface.

The security relies on Layer-2 security between UE and TNAP, which is a trusted entity so that no IPSec encryption would be necessary between UE and TNGF, i.e. NULL encryption is sufficient for the user plane and signalling.

Separate IPSec SAs may be used for NAS transport and PDU Sessions. At the end of the UE's registration to 5GC, an IPSec SA is established between the UE and TNGF (step 11). This is used to protect NAS messages between the UE and TNGF. Later when the UE initiates a PDU session establishment, the TNGF initiates the establishment of one or more IPSec child SAs per PDU session. This results in additional IPSec SAs to be set up

between the UE and TNGF, which are then for user plane transport between the two.

The main advantage of using IKEv2/IPsec is that it makes the solution for trusted Non-3GPP Access almost identical with the solution for untrusted Non-3GPP Access specified in TS 33.501 [8]. Thus, the UE can use the same protocols and procedures for both trusted and untrusted Non-3GPP Access and the TNGF can become very similar to N3IWF.

4.2 5GC Access from WLAN UEs that do not Support NAS

Another use case is targeting the 5G core network access from WLAN UEs that do not support NAS, i.e. those UE would not be able to connect to the 5G core network via trusted access as described in the previous clause or via untrusted access (see clause 2) since NAS protocol support is required. A WLAN UE that does not support NAS has the following capabilities:

- The UE is capable to register to 5GC and to establish 5GC connectivity via a trusted WLAN access network.
- The UE is not capable to operate as 5G UE over a WLAN access network.
- The UE may be without any NAS capability at all.
- The UE has 3GPP credentials, i.e. a USIM for EAP-AKA' authentication.

Two new functional entities were introduced in the system:

Trusted WLAN Access Point (TWAP): the trusted WLAN access point the UE is connected to.

Trusted WLAN Interworking Function (TWIF): The interworking functionality that enables connectivity of the UE with the 5GC. The TWIF contains the NAS protocol stack and exchanges NAS messages with the AMF on behalf of the UE.

The following figure shows the registration and authentication procedure for a WLAN UE that does not support the NAS protocol.

A single EAP-AKA' authentication procedure is executed for connecting the UE both to the trusted WLAN access network and to the 5G core network. The UE selects a TWAP and the EAP-AKA' authentication is initiated by the TWAP in step 1. The TWAP selects a TWIF for the interworking between UE and 5G core network. The TWIF creates a NAS Registration Request and after AMF selection sends it to the selected AMF in step 6.

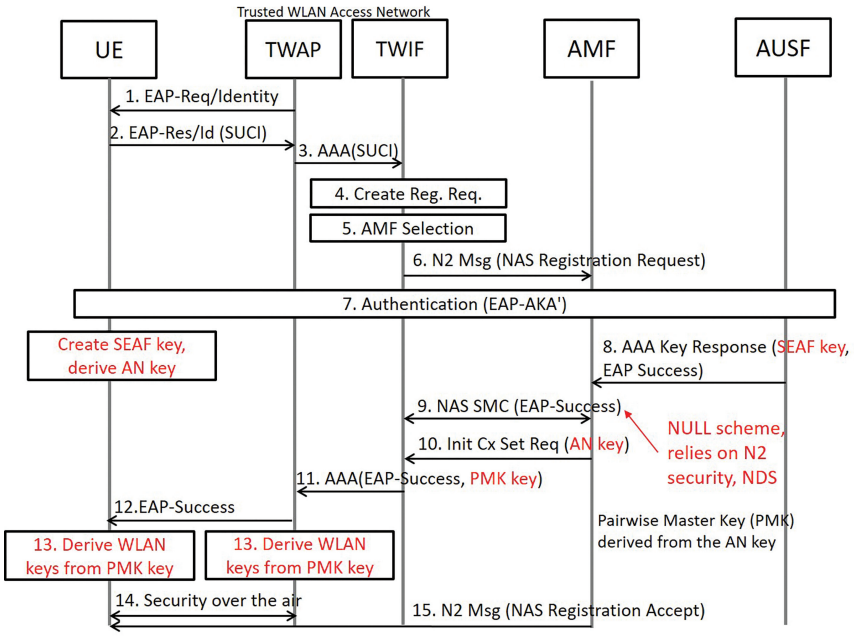

Figure 6 5GC Access from WLAN UEs that do not support NAS.

After authentication, the AUSF provides the SEAF key to the AMF in step 8 and the UE creates the SEAF key and derives the AN key. The connection between TWIF and AMF relies on the N2 security specified in TS 33.501 [8], clause 9.2, therefore no specific NAS security is used between the TWIF to the AMF. The AMF selects the NULL scheme for ciphering and integrity protection in the Security Mode Command in step 9.

The AMF derives the AN key from the SEAF key and sends it to the TWIF in step 10. The TWIF now derives a Pairwise Master Key (PMK) from the AN key and sends the PMK key and the EAP-Success message to the Trusted WLAN Access Point (step 11), which forwards the EAP-Success to the UE (step 12). Now WLAN keys are derived in the UE and the TWAP, i.e. the security on the air interface relies on Layer-2 security between UE and TNAP (security context to encrypt and integrity protect unicast and multicast traffic over the air). Since the TWIF is a trusted entity, no IPSec encryption would be necessary between UE and TWIF, and NULL encryption is sufficient for the user plane and signalling similarly to the trusted Non-3GPP Access as described in clause 4.1.

5 Conclusions

The first Non-3GPP Access specified in Release 15, i.e. 5G Phase 1 was the untrusted access scenario, which is also implementing the same primary authentication in NAS as the 3GPP Access. In order to be able to carry both primary authentication methods over the IKEv2, the EAP-5G transport protocol was specified in 3GPP and was reused as the transport protocol for the trusted access in Release 16. Furthermore, a new scenario for WLAN UEs that do not support NAS but have 3GPP credentials and support the EAP-AKA' authentication procedure is introduced in Release 16. This opens up many more business scenarios for other types of devices other than normal mobile phones. The upcoming Release 17 might have more WLAN scenarios and may open up the 5G system more for non-3GPP Access.

References

[1] 3GPP TS 23.234 "3GPP system to Wireless Local Area Network (WLAN) interworking; System description", Mar. 2017.
[2] 3GPP TS 23.401 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", Sep. 2019.
[3] 3GPP TS 23.402 "Architecture enhancements for non-3GPP accesses", Sep. 2019.
[4] IETF RFC 5448 "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", 2009.
[5] https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers
[6] 3GPP TS 23.501 "System Architecture for the 5G System; Stage 2, (Release 15)", June 2019.
[7] 3GPP TS 23.502 "Procedures for the 5G System; Stage 2, (Release 15)", Sep. 2019.
[8] 3GPP TS 33.501 "Security architecture and procedures for 5G System", Sep. 2019.
[9] 3GPP TS 24.501 "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3", June 2019.
[10] IETF RFC 7296 "Internet Key Exchange Protocol Version 2 (IKEv2)", 2014.

[11] 3GPP TR 33.807 “Study on the security of the wireless and wireline convergence for the 5G system architecture”, Sep. 2019.
[12] 3GPP TS 33.402 “3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses.”

Biographies

Andreas Kunz received his diploma degree and his Ph.D. in Electrical Engineering from the University of Siegen, Germany in 2005. Afterwards he joined NEC Laboratories Europe in 2005 with focus on 3GPP standardization, mainly in the system architecture working group SA2. Besides 3GPP he was also participating in other standardization bodies like GSMA or ETSI. Since 2017 he joined Lenovo Germany as member of the research and technology team, representing Lenovo/Motorola Mobility in the 3GPP security group SA3.

Apostolis Salkintzis received his Diploma in 1991 and his Ph.D. degree in 1997, both from the Department of Electrical and Computer Engineering, Democritus University of Thrace, Greece. During 1999 he was a sessional

lecturer and a post-doctoral fellow at the Department of Electrical and Computer Engineering, The University of British Columbia, Canada. He's currently working for Motorola Mobility and Lenovo on defining and standardizing 5G mobile communications. His primary research interests include mobile communications, IoT and Network Function Virtualization (NFV).