A Comparative Introduction to 4G and 5G Authentication

WINTER 2019

INFORMED™ INSIGHTS

CableLabs®

CableLabs

As the leading Innovation and R&D lab for the cable industry, CableLabs creates global impact through its 60+ cable-network-operator members located in the United States, Canada, Mexico, Central America, South America, Europe, Asia, and Australia, representing approximately 180 million subscribers and roughly 500 million individuals.

CableLabs' innovation and R&D efforts are focused in the areas of wireless network technologies, including in both licensed and unlicensed spectrum; wired network technologies, including both fiber and coaxial cable technologies; cybersecurity; and artificial intelligence. With a state-of-the art research and innovation facility and a collaborative ecosystem of partners including academia, government, and thousands of vendors, CableLabs delivers impactful network technologies for the entire industry.

Inform[ED] Insights

CableLabs created the Inform[ED] Insights series to address major technology developments that have the potential to transform the cable business and society at large.

The cable industry connects and entertains people across the globe, contributing significantly to economic growth and enabling rich discourse in its countries of operation. Inform[ED] Insights provides leaders across sectors and disciplines with communications technology facts and insights on which to base major decisions.

For more information, please visit https://www.cablelabs.com/informed-insights/.

Authentication and key management are fundamental to the security of cellular networks because they provide mutual authentication between users and the network and derive cryptographic keys to protect both signaling and user plane data.

Each generation of cellular networks always defines at least one authentication method. For example, 4G defines 4G EPS-AKA, and 5G defines three authentication methods—5G-AKA, EAP-AKA', and EAP-TLS.

Because additional authentication methods are defined in 5G, wireless practitioners often ask what motivates the adoption of these new authentication methods in 5G and how they differ from 4G authentication. This paper attempts to answer those questions by providing a comparative study of 4G and 5G authentication. The analysis shows that 5G authentication improves upon 4G authentication through a number of features, including a unified authentication framework that can support more user cases, better user equipment identity protection, enhanced home-network control, and more key separation in key derivation, among others. The paper also discusses the weaknesses of 5G authentication and its need to continuously evolve.

Contents

1. Introduction

Cellular network technologies have evolved over several generations, including 2G, 3G, and 4G, and 3GPP (3rd Generation Partnership Project) is actively developing 5G specifications. 5G differs from prior generations primarily in that it will not only provide faster speed, higher bandwidth, and lower delays, but also support more use cases such as enhanced mobile broadband (eMBB), massive machine-type communications (mMTC), and ultra-reliable low-latency communications (uRLLC). It is anticipated that 5G will begin deploying around the globe starting in 2019, and establishing security and privacy with 5G is of critical importance to its successful deployment in the real world.

Security and privacy issues in prior generations, particularly in radio access networks (RANs), have been extensively studied. A few of the many issues discovered are listed below.

- **Lack of network authentication in 2G, resulting in attacks such as network spoofing by faked base stations**—For example, a faked base station can advertise a different tracking area code with a stronger signal strength to lure user equipment (UE) away from its legitimate cellular network to register with the faked base station [1]. As a result, the faked base station can then send text messages to the UE and thus attempt to defraud the user.

- **Lack of integrity protection for certain signaling messages, thus allowing signal spoofing and tampering**—For example, an Identity Request (a non-access stratum [NAS] signaling message in Long-Term Evolution [LTE]), if not protected with authentication and integrity, can be sent by a faked base station to steal UE permanent identifiers, e.g., the international mobile subscriber identity (IMSI) [1].

- **Lack of confidentiality in certain signaling messages, resulting in privacy violation**—For example, paging information, which is not encrypted, can be used to detect the presence of a particular user and even to track the user to a precise location [2].

To help mitigate those issues, the 3GPP defines an Authentication and Key Agreement (AKA) protocol and procedures that support entity authentication, message integrity, and message confidentiality, among other security properties. The 3GPP AKA protocol

The 3GPP AKA protocol is a challenge-and-response authentication protocol based on a symmetric key shared between a subscriber and a home network. After the mutual authentication between a subscriber and a home network, cryptographic keying materials are derived to protect subsequent communication between a subscriber and a serving network, including both signaling messages and user plane data (e.g., over radio channels).

is a challenge-and-response authentication protocol based on a symmetric key shared between a subscriber and a home network, cryptographic keying materials are derived to protect subsequent communication between a subscriber and a serving network, including both signaling messages and user plane data (e.g., over radio channels).

This paper provides an overview of the 4G and 5G authentication methods defined by the 3GPP—4G EPS-AKA [3] and 5G AKA, EAP-AKA', and EAP-TLS [4]. It also highlights the differences between 4G AKA and 5G AKA protocols and among the three 5G authentication methods.

2. 4G Authentication

From an authentication perspective, a cellular network consists of three main components: UEs, a serving network (SN), and a home network (HN) (Figure 1).

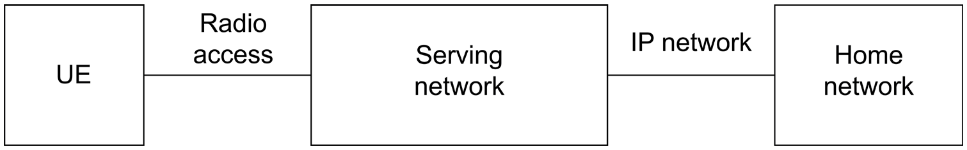

Figure 1 – Cellular Network Architecture

Each UE has a universal integrated circuit card (UICC) hosting at least a universal subscriber identity module (USIM) application, which stores a cryptographic key that is shared with the subscriber's home network. A serving network in 4G consists of radio access equipment such as an Evolved NodeB (eNodeB) base station and Mobility Management Entities (MMEs), among others. The UE communicates with a serving network through radio interfaces. A home network in 4G usually consists of authentication servers such as the home subscriber server (HSS), which stores user credentials and authenticates users. Communication between serving networks and a home network is based on IP; the core entities that are connected over an IP network are collectively referred to as the Evolved Packet System (EPS).

a. 4G EPS-AKA

The EPS-AKA is triggered after the UE completes the Radio Resource Control (RRC) procedure with eNodeB and sends an Attach Request message to the MME (see Figure 2). The MME sends an Authentication Request, including UE identity (i.e., IMSI) and the serving network identifier, to the HSS located in the home network. The HSS performs cryptographic operations based on the shared secret key, K_i (shared with the UE), to derive one or more authentication vectors (AVs), which are sent back to the MME in an Authentication Response message. An AV consists of an authentication (AUTH) token and an expected authentication response (XAUTH) token, among other data.

After receiving an Authentication Response message from the HSS, the MME sends an Authentication Request to the UE, including the AUTH token. The UE validates the AUTH token by comparing it to a generated token based on K_i. If the validation succeeds, the UE considers the network to be legitimate and sends an Authentication Response message back to the MME, including a response (RES) token, which is also generated based on K_i.

The MME compares the RES token with an expected response (XRES) token. If they are equal, the MME performs key derivation and sends a Security Mode Command message to the UE, which then derives the corresponding keys for protecting subsequent NAS signaling messages. The MME will also send the eNodeB a key from which the keys for protecting the RRC channel are derived. After the UE also derives the corresponding keys, subsequent communication between the UE and the eNodeB is then protected.

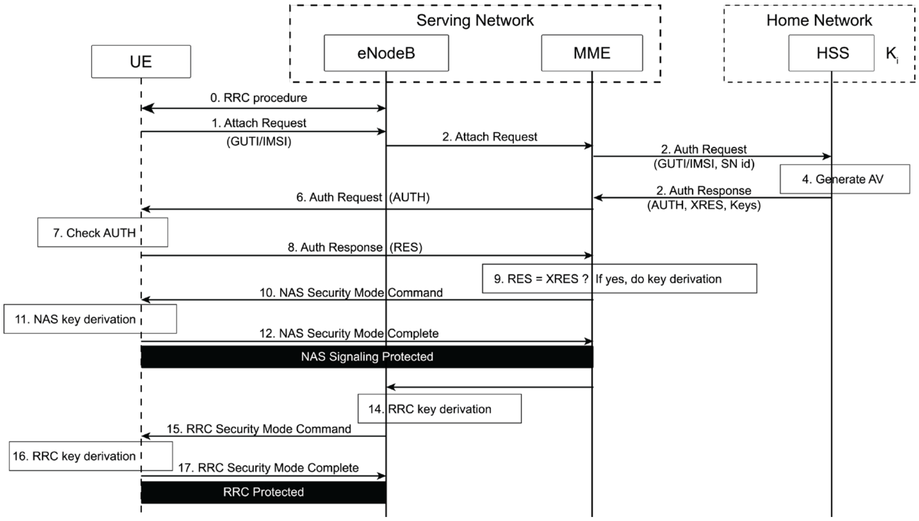

Figure 2 – LTE Authentication Procedure

There are two weaknesses in 4G EPS-AKA.

1. First, the UE identity is sent over radio networks without encryption. Although a temporary identifier (e.g., Globally Unique Temporary Identity, GUTI) may be used to

hide a subscriber's long-term identity, researchers have shown that GUTI allocation is flawed: GUTIs are not changed as frequently as necessary [1], and GUTI allocation is predictable (e.g., with fixed bytes) [5]. More importantly, the UE's permanent identity may be sent in clear text in an Identity Response message when responding to an Identity Request message from a network.

2. Second, a home network provides AVs when consulted by a serving network during UE authentication, but it is not a part of the authentication decision. Such a decision is made solely by the serving network.

The following sections show that 5G authentication has improved on these issues.

3. 5G Authentication

Service-based architecture (SBA) has been proposed for the 5G core network. Accordingly, new entities and new service requests have also been defined in 5G. Some of the new entities relevant to 5G authentication are listed below.

- The Security Anchor Function (SEAF) is in a serving network and is a "middleman" during the authentication process between a UE and its home network. It can reject an authentication from the UE, but it relies on the UE's home network to accept the authentication.

- The Authentication Server Function (AUSF) is in a home network and performs authentication with a UE. It makes the decision on UE authentication, but it relies on backend service for computing the authentication data and keying materials when 5G-AKA or EAP-AKA' is used.

- Unified data management (UDM) is an entity that hosts functions related to data management, such as the Authentication Credential Repository and Processing Function (ARPF), which selects an authentication method based on subscriber identity and configured policy and computes the authentication data and keying materials for the AUSF if needed.

- The Subscription Identifier De-concealing Function (SIDF) decrypts a Subscription Concealed Identifier (SUCI) to obtain its long-term identity, namely the Subscription Permanent Identifier (SUPI), e.g., the IMSI. In 5G, a subscriber long-term identity is always transmitted over the radio interfaces in an encrypted form. More specifically, a public key-based encryption is used to protect the SUPI. Therefore, only the SIDF has access to the private key associated with a public key distributed to UEs for encrypting their SUPIs.

The next section introduces the 5G authentication framework and three authentication methods: 5G-AKA, EAP-AKA', and EAP-TLS. It includes detailed message flows for 5G-AKA and summarizes the differences between 5G-AKA and both EAP-AKA' and EAP-TLS.

a. 5G Authentication Framework

A unified authentication framework has been defined to make 5G authentication both open (e.g., with the support of EAP) and access-network agnostic (e.g., supporting both 3GGP access networks and non-3GPP access networks such as Wi-Fi and cable networks) (see Figure 3).

When EAP (Extensible Authentication Protocol) is used (e.g., EAP-AKA' or EAP-TLS), EAP authentication is between the UE (an EAP peer) and the AUSF (an EAP server) through the SEAF (functioning as an EAP pass-through authenticator).

A unified authentication framework has been defined to make 5G authentication both open (e.g., with the support of EAP) and access-network agnostic (e.g., supporting both 3GGP access networks and non-3GPP access networks such as Wi-Fi and cable networks) .

When authentication is over untrusted, non-3GPP access networks, a new entity, namely the Non-3GPP Interworking Function (N3IWF), is required to function as a VPN server to allow the UE to access the 5G core over untrusted, non-3GPP networks through IPsec (IP Security) tunnels.

Several security contexts can be established with one authentication execution, allowing the UE to move from a 3GPP access network to a non-3GPP network without having to be reauthenticated.

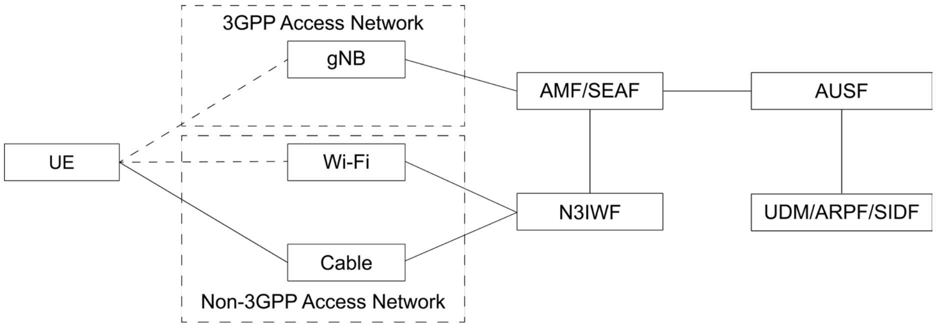

Figure 3 – 5G Authentication Framework

b. 5G-AKA

5G defines new authentication-related services. For example, the AUSF provides authentication service through Nausf_UEAuthentication, and UDM provides its authentication service through Nudm_UEAuthentication. For simplicity, generic messages such as Authentication Request and Authentication Response are used in Figure 4 without referring to the actual authentication service names. Further, an authentication vector includes a set of data, but only a subset is shown in Figure 4.

In 5G-AKA, the SEAF may start the authentication procedure after receiving any signaling message from the UE. Note that the UE should send the SEAF a temporary identifier (a 5G-GUTI) or an encrypted permanent identifier (a SUCI) if a 5G-GUTI has not been allocated by the serving network for the UE. The SUCI is the encrypted form of the SUPI using the public key of the home network. Thus, a UE's permanent identifier, e.g., the IMSI, is never sent in clear text over the radio networks in 5G. This feature is considered a major security improvement over prior generations such as 4G.

The SEAF starts authentication by sending an authentication request to the AUSF, which first verifies that the serving network requesting the authentication service is authorized. Upon success, the AUSF sends an authentication request to UDM/ARPF. If a SUCI is provided by the AUSF, then the SIDF will be invoked to decrypt the SUCI to obtain the SUPI, which is further used to select the authentication method configured for the subscriber. In this case, it is 5G-AKA, which is selected and to be executed.

UDM/ARPF starts 5G-AKA by sending the authentication response to the AUSF with an authentication vector consisting of an AUTH token, an XRES token, the key K_{AUSF}, and the SUPI if applicable (e.g., when a SUCI is included in the corresponding authentication request), among other data.

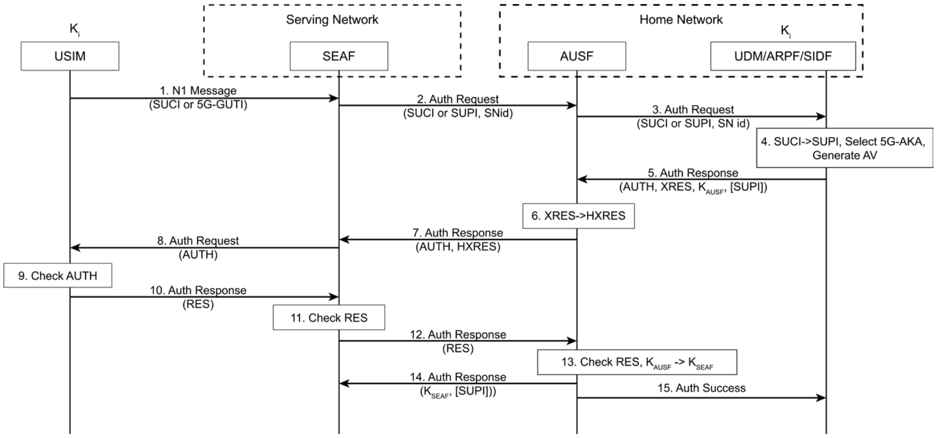
Serving Network
Home Network
K_i
K_i
USIM
SEAF
AUSF
UDM/ARPF/SIDF
1. N1 Message (SUCI or 5G-GUTI)
2. Auth Request (SUCI or SUPI, SNid)
3. Auth Request (SUCI or SUPI, SN id)
4. SUCI->SUPI, Select 5G-AKA, Generate AV
5. Auth Response (AUTH, XRES, K_{AUSF}, [SUPI])
6. XRES->HXRES
7. Auth Response (AUTH, HXRES)
8. Auth Request (AUTH)
9. Check AUTH
10. Auth Response (RES)
11. Check RES
12. Auth Response (RES)
13. Check RES, K_{AUSF} -> K_{SEAF}
14. Auth Response (K_{SEAF}, [SUPI]))
15. Auth Success

Figure 4 – 5G Authentication Framework

The AUSF computes a hash of the expected response token (HXRES), stores the K_{AUSF}, and sends the authentication response to the SEAF, along with the AUTH token and the HXRES. Note that the SUPI is not sent to the SEAF in this authentication response. It is only sent to the SEAF after UE authentication succeeds.

The SEAF stores the HXRES and sends the AUTH token in an authentication request to the UE. The UE validates the AUTH token by using the secret key it shares with the home network. If validation succeeds, the UE considers the network to be authenticated. The UE continues the authentication by computing and sending the SEAF a RES token, which is validated by the SEAF. Upon success, the RES token is further sent by the SEAF to the AUSF for validation. Note that the AUSF, which is in a home network, makes the final decision on authentication. If the RES token from the UE is valid, the AUSF computes an anchor key (K_{SEAF}) and sends it to the SEAF, along with the SUPI if applicable. The AUSF also informs UDM/ARPF of the authentication results so they can log the events, e.g., for the purpose of auditing.

Upon receiving the K_{SEAF}, the SEAF derives the AMF key (K_{AMF}) (and then deletes the K_{SEAF} immediately) and sends the K_{AMF} to the co-located Access and Mobility Management Function (AMF). The AMF will then derive from the K_{AMF} (a) the confidentiality and integrity keys needed to protect signaling messages between the UE and the AMF and (b) another key, K_{gNB}, which is sent to the Next Generation NodeB (gNB) base station for deriving the keys used to protect subsequent communication between the UE and the gNB. Note that the UE has the long-term key, which is the root of the key derivation hierarchy. Thus, the UE can derive all above keys, resulting a shared set of keys between the UE and the network.

5G-AKA differs from 4G EPS-AKA in primarily the following areas.

- Entities involved in the authentication are different because of the new service-based architecture in 5G. Particularly, the SIDF is new; it does not exist in 4G.

- The UE always uses the public key of the home network to encrypt the UE permanent identity before it is sent to a 5G network. In 4G, the UE always sends its permanent identifier in clear text to the network, allowing it to be stolen by either a malicious network (e.g., a faked base station) or a passive adversary over the radio links (if communication over radio links is not protected).

- The home network (e.g., the AUSF) makes the final decision on UE authentication in 5G. In addition, results of UE authentication are also sent to UDM to be logged. In 4G, a home network is consulted during authentication only to generate authentication vectors; it does not make decisions on the authentication results.

- Key hierarchy is longer in 5G than in 4G because 5G introduces two intermediate keys, K_{AUSF} and K_{AMF} (see Figure 5). Note: K_{SEAF} is the anchor key in 5G, equivalent to K_{ASME} in 4G.

c. EAP-AKA’

EAP-AKA’ [6] is another authentication method supported in 5G. It is also a challenge-and-response protocol based on a cryptographic key shared between a UE and its home network. It accomplishes the same level of security properties as 5G-AKA, e.g., mutual authentication between the UE and the network. Because it is based on EAP [7], its message flows differ from those of 5G-AKA. Note that EAP messages are encapsulated in NAS messages between the UE and the SEAF and in 5G service messages between the SEAF and the AUSF. Other differences between 5G-AKA and EAP-AKA’ are as follows.

- The role of the SEAF in authentication differs slightly. In EAP-AKA’, EAP message exchanges are between the UE and the AUSF through the SEAF, which transparently forwards the EAP messages without being involved in any authentication decision. In 5G-AKA, the SEAF also verifies the authentication response from the UE and may take action if the verification fails, albeit such action has not yet been defined in 3GPP TS 33.501 [4].

- Key derivation differs slightly. In 5G-AKA, the K_{AUSF} is computed by UDM/ARPF and sent to the AUSF. In EAP-AKA’, the AUSF derives the K_{AUSF} itself in part based on the keying materials received from UDM/ARPF. More specifically, the AUSF derives an Extended Master Session Key (EMSK) based on the keying materials received from UDM according to EAP and then uses the first 256 bits of the EMSK as the K_{AUSF}.

d. EAP-TLS

EAP-TLS [8] is defined in 5G for subscriber authentication in limited use cases such as private networks and IoT environments. When selected as the authentication method by UDM/ARPF, EAP-TLS is performed between the UE and the AUSF through the SEAF, which functions as a transparent EAP authenticator by forwarding EAP-TLS messages back and forth between the UE and the AUSF. To accomplish mutual authentication, both the UE and the AUSF can verify each other's certificate or a pre-shared key (PSK) if it has been established in a prior Transport Layer Security (TLS) handshaking or out of band. At the end of EAP-TLS, an EMSK is derived, and the first 256 bits of the EMSK is used as the K_{AUSF}. As in 5G-AKA and EAP-AKA', the K_{AUSF} is used to derive the K_{SEAF}, which is further used to derive other keying materials (see Figure 5) needed to protect communication between the UE and the network.

EAP-TLS fundamentally differs from 5G-AKA and EAP-AKA' in its trust establishment between a UE and the network, i.e., it uses a different a trust model. In EAP-TLS, mutual authentication between a UE and a 5G network is obtained primarily based on the mutual trust of their public key certificates, acknowledging that TLS with a PSK is possible but is rarely used except for session resumption. In AKA-based methods, such trust is based solely on a symmetric key shared between a UE and the network.

Such a fundamental difference is significant in that EAP-TLS removes the need to store a large number of long-term keys in the home network (e.g., in UDM), thus reducing operational risks in the life cycle of symmetric key management. On the other hand, EAP-TLS introduces new overhead in certificate management, such as certificate issuance and revocation.

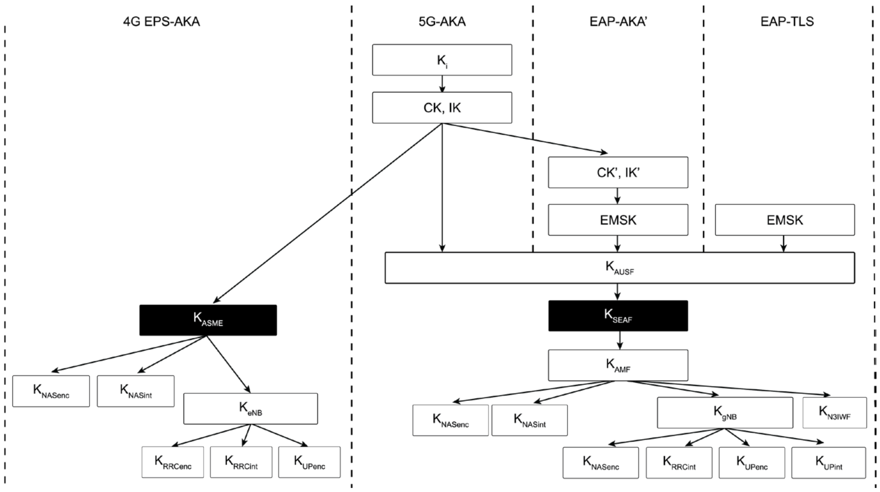

Figure 5 – Key Hierarchy in 4G and 5G

4. Comparison

Table 1 compares 4G and 5G authentication methods, highlighting differences between the two. For example, 5G authentication has different entities from 4G because 5G adopts service-based architecture. Other major differences include the trust models in methods based on EAP-TLS or AKA protocol, the entities that make authentication decisions, and anchor key hierarchy (see Figure 5).

Table 1 - Comparison of 4G and 5G Authentication Methods

		4G Authentication	5G Authentication		
		EPS-AKA	5G-AKA	EAP-AKA'	EAP-TLS
ENTITIES (LOCATED IN)	USER EQUIPMENT (UE)	USIM	USIM		USIM/Non-USIM
	SERVING NETWORK (SN)	MME	SEAF		
	HOME NETWORK (HN)	HSS	AUSF UDM/ARPF/SIDF		
MESSAGE FORMAT	UE <-> SN	NAS	NAS	NAS|EAP	NAS|EAP
	SN <-> HN	Diameter	HTTP-based web APIs		
TRUST MODEL		Shared symmetric key	Shared symmetric key		Public key certificate
UE IDENTITY	UE -> SN	IMSI/GUTI	SUCI/5G-GUTI		
	SN -> HN	IMSI	SUCI/SUPI		
SN IDENTITY		SN id (MCC+MNC)	SN name (5G:MCC+MNC)		
AUTHENTICATION VECTOR GENERATED BY		HSS	UDM/ARPF	UDM/ARPF	N/A
AUTHENTICATION OF UE DECIDED BY		MME	SEAF & AUSF	AUSF	AUSF
HN INFORMED OF UE AUTHENTICATION?		No	Yes	Yes	Yes
ANCHOR KEY HIERARCHY		K_i -> CK+IK -> K_{ASME}	K_i -> CK+IK -> K_{ASME} -> K_{SEAF}	K_i -> CK+IK -> CK'+IK' -> EMSK -> K_{SEAF}	EMSK -> K_{AUSF} -> K_{SEAF}

5. Conclusions

Authentication and key management are of critical importance to cellular networks because they form the foundation for protecting users, networks, and communication between them. Authentication in cellular networks has evolved over each generation—5G authentication improves upon 4G authentication in a number of areas, including a unified authentication framework, better UE identity protection, enhanced home-network control, and more key separation in key derivation. However, 5G authentication is not without its weaknesses. For example, user trackability may still be possible in 5G [9].

Authentication in cellular networks has evolved over each generation—5G authentication improves upon 4G authentication in a number of areas, including a unified authentication framework, better UE identity protection, enhanced home-network control, and more key separation in key derivation.

Another noticeable difference in 5G authentication is its open framework and the support of multiple authentication methods, particularly non-AKA-based methods such as EAP-TLS (albeit with limited use). This feature is encouraging, given that AKA-based methods have always been the only primary authentication methods supported in 4G and its prior generations. 5G is intended to support a variety of use cases, and some of them might be more suited to non-AKA-based methods. For example, in the scenario of wireless and wireline convergence, a piece of user equipment such as a laptop behind a residential gateway may not have a USIM; it would not be able to execute AKA protocols even though it needs to be able to register and connect to the 5G core. In such a case, non-AKA-based methods such as EAP-TLS or EAP-TTLS can be used to authenticate the user to the 5G core.

A variety of use cases is envisioned for 5G. Future work on 5G authentication could support those use cases by including additional security enhancements and other authentication methods.

6. Endnotes

[1] Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, and Yunhao Liu, "FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild," Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (February 2017).

[2] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert, "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (Feburary 2016).

[3] 3GPP, "3GPP System Architecture Evolution (SAE)—Security Architecture" (Release 15), technical specification (TS) 33.401, v15.2.0 (September 2018).

[4] 3GPP, "Security Architecture and Procedures for 5G System" (Release 15), technical specification (TS) 33.501, v15.5.0 (September 2018).

[5] Byeongdo Hong, Sangwook Bae, and Yongdae Kim, "GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier," Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (February 2018).

[6] Internet Engineering Task Force, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')," Request for Comments (RFC) 5448 (May 2009).

[7] Internet Engineering Task Force, "Extensible Authentication Protocol (EAP)," Request for Comments (RFC) 3748 (June 2004).

[8] Internet Engineering Task Force, "The EAP-TLS Authentication Protocol," Request for Comments (RFC) 5216 (March 2008).

[9] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler, "A Formal Analysis of 5G Authentication," Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18) (October 2018).

7. Abbreviations

3GPP	3rd Generation Partnership Project
AKA protocol	Authentication and Key Agreement protocol
AMF	Access and Mobility Management Function
API	application program interface
ARPF	Authentication Credential Repository and Processing Function
AUSF	Authentication Server Function
AUTH token	authentication token
AV	authentication vector
CK	cipher key
EAP	Extensible Authentication Protocol
eMBB	enhanced mobile broadband
EMSK	Extended Master Session Key
eNodeB	Evolved NodeB
EPS	Evolved Packet System
gNB	Next Generation NodeB
GUTI	Globally Unique Temporary Identity
HN	home network
HSS	home subscriber server
HTTP	HyperText Transfer Protocol
HXRES	hash of the expected response token
IK	integrity key
IMSI	international mobile subscriber identity
IoT	Internet of things
IP	Internet Protocol
IPsec	Internet Protocol Security
K_{AMF}	key for the Access and Mobility Management Function
K_{ASME}	anchor key (in 4G, for the Access Security Management Entity)
K_{AUSF}	key used to derive other keys for authentication and encryption
K_{gNB}	key used with a gNB base station

K_i	shared secret key
K_{SEAF}	anchor key (in 5G, for the Security Anchor Function)
LTE	Long-Term Evolution
MCC	mobile country code
MME	Mobility Management Entities
mMTC	massive machine-type communications
MNC	mobile network code
N3IWF	Non-3GPP Interworking Function
NAS	non-access stratum
PSK	pre-shared key
RAN	radio access network
RES token	response token
RRC	Radio Resource Control
SBA	service-based architecture
SEAF	Security Anchor Function
SIDF	Subscription Identifier De-concealing Function
SN	serving network
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
UDM	unified data management
UE	user equipment
UICC	universal integrated circuit card
uRLLC	ultra-reliable low-latency communications
USIM	universal subscriber identity module
VPN	virtual private network
XAUTH token	expected authentication token
XRES token	expected response token