Authentication Mechanisms in the 5G System

Xiaoting Huang[1,*], Takahito Yoshizawa[2] and Sheeba Backia Mary Baskaran[3]

[1]*China Mobile Research Institute, Beijing, China*
[2]*ESAT, COSIC, KU Leuven, Kasteelpark Arenberg 10 Bus 2452, B-3001 Leuven, Belgium*
[3]*Lenovo, Motorola Mobility, Oberursel, Germany*
E-mail: huangxiaoting@chinamobile.com; takahito.yoshizawa@esat.kuleuven.be; smary@lenovo.com
[*]*Corresponding Author*

Received 20 October 2020; Accepted 28 February 2021;
Publication 26 May 2021

Abstract

The 5G system introduces multiple new authentication mechanisms. The initial 5G specification in 3GPP Release 15 defines the initial security solution including primary and secondary authentication. Further enhancements and additional security features are added in Release 16; some of them introduce new types of authentication. As a result, the scope and meaning of 'authentication' has expanded. This is a new trend in the 5G system as it introduces new concepts that did not exist in the preceding generation systems. One such example is the slice authentication for which the authentication is performed at the network slice level. As a result, the authentication mechanisms become more complex. This paper clarifies the details of each of these different authentication mechanisms.

Keywords: 5G, 5G security, AKMA, primary authentication, secondary authentication, slice authentication.

Journal of ICT Standardization, Vol. 9_2, 61–78. *River Publishers*
doi: 10.13052/jicts2245-800X.921

1 Introduction

3GPP has specified the system and security architecture for the 5G System (5GS). The first 5G specifications were published around the end of 2017 to the beginning of 2018 as Release 15 version. Release 15 is called 5G phase 1, which specifies the initial set of features to launch the commercial 5G deployment. Under Release 16, called 5G phase II, 3GPP continues the 5G specification work by introducing enhancements and additional new features. The latest version of the 5G system architecture, procedures and security architecture are defined in TS 23.501 [1], TS 23.502 [2] and TS 33.501 [3].

In the 5G system, a number of security enhancement features are introduced to make the mobile system even more secure and robust compared to the preceding generation systems. The 5G version of the authentication mechanism is one example. Primary authentication offers two mechanisms: (1) 5G Authentication and Key Agreement (5G AKA), and (2) Extensible Authentication Protocol AKA' (EAP-AKA'). They address existing security issues in earlier generation systems. Specifically, introducing "Home Control", i.e. authentication to take place in the home network, and the concept of Subscription Concealed Identifier (SUCI) in the signaling prevents the exposure of permanent subscriber ID to ensure user privacy: Subscription Permanent Identifier (SUPI), which can have also the format of a traditional International Mobile Subscription Identifier (IMSI). Secondary authentication provides a mechanism for external network to authenticate the user with the support of mobile operator.

In addition, the 5G system introduces several new concepts that did not exist in preceding generation systems. One such area is the concept of network slice, which was originally proposed by Next Generation Mobile Networks (NGMN) Alliance as one of the key concepts in the 5G system. It allows mobile operators to deploy emerging technologies such as network virtualization based on Software Defined Network/Network Function Virtualization (SDN/NFV). Network slicing provides network isolation tailored to fulfil diverse service requirements for various applications of vertical industries. The introduction of the network slice concept also enables authentication at network slice level. Finally, Release 16 introduces "Authentication and Key Management for Applications based on 3GPP credentials in 5G" (AKMA). This new bootstrapping architecture enhances the existing Generic Bootstrapping Architecture (GBA)-based solution of the 4G and 3G systems.

Due to the introduction of these additional features, the 5G system has various authentication mechanisms – all of them are intended for different

purposes. The goal of this paper is to clarify the differences and usages of these authentication mechanisms in the 5G system.

This paper is organized as follows. We first present the overall 5G security architecture of Release 16 in Section 2. In Sections 3 and 4, we describe the details of primary and secondary authentication, respectively. Then, we further discuss two new authentication mechanisms introduced in Release 16, namely slice authentication and AKMA in Sections 5 and 6, followed by conclusion and outlook in Sections 7 and 8.

2 Security Architecture

The 5G system architecture [1] was specified to support the new principle of the Service Based Architecture (SBA). It allows scalable deployment of virtualized network functions (NF) that enables operators to deploy it in data centers. The idea is to shift from the hardware "box" paradigm where individual functional entities are separately defined to a model, in which NFs follow the web-based approach using RESTful client server communication. A NF as a service consumer can subscribe to certain events from another NF that acts as a service producer of the requested service information. On the other hand, the 5G system architecture can also be depicted in a traditional reference model and not only in the form of the new SBA reference model. For the security architecture, this type of visualization is chosen in order to show the co-location of functions with others more easily.

Figure 1 shows the overall 5G system architecture and its NFs involved in the different security procedures, especially for authentication. The User Equipment (UE) is the mobile device comprising the Mobile Equipment (ME) and the Universal Subscriber Identity Module (USIM), which securely

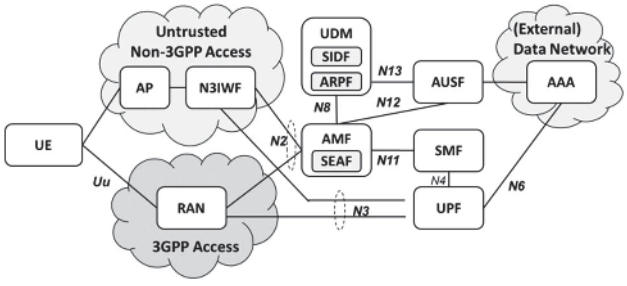

Figure 1 Security architecture.

stores the shared credentials with the mobile operator. The UE can connect to the mobile core network via Non-3GPP access, e.g. WLAN, or via 3GPP Access. Untrusted non-3GPP access is shown here as an example.

The untrusted non-3GPP access consists of the access point (AP) and the Non-3GPP Interworking Function (N3IWF). The 3GPP Access consists of the Radio Access Network (RAN), gNB, i.e. the 5G base station. The UE connects to the Access and Mobility Management Function (AMF) over the Non Access Stratum (NAS) protocol either via non-3GPP Access or 3GPP Access. The AMF hosts the SEcurity Anchor Function (SEAF). The Authentication Server Function (AUSF) is the peer point of the UE for the primary authentication. The Unified Data Management (UDM) hosts the subscription data in the Unified Data Repository (UDR) and also has additional functionality such as the Subscription Identifier De-concealing Function (SIDF) and Authentication credential Repository and Processing Function (ARPF). For user plane management, the Session Management Function (SMF) is used to interact with the User Plane Function (UPF) to connect to a Data Network (DN), e.g., the Internet. The Authentication, Authorization, and Accounting (AAA) Server can be located within the mobile operator domain or can belong to an external third-party service provider.

3 Primary Authentication

3.1 Purpose of Primary Authentication

The primary authentication achieves mutual authentication between the UE and the operator's network. In the AKA procedure between the UE and the network, the serving network authenticates the SUPI of the UE and the UE in turn authenticates the serving network identifier through implicit key authentication. For 3GPP access, the SUPI is based on IMSI; for non-3GPP access, the SUPI is based on Network Access Identifier (NAI). The 'implicit key authentication' is a process, where the authentication is confirmed through the successful use of keys generated from the successful AKA in subsequent procedures (e.g. protecting control plane and user plane messages). To perform primary authentication for the 3GPP access, the 5G system defines EAP-AKA' and 5G AKA as mandatory methods and uses either one based on the subscription information. For non-3GPP access, a vendor specific method, EAP-5G is used between the UE and the N3IWF to encapsulate NAS messages. Between the UE and the AUSF, any of the authentication methods similar to 3GPP access can be used for authentication

by the home network. The primary authentication can be initiated by the SEAF in serving network whenever a UE sends a registration request to the SEAF or during any procedure establishing a signaling connection with the UE, according to the SEAF's policy.

3.2 Primary Authentication Procedure

The primary authentication procedure based on EAP-AKA' involving AUSF and UDM service operations for a 3GPP access is shown in Figure 2. Due to the limited space, we focus on the EAP-AKA'-based primary authentication method in this section.

The detailed discussion of the service operations is omitted to keep the procedure concise.

1. The UE sends the Registration Request NAS message to the SEAF in the serving network, containing either a SUCI or a 5G Globally Unique Temporary UE Identifier (5G-GUTI).
2. On receiving the registration request, the SEAF invokes primary authentication by sending authentication request to the AUSF in the home network (in non-roaming scenario both serving and home network are the same) containing the received SUCI and its serving network name (SNN). Otherwise, the SEAF sends the SUPI if the SEAF has a valid 5G-GUTI and re-authenticates the UE.

3–4. The AUSF verifies the SNN in the authentication request to check if it is the same as the expected serving name. If the AUSF verifies the serving network as authorized, it sends an authentication data request to the UDM, including the received SUCI and SNN values.

5–6. On receiving the SUCI, the UDM invokes the SIDF to de-conceal the SUCI into SUPI. Based on the SUPI, the UDM/ ARPF chooses the authentication method (i.e. 5G-AKA or EAP-AKA') and generates a method-specific authentication vector (AV). For EAP-AKA', a transformed AV called AV' [RAND, AUTN, XRES, CK', IK'] is generated. In this discussion, we assume EAP-AKA' is selected and a transformed AV called AV' is sent in authentication data response to the AUSF including an indication of the selected authentication method (i.e. indicator for EAP-AKA').

7. The AUSF sends the authentication challenge (RAND and AUTN) from the AV' to the SEAF in the authentication response message.
8. The SEAF forwards the received authentication challenge to the UE including Key Set Identifier (ngKSI) and Anti-Bidding down

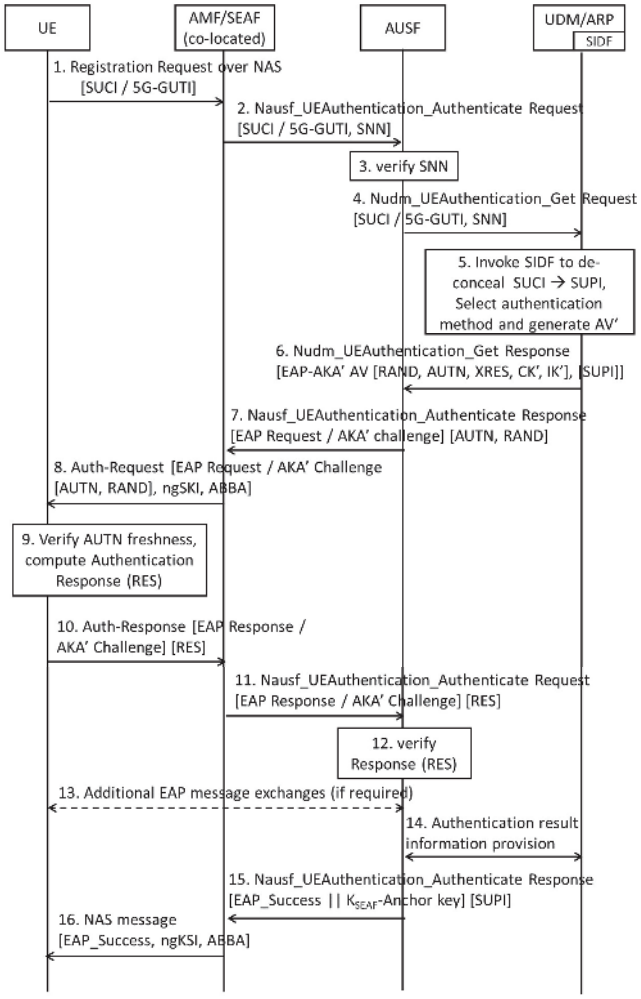

Figure 2 EAP-AKA' based primary authentication procedure.

Between Architectures (ABBA) parameters in the Authentication Request NAS message. The ngKSI and the ABBA are to identify the key set and for anti-bidding down protection in the 5GS [3], respectively.

9–10. At the UE, on receiving the RAND and AUTN, the USIM verifies the freshness of the AV by checking whether AUTN is valid (TS 33.102) [4]. If the AUTN is valid, the UE computes a response

(RES), and the keys (CK/IK) or (CK'/IK' for EAP-AKA'). The UE then responds to the SEAF by sending Authentication Response NAS message including the RES.

11. The SEAF forwards challenge response transparently to the AUSF in an Authentication Request message.

12–14. The AUSF verifies the challenge response and if the verification is successful, the AUSF informs the UDM about the authentication result as 'Success.' For EAP-AKA' method, there may be additional EAP message exchanges between the UE and the AUSF.

15. The AUSF derives Extended Master Session Key (EMSK) from CK' and IK' (RFC 5448 [5]) and uses the most significant 256 bits of EMSK as the key K_{AUSF}, then calculates the key K_{SEAF} (the anchor key from which the AS and NAS protection keys are derived) from K_{AUSF}.

16. The SEAF further generates K_{AMF} from K_{SEAF} received from the AUSF. If the AUSF and the SEAF confirms a successful authentication, then the SEAF provides the ngKSI and the K_{AMF} to the AMF. The SEAF further sends the EAP Success message to the UE along with the ngKSI and the ABBA parameters.

On receiving the authentication success message, the UE generates the security context equivalent to the one in the network. The use of security context for control plane and user plane message protection between the UE and the network ensures successful completion of the authentication between the network and the UE.

4 Secondary Authentication

4.1 Principle of Secondary Authentication

Secondary authentication occurs between the UE and the DN outside the mobile operator domain. In the older generation systems, DNs conduct the access control by themselves without the support of mobile operator after the user plane tunnel has been established between the UE and the DN. This may allow malicious UEs to invoke authentication service provided by the DN resulting in a Denial of Service (DoS) attack. The 5G system allows mobile operators to delegate the authentication and authorization to a third party hosting the DN. This is achieved by introducing the concept of secondary authentication. This procedure is executed during the establishment of user plane connection after the successful primary authentication.

One of the delicate designs of secondary authentication is the use of EAP framework, which is widely used and enables various credential types and authentication methods used by different application service providers.

4.2 Secondary Authentication Procedure

The prerequisite of secondary authentication is the successful completion of primary authentication based on the UE's 5G network access credentials, and the establishment of NAS security context between the UE and the AMF. Additionally, the UE needs to be provisioned with the external credentials used for the authentication between itself and corresponding Data Network Authentication Authorization and Accounting (DN-AAA) server.

Figure 3 illustrates the secondary authentication procedure. During this procedure, the SMF in the 5G core network performs the role of EAP authenticator while the DN-AAA server performs the role of EAP authentication server.

1. The UE requests to establish a new PDU session; PDU Session Establishment Request message is contained in a NAS message to the SMF.
2. If the DN-specific identity, Data Network Name (DNN), is provided by the UE in step 1, and the SMF determines that authentication/authorization of the PDU session establishment is required based on the SMF policy associated with the DN, the SMF triggers the secondary authentication procedure with the UE.
3. The SMF triggers EAP Authentication to obtain authorization from an external DN-AAA server.
4. The SMF requests the EAP identity from the UE, and the UE responds with EAP identity (Note: The EAP identity may also be sent in step 1 to avoid interactions in this step).
5. The SMF forwards the EAP Response/Identity message to the DN-AAA server via the UPF.
6. The DN-AAA server and the UE exchange EAP messages, as required by the EAP method.
7. Once the authentication is successfully completed, the DN -AAA server sends EAP Success message to the SMF via the UPF.
8. The SMF completes the EAP authentication procedure and saves the authentication results of the specific UE and the DN.
9. If the EAP authentication procedure is successful, PDU session establishment proceeds further.

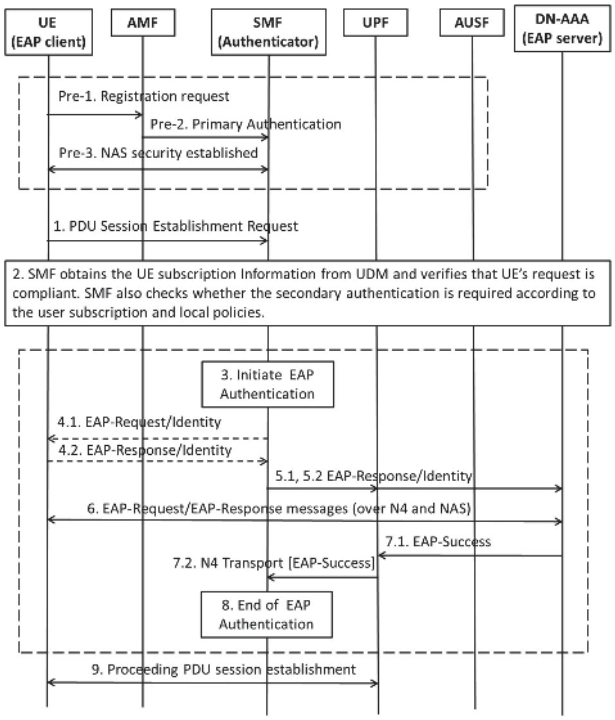

Figure 3 Secondary authentication procedure.

The DN-AAA server or the SMF may initiate the re-authentication with the UE. If the re-authentication is initiated by the DN-AAA server, the UE is addressed by Generic Public Subscription Identifier (GPSI), which is notified to the DN-AAA server at step 3.

4.3 Comparison of Primary and Secondary Authentication

Purposes and characteristics of the primary and secondary authentication can be summarized as follows:

1. Primary authentication provides the access control to the operator network, while secondary authentication enables the UE to access the user plane data towards the DN.
2. Primary authentication is a mandatory procedure when the UE connects to the operator network. On the other hand, secondary authentication is optional to use depending on the agreement between operators and the external service provider.

3. Primary authentication uses 3GPP credentials while secondary uses external credentials provided by 3rd party application service providers.

5 Slice Authentication

5.1 Purpose of Slice Authentication

3GPP defines network slice as a logical network resource that provides specific network capabilities and characteristics. The slice authentication, as described in TR 33.813 [7], enables the third-party application service provider hosted with an AAA server to authenticate the end-user to access its slice. A third-party application service provider offers communication service to end-users using the service built with network slice over the operator network, e.g. a taxi company using a network slice optimized to dispatch and manage their vehicles by tracing vehicle location and providing an uncongested route for the vehicle. Slice authentication enables customized authentication of UEs for slice selection and access to it. In addition to primary authentication, slice authentication is executed at the time of the registration when access control to network slices requires slice specific additional authorization and authentication. In this case, a slice specific user identity (e.g. NAI of the form user@domain) and third party provisioned credential different from the 3GPP credential in primary authentication is used. Without slice authentication, unauthorized UEs may consume resources of the network slice leading to DoS for other legitimate UEs.

5.2 Slice Authentication Procedure

The UE needs to be provisioned with a slice-specific credential necessary to authenticate itself with the AAA server. The assumption is that the slice authentication is performed for a specific Single Network Slice Selection Assistance Information (S-NSSAI) only after the primary authentication is successfully completed. This procedure is shown in Figure 4. If multiple slices are requested by the UE and some of them require slice-specific authentication, then the authentication procedure is performed for each of those S-NSSAIs.

During the primary authentication as discussed in Section 3.2, the UE sends Registration Request message to the network containing a list of NSSAIs corresponding to the network slices and indicates if it has the capability to support slice authentication. The UE and the network complete the primary authentication either using the 5G AKA or EAP-AKA' procedure

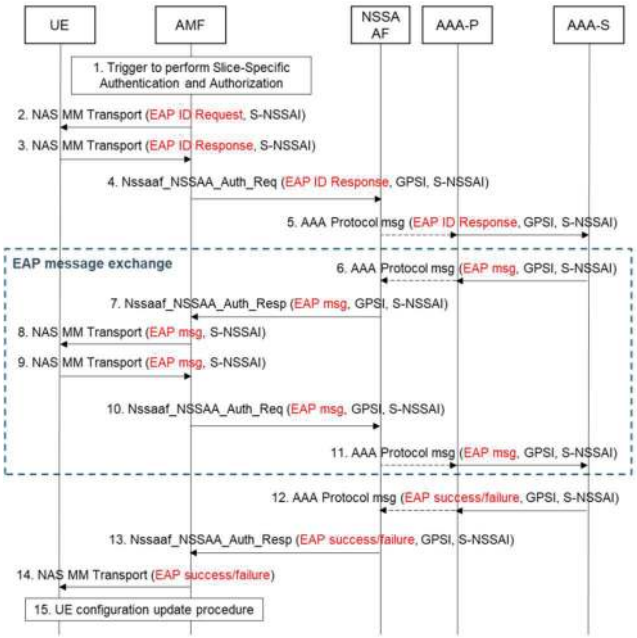

Figure 4 Slice authentication procedure.

as discussed in section 3. After the successful primary authentication, the AMF sends Registration Accept message to the UE with a list of all allowed NSSAIs (except the S-NSSAIs which require slice-specific authentication) based on the subscription information available in the UDM. The UE sends Registration Complete message, indicating the successful completion of the primary authentication.

Then the AMF initiates slice specific authentication using the procedure shown in Figure 4 for all slices that require slice-specific authentication.

1, 2. If the AMF determines that a slice-specific authentication is required, the AMF acts as the EAP authenticator and sends EAP Identity Request message to the UE to initiate slice specific authentication corresponding to the NSSAI of the network slice.
The UE provides the EAP ID by sending the EAP Identity Response message to the AMF for the requested S-NSSAI.
The AMF forwards the EAP ID along with the S-NSSAI to the NSSAAF.
The NSSAAF forwards the EAP Identity Response message in the AAA protocol message to the Serving AAA (AAA-S) server. A

proxy-AAA server (AAA-P) may be present if the AAA-S is located in the 3rd party.

6–11. The AAA-S and the UE exchanges the EAP messages.

12. EAP authentication completes. The AAA-S delivers either EAP success or failure message to the NSSAAF.

13, 14. The NSSAAF forwards the EAP success/failure message to the AMF in Nssaaf_NSSAA_Authenticate Response message, and the AMF forward it over MM NAS transport message.

15. Once the slice-specific authentication is successfully completed for all S-NSSAIs, the AMF triggers a UE Configuration Update procedure to deliver a new list of allowed NSSAIs to the UE reflecting the slice authentication result.

In addition, the slice authentication supports two additional procedures: (1) slice-specific re-authentication and re-authorization, and (2) slice-specific authorization revocation. These procedures allow the AAA-S to either re-authenticate/re-authorize or revoke the access to a specific slice that has already been granted to the UE as needed. If AAA-P is present, then it routes the message to the serving AMF based on the binding between the User ID and the GPSI of the UE established when the UE was authorized for the slice.

6 AKMA

6.1 Purpose of AKMA

5G promises to enable massive Internet of Things (mIoT) applications. When getting access to the IoT application server, IoT devices may have limitations in applying user name/password authentication mechanism to their application servers, which is common in Internet style authentication mechanisms. An IoT device may lack resources in storing and/or processing certificates or may not have provisioning interfaces such as a Graphical User Interface (GUI). Therefore, a new authentication scheme applied to IoT devices and their application servers is needed to allow only the authentic devices to access application servers. Besides, the question of how to enable the secure communication between UE and application providers draws attention.

In preceding generation systems, 3GPP has developed well-designed mechanisms, e.g. GBA [8] and Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices (BEST) [9] that leverage operators' assets, namely using 3GPP credentials, to achieve authentication and key distribution for application providers. However, two gaps

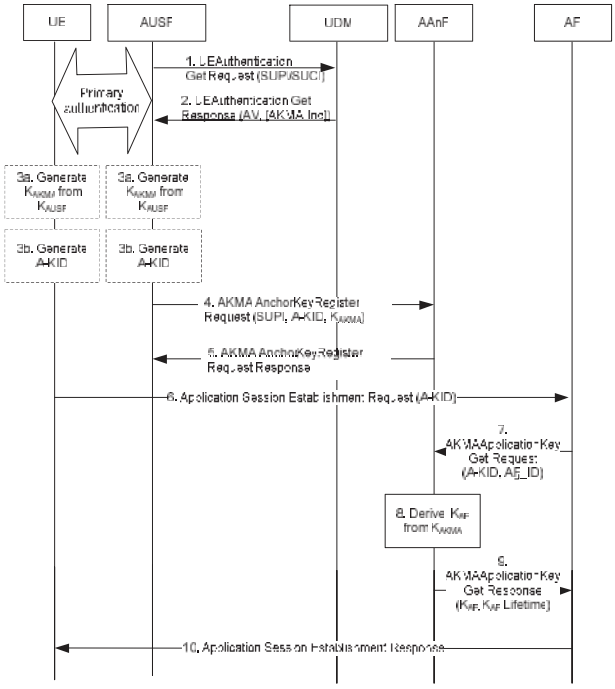

Figure 5 AKMA procedure.

need to be filled to fit these mechanisms into the 5G system. First, the 5G architecture introduces the concept of SBA and new network functions different from the preceding generation systems. Second, the variation of IoT application layer protocols, which are not supported by both GBA and BEST, needs to be supported.

To solve the above mentioned problems, 3GPP has studied [10] and specified [11] a new feature in Release 16, which is called AKMA (Authentication and Key Management for Applications). The goal of this feature is to enable the authentication and generation of application keys based on 3GPP credential for all UE types in the 5G system, especially IoT devices, ensuring to bootstrap the security between the UE and the applications in the 5G system.

6.2 AKMA Procedures

Since AKMA is intended to leverage the 5G authentication mechanism to provide applications with session keys that are afterwards used to protect

the communication between the UE and the application servers, an anchor function is needed to act as the role of generating and managing such session keys. In 3GPP TS 33.535 [11], the AKMA anchor function (called AAnF) has been defined in the 5G system to obtain the intermediate AKMA key (K_{AKMA}) from the AUSF, as well as to provide session key (K_{AF}) to application providers. Considering the 5G security design of enabling K_{AUSF} storage in the home network and the UE for further services, AKMA is designed to leverage primary authentication and namely K_{AUSF} to simplify the procedures. Specifically, if the UE is subscribed with AKMA service capability, there will be K_{AUSF} stored and further K_{AKMA} derived from K_{AUSF} after the successful primary authentication.

1, 2. During the primary authentication, the AUSF interacts with the UDM to fetch authentication information. If the UE is capable and allowed to use AKMA service, the UDM indicates the AUSF to generate AKMA related keys with the parameter of AKMA Ind which is stored in UDM as subscription data.

3. While receiving the AKMA indication from UDM, the AUSF and UE both generates K_{AKMA} from K_{AUSF} and the related key identifier A-KID (AKMA Key IDentifier).

4, 5. The AUSF sends the AKMA key material (A-KID and K_{AKMA}) together with SUPI to the AAnF for further key derivation.

6. When the UE is about to communicate with the application server (AKMA AF), it sends an application session establishment request message carrying A-KID.

7–9. If the AF does not have the key material associated with the A-KID, then the AF requests the K_{AF} (derived from K_{AKMA}) from the AAnF , by carrying the A-KID and the AF identifier (AF_Id). The AAnF derives K_{AF} from K_{AKMA} and sends it to AF with its lifetime.

10. After obtaining K_{AF}, the AKMA AF responds to the UE's application session establishment request. Afterwards, the UE derives K_{AF} accordingly and both the UE and AF are in possession of the K_{AF} for further use.

7 Conclusion

This paper discussed an overview of different authentication procedures used for different purposes in the 5G system. Primary Authentication is used for the mutual authentication of the UE and the network with its new

enhancements such as home control of the authentication and the possibility of running the primary authentication also over non-3GPP accesses (e.g. WLAN), resulting in multiple NAS connections.

Primary authentication allows either EAP-AKA' or 5G-AKA method for public networks and mandates the security credentials to be stored on the USIM. Secondary authentication is an optional authentication outside of the registration procedure and may be required when the UE is requesting a PDU session towards an external DN. This is either a subscription feature or based on network configuration in the SMF, which has the role of the EAP authenticator. The signaling towards the SMF is encapsulated in NAS containers and then sent as user plane traffic from the SMF via the UPF to the AAA server.

Slice authentication, on the other hand, is performed together with the registration procedure and requires a successful primary authentication as a prerequisite before accessing the AAA server for the slice specific authentication identified by the NSSAI. The EAP authenticator role is performed by the AMF instead of the SMF and the signaling traverses the AUSF in the home network before reaching the AAA server and is not sent via user plane as in the secondary authentication.

AKMA is also building on the primary authentication and offers applications and 3GPP services in 5G authentication and key management procedures so that the UE can exchange data with an application server in a secure manner.

8 Outlook

Extensive work has been carried out on authentication procedures in different aspects in 5G Phase 1 and 2. Still ongoing study items are discussing further enhancements on the authentication, such as study in TR 33.846 [12]. This study examines different authentication aspects, e.g. how to mitigate the linkability attacks when the long-term key is leaked, DDoS attacks due to SUPI concealment or the leaking of SQN values during AKA re-synchronization. Further work is also ongoing in the study of secure parameter storage in the 5G System in TR 33.845 [13]. This study resulted from the agreement that the Unified Data Repository (UDR) is also allowed to store subscription data and authentication subscription data, for which UDM was previously considered to be the only valid NF to store these data.

It is foreseen that further enhancements and improvements for the authentication procedures will be studied in the upcoming Release 17.

Acknowledgements

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203 and by the Research Council KU Leuven C1 project on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058.

References

[1] 3GPP TS 23.501 (v16.4.0), March 2020, System architecture for the 5G System (5GS)
[2] 3GPP TS 23.502 (v16.6.0), September 2020, Procedures for the 5G System (5GS)
[3] 3GPP TS 33.501 (v16.4.0), September 2020, Security architecture and procedures for 5G System
[4] 3GPP TS 33.102 (v15.1.0), December 2018, 3G security; Security architecture
[5] IETF RFC 5448, May 2009, Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')
[6] IETF RFC 3748, Extensible Authentication Protocol (EAP), June 2004
[7] 3GPP TR 33.813 (v0.9.0), May 2020, Study on security aspects of network slicing enhancement
[8] 3GPP TS 33.220 (v16.2.0), September 2020, Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)
[9] 3GPP TS 33.163 (v16.2.0), September 2019, Battery Efficient Security for very low Throughput Machine Type Communication (MTC) device (BEST)
[10] 3GPP TR 33.835 (v16.1.0), July 2020, Study on authentication and key management for applications based on 3GPP credential in 5G
[11] 3GPP TS 33.535 (v16.1.0), September 2020, Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)
[12] 3GPP TR 33.846 (v0.7.0), September 2020, Study on authentication enhancements in the 5G System (5GS)
[13] 3GPP TR 33.845 (v0.4.0), September 2020, Storage of secure parameters in 5G System (5GS)

Biographies

Xiaoting Huang received her B.Sc. degree in Telecommunications Engineering with Management from Beijing University of Posts and Telecommunications and Queen Mary University of London in 2014. Subsequently she received her M.Sc. degree in Communications and Signal Processing from Imperial College London in 2015. She is now working in China Mobile Research Institute as a research engineer and standardization delegate of 3GPP SA3 and NGMN. She has been an active contributor to standard organizations, mainly focusing on 5G service capabilities and their related security aspects.

Takahito Yoshizawa received B.S. degree in information and computer science from Georgia Institute of Technology in 1992 and M.S degree in Telecommunication from Southern Methodist University in 2002. He has over 30 years of industry experience in mobile communication systems, including product development and standardization, and has done engineering work of all phases of mobile system development lifecycle. He has participated in and contributed to standardization such as 3GPP, and holds over 10 granted patents on communication systems. He received inaugural

Femto Forum Industry Award (current Small Cell Forum) in 2009 for his contribution to standardization. He is currently with COSIC group in Katholieke Universiteit Leuven in Belgium, focusing on research on V2X communication security.

Sheeba Backia Mary Baskaran received Ph.D. degree in information and communication engineering from Anna University, Chennai, India, in 2017. She worked with NEC India Private Ltd., as a Research Engineer since 2016 until 2019. She then worked as a Senior Researcher with Huawei Technologies, Sweden during 2019. She is currently working as an Advisory Researcher with Lenovo, Motorola Mobility, Germany. She is also a delegate to 3GPP SA3, NGMN and ETSI working groups. She carried out her research in security aspects of 4G and 5G Technologies. She has four plus years of industrial research experience in mobile communication networks security aspects. She has also contributed to Global ICT Standardization Forum for India. She was a recipient of the UGC Maulana Azad National Fellowship from 2013 to 2016. She holds significant patents on 5G security aspects and has numerous journal publications.