SCTE·ISBE CABLE-TEC EXPO 2019 NEW ORLEANS, LA SEPT. 30-OCT. 3

2019 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS

Authentication In 5G Wireline And Wireless Convergence

A Technical Paper prepared for SCTE•ISBE by

Tao Wan
Principal Architect
CableLabs
858 Coal Creek Circle, Louiville, CO 80027
303.661.3326
t.wan@cablelabs.com

Yildirim Sahin
Principal Wireless Engineer
Charter Communications
6360 Fiddlers Green Circle, Greenwood Village, CO 80111
720.536.9394
yildirim.sahin@charter.com

Max Pala
Principal Architect
CableLabs
858 Coal Creek Circle, Louiville, CO 80027
303.661.3334
m.pala@cablelabs.com

Table of Contents

List of Figures

Introduction

5G is one of the hottest technologies being trialed and deployed by network operators worldwide. Not only does 5G provide the superior services of fast speed, high bandwidth, and low latency, it also supports new use cases. One of these use cases is support for wireline and wireless convergence (WWC). In WWC, the 5G core manages both wireless access networks and wireline access networks (e.g., cable networks). This provides at least two benefits to residential network users. First, 5G user equipment with both cellular and Wi-Fi (WLAN) and/or wireline access can perform a seamless handover between cellular networks and residential networks. Second, residential user equipment without cellular access (e.g., a laptop or IoT devices at home) can also register to the 5G core to obtain services such as the Quality of Services (QoS) guarantee offered by 5G.

To enable WWC, authentication in cellular networks must evolve. More specifically, 5G authentication must allow the authentication of user equipment over wireline networks. This is in contrast to prior generations of cellular networks (e.g., 4G) which only allow authentication of subscribers over radio access networks. Further, 5G authentication must also allow user equipment without 3GPP credentials (e.g., a secret key stored in a UICC and shared with a network operator) to be authenticated by the 5G core. Prior generations of cellular networks authenticate only user equipment with 3GPP credentials.

In this paper, we provide a comprehensive analysis of 5G authentication that has been defined by 3GPP to support WWC. We include the 5G unified authentication framework which allows authentication to become agonistic to access networks and consistent between wireless and wireline networks. We also describe work-in-progress mechanisms that 3GPP is developing to authenticate non-3GPP-capable user equipment.

The rest of the paper is organized as follows. In Section 2, we provide background information on WWC. In Section 3, we introduce the 5G authentication framework which supports multiple authentication methods over multiple access types. In Section 4, we focus on the authentication of network elements in WWC. We conclude the paper in Section 5.

Background on WWC

One of the objectives of the 3GPP 5G system architecture is to minimize dependencies between the access network and 5G Core (5GC) network in order to integrate different 3GPP access and non-3GPP access networks. Based on this objective, in 3GPP Release-15, the support for untrusted non-3GPP access in the 5GC network was introduced. In 3GPP Release 16, which is planned to be completed in March 2020, the support for trusted non-3GPP access and wireline access in the 5GC network will be introduced.

In 3GPP Release 16, the 5GC network supports connectivity to two types of Wireline 5G Access Networks (W-5GAN): Wireline 5G Broadband Access Network (W-5GBAN) and Wireline 5G Cable Access Network (W-5GCAN), which are specified by the Broadband Forum (BBF) and CableLabs® organizations, respectively. The 5GC network interfaces these wireline access networks via a gateway finction called Wireline Access Gateway Function (W-AGF).

As depicted in Figure 1 [1] and Figure 2 [1], W-AGF provides N1, N2 and N3 interfaces towards the 5GC network. In the southbound direction W-AGF provides connectivity towards two types of Residential Gateways (RGs), called Fixed Network RG (FN-RG) and 5G-RG via Y4 and Y5 interfaces, respectively.

FN-RG is a legacy RG in existing wirelline access networks that does not support N1 signalling and it is not 5GC capable. The FN-RG is defined by BBF and CableLabs organizations; and it can either be an FN-BRG or an FN-CRG depending it is part of W-5GBAN or W-5GCAN, respectively.

5G-RG is an RG capable of connecting to the 5GC network playing the role of user equipment (UE) with regard to the 5GC. It supports secure elements and exchanges N1 signalling with 5GC. The 5G-RG can either be a 5G-BRG or 5G-CRG depending it is part of a W-5GBAN or W-5GCAN, repsectively.

As depicted in Figure 2, 5G-RG can be connected to 5GC via W-5GAN, NG-RAN or via both accesses. If 5G-RG conects to 5GC via NG-RAN, it is also called Fixed Wireless Access [1].

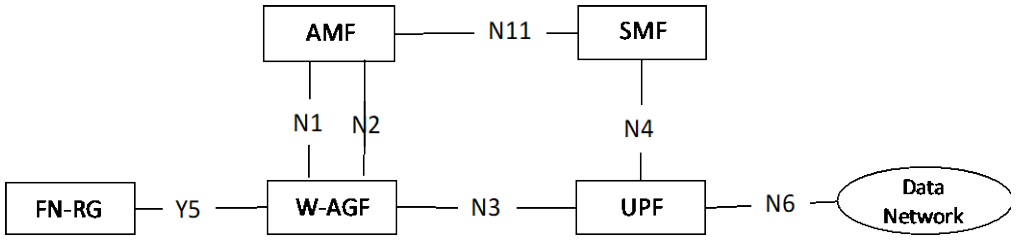

Figure 1 - Reference architecture for 5GC network for FN-RG connecting to W-5GAN (based on 3GPP TS 23.501)

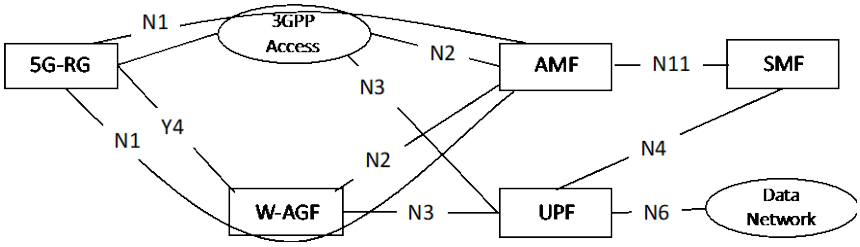

Figure 2 - Reference architecture for 5GC network for 5G-RG connecting to W-5GAN and 3GPP Access (based on 3GPP TS 23.501)

In the reference architecture diagrams depicted in Figure 1 and Figure 2, FN-RG or 5G-RG can provide connectivity to devices behind them. Such devices could be 5G capable UEs or devices with no 5G capabilities, e.g. laptops, tablets, etc.

Detailed WWC architecture information can be found in 3GPP specifications [1] and [2].

5G Authentication Framework

In the following sectin, we first descibe the network functions that are involved in the authentication framework and then discuss the authentication framework itself.

5G Authentication Functions

Service-based architecture (SBA) has been introduced 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**) stores subscription data associated with subscribers and selects an authentication method based on the subscriber identity and configured policy, but it relys upon Authentication Credential Repository and Processing Function (ARPF) where the shared keys are stored to compute 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's long-term identity is always transmitted over 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.

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 Wireless Local Area Network [WLAN] and wireline access 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).

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.

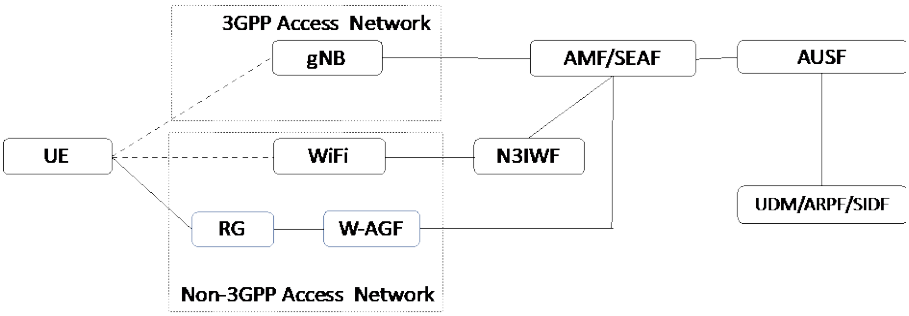

Figure 3 - 5G Authentication Framework

WWC Authentication

Trusted and Untrusted Access

Access networks in 5G systems can be either trusted or untrusted. For untrusted access networks, an IPsec tunnel is first established between a UE and a Non-3GPP Interworking Function (N3IWF). Afterwards, the UE can use one of the 5G primary authentication methods to authenticate to the 5G core. Non-5G UE will not be able to authenticate to the 5G core over the untrusted access network since it may not support the capabilities required to discover the N3IWF or to establish IPsec tunnel with N3IWF. For access networks considered as trusted, an IPsec tunnel may not be necessary, making it possible for non-5G UE to be authenticated to the 5G core, e.g., using an IETF EAP authentication method. This paper focuses on the authentication in wireline access networks with 5G core, which are considered as trusted access networks although not explicitly stated so in 3GPP spcifications.

Authentication in Wireline Access Networks

We consider the authentication of five network elements in 5G systems with wireline access networks. These five elements are 5G UE, non-5G UE, 5G-RG, FN-RG and W-AGF.

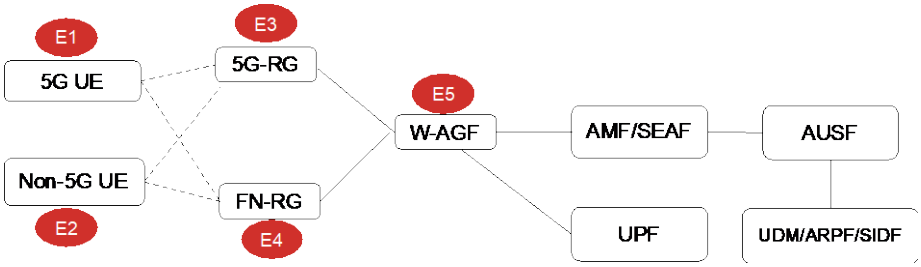

Figure 4 - Architecture of WWC Authentication

Authentication of W-AGF

W-AGF (Wireline Access Gateway Function) is a gateway providing both signaling and user plane connectivity from the wireline access networks to 5G core. Since the network operator owns both the access networks and the 5G core networks, W-AGF is considered trusted and is authenticated by the 5G core network functions such as AMF and SEAF by establishing mutually authenticated TLS with the core. This requires W-AGF to be provisioned with server public key certificates for the authentication.

Authentication of FN-RG

FN-RG is a legacy residential gateway which does not have any 5G capability nor does it interact directly with the 5G core. It is authenticated by the access network using the authentication method defined by either CableLabs or BBF.

After FN-RG is authenticated by the access network, it can be registered as 5G core via W-AGF using a transitive trust model. More specifically, W-AGF will indicate to the core that FN-RG has been authenticated in the registration message so that 5G core (i.e., AUSF) will skip the authentication of FN-RG during its registration (see Figure 5, based on TS 23.316 and TR 33.807).

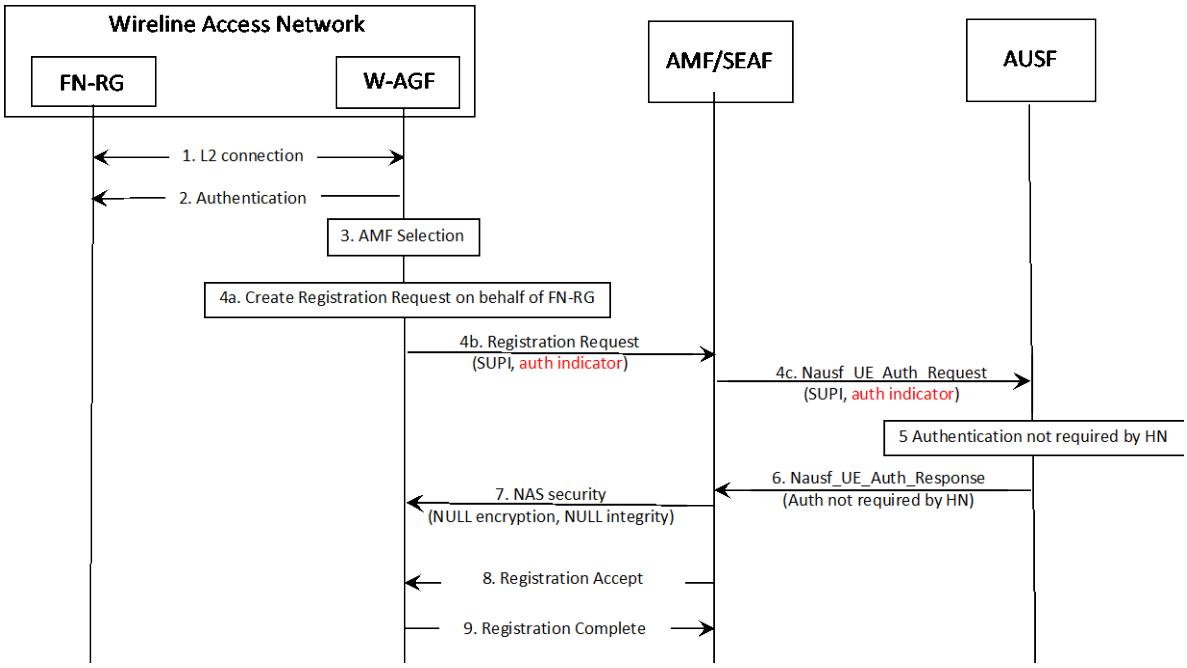

Figure 5 - Registration of FN-RG to 5G Core

5G-RG is treated as a 5G UE and is authenticated by the 5G core using one of the primary authentication methods, e.g., 5G-AKA or EAP-AKA'. Since the wireline network does not support NAS capability, an EAP method (i.e., EAP-5G) is used to encapsulate NAS messages within EAP between 5G-RG and W-AGF.

Since 5G-RG should also support the authentication methods required by the access networks (e.g., BPI+), and will always be authenticated by the access network, we suggest that the transitive trust model assumed by the authentication of FN-RG may also be made applicable to 5G-RG. More specifically, 5G-RG can be authenticated by the wireline access network, and W-AGF indicates its authentication result to the 5G core without having to execute the authentication of 5G-RG by the 5G core directly. This would reduce the overhead of running the 5G authentication of 5G-RG, and make the authentication process consistent for both 5G-RG and FN-RG.

Authentication of 5G-UE

5G-UE supports the primary authentication methods including 5G-AKA and EAP-AKA' and can use one of such methods to authenticate to the 5G core. If authenticated through wireline access networks, EAP-5G will be used to encapsulate NAS messages inside EAP frames.

Authentication of Non-5G Capable Devices

There are large numbers of devices connecting to fixed access networks today which do not support 5G. It is desirable to allow those non-5G capable (N5GC) devices to also register to the 5G core so that they can be treated consistently as 5G UE.

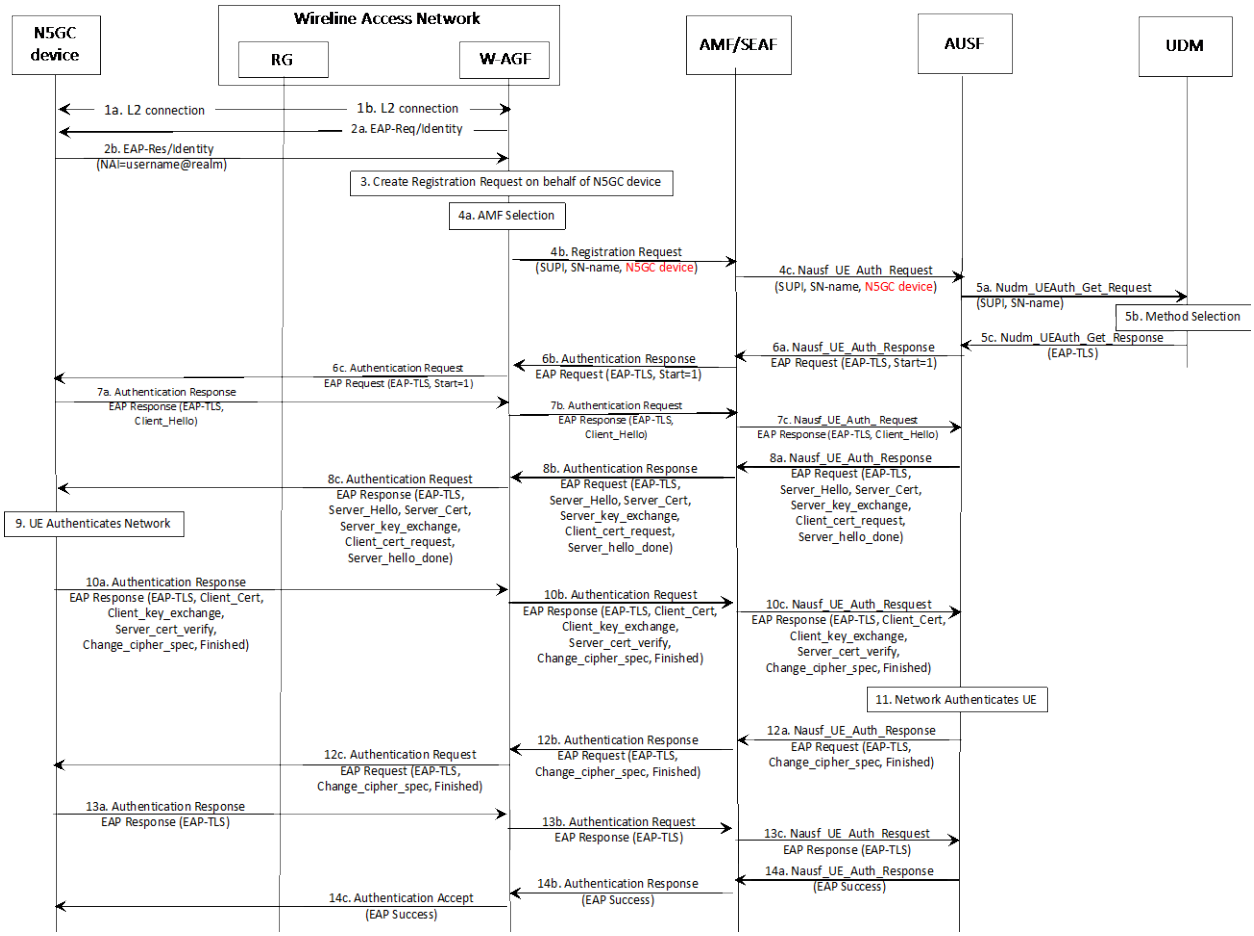

Figure 6 - Authentication Procedure of Non-5G Capable Devices in WWC

To do so, non-5G capable devices can use one of the EAP methods such as EAP-TLS to authenticate to the 5G core. EAP-TLS is defined in TS 33.501 Annex B, which, however, cannot be directly used to authenticate non-5G capable devices since it requires the EAP peer to be capable of receiving and processing 5G specific paramters such as ABBA and ngKSI, as well as performing 5G specific key derivation. We proposed a new procedure (see Figure 6) for authenticating non-5G capable devices, which is under discussion at 3GPP.

Conclusion

5G standards are being actively developed, and one of the 5G use cases is to support convergence. In this paper, we discussed the authentication of each of the network elements in WWC. Due to the diversity of network elements and different trust models, WWC demands the support of different authentication methods and procedures, some of which have been agreed to in 3GPP and some have not. We hope this paper can serve the purpose of not only providing an overview of this subject, but facilitate the development of WWC authentication related specifications in 3GPP.

Abbreviations

3GPP	3rd Generation Partnership Project
5GC	5G Core
5G-RG	5GG Residential Gateway
5G-BRG	5G Broadband Residential Gateway
5G-CRG	5G Cable Residential Gateway
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
BBF	Broadband Forum
FN-BRG	Fixed Network Broadband RG
FB-CRG	Fixed Network Cable RG
FN-RG	Fixed Network RG
NG-RAN	Next Generation Radio Access Network
RG	Residential Gateway
SMF	Session Management Function
UPF	User Plane Function
W-5GAN	Wireline 5G Access Network
W-5GBAN	Wireline 5G Broadband Access Network
W-5GCAN	Wireline 5G Cable Access Network
W-AGF	Wireline Access Gateway Function
WLAN	Wireless Local Area Network
WWC	Wireless Wireline Convergence

Bibliography & References

[1] 3GPP TS 23.501, "System Architecture for 5G System", Release 16

[2] 3GPP TS 23.316, "Wireless and wireline convergence access support for the 5G System (5GS)", Release 16

[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).

