**3GPP TSG-SA3 Meeting #101e *S3-202887***

**e-meeting, 9-20 November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | 0960 | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Error correction and clarification of Annex O | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | CableLabs | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5WWC | | | | |  | ***Date:*** | | | 2020-10-28 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | |  |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) Rel-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Correction of typo and an error in the figure, and clarification of authentication method selection for anoymous SUPI | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1. Text color of red is removed 2. A typo is corrected 3. An outplaced line in the figure is corrected 4. An clarification of authentication method selection based on anoymous SUPI is added | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Errors and misunderstanding may persist | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex O | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

**\*\*\*\* BEGIN CHANGES \*\*\*\***

Annex O (Informative):  
Authentication for non-5G capable devices behind residential gateways

# O.1 General

This annex describes the authentication procedure, using EAP-TLS as an example, for Non-5G Capable (N5GC) devices behind Residential Gateways (RGs) in private networks or in isolated deployment scenarios (i.e., roaming is not considered) with wireline access. The registration procedure of N5GC devices behind Cable RGs is described in clause 4.10a of TS 23.316 [79].

# O.2 Baseline for using non-5G capable devices with 5GC

N5GC devices lack some key 5G capabilities, including NAS and the derivation of 5G key hierarchy. Those devices exist in wireline networks and need to be able to access the converged 5G core. The authentication of N5GC devices can be based on additional EAP methods other than EAP-AKA’. The procedure in O.3 uses EAP-TLS as in Annex B as an example, but it differs from the Annex B in the following:

a) the W-AGF creates the registration request on behalf of the N5GC device,

b) 5G related parameters (including ngKSI and ABBA) are not sent to the N5GC device. When received from the AMF, these parameters are ignored by the W-AGF, and

c) Neither the N5GC device nor the AUSF derives any 5G related keys after EAP authentication.

# O.3 Authentication procedure

Figure O.3-1 shows the details of the authentication procedure as part of the initial registration procedure specified in clause 4.10a of TS 23.316 [79] following the principles listed in clause O.2. It uses EAP-TLS as an example, but other EAP methods can also be supported. The W-AGF acts on behalf of the N5GC device during the registration process. The link between the N5GC device and the RG, and between the RG and the W-AGF can be any data link (L2) that supports EAP encapsulation.



Figure O.3-1: Registration and authentication of a non-5G capable device to the 5GC

In the following, the procedure for registration and authentication of an N5GC device to the 5GC is described:

1. The N5GC device connects to the W-AGF via a RG which is configured as a layer 2 bridge. The W-AGF is associated with a 5GC and acts on behalf of the N5GC device during its registration process.

2a. The W-AGF initiates the EAP authentication procedure by sending an EAP request/Identity to the N5GC device via the RG, which acts as an L2 bridge device and forwards the ethernet frame to the N5GC device. The EAP message is encapsualted inside an L2 frame (e.g., EAPOL).

2b. In response, the N5GC device sends back an EAP response/Identity including its Network Access Identifier (NAI) in the form of username@realm.

NOTE 1: If TLS subscription identifier privacy protection is supported , as in "Section 2.1.4. Privacy" of RFC 5216 [38] for TLS 1.2 or in RFC 8446 [60] for TLS 1.3, the "username" part must be is either omitted or "anonymous".

3. The W-AGF creates a registration request on behalf of the N5GC device with an indication that the registration is on behalf of an N5GC device. The SUPI of the N5GC device is the NAI as received from the device, and the W-AGF constructs the SUCI from this SUPI using the NULL scheme.

4a. The W-AGF selects the AMF/SEAF.

4b. The W-AGF sends to the AMF/SEAF a registration request on behalf of the N5GC device. The registration request includes the NAI SUCI, wireline network name if available, and a device capability indicator (e.g., the device is non-5G capable).

4c. The AMF/SEAF selects the AUSF based on the SUCI in the received registration request and sends a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. It contains the SUCI of the N5GC device, and an indicator that the request is on behalf of the N5GC device.

5a. The AUSF sends a Nudm\_UEAuthentication\_Get Request to the UDM. It contains the SUCI of the N5GC device and the N5GC device indicator

5b. The UDM invokes the SIDF to map the SUCI to the SUPI and selects an authentication method, e.g., EAP-TLS, based on the SUPI and the N5GC device indicator. 5c. The UDM sends a Nudm\_UEAuthentication\_Get Response to the AUSF, which contains the SUPI of the N5GC device and an indicator of the selected authentication method, e.g., EAP-TLS.

NOTE 2: Steps 6a-14c describe the exchange of EAP-TLS between the AUSF and the N5GC device, based on TLS 1.2 without subscription identifier privacy protection. If the operator determines to provide subscription identifier privacy for the N5GC in TLS layer, the EAP TLS server needs to support privacy either inherently (e.g., in TLS 1.3) or via separate privacy option (e.g., in TLS 1.2). When TLS 1.2 is used, the N5GC device would need to behave as described in "Section 2.1.4. Privacy" of RFC 5216 [38] where instead of sending the client certificate in cleartext over the air, the N5GC device sends TLS certificate (no cert) during the first TLS handshake and sends TLS certificate (client certificate) during the second TLS handshake within the TLS session negotiated form the first TLS handshake.

6a. The AUSF starts EAP-TLS by sending to the AMF/SEAF a Nausf\_UEAuthentication\_Authenticate Response message containing an EAP-Request message of EAP-type=EAP-TLS with the Start (S) bit set, denoted as EAP-Request/EAP-TLS [TLS start].

6b. The AMF/SEAF forwards the EAP-Request/EAP-TLS [TLS start] in the Authentication Request message to the W-AGF.

6c. After receiving the EAP-Request/EAP-TLS [TLS start] message from AMF/SEAF, the W-AGF forwards the EAP-Request/EAP-TLS [TLS start] message to the N5GC device in an L2 message, leaving out the ABBA and ngKSI parameters.

7a. After receiving the EAP-Request/EAP-TLS [TLS start] message from the W-AGF, the N5GC device replies to the W-AGF with an EAP-Response/EAP-TLS message whose data field encapsulates a TLS client\_hello message. Such EAP-Response message, denoted as EAP-Response/EAP-TLS [client\_hello], is encapsulated in an L2 message.

7b. The W-AGF forwards the EAP-Response/EAP-TLS [client\_hello] to the AMF/SEAF in an Authentication Response message.

7c. The AMF/SEAF forwards the EAP-Response/EAP-TLS [client\_hello] message to the AUSF in a Nausf\_UEAuthentication\_Authenticate Request message.

8a. The AUSF replies to the AMF/SEAF with EAP-Request/EAP-TLS message whose data field encapsulates a TLS server\_hello message, a TLS server certificate message, a TLS server\_key\_exchange message, a TLS client certificate\_request message, and a TLS server\_hello\_done message. Such EAP-Request message, denoted as EAP-Request/EAP-TLS [server\_hello], is encapsulated in a Nausf\_UEAuthentication\_Authenticate Response message.

8b. The AMF/SEAF forwards the EAP-Request/EAP-TLS [server\_hello] message to the W-AGF in an Authentication Request message.

8c. The W-AGF forwards the EAP-Request/EAP-TLS [server\_hello] to the N5GC device in an L2 message.

9. The N5GC device authenticates the AUSF by validating the server certificate included in the EAP-Request/EAP-TLS [server\_hello] message received in step 8c. The N5GC device needs to be provisioned with certificates of a trust anchor to validate the AUSF server certificate. In addition, the N5GC device also needs to be provisioned with its own client certificate.

10a. If the TLS server authentication is successful, then the N5GC device replies to the W-AGF with EAP-Response/EAP-TLS in an L2 message. The data field of the EAP-Response/EAP-TLS message contains a TLS client certificate message, a TLS client\_key\_exchange message, a TLS certificate\_verify message, a TLS change\_cipher\_spec message, and TLS finished message. This EAP-Response message is denoted as EAP-Response/EAP-TLS [client\_certificate].

10b. The W-AGF forwards to the AMF/SEAF the EAP-Response/EAP-TLS [client\_certificate] in an Authentication Response message.

10c. The AMF/SEAF forwards the EAP-Response/EAP-TLS [client\_certificate] message to the AUSF in a Nausf\_UEAuthentication\_Authenticate Request message.

11. The AUSF authenticates the N5GC device by verifying the client certificate received in the EAP-Response/EAP-TLS [client\_certificate] message. Among other validations, the AUSF verifies that the client certificate is issued by a certificate authority trusted by the AUSF. If the client certificate is verified successfully, the AUSF continues to step 12a. Otherwise the AUSF returns an EAP-failure message. The AUSF needs to be provisioned with certificates of trust anchor to verify client certificates.

12a. The AUSF sends to the AMF/SEAF an EAP-Request/EAP-TLS message with its data field encapsulating a TLS change\_cipher\_spec message and a TLS server finished. This EAP-Request message, denoted as EAP-Request/EAP-TLS [server\_finished], is encapsulated in a Nausf\_UEAuthentication\_Authenticate Response message.

12b. The AMF/SEAF forwards EAP-Request/EAP-TLS [server\_finished] message to the W-AGF in an Authentication Request message.

12c. The W-AGF forwards EAP-Request/EAP-TLS [server\_finished] message to the N5GC device in an L2 message.

13a. The N5GC sends to the W-AGF an EAP-Response/EAP-TLS message with its data field set to empty, denoted as EAP-Response/EAP-TLS [empty], in an L2 message

13b. The W-AGF forwards to the AMF/SEAF the EAP-Response/EAP-TLS [empty] message in an Authentication Response message.

13c. The AMF/SEAF forwards the EAP-Response/EAP-TLS [empty] message to the AUSF in a Nausf\_UEAuthentication\_Authenticate Request message.

14a. The AUSF sends to the AMF/SEAF an EAP-Success message along with the SUPI in a Nausf\_UEAuthentication\_Authenticate Response message. If the SUPI received from the UDM in step 5c is anonymous, the AUSF derives the SUPI from the client identifier in the TLS client certificate. AUSF does not perform the derivation of KAUSF nor KSEAF based on the indicator of an N5GC device received in step 4c, nor sends KSEAF to AMF/SEAF.

NOTE X: It is left to implementation, the AUSF verifies that the SUPI derived from the client certificate belongs to a valid susbcription in the network. If there is a miss-match, the AUSF returns an EAP-failure message

14b. The AMF/SEAF forwards to the W-AGF the EAP-Success message in an Authentication Result message or a Security Mode Command message.

14c. The W-AGF forwards to the N5GC device the EAP-Success message in an L2 message, and the authentication procedure is finished.

NOTE 3: Neither the AUSF nor the N5GC device performs further 5G related key derivation from EMSK, since neither 5G AS nor 5G NAS security is used in this setting.

15. The AMF sends Registration Accept message to the W-AGF.

**\*\*\*\*\* END OF CHANGES \*\*\*\*\*\***