A comparison of 4G and 5G authentication methods

Ranganathan Mavureddi Dhanasekaran, Nokia Standards, Munich, Germany.
Suresh Nair, Nokia Standards, Murray Hill, USA.

White paper

Contents

Abstract	3
1. Introduction	3
2. 4G (LTE) Authentication overview	4
2.1 Authentication procedure	5
2.2 Non-Access stratum security	7
2.3 Access stratum security	7
3. 5G Authentication	9
3.1 5G AKA procedure	12
3.2 EAP AKA Prime procedure	17
3.3 EAP TLS procedure	19
4. Comparison of EPS AKA / 5G AKA / EAP AKA prime / EAP TLS	22
5. Conclusion	23
Acknowledgement	23

Abstract

3GPP Standards has developed a new authentication framework for the fifth generation (5G) network that significantly improves the security posture compared to previous generations. In this paper we describe the authentication procedures for 4G (EPS-AKA) and 5G (5G AKA, EAP-AKA prime, EAP-TLS) and provide a comparison of all the variants at each node level.

1. Introduction

Mobile communication has become an indispensable tool for a majority of people globally (around 5.2 billion mobile subscribers by 2020). Beginning with second generation GSM, third generation UMTS and fourth generation LTE, the reach of mobile communication has extended to every corner of the world. With the advent of 5G and growing importance of mobile services in our daily activities, it is necessary to provide subscribers security and privacy protections.

The authentication and Key Agreement (AKA) [1] protocols designed by 3GPP target the mutual authentication of both UE (USIM) and network, and further generate keys for securing the communication between two entities. AKA protocols have already been implemented in 3G, 4G USIMs and respective networks [2]. In 5G, 3GPP has enhanced the AKA procedure and standardized 5G AKA. In addition to 5G AKA, other mechanisms such as Extensible Authentication Protocol - Authentication and Key Agreement prime (EAP AKA´) [´ denotes prime] and Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) were adapted in 3GPP to secure communication in private networks, communication with Non-5G Capable (N5GC) devices behind Residential Gateway and with N5GC devices via trusted WLAN access network(N5CW).

This paper provides an overview of 4G and 5G Authentication methods and differences at each network node level.

NOTE 1: Only Network nodes relevant to security procedures are considered in this paper.

2. 4G (LTE) Authentication overview

3GPP LTE security defines five security feature groups [3]

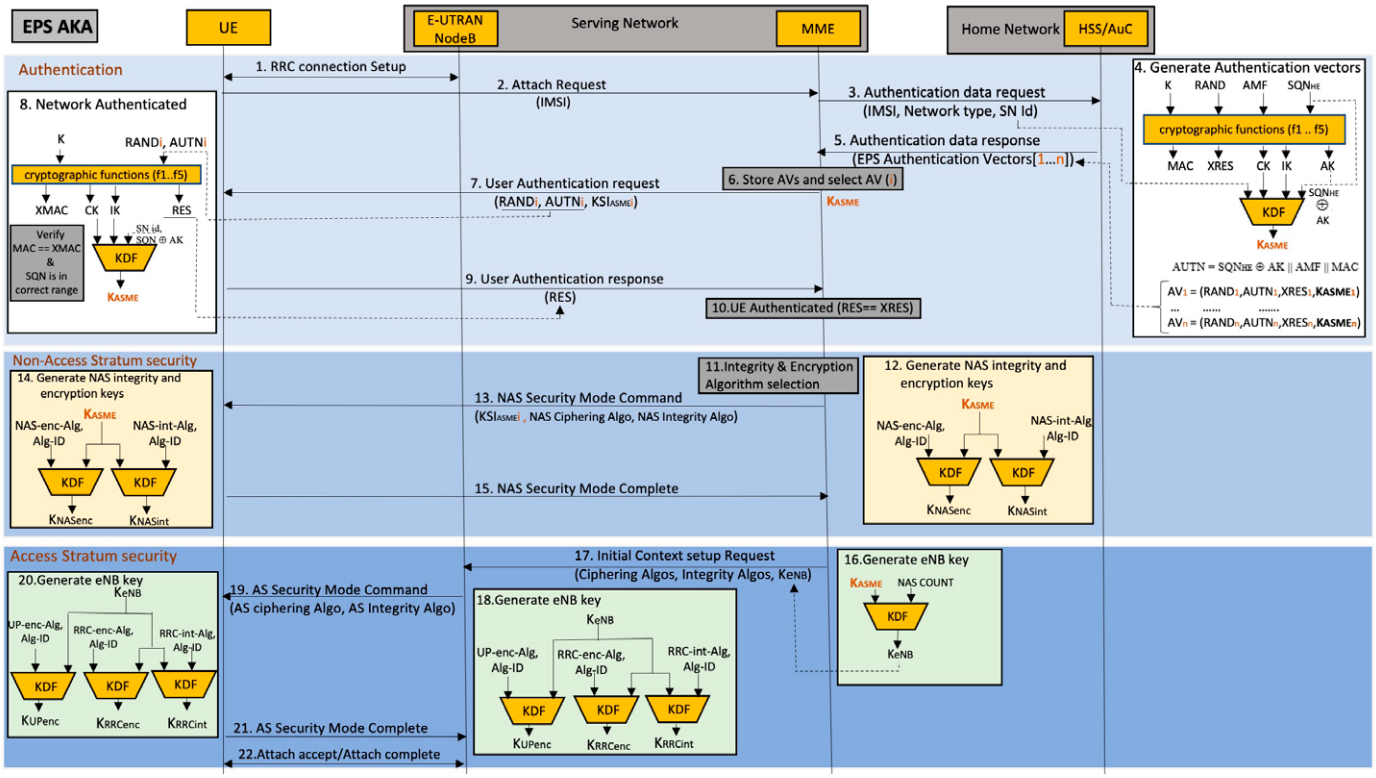
- network access security
- network domain security
- user domain security
- Application domain security
- Visibility & configuration of security.

Each meets certain threats, and accomplishes specific security objectives, such as secure access to mobile stations, secure access to services and protection against attacks on radio access and in wireline networks. LTE network offers basic security features, including LTE authentication, Non-Access Stratum (NAS) security and Access Stratum (AS) security. LTE authentication is the process of determining if a user is an authorized subscriber to the network he is trying to access. NAS security and AS security are features required to securely deliver user data over LTE radio links at NAS and AS levels [4]. Evolved Packet System Authentication and Key Agreement (EPS-AKA) method is used in LTE when the user accesses the network through E-UTRAN, by mutual authentication between the user and the network.

Figure 2-1 shows the overview of the LTE authentication procedure using EPS-AKA method, followed by NAS and AS security procedures covering the key generations between three different entities: UE, Serving network and Home network.

- The Mobile Equipment (ME) and Universal Subscriber Identity Module (USIM), applications running on the physical hardware / smart card Universal Integrated Circuit Card (UICC), together form the User Equipment (UE). The Permanent key is stored on the USIM of UICC and all cryptographic computation is performed within it.
- The Serving network consists of the eNB (e-UTRAN Node Base transceiver station) and Mobility Management Entity (MME).
- The Home Subscriber Server (HSS) and Authentication Centre (AuC) represents home network. The Permanent key is stored in AuC. The AuC is a functionality of the HSS.
- The UDR stores the subscriber related authentication data.

Figure 1 Overview of LTE security procedure



2.1 Authentication procedure

The overall LTE authentication procedure consists of the following basic phases:

- UE attach procedure initiation
- AKA challenge generation at home network
- Serving network authenticated by UE
- UE authenticated by serving network

UE attach procedure initiation

Step 1. When the user wants to access the LTE network, after the random access procedure, the RRC connection is setup between the UE and eNB.

Step 2. The UE sends an attach request (NAS level message) to the MME via the eNB with user identity (International Mobile Subscriber Identity -IMSI) and UE security capabilities. UE security capability information is used by the network to indicate which security algorithms are supported by the UE in S1 / Iu / Gb mode.

Step 3. The MME sends an authentication data request message with IMSI, serving network identity (MCC + MNC) and network type (i.e. E-UTRAN) to the HSS.

AKA challenge generation at home network

Step 4. The HSS/AuC, using cryptographic functions (f1,f2,f3,f4,f5) [5, 6, 7] , computes a message authentication code MAC, an expected response XRES, a cipher key CK, an integrity key IK and an anonymity key AK by considering the following inputs: Long term key K, generated new random number RAND, authentication & key management field AMF and freshly generated sequence number SQN (created by incremental of stored SQN or time-based SQN generation or partial time-based SQN generation [8]). HSS/AuC using key derivative functions KDF, computes the key KASME from cipher key CK, integrity key IK, serving network identity SN id and 'exclusive or' (XOR) of Sequence Number SQN and the Anonymity Key AK.

Step 5. Generated EPS Authentication vectors (1 to n) containing RAND, AUTN (AUTN = SQN ⊕ AK || AMF || MAC), XRES and KASME are sent in an authentication data response message, from the home network HSS to serving network MME.

Step 6. Multiple EPS authentication vectors are stored in the MME in the order of received sequence numbers.

Step 7. The MME sends a user authentication request message to the USIM via eNB, including the random challenge RAND and an authentication token AUTN for network authentication from the selected authentication vector. It also includes a key set identifier KSIASME for the ME, which will be used to identify the KASME (and further keys derived from the KASME) that results from the EPS AKA procedure.

Serving network authenticated by UE

Step 8. At receipt of this message, the USIM verifies the freshness of the authentication vector by checking whether the AUTN token can be accepted (find the explanation of AUTN verification in table 2-2). If verification is successful, the USIM computes a response RES. The USIM also computes CK and IK which are sent to the ME. With inputs such as CK, IK, serving network identifier SN Id, exclusive or (XOR) of Sequence Number SQN and the Anonymity Key AK (received from AUTN) given to key derivative function, KASME at ME is generated.

Table 2-2 AUTN token verification

As part of AUTN verification at USIM, integrity and replay protection checks are performed [8, 9].

Integrity check	Replay protection check
• USIM first computes anonymity key AK and retrieves the sequence number from AUTN. • Then USIM computes expected message authentication code XMAC and compares this with MAC received from network in AUTN. • If the MAC comparison is successful, then USIM considers integrity check is verified.	• USIM maintains an array of previously accepted sequence numbers. • To verify that the received sequence number SQN is fresh, the USIM will compare the received SQN with the sequence number in the array element indexed using the index value IND.

UE authenticated at serving network

Step 9. The UE sends the user authentication response message including computed RES to the serving network MME.

Step 10. The MME checks that the RES is equal to the XRES, and if so, the authentication is successful.

2.2 Non-Access stratum security

Non-Access stratum security is designed to securely deliver messages between the UE and MME over radio channels. The UE and MME will generate the integrity and ciphering key independently and use those keys for secure transmission of NAS messages between these entities. Integrity protection is made mandatory by 3GPP specs (3), while ciphering is offered as optional functionality for NAS messages.

Step 11. The MME selects the NAS integrity protection and encryption algorithm depending on the UE security capabilities (received from the UE in Step 2) and the configured allowed list of security capabilities of the current serving network entity.

NAS keys generation at MME

Step 12. The MME generates the integrity key KNASint from inputs of the 256-bit KASME, the selected NAS integrity protection algorithm and the algorithm type distinguisher. The MME also generates ciphering key KNASenc from inputs of the 256-bit KASME, selected NAS encryption algorithm (algo identity) and the algorithm type distinguisher.

Step 13. The security mode command message is generated in the MME and a corresponding NAS-MAC for integrity is also computed (with NAS integrity key KNASint), so that the UE is assured that the algorithm selection was not manipulated by attacker.

UE security capabilities, that the UE has communicated to the network during the attach procedure are now repeated in the message (Security mode command) from the MME to the UE. The MME delivers the NAS security mode command with selected NAS algorithms (integrity and ciphering algorithms), the replayed UE capabilities and the key set identifier to the UE.

NAS keys generation at ME

Step 14. The ME will verify the integrity of the NAS security mode command message. A bidding down attack can be detected at the ME with the following verification procedure. If the ME detects a mismatch between the security capabilities it sent to the network and the ones received now from the network, meaning verification has failed, the ME sends a security mode reject message to the network. If verification is successful, it assures no bidding down attack has happened. Similar to the MME entity, the ME then generates the integrity key KNASint and ciphering key KNASenc.

Step 15. The UE will respond with a NAS security mode complete message which is both ciphered and integrity protected. The NAS security mode complete message will include an IMEISV (International Mobile Equipment Identity Software Version) in case the MME requested it in the NAS security mode command message. The MME will decipher and check the integrity protection on the NAS Security Mode Complete using the keys and algorithms indicated in the NAS Security Mode Command [10].

2.3 Access stratum security

Access stratum security is designed to deliver messages between the UE and eNB securely over radio channels. The UE and eNB will generate the integrity and ciphering key independently (separate keys for user plane and control plane) and use those keys for secure transmission of AS messages between these entities. Integrity protection is made mandatory while ciphering is offered as an optional functionality for

RRC control plane messages. Note that only ciphering is offered as an optional feature, and there is no integrity protection functionality available for user plane messages. UP integrity was introduced only for relay node architecture (between RN and DeNB).

Step 16. The MME derives the key KeNB from the 256-bit KASME and uplink NAS COUNT.

Step 17. The MME sends the UE EPS security capabilities with encryption algorithms, integrity protection algorithms and generated key KeNB in the Initial context setup request message to the eNB.

AS keys generation at eNB

Step 18. The eNB selects the ciphering and integrity protection algorithm from the configured list which has the highest priority, and is also present in the UE EPS security capabilities. The eNB generates the RRC integrity key KRRCint from inputs of 256-bit KeNB, selected AS integrity protection algorithm and algorithm type distinguisher. The eNB also generates the RRC ciphering key KRRCenc and UP ciphering key KUPenc from inputs of 256-bit KeNB, selected AS encryption algorithm and algorithm type distinguisher.

Step 19. The eNB sends the AS security mode command with selected integrity algorithm, ciphering algorithm. This message is integrity protected with RRC integrity keys. RRC and UP downlink ciphering (encryption) at the eNB starts after sending the AS security mode command message.

AS keys generation at ME

Step 20. Similar to the MME entity, the ME derives the key KeNB. The ME also derives the KRRCint key with the integrity protection algorithm indicated in the AS security mode command message. The ME will verify the integrity of the received security mode command message using the algorithm indicated and generated KRRCint key. Once the integrity protection check passes for the message, further keys like KRRCenc and KUPenc associated with a ciphering algorithm, are generated. The RRC and UP downlink deciphering (decryption) at the UE starts after receiving and successful verification of the AS security mode command message [11].

Step 21. The ME sends the AS security mode complete with integrity protection to the eNB. RRC and UP uplink ciphering (encryption) in the UE starts after sending the AS security mode complete message.

The integrity of the AS security mode complete is verified in the eNB. RRC and UP uplink deciphering (decryption) in the eNB starts after receiving and successfully verifying the AS security mode complete message.

Step 22. If the attach request is accepted by network, the MME will send the Attach accept message to the UE and the UE will respond with the attach complete message.

3. 5G Authentication

The 5G system aims to have inbuilt security features for different domains like network access, network domain, user domain, application domain, Service based Architecture (SBA) domain, Visibility and configurability of security domain.

For the 5G Authentication framework, the entities involved are the User equipment/USIM, AMF/SEAF from serving network and AUSF, and the UDM/ARPF/SIDF/UDR from the home network.

AMF/SEAF

The security anchor function (SEAF) provides the authentication functionality via the AMF in the serving network. The SEAF supports primary authentication using SUCI.

AUSF

The authentication server function (AUSF) in the home network handles authentication requests for both, 3GPP access and non-3GPP access. The AUSF provides SUPI to the Visited PLMN only after an authentication confirmation if the authentication request with SUCI was sent by Visited PLMN. The AUSF informs the UDM whether a successful or unsuccessful authentication of a subscriber has occurred.

UDM/ARPF/SIDF/UDR

Long-term key(s) used for authentication and security association setup purposes are protected from physical attacks and never leave the secure environment of the UDM/ARPF unprotected. The algorithm used for subscriber privacy is executed in the secure environment of the UDM. The SIDF is responsible for de-concealing the SUPI from the SUCI. When the Home Network Public Key is used for encryption of the SUPI, the SIDF uses the Home Network Private Key that is securely stored in the UDM to decrypt the SUCI. The Unified Data Repository (UDR) supports storage and retrieval of subscription data from the UDM and policy data from the PCF.

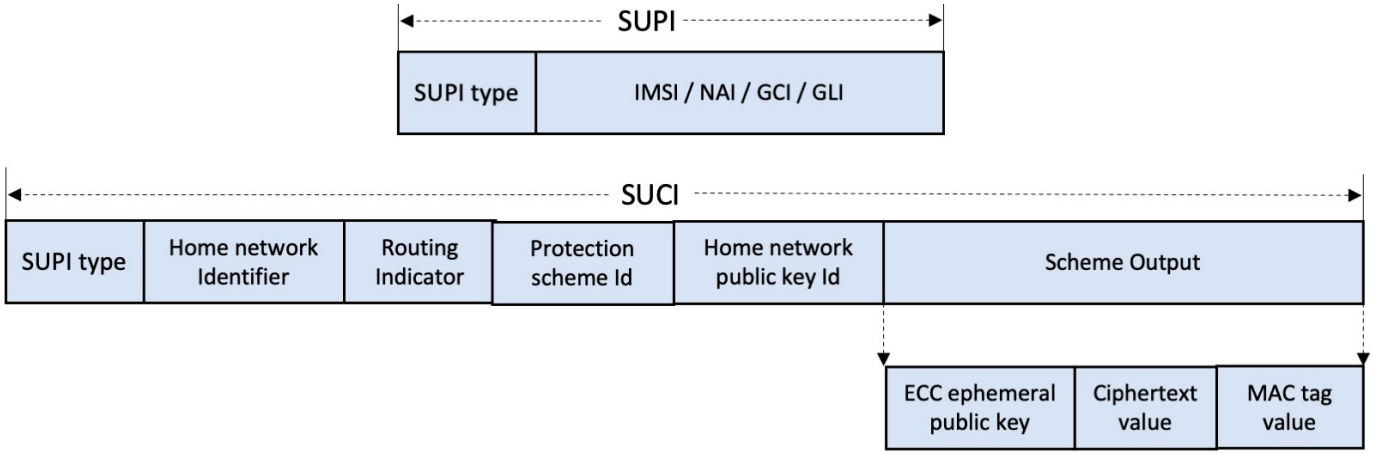
SUPI/SUCI

The 5G Authentication framework makes use of the subscriber and/or subscription identifiers (SUCI/SUPI). A globally unique 5G Subscription Permanent Identifier (SUPI) is allocated to each subscriber in the 5G system and is provisioned in the UDM/UDR.

The Subscription Concealed Identifier (SUCI) is a privacy preserving identifier containing the concealed SUPI. It is expected to be used in the NAS messages [12].

Figure 3-1 shows the structure of the SUPI and SUCI. The SUPI contains the SUPI type and followed by an IMSI or Network Access Identifier (NAI) or Global Cable Identifier (GCI) or Global Line Identifier (GLI). The SUCI contains the SUPI type, home network identifier, routing indicator, protection scheme identifier, home network public key identifier, scheme output.

Figure 3-1 Structure of SUPI and SUCI



SUCI concealment and de-concealment

SUCI concealment and de-concealment uses ECIES. Elliptic Curve Integrated Encryption Scheme (ECIES) encryption combines ECC based asymmetric cryptography with a symmetric cipher to provide data encryption by the EC private key and data decryption by the corresponding EC public key [13, 14]. All the symmetric keys can be derived in the UE and network independently.

Figure 3-2 depicts the brief overview of SUPI concealment and de-concealment using IMSI [15]. The UE constructs the SUCI using the HN public key and Ephemeral private key to generate the encrypted MSIN (concealed) with routing information, home network identifier in plain text (not concealed). The SIDF deciphers the encrypted MSIN using the HN private key and Ephemeral public key.

Figure 3-3 shows the detailed overview of SUPI concealment and de-concealment using ECIES, where A, B and C are results / output of SUPI concealment from the UE. Similarly, those are the inputs of SUPI de-concealment functionality at the home environment.

At UE, generate key pair (Ephemeral public key and private key) using key pair generation primitive. Based on the Diffie-Hellman primitive, a shared secret key element is derived (from public key of HN and generated ephemeral private key). Followed by that, key derivative function KDF is used to generate keying data K of length Encryption Key EK + Initial counter block ICB + MAC key. With the derived keys EK and ICB, symmetric encryption is performed to encrypt the plaintext block (SUPI) to generate the ciphered text. Use the tagging operation of the MAC scheme to compute the tag for the ciphered text using generated MAC key.

At SIDF, the received UE ephemeral public key and private key of home network is used to generate the ephemeral shared key. With the key derivative functions, generate keying data K of length decryption Key DK + Initial counter block ICB + MAC key. The generated DK and ICB is used to de-cipher the cipher text using symmetric decryption. Ephemeral MAC keys are used on ciphered text to generate the expected MAC, which is compared against the received MAC, and with this comparison the integrity of the SUCI is verified.

Figure 3-2 Brief overview of SUPI concealment / de-concealment

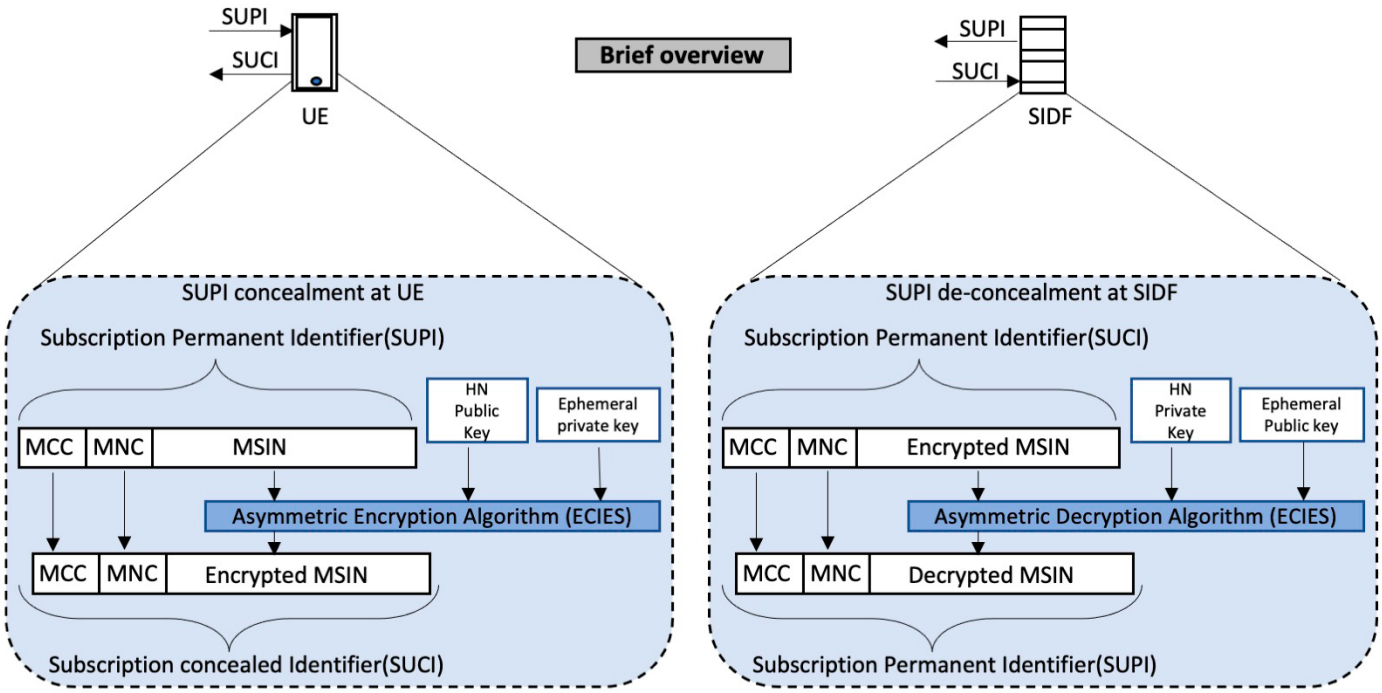
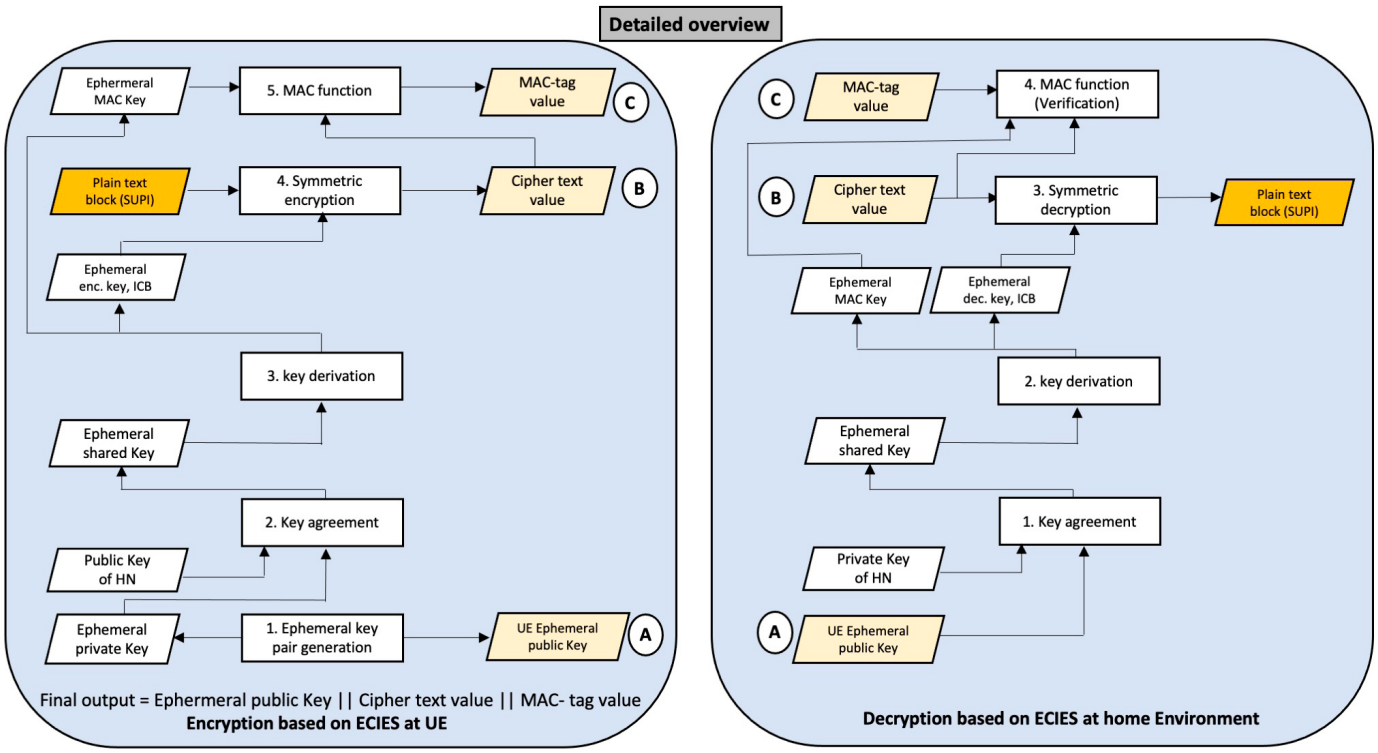


Figure 3-3 Detailed overview of SUPI concealment / de-concealment



3.1 5G AKA procedure

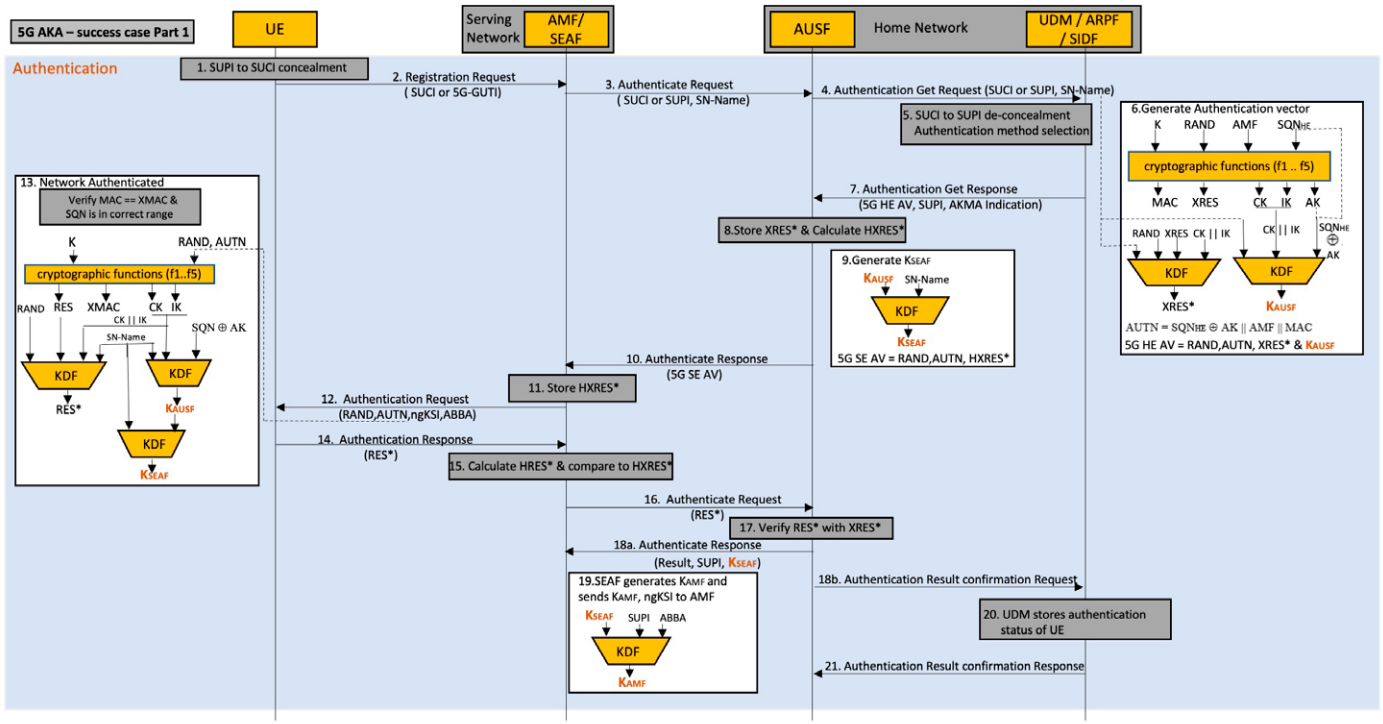
5G AKA enhances the EPS AKA from LTE by providing the home network with results of successful authentication of the UE from a visited or serving network, thus it provides assurance that the UE is present in the visited network at the authentication instance. Only after this successful verification is the SUPI of the UE is given to the serving network by the home network. This verified SUPI will be used in the serving network for Lawful Interception (LI) as well as billing purposes. In 4G, the home network provides multiple AVs to the serving network for UE authentication, but was not updated with UE authentication decisions, which was considered one of the weakness of 4G EPS-AKA. In 5G AKA, the authentication vectors are restricted to one vector per authentication run to ensure that the home network is always involved in the authentication and verification (presence of the UE in the serving network) of every UE.

3.1.1 Success case

The overall 5G AKA authentication procedure consists of the following basic phases:

- UE initiating registration procedure
- Home network computes AKA challenge
- Network authenticated by UE
- UE authenticated by serving network
- UE authenticated by home network
- Authentication result storage

Figure 3.1.1-1 5G AKA procedure for success case



UE initiating registration procedure

Step 1. When the user wants to access the 5G network, the UE performs the random access procedure and the RRC connection is setup between the UE and gNB. At the ME or USIM, the SUCI concealment is performed.

Step 2. The UE sends either the SUCI or 5G-GUTI (if assigned previously) in the Registration request message to the AMF/SEAF.

Step 3. The AMF/SEAF initiates the authentication by sending the Authenticate Request message with SUCI or SUPI (in case of valid 5G-GUTI) and the serving network name (SNN) to the AUSF.

Step 4. The AUSF checks the received serving network name with the expected serving network name. If authorized, the AUSF sends the Authentication Get Request message with the SUCI or SUPI and the serving network name to the UDM.

Step 5. The UDM invokes the SIDF if the SUCI is received. The SIDF will de-conceal the SUCI to gain the SUPI before the UDM can process the request. Based on the SUPI (subscription information), the UDM will give the inputs for invoking the authentication method (5G AKA, EAP-AKA' or EAP-TLS) by the AUSF.

NOTE 2: If the UE has the USIM, the 5G AKA or EAP-AKA´ can be used in any network. Key generating EAP methods such as EAP-TLS were introduced in 5G for non-public networks as well.

Home network computes AKA challenge

Step 6. The UDM/ARPF using cryptographic functions (f1,f2,f3,f4,f5) [5, 6, 7], computes a message authentication code MAC, response XRES, a cipher key CK, an integrity key IK and an anonymity key AK, by considering the inputs like the Long term key K, the generated new random number RAND, the authentication & key management field AMF and the freshly generated sequence number SQN (created by incrementing the stored non time based SQN or time based SQN generation or partial time based SQN generation [8]). The UDM/ARPF using key derivative functions KDF, computes the key KAUSF from the cipher key CK, integrity key IK, SNN and "XOR" of Sequence Number SQN and Anonymity Key AK. The UDM/ARPF also calculates expected response XRES* from RES, RAND, SNN with concatenated input keys CK and IK. Finally, the UDM/ARPF creates a 5G home environment authentication vector (5G HE AV) containing RAND, AUTN, XRES* and KAUSF.

Step 7. The UDM/ARPF sends the Authenticate Get Response message to the AUSF with 5G HE AV, SUPI and AKMA indication (if AKMA subscription is present).

Step 8. The AUSF stores the received KAUSF and XRES* temporarily together with the received SUPI. The AUSF computes the hashed expected response HXRES* by using the SHA-256 algorithm with the concatenated inputs RAND and XRES*.

Step 9. The AUSF generates the KSEAF using key derivative function with the KAUSF and serving network name as inputs. The generated KSEAF is stored in the AUSF temporarily. The AUSF returns the 5G Serving Environment Authentication vector (5G SE AV) containing the RAND, AUTN and HXRES*.

Step 10. The AUSF sends the Authenticate Response with the 5G Serving Environment Authentication vector to the AMF/SEAF.

Step 11. The AMF/SEAF stores the received hashed expected response HXRES*.

Step 12. The AMF/SEAF sends the RAND, the AUTN along with the next generation key set identifier (ngKSI) and Anti-Bidding down Between Architectures (ABBA) parameter in NAS message Authentication Request to the UE.

Network authenticated by UE

Step 13. At receipt of this message, the USIM verifies the freshness of the authentication vector by checking whether the AUTN can be accepted (an explanation of the AUTN verification is in section 2.1, step 8). If verification is successful, the USIM computes a response RES. The USIM also computes CK and IK which are sent to the ME. The KAUSF, RES* (like the XRES* generation) and KSEAF are computed in the ME, similar to generation at the UDM/ARPF.

Step 14. The UE responds with RES* in the NAS message Authentication Response to the SEAF.

UE authenticated by serving network

Step 15. The AMF/SEAF computes the HRES* using the SHA-256 hashing algorithm with the received response RES* and compares the HRES* with the expected hash value HXRES*. Authentication is considered as successful from the serving network point of view, if compared values are equal.

Step 16. The AMF/SEAF sends the RES*, as received from the UE in the Authenticate Request message to the AUSF.

UE authenticated by home network

Step 17. The AUSF considers that Authentication is successful from the home network point of view, if the received RES* is equal to the stored and expected response from the XRES*.

Step 18. The AUSF sends the Authenticate Response with the resulting key KSEAF and SUPI to the SEAF. The AUSF in parallel will inform the UDM about the authentication results (containing the SUPI, timestamp of authentication, authentication type and serving network name) in the Authentication Result confirmation Request message.

Step 19. The SEAF generates the key KAMF with received KSEAF, IMSI and ABBA parameter. The SEAF shares the generated KAMF, ngKSI to the AMF entity.

Authentication results storage

Step 20. The UDM stores the authentication status of the UE.

Step 21. The UDM replies to the AUSF with the Authentication Result Confirmation Response message.

Non-Access stratum security

Figure 3.1.1-2 5G AKA NAS and AS security procedure

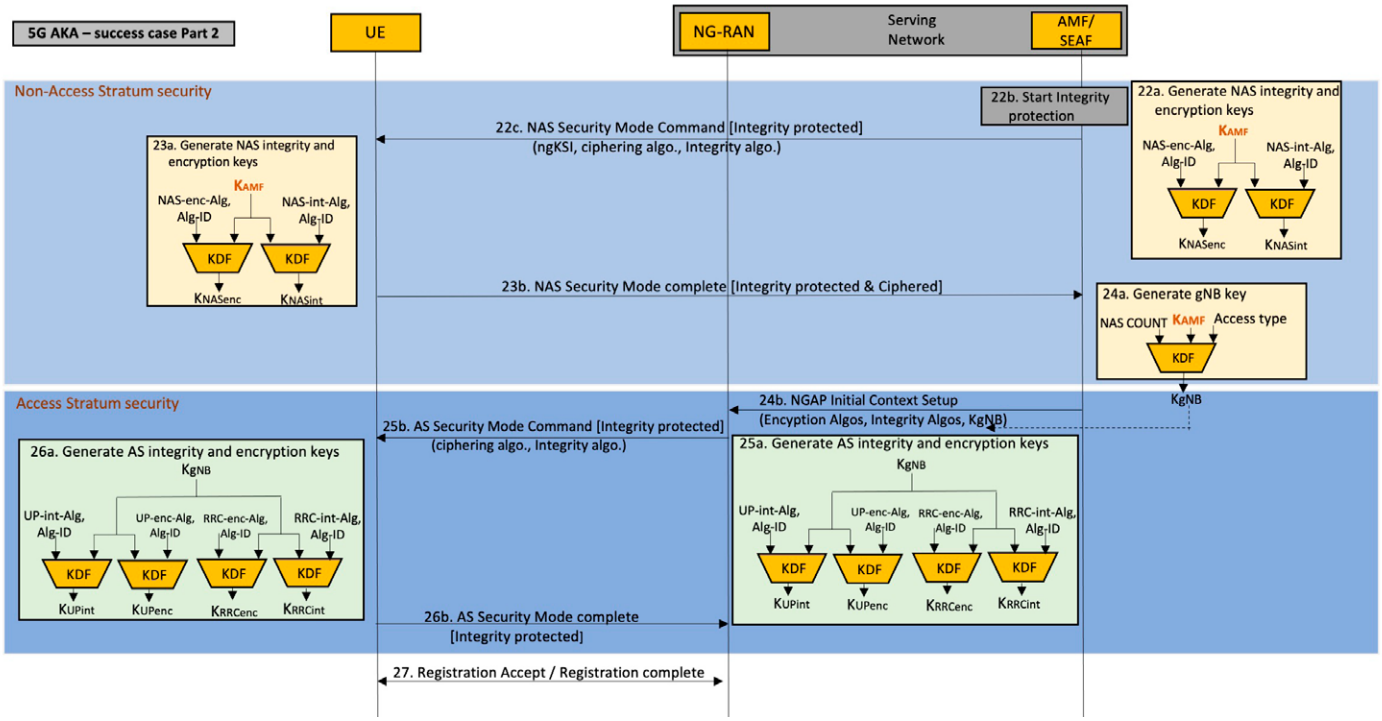


Figure 3.1.1-2 shows 5G AKA NAS and AS security procedure for 5G authentication.

Step 22. The AMF selects the NAS integrity protection and ciphering algorithms. Using the key derivative function, with selected algorithms and algorithm type distinguisher and received KAMF key, the NAS integrity and encryption keys (KNASint, KNASenc) are generated. The AMF/SEAF starts integrity protection for all downlink NAS messages. The NAS Security Mode Command (SMC) is sent to the UE with integrity protection and contains the selected ciphering algorithm, integrity algorithm and ngKSI. The AMF/SEAF activates the NAS uplink de-ciphering after sending the NAS SMC message.

Step 23. The UE verifies the NAS SMC integrity and if successful begins uplink ciphering, downlink de-ciphering and integrity protection. The UE with received algorithms, generates the NAS integrity and ciphering keys such as the AMF entity. The NAS security mode complete is sent to the AMF with the ciphered and integrity protected.

Step 24. The AMF de-ciphers and checks the integrity protection of the received NAS security mode complete using the key and algorithm indicated in the NAS security mode command. The NAS downlink ciphering at the AMF will start after receiving the NAS security mode complete message. The AMF generates the key KgNB with uplink NAS COUNT, KAMF and access type distinguisher (3GPP or non-3GPP access). The AMF sends the UE 5G security capabilities with ciphering and integrity protected algorithms and generated KgNB key in the NGAP initial context setup message to the gNB.

Access stratum security

Step 25. The gNB chooses the integrity and ciphering algorithm which has the highest priority from its configured list and presents it in the UE 5G security capabilities received from the AMF. The gNB generates the RRC integrity key KRRCint and the UP integrity key KUPint from inputs of the 256-bit KgNB, selected AS integrity algorithm (algo identity) and algorithm type distinguisher. The gNB also generates the RRC ciphering key KRRCenc and UP ciphering key KUPenc from inputs of the 256-bit KgNB, selected AS encryption algorithm (algo identity) and algorithm type distinguisher. The gNB starts integrity protection for all RRC messages. The integrity protected AS security mode command (SMC) message is sent from the gNB to the UE with the integrity algorithm and ciphering algorithm. The RRC downlink ciphering at the gNB starts after sending the AS security mode command message.

Step 26. The UE verifies the AS SMC integrity and if successful starts the RRC integrity protection and RRC downlink de-ciphering. The UE generates control plane and data plane ciphering and integrity keys like the gNB. The AS security mode complete message with integrity protection is sent to the gNB. The RRC uplink ciphering at the UE starts after sending the AS security mode complete message. Integrity of this message is verified at the gNB and it also starts the RRC uplink deciphering.

Step 27. The NAS level registration accepts and registration complete messages are exchanged between the UE and network.

3.1.2 Failure case (Synch failure)

Figure 3.1.2-1 5G AKA procedure with sync failure case

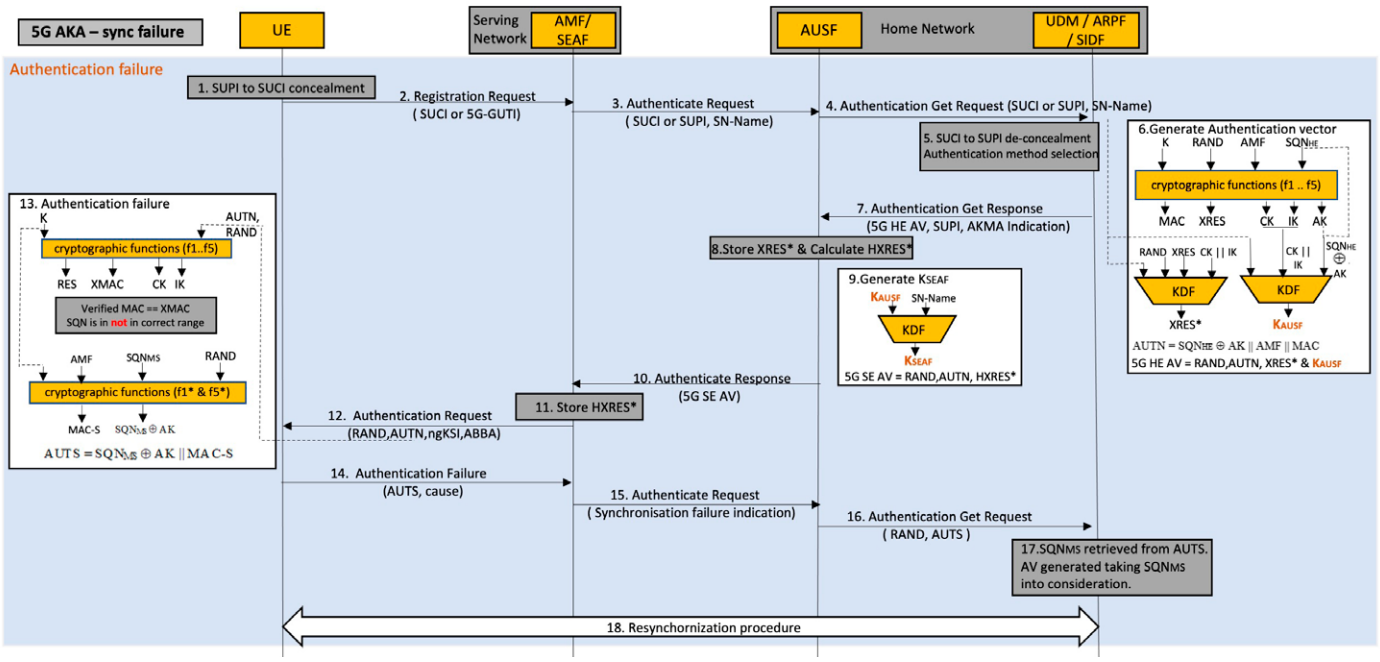


Figure 3.1.2-1 shows 5G AKA procedure for synchronization failure case.

Step 1. to 12. are the same as section 4.1 procedures.

Step 13. Upon receipt of the Authentication request message, the USIM verifies the freshness of the authentication vector by checking whether the AUTN can be accepted. If MAC verification has passed (MAC == XMAC) but the received sequence number is not in range or is invalid (when compared to previously store SQNMS), synchronization failure results. The USIM calculates the AUTS using cryptographic functions f1* and f5* with inputs like Key K, received RAND, AMF field and SQNMS (the accepted SQN from previous successful authentication). The calculated AUTS is sent from the USIM to the ME.

Step 14. The ME sends the Authentication failure message with the synchronization failure cause and the AUTS to the AMF/SEAF.

Step 15. The AMF/SEAF sends the Authenticate Request message with the "synchronization failure indication" to the AUSF.

Step 16. The AUSF sends the Authentication Get Request message with RAND and AUTS to the UDM/ARPF.

Step 17. The UDM/ARPF retrieves the SQNMS received in the AUTS from the UE and generates a new Authentication vector.

Step 18. The re-synchronization procedure (new 5G AKA challenge) begins between the UE and home network.

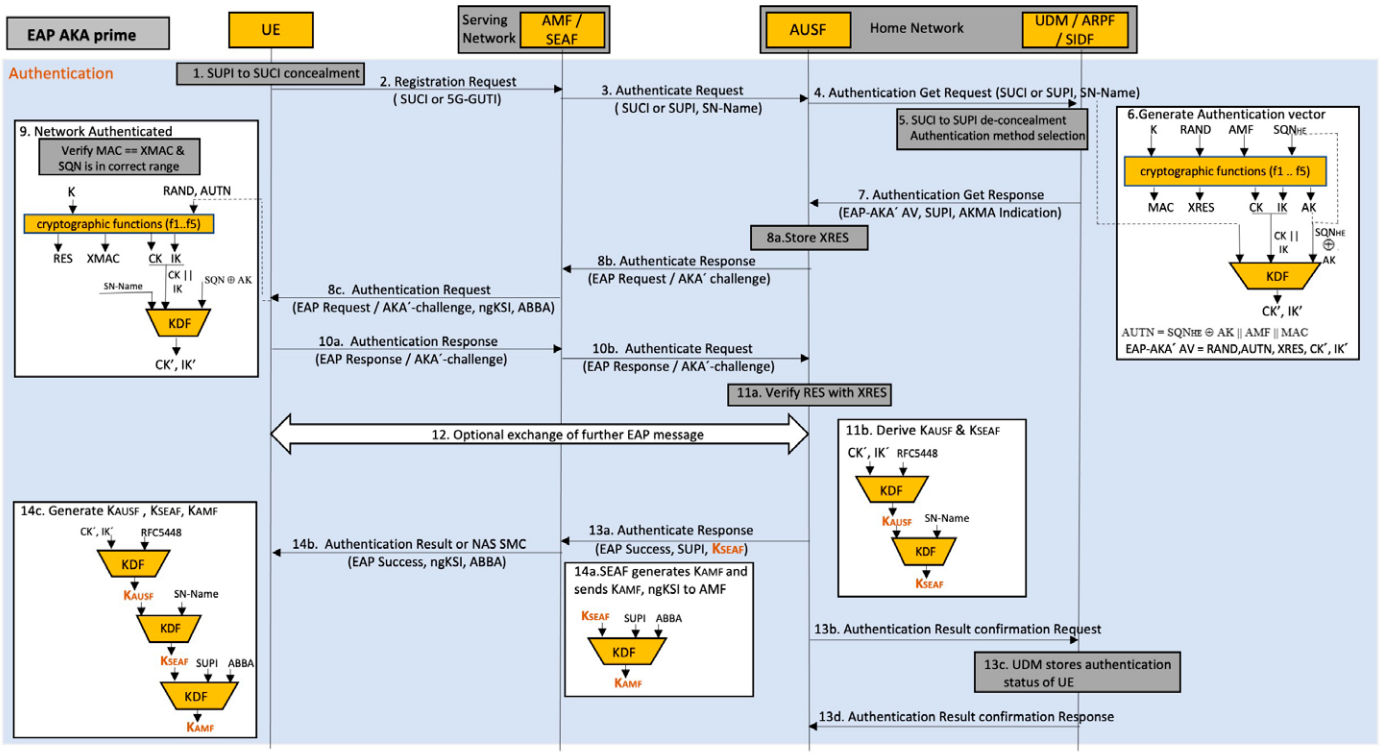
3.1.2.1 Avoiding frequent sync failures:

The UE may change the domains, for example from 3G to 4G, and the SQN at the USIM might not be synced with the Home environment database. To avoid frequent sync failures at the UE, it is recommended to use SQN ranges specific to the domains (example: IMS,3G,4G,5G) in the HE. This means detecting the domain from the authentication messages in the Home environment and managing the SQN separately for each domain. Example: IND within SQN for IMS is having a range of 0 to 6, for 3G AKA range is from 7 to 12, etc.

3.2 EAP AKA Prime procedure

Another authentication supported by 5GS is EAP AKA ´[16]. EAP is extensible in the sense that different authentication methods can be used within this framework. In LTE, the EAP-AKA´ method is specified only for non-3GPP access. In 5G, however, it can be used for any kind of access. When comparing EAP-AKA´ with EAP-AKA, the primary change is that the newly derived keys are bounded to the name of the access network. Message flow differs from 5G-AKA with the NAS messages in the EAP encapsulated in EAP-AKA´. Differing from 5G AKA, the serving network is transparent and is not involved in authentication verifications. Figure 3.2-1 shows the EAP AKA' method with key derivations incorporated in the flow.

Figure 3.2-1 EAP AKA prime procedure



UE initiating Registration procedure

Step 1. to 5. are the same as section 4.1 procedures.

Home network computes AKA challenge

Step 6. The UDM/ARPF using cryptographic functions (f1,f2,f3,f4,f5) [5, 6, 7], computes a message authentication code MAC, expected response XRES, a cipher key CK, an integrity key IK and an anonymity key AK by considering the inputs like Long term key K, generated new random number RAND, authentication & key management field AMF and freshly generated sequence number SQN (created by incremental of stored non time based SQN or time based SQN generation or partial time based SQN generation [8]). The UDM/ARPF using the key derivative functions KDF, computes the key CK´ and IK´ from cipher key CK, integrity key IK, SNN, 'exclusive or' (XOR) of Sequence Number SQN and Anonymity Key AK. Finally, the UDM/ARPF creates the EAP AKA´ Authentication Vector containing the RAND, AUTN, XRES CK´ and IK´.

Step 7. The UDM/ARPF sends the Authentication Get Response with the EAP-AKA´ authentication vector, SUPI and AKMA indication (if the AKMA is subscribed) to the AUSF.

Step 8. The AUSF stores the expected response XRES temporarily for future verification and sends the EAP-Request/AKA´ challenge message in Authenticate Response message to the SEAF. The SEAF transparently forwards the EAP-Request/AKA´-challenge message to the UE in the NAS message Authentication Request with the ngKSI and ABBA parameter.

Network authenticated by UE

Step 9. At receipt of this message, the USIM verifies the freshness of the authentication vector by checking whether the AUTN can be accepted (an explanation of the AUTN verification is in section 2.1, step 8). If verification is successful, the USIM computes a response RES, CK and IK which are sent to the ME. The CK´ and IK´ are computed in the ME, similar to the generation at UDM/ARPF. The network is now considered as authenticated by the UE.

Step 10. The UE responds with the RES in the NAS message Authentication Response to the SEAF. The SEAF forwards the EAP-Response/ AKA'-Challenge message transparently in the Authenticate Request message to the AUSF.

UE authenticated by home network

Step 11. The AUSF verifies the received RES with the expected response XRES and the authentication is considered as successful from the home network point of view. The AUSF derives the Extended Master Session Key EMSK from CK´ and IK´. The most significant 256 bits of EMSK are considered as KAUSF and KSEAF is derived from KAUSF and Serving network name.

Step 12. The AUSF and UE can have optional an AKA´-Notification exchange of messages for result or error indication.

Step 13. The AUSF informs the UDM about the results of the authentication, which is stored in the UDM. In parallel, the AUSF sends the EAP-Success message in the Authenticate Response with KSEAF and the SUPI to the SEAF.

Step 14. The SEAF derives the KAMF from the KSEAF with other inputs like the ABBA parameter and SUPI and forwards the KAMF to the AMF. The SEAF also sends the EAP-Success message in either the NAS SMC or Authentication result message with the ngKSI and ABBA parameter to the UE. The UE derives all keys KAUSF, KSEAF, KAMF like key derivation at the network side.

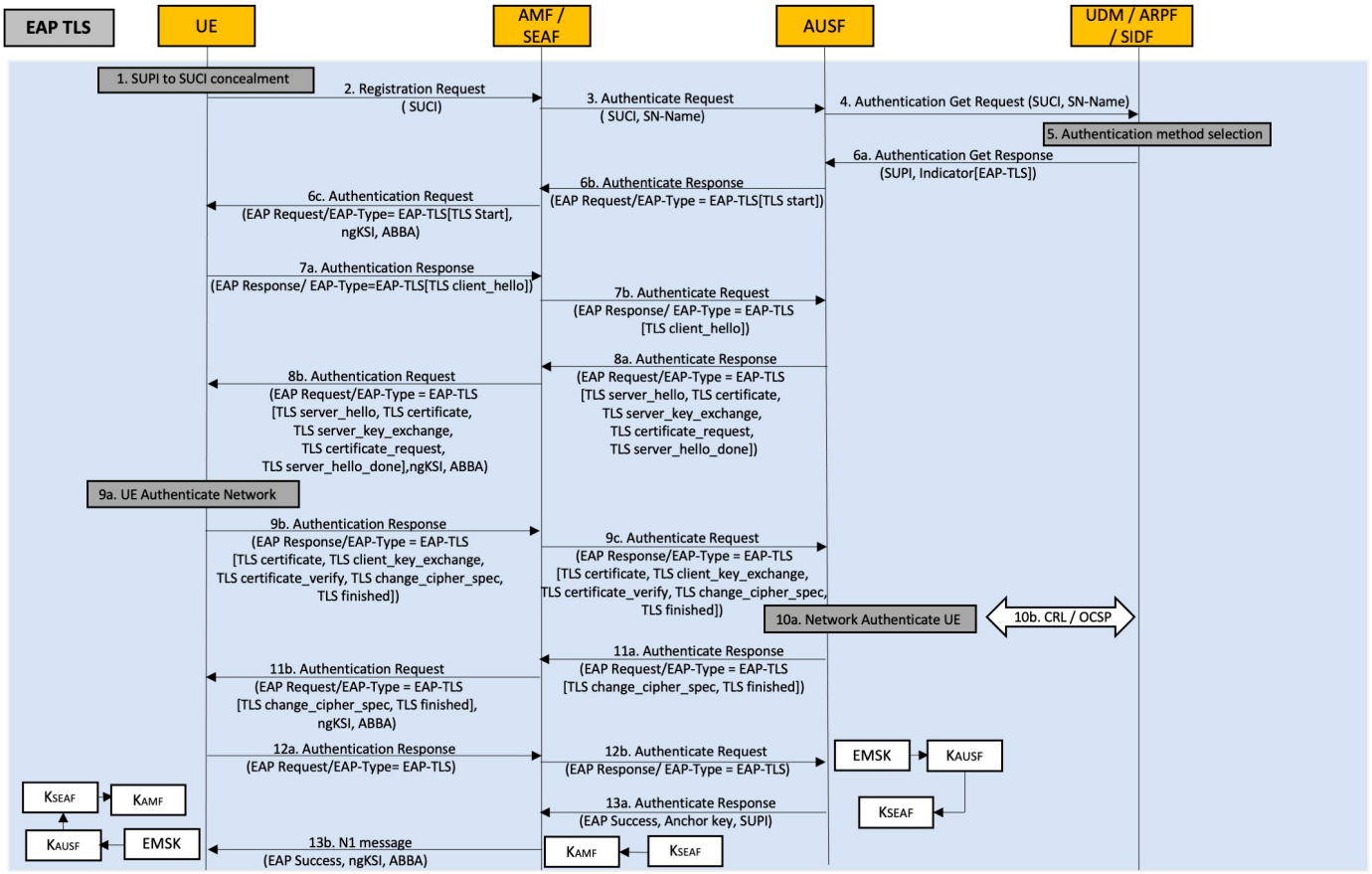
NOTE 3: The NAS and AS security procedures are same as in the 5G AKA as described in chapter 4.1.

3.3 EAP TLS procedure

EAP-TLS is another mutual authentication method supported by 5GS and uses the EAP method, where the EAP peer and EAP server will authenticate each other. In EAP-TLS, mutual authentication between the UE and 5G home environment is obtained based on mutual trust of their public key certificates. EAP-TLS is widely used in vertical industries, for example, in the authentication of WIFI devices. Therefore, the support of EAP-TLS within the 5GS is a further step to facilitate the integration with verticals and enterprises.

EAP-TLS supports several TLS versions. The main principle behind the EAP-TLS version negotiation is that the EAP server indicates the support of EAP-TLS, and if the peer chooses EAP-TLS, it responds with a ClientHello message with the TLS versions it supports. The EAP server chooses the TLS version and indicates the chosen version in a ServerHello message. This authentication procedure is intended for private networks or with IoT devices in isolated deployment scenarios (roaming is not considered) or to support N5GC devices.

Figure 3.3-1 EAP TLS procedure



Step 1. to 5. are the same as section 4.1 procedures.

NOTE 4: In case of privacy considerations, the username part from the NAI is omitted and only the realm part is included in the SUCI in step 1 of figure 3.3-1.

Step 6. The UDM forwards the SUPI and EAP-TLS indicator in the Authenticate Get Response message to the AUSF. The AUSF uses the EAP-TLS as the authentication method with received SUPI and indicator. The AUSF sends the Authenticate Response message with the EAP-Request/EAP-TLS [TLS start] message to the SEAF. The SEAF forwards the content transparently in the Authentication request message to the UE along with ngKSI and ABBA parameters.

Step 7. The UE replies with the EAP-Response/EAP-TLS[Client_hello] to the SEAF in the Authentication response message. The content of the "client_hello" is a UE TLS version, Session id, random number and set of cipher suites supported by the UE. The SEAF forwards the same content to the AUSF.

Step 8. The AUSF replies to the SEAF with the EAP request / EAP-TLS with further info elements like the server_hello, server certificate, server key exchange, certificate request, server hello done (last handshake message). The server_hello handshake message contains a TLS version number, another random number, a sessionId, and a ciphersuite. The SEAF forwards the same content in the Authentication request to the UE.

Step 9. The UE is required to be pre-configured with the UE certificates and the CA root certificate, which is used to verify server certificates. If the TLS server authentication is successful, then the UE replies to

the SEAF with an Authentication response with a client certificate, client key exchange, cipher spec and client finished. The SEAF forwards the same content to the AUSF.

NOTE 5: In case of privacy considerations, in steps 9b and 9c, the UE instead of sending the client certificate in cleartext, will first send no certificate and then later sends the TLS certificate (after the TLS is setup)

Step 10. The AUSF verifies that the client certificate provided by the UE belongs to the subscriber identified by the SUPI. If there is a mismatch in subscriber identifiers in the SUPI, the AUSF does not accept the client certificate. The AUSF is required to be pre-configured with the root or any intermediary CA certificates used to verify the UE certificates. The UDM/ARPF is responsible for such subscriber status information, provided to the AUSF with one of the methods CRL / OCSP (more details in 3.3.1).

NOTE 6: In case of privacy consideration, the AUSF derives the SUPI from the client identifier in the TLS client certificate. The AUSF can verify the received the SUPI with the UDM. The AUSF also forwards the authentication results to the UDM for storage.

Step 11. The AUSF sends the EAP request with the EAP-TLS message with the change cipher spec info and server finished indication to the SEAF. The SEAF forwards it to the UE along with the ngKSI and ABBA parameters.

Step 12. The UE sends the empty EAP-TLS message to the SEAF in the Authentication response message. The SEAF forwards the EAP-Response/EAP-TLS message to the AUSF.

Step 13. The AUSF uses the most significant 256 bits of EMSK [18] as KAUSF and calculates KSEAF from KAUSF. The AUSF forwards the EAP-success message with the SUPI and anchor key KSEAF to the SEAF. The SEAF derives KAMF from key KSEAF and the NAS SMC or Authentication result with the EAP success message is sent to the UE. The UE derives all required keys similar to the network key derivation.

3.3.1 Certificate enrollment

The UE needs to have a private key and the corresponding UE certificate (containing the UE public key) and a CA root certificate, which needs to be enrolled to the UE, prior to the initial authentication. Certificate management infrastructure of an enterprise might be re-used for the enrollment of the UE certificate. Exact storage and usage of this certificate-based UE credentials might depend on the specific needs of the vertical industry. It is currently an ongoing subject for further studies.

The AUSF needs a private key and a server certificate (containing the server public key) and a CA root certificate, used for the verification of the UE certificate. The UE and server certificate can be issued by the same certificate authority (CA). In this case, the CA root certificate on the UE and AUSF are the same.

3.3.2 Revocation

When a subscriber certificate is issued, it is expected to be in use for its entire or scheduled validity period. However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period. Under such circumstances, the issuing certificate authority (CA) needs to revoke the certificate. There are two ways in which certificates can be revoked.

1) Certificate Revocation List (CRL)

2) Online Certificate Status Protocol (OCSP)

Certificate Revocation List

The UDM/ARPF maintains the CRLs and the list can be periodically requested by the AUSF with a TLS certificate revocation list download request message. The UDM/AUSF responds with the list in a TLS certificate revocation list message. Once the list is received, the AUSF stores the CRL locally.

Online Certificate Status Protocol

If the UDM/ARPF supports OCSP, then the AUSF will check the certificate status by sending a TLS certificate status request to the UDM/ARPF. The certificate status (good, revoked or unknown) response is sent in a TLS certificate status response. If the status is revoked, it indicates the time at which the certificate was revoked and, optionally, the reason why it was revoked.

4. Comparison of EPS AKA / 5G AKA / EAP AKA prime / EAP TLS

Comparison of EPS AKA used in 4G and all other authentication methods in 5G are shown in below table [17].

Comparision 4G vs 5G	EPS-AKA (4G Authentication)	5G-AKA (5G Authentication)	EAP AKA´ (5G Authentication)	EAP TLS (5G Authentication)
Entity in User Equipment [UE]	USIM	USIM	USIM	Non-USIM
Entity in Serving Network [SN]	MME	AMF / SEAF	AMF / SEAF	AMF / SEAF
Entity in Home Environment [HE]	HSS	AUSF / UDM / ARPF / SIDF	AUSF / UDM / ARPF / SIDF	AUSF / UDM / ARPF / SIDF
UE Identity between UE & SN	IMSI / GUTI	SUCI / 5G-GUTI	SUCI / 5G-GUTI	SUCI / 5G-GUTI
UE Identity between SN & HE	IMSI	SUCI / SUPI	SUCI / SUPI	SUCI / SUPI
SN Identity	SN Id [MCC+MNC]	SN Name [5G: MCC+MNC],NID(SNPN)	SN Name [5G: MCC+MNC], NID(SNPN)	SN Name [5G: MCC+MNC], NID(SNPN)
Messaging between UE & SN	NAS	NAS	NAS - EAP	NAS - EAP
Messaging between SN & HE	Diameter	HTTP based API	HTTP based API	HTTP based API
Cryptography	Shared key cryptography	Shared key cryptography	Shared key cryptography	Public Key cryptography
AV generated by	HSS	UDM / ARPF	UDM / ARPF	AV not generated
AV generation	HSS generates many AV & stores in MME	UDM / ARPF generates only one AV at a time	UDM / ARPF generates only one AV at a time	AV not generated
Authentication of UE decided by which Entity	MME	SEAF & AUSF	AUSF	AUSF
HE is informed of UE Authentication	No	Yes	Yes	Yes
When are Key generated	- K_{ASME} generated at HSS during AV generation. - K_{ASME} generated at UE when network is authenticated	- K_{AUSF} generated at UDM and K_{SEAF} in AUSF during initial AKA challenge. K_{AMF} generated after successful authenitcation. - K_{AUSF},K_{SEAF}, K_{AMF} generated at UE when network is authenticated	- K_{AUSF} & K_{SEAF} in AUSF, K_{AMF} in SEAF are generated only after successful authenitcation. - K_{AUSF},K_{SEAF}, K_{AMF} are generated at UE only after successful authentication.	- K_{AUSF} & K_{SEAF} in AUSF, K_{AMF} in SEAF are generated only after successful authenitcation. - K_{AUSF},K_{SEAF}, K_{AMF} are generated at UE only after successful authentication.
Key Hierachy	K -> CK,IK -> K_{ASME}	K -> CK,IK -> K_{AUSF} -> K_{SEAF} ->K_{AMF}	K -> CK,IK -> CK´,IK´->EMSK ----> K_{AMF} <- K_{SEAF} <- K_{AUSF} <---------	EMSK-> K_{AUSF} -> K_{SEAF} -> K_{AMF}

5. Conclusion

4G system security has a few weaknesses. For example, the UE identity - IMSI is transmitted in plain text. This can result in the tracking of a user and home network that are never involved in the authentication decision (HE is consulted only for AV generation, but results of UE authentication while using individual AV, is never updated by serving network).

5G system security solves the issues that are considered as weaknesses in 4G. The 5G system supports the different authentication methods, 5G-AKA, EAP-AKA' and EAP-TLS. Each of these are strong protocols well suited for different deployment scenarios corresponding to the different industry segments 5G addresses. The protocol choice for deployment should be based on the network and industry scenario. Nokia product and services teams are eager to offer their expertise to support network operators in the technical analysis and final choice, as well as the implementation.

Acknowledgement

We would like to express our special gratitude and thanks to German Peinado, Markus Staufer, Anja Jerichow, Annett Seefeldt, Saurabh Khare and Raphael Lasar for their review and suggested enhancements.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID210846 (February)