Technical Disclosure Commons

Defensive Publications Series

April 2020

Handling of Extensible Authentication Protocol Based Non-Access Stratum Authentication Failures

Roy Lin

Poying Chuang

Recommended Citation

Lin, Roy and Chuang, Poying, "Handling of Extensible Authentication Protocol Based Non-Access Stratum Authentication Failures", Technical Disclosure Commons, (April 23, 2020)
https://www.tdcommons.org/dpubs_series/3191

Handling of Extensible Authentication Protocol Based Non-Access Stratum Authentication Failures

Abstract:

In a 5G System (5GS), the network initiates and controls the authentication method, meaning that the network determines whether the user equipment (UE) and the network use EAP-based NAS authentication or 5G AKA-based NAS authentication for the mutual authentication of the UE and the network. The specification for 5GS presumes that in a 5G standalone case, the UE supports both EAP-based NAS authentication and 5G AKA-based NAS authentication. However, not all wireless carriers have required support for EAP-based NAS authentication. As a result, many UEs manufactured do not support EAP-based NAS authentication. This publication describes techniques for preventing an authentication failure in 5GS when the network selects an authentication method (*e.g.*, EAP-based NAS authentication) that the UE does not support.

Keywords:

authentication, Authentication and Key Agreement (AKA), Extensible Authentication Protocol (EAP), non-access stratum (NAS), user equipment (UE), negative acknowledgment (NAK; NACK), protocol, Public Land Mobile Network (PLMN), cellular network, Internet of Things (IoT), 5th Generation (5G)

Background:

The 5th Generation (5G) of wireless communication technologies provides for the wide use of public networks (*e.g.*, cellular networks), non-public networks (*e.g.*, wireless local area network (WLAN), private networks), and IoT environments by user equipment (UE) devices. In a standalone 5G System (5GS), a UE accesses a network, such as a Public Land Mobile Network (PLMN), through a communication link with a base station (*e.g.*, Evolved NodeB (eNB) node, Next Generation NodeB (gNB) node) of the network. The base station can act as a serving cell (serving base station) of the network, and a network may have multiple serving cells (serving base stations).

After the UE connects with the base station, for example, after completion of a Radio Resource Control connection setup procedure, the UE initiates registration with the network utilizing an NAS Attach Procedure. During the NAS Attach Procedure, the UE and the network utilize a credential-based mutual authentication method for the authentication of the UE and the network. In some aspects, the credentials are a shared key that both the UE and the network have access to, such as a SIM-based credential (*e.g.*, Subscriber Identification Module (SIM), Universal Subscriber Identification Module (USIM), Universal Integrated Circuit Card (UICC)) utilized by the 5G Authentication and Key Agreement (5G AKA) and Extensible Authentication Protocol Authentication and Key Agreement Prime (EAP-AKA’) protocols. In other aspects, the credentials are certificate-based, such as a public key certificate shared between the UE and the network utilized by the EAP Transport Layer Security (EAP-TLS) protocol.

In 5GS, the network initiates and controls the authentication method, meaning that the network determines whether the UE and the network use an EAP-based authentication over 5G NAS (EAP-based NAS authentication, such as EAP-AKA’ or EAP-TLS) or a 5G AKA-based authentication over 5G NAS (5G AKA-based NAS authentication, such as 5G AKA) for the mutual authentication of the UE and the network. The NAS authentication method selected by the network may vary based on the environment. For example, the same system may use: (a) the EAP-TLS protocol for access to non-public (private) networks and IoT environments, (b) the 5G AKA protocol for 3GPP access to a 3GPP core network, and (c) the EAP-AKA' protocol for non-3GPP access (*e.g.*, Evolution-Data Optimized (EV-DO), wireless local area network (WLAN), WiMAX) to a 3GPP core network.

The specification for 5GS (*e.g.*, 3GPP TS 24.501 v.16.3.0 (2019-12), section 5.4.1.1) presumes that in a 5G standalone case, the UE supports both EAP-based NAS authentication and 5G AKA-based NAS authentication. However, not all wireless carriers have required support for EAP-based NAS authentication. As a result, many UEs manufactured do not support EAP-based NAS authentication.

Figure 1 illustrates an example in 5GS, where the network selects an authentication method that the UE does not support.

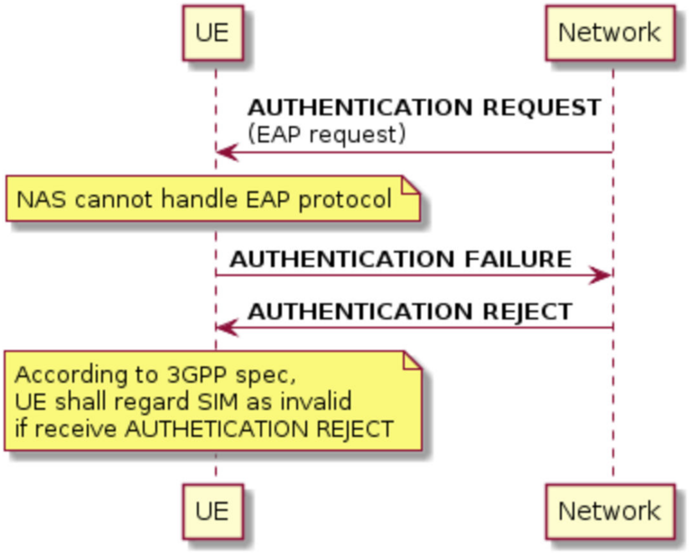

Figure 1

After the UE connects with the base station, the UE initiates registration with the network through an NAS Attach Procedure where the UE sends an ATTACH message to the network (not shown in Figure 1). Upon receiving the ATTACH message from the UE, the network determines the authentication method used by the system and initiates the authentication of the UE by sending an Authentication Request message to the UE. For example, the network may send an EAP Request message to the UE for EAP-based NAS authentication.

In the example of Figure 1, the UE is not configured to support the utilization of EAP-based NAS authentication and cannot decode or encode EAP messages. This occurs when, for example, the UE has a non-public network SIM card (or an Internet of Things capable (IoT-capable) SIM card) that does not support the EAP protocol over NAS inserted. Upon receiving the EAP Request message from the network, the UE replies with an Authentication Failure message. The Authentication Failure message triggers the network to send an Authentication Reject message to the UE. Upon receiving such an Authentication Reject message, the 5GS specification directs the UE to regard the SIM-based credential (*e.g.*, SIM, USIM) as invalid for 5GS services and invalid for non-Evolved Packet System (EPS) service. As a result, the UE will not have access to normal service until after power-cycling the UE or removal of the UICC containing the SIM-based credential.

Description:

This publication describes techniques for preventing an authentication failure in 5GS when the network selects an authentication method that the UE does not support. One or more of the techniques described herein may be utilized individually or together.

Figure 2 illustrates a first technique for preventing an authentication failure in 5GS when the network selects an authentication method (*e.g.*, EAP-based NAS authentication) that the UE does not support.

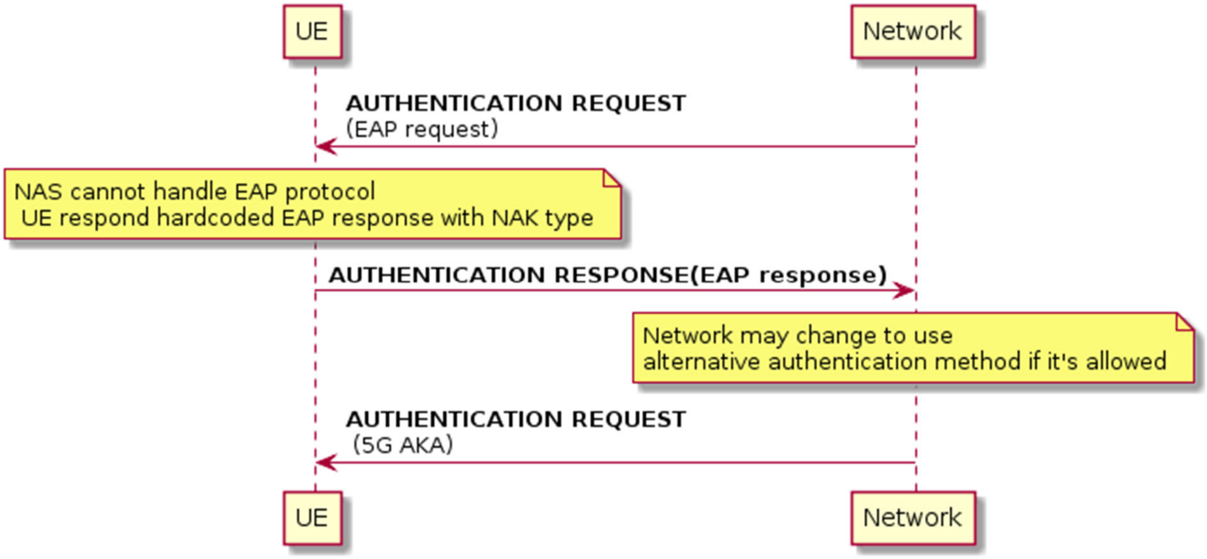
UE
Network
AUTHENTICATION REQUEST
(EAP request)
NAS cannot handle EAP protocol
UE respond hardcoded EAP response with NAK type
AUTHENTICATION RESPONSE(EAP response)
Network may change to use
alternative authentication method if it's allowed
AUTHENTICATION REQUEST
(5G AKA)
UE
Network

Figure 2

After the UE connects with the base station, the UE initiates registration with the network through an NAS Attach Procedure (*e.g.*, sends an ATTACH message to the network, not shown in Figure 2). Upon receiving the ATTACH message from the UE, the network determines to use an EAP-based authentication method (*e.g.*, EAP-AKA') and initiates the authentication of the UE by sending an EAP Authentication Request message (EAP Request) to the UE for EAP authentication over 5G NAS.

Upon receiving the EAP Request message from the network, the UE determines if it supports EAP-based NAS authentication. If the UE cannot handle the EAP protocol, instead of sending an Authentication Failure message, the UE sends a hard-coded Authentication Response (EAP Response) message to the network. The hard-coded Authentication Response message indicates that the UE does not support EAP-based NAS authentication and/or requests the network to change the authentication method to an alternative authentication protocol (*e.g.*, 5G AKA) if the network is allowed to do so. The hard-coded Authentication Response (EAP Response) message may be a negative acknowledgment response (NAK Response) message, when the UE finds the desired authentication Type in the EAP Request message unacceptable. In such a NAK Response, Type zero (0) may be used to indicate that the sender (the UE) has suggested no particular alternative authentication methods. Other Type values may indicate that the UE suggests one or more alternative authentication methods (*e.g.*, 5G AKA). The receipt of an Authentication Response message that includes a hard-coded EAP Response prompts the network to select an alternative authentication method (*e.g.*, 5G AKA protocol) and send a second Authentication Request (5G AKA) message to the UE requesting 5G AKA-based NAS authentication.

Figure 3 illustrates a second technique for preventing an authentication failure in 5GS when the network selects an authentication method that the UE does not support.

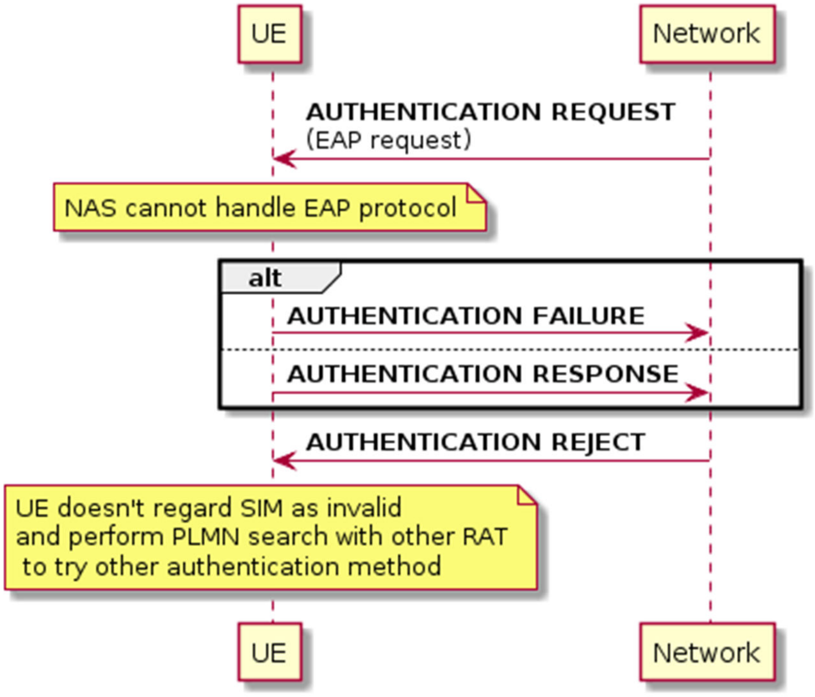
UE
Network
AUTHENTICATION REQUEST
(EAP request)
NAS cannot handle EAP protocol
alt
AUTHENTICATION FAILURE
AUTHENTICATION RESPONSE
AUTHENTICATION REJECT
UE doesn't regard SIM as invalid
and perform PLMN search with other RAT
to try other authentication method
UE
Network

Figure 3

After the UE connects with the base station, the UE initiates registration with the network through an NAS Attach Procedure (*e.g.*, sends an ATTACH message to the network, not shown in Figure 3). Upon receiving the ATTACH message from the UE, the network determines to use an

EAP-based authentication method (*e.g.*, EAP-AKA', EAP-TLS) and initiates the authentication of the UE by sending an EAP Authentication Request message (EAP Request) to the UE for EAP authentication over 5G NAS.

Upon receiving the EAP Request message from the network, the UE determines if it supports EAP-based NAS authentication. If the UE does not support the EAP protocol, the UE sends an Authentication Failure message and an Authentication Response message to the network. The Authentication Failure message triggers the network to send an Authentication Reject message to the UE. Upon receiving such an Authentication Reject message, the UE does not regard the SIM-based credential (*e.g.*, SIM) as invalid for 5GS services, nor does the UE regard the USIM as invalid for non-EPS service. Instead, the UE performs a Public Land Mobile Network (PLMN) search with another Radio Access Technology (RAT) in an attempt to find another PLMN/RAT to perform an NAS Attach procedure with to obtain service that does not require EAP-based NAS authentication.

Figure 4 illustrates a third technique for preventing an authentication failure in 5GS when a PLMN (network) selects an authentication method that the UE does not support. After the UE connects with a first cell of a base station of the PLMN, the UE initiates registration with the network through an NAS Attach Procedure (*e.g.*, sends an ATTACH message to the network, not shown in Figure 4). Upon receiving the ATTACH message from the UE, the network determines to use an EAP authentication method (*e.g.*, EAP-AKA', EAP-TLS) and initiates the authentication of the UE by sending an EAP Authentication Request message (EAP Request) to the UE for EAP authentication over 5G NAS.

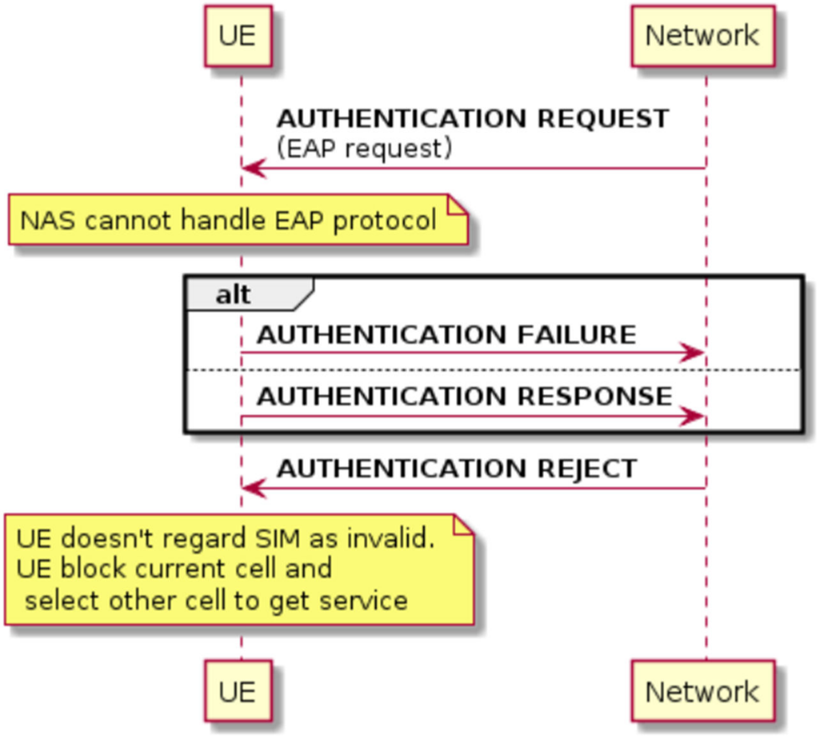

Figure 4

Upon receiving the EAP Request message from the network, the UE determines if it supports EAP-based NAS authentication. If the UE cannot handle the EAP protocol, the UE sends an Authentication Failure message and an Authentication Response message to the network. The Authentication Failure message triggers the network to send an Authentication Reject message to the UE. Upon receiving such an Authentication Reject message, the UE does not regard the SIM-based credential (*e.g.*, SIM) as invalid for 5GS services, nor does the UE regard the SIM-based credential as invalid for non-EPS service. Instead, the UE blocks the first cell of the PLMN and performs a cell selection procedure that selects a second cell of the PLMN that differs from the first cell, where the second cell provides service but does not require EAP-based NAS authentication. By blocking the first cell, the technique prevents camping on a private network or IoT cell with the same PLMN.

In a fourth technique for preventing an authentication failure in 5GS when a 3GPP core network selects an authentication method that the UE does not support, after the UE connects with the base station providing 3GPP access to the network, the UE initiates registration with the network through an NAS Attach Procedure (*e.g.*, sends an ATTACH message to the network). Upon receiving the ATTACH message from the UE, the network determines to use an EAP authentication method (*e.g.*, EAP-AKA', EAP-TLS) and initiates the authentication of the UE by sending an EAP Authentication Request message (EAP Request) to the UE for EAP authentication over 5G NAS. Upon receiving the EAP Request message from the network, the UE determines if it supports EAP-based NAS authentication. If the UE cannot handle the EAP protocol, the UE sends an Authentication Failure message and an Authentication Response message to the network. The Authentication Failure message triggers the network to send an Authentication Reject message to the UE. Upon receiving such an Authentication Reject message, the UE does not regard the SIM-based credential (*e.g.*, SIM) as invalid for 5GS services, nor does the UE regard the SIM-based credential as invalid for non-EPS service. Instead, the UE performs a cell selection procedure that selects a second base station providing non-3GPP access to the network that does not require EAP-based NAS authentication.

References:

[1] Patent Publication: US20170078333A1. "Improved end-to-end data protection." Priority to March 17, 2014.

[2] ETSI TS 124 501 V15.1.0 (2018-10). "5G; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (3GPP TS 24.501 version 15.1.0 Release 15)." October 2018. https://www.etsi.org/deliver/etsi_ts/124500_124599/124501/15.01.00_60/ts_124501v150100p.pdf.

[3] NETMANIAS. "Seven Deployment Scenarios of Private 5G Networks." https://www.netmanias.com/en/post/blog/14500/5g-edge-kt-sk-telecom/7-deployment-scenarios-of-private-5g-networks.

[4] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, DOI 10.17487/RFC3748, June 2004, https://www.rfc-editor.org/info/rfc3748.

[5] 3GPP TS 22.261.

[6] 3GPP TS 24.501 v16.3.0(2019-12).

[7] 3GPP TS 33.501 v16.1.0(2019-12).