**SA WG2 Meeting #154S2-2210280**

**November 14th – 18th, 2022; Toulouse (revision of S2-2210280)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.502** | **CR** | **3553** | **rev** | **3** | **Current version:** | **17.6.0** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Secondary DN authentication and authorization in EPS IWK case | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Ericsson, Samsung | | | | | | | | | |
| ***Source to TSG:*** | S2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI18\_SDNAEPC | | | | |  | ***Date:*** | | | 2022-10-24 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Secondary authentication/authorization by a DN-AAA server during the establishment of a PDU Session has been defined since R15 in TS 23.501 clause 5.6.6  No such mechanism has been defined for EPC; this means that if an operator has negotiated with a 3rd party owning a DN that access to this DN (data connectivity to a DNN corresponding to this DN) is to be controlled by UE authentication / authorization run by a 3rd party DN AAA, UE(s) cannot establish a data connectivity to the DN when the UE is served by EPC.  In the “Reply LS on Secondary AUTH for 5GS interworking with EPS”, S2-2101305, SA2 wrote: “EAP based secondary authorization/ authentication has only been defined for 5GS and is thus not applicable to EPS in existing releases. SA2 expects that in case EAP based secondary authorization/ authentication is to be introduced in EPS it would require a new work item in SA2.”  A similar issue has been discussed as part of R17 for UTM based authentication and authorization of UAS. TS 23.256 supports UTM based authentication and authorization regardless of whether the UE (UAS) is served by 5GC or by EPC (via MME and SGW). This is defined in TS 23.256 clause 5.2.3.3. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Support Secondary authentication/authorization by a DN-AAA server during the establishment of a PDN connection over EPC, reusing the principles of the solution defined in TS 23.256 clause 5.2.3.3:   * A SMF+PGW-c is used to serve DNN(s) requiring Secondary authentication/authorization by a DN-AAA server. * For Secondary authentication/authorization by a DN-AAA server, the SMF+PGW-c runs the same procedures with PCF, UDM and DN-AAA and uses the same corresponding interfaces regardless of whether the UE is served by EPC or 5GC * Only the interface towards the UE is different (usage of 4G NAS instead of 5G NAS) between the EPC and 5GC cases. * The MME and SGW are not impacted by the procedure. Specific exchanges between the UE and the SMF+PGW-c for Secondary authentication/authorization by a DN-AAA server are carried via PCO. This includes the support of EAP exchanges between the UE and the DN AAA server * As it is not possible to exchange PCO between the UE and the PGW without first establishing the PDN connection, the PDN connection is established before Secondary authentication/authorization by a DN-AAA server has taken place. * When Secondary authentication/authorization by a DN-AAA server has successfully taken place, the SMF+PGW-c allows traffic exchange at the UPF and indicates to the UE that User plane traffic is now possible; | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | if an operator has negotiated with a 3rd party owning a DN that access to this DN (data connectivity to a DNN corresponding to this DN) is to be controlled by UE authentication / authorization run by a 3rd party DN AAA, UE(s) cannot establish a data connectivity to the DN when the UE is served by EPC. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.11.0a.7, Annex X (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **X** |  | Other core specifications | | | | TS 23.501 CR3701. | | |
| ***affected:*** | |  | **x** | Test specifications | | | |  | | |
| ***(show related CRs)*** | |  | **x** | O&M Specifications | | | |  | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Changes in rev02:  Following EN is removed:  Editor’s Note: if the UE IP address is to be provided by the DN AAA it is FFS how the DN AAA would provide the UE IP address before having authenticated it  And replaced by highlighted text, mostly   * Step 1: Secondary DN authorization is invoked as described in TS 29.561. During this step the DN-AAA may provide an IP address for the UE and other DN authorization data as described in TS 23.501, clause 5.6.6 * Then EAP based secondary DN Authentication is triggered * During step 3 the SMF+PGW-C may, as described in step 5 of Figure 4.3.2.3-1, contact the PCF to provide the PDN Connection parameters received from the DN AAA at step 1 (and former step 5 removed)   Changes in rev03   * Put this in step 2: The SMF may perform an SM Policy Association Establishment procedure as defined in clause 4.16.4. If the SMF received the DN Authorization Profile Index or DN authorized Session AMBR in DN Authorization Data from the DN-AAA, it provides this information to the PCF. * EN about stage 3 work transformed into a NOTE * And in step 7: If dynamic PCC is to be used for the PDU Session and the SMF+PGW-C received DN Authorization information from the DN-AAA as part of step 5 and 6, the SMF+PGW-C contacts the PCF to update the PDN Connection as described in step 5 of Figure 4.3.2.3-1 | | | | | | | | |

*First CHANGE*

#### 4.11.0a.7 Interactions with DN-AAA Server

EAP-based secondary authentication and authorization at PDU session establishment is supported as defined in clause 4.3.2.3. EAP-based secondary authentication and authorization at PDN connection establishment is supported as defined in Annex X.

This clause 4.11.0a.7 defines the support of secondary authorization over EPS without EAP-based authentication when one of the UE, the 5GC, and the DN does not support (or is configured not to use) the mechanisms defined in Annex X.

Secondary authorization (without authentication of the UE) with a DN-AAA Server, as specified in clause 4.3.2.3, is supported when the UE is in EPS.

NOTE 1: This implies that when data connectivity to the DN is initiated as a PDU session over 5GC it can be subject to EAP based secondary authentication mechanism (see TS 33.501 [15]) whereas, when data connectivity to the same DN is initiated as a PDN connection over EPC it cannot be subject to EAP based secondary authentication mechanism. This discrepancy occurs regardless of whether the data connection is later on moved between EPC and 5GC.

NOTE 2: Secondary authorization without authentication means no signalling exchange with the UE.

If secondary authentication and authorization has been performed for the PDU Session while the UE was in 5GS and the UE has moved to EPS, the following applies:

- DN-AAA re-authorization (without re-authentication signalling) can be performed even when the UE is in EPS, e.g. to provide new parameters from the DN-AAA Server to SMF+PGW-C.

- Re-authentication cannot be performed while the UE is in EPS because there is no support of the related signalling in EPS. In case the SMF+PGW-C receives a re-authentication request from the DN-AAA, the SMF+PGW-C informs the DN-AAA Server that the UE is not available for re-authentication at the moment. The SMF+PGW-C should not initiate PDN connection release at this point: the DN-AAA decides the actions to take, based on the reply from SMF+PGW-C and local policy which may also trigger a DN-AAA Server request to release the PDU Session/PDN connection of the UE.

*Second CHANGE all text is new*

Annex X (normative): Support of EAP-based secondary authentication and authorization by DN-AAA over EPC

# X.1 Introduction

Secondary authentication/authorization by a DN-AAA server during the establishment of a PDN connection over 3GPP access to EPC, is supported based on following principles:

* A SMF+PGW-C shall be used to serve DNN(s) requiring secondary authentication/authorization by a DN-AAA server,
* For secondary authentication/authorization by a DN-AAA server, the SMF+PGW-C runs the same procedures with PCF, UDM and DN-AAA and uses the same corresponding interfaces, as defined in clause 4.3.2, regardless of whether the UE is served by EPC or 5GC,
* If the UE has included the PDU session ID in PCO, the UE may indicate in the PDN connection establishment request its support for EAP-based secondary authentication and authorization by DN-AAA over EPC. The SMF+PGW-C may reject the PDN connection establishment if the UE does not support EAP-based secondary authentication and authorization by DN-AAA over EPC while local policies tell that secondary authentication and authorization by DN-AAA is mandatory to access to the DN. When a PDU session is established, the UE may also indicate via PCO that it supports secondary DN authentication and authorization over EPC.
* Only the interface towards the UE is different (usage of EPC NAS instead of 5GC NAS) between the EPC and 5GC cases,
* The MME and SGW are not impacted by the procedure. Specific exchanges between the UE and the SMF+PGW-C for secondary authentication/authorization by a DN-AAA server are carried via PCO. This includes the support of EAP exchanges between the UE and the DN-AAA server,
* As it is not possible to exchange PCO between the UE and the PGW without first establishing the PDN connection, the PDN connection is established before secondary authentication/authorization by a DN-AAA server takes place,
* When secondary authentication/authorization by a DN-AAA server has successfully taken place, the SMF+PGW-C allows traffic exchange at the UPF and indicates to the UE that User plane traffic is now possible.

# X.2 Procedures

## X.2.1 Secondary authentication and authorization by DN-AAA at PDN Connection Establishment

In the figure X.2.1-1, the execution of the secondary authentication and authorization by DN-AAA is specified. The procedure assumes that:

* the APN is associated with the selection of a SMF+PGW-C to serve APN(s) that require secondary authentication and authorization by DN-AAA at PDN connection establishment,
* the SMF+PGW-C is configured with local policies indicating that the APN requires secondary authentication and authorization by DN-AAA at PDN connection establishment

Figure X.2.1-1: EAP-based secondary authentication and authorization by DN-AAA at PDN connection establishment

0. As Steps 1 - 13 in TS 23.401 [13] Figure 5.3.2.1-1 (Attach Request) or as steps 1 to 3 in TS 23.401 [13] Figure 5.10.2 (UE requested PDN connectivity) with following modifications: The UE may indicate in PCO its capability to support EAP-based secondary DN authentication over EPC if the UE included the PDU Session Id in PCO

1. The SMF+PGW-C gets subscription data from UDM as defined in step 4 of Figure 4.3.2.2.1-1 (not shown in the figure). The procedure assumes that subscription data from UDM require EAP-based secondary authentication and authorization by DN-AAA.

Secondary DN authorization is invoked as described in TS 29.561 [63]. During this step the DN-AAA may provide an IP address for the UE and other DN authorization data as described in TS 23.501, clause 5.6.6

2. If dynamic PCC is to be used for the PDU Session, the SMF+PGW-C performs an SM Policy Association Establishment procedure as defined in clause 4.16.4. If the SMF+PGW-C received the DN Authorization Profile Index or DN authorized Session AMBR in DN Authorization Data from the DN-AAA, it provides this information to the PCF.

UPF selection and N4 session establishment is executed with the difference that the SMF+PGW-C configures the UPF+PGW-U to block any UE traffic over the PDN Connection (until the Secondary DN authentication and authorization has been done and is successful).

3. Steps 15 - 24 in TS 23.401 [13] Figure 5.3.2.1-1 or steps 5 to 16 in TS 23.401 [13] Figure 5.10.2.

During the Attach procedure, at step 15 of TS 23.401 [13] Figure 5.3.2.1-1 or during UE requested PDN connectivity in step 5 of TS 23.401 [13] Figure 5.10.2, the SMF+PGW-C includes, in PCO, an Indication to the UE that "UpLink Data is NOT ALLOWED" on the PDN connection. The UE shall not send Uplink data to the network, until it receives an indication further from the network that "UpLink Data is ALLOWED".

NOTE:: How the Indication that Uplink data allowed/not allowed is carried in PCO is defined in TS 24.501 [].

During steps 2 or 3 the SMF+PGW-C may, as described in step 5 of Figure 4.3.2.3-1, contact the PCF to provide the PDN Connection parameters received from the DN AAA at step 1.

4. [Conditional] The PGW-C+SMF initiates EAP-based authentication by sending EAP-Request as described in step 2 of Figure 4.3.2.3-1.

5. Multiple round-trip messages as required by the authentication method used by DN-AAA may follow. The PCO including the authentication message from the DN-AAA is transferred to the UE by the SMF+PGW-C in Update Bearer Request and then over S1 by Downlink NAS Transport (steps 4b - 4d). The response from the UE is transferred to the SMF+PGW-C in an Uplink NAS Transport over S1 and Update Bearer Response (steps 4e - 4g) over EPS.

6. Secondary authentication and authorization by DN-AAA procedure continues as described in Step 4 of Figure 4.3.2.3-1.

7. The SMF+PGW-C updates the N4 rules in the UPF+PGW-U to allow traffic over the PDN Connection.If dynamic PCC is to be used for the PDU Session and the SMF+PGW-C received DN Authorization information from the DN-AAA as part of step 5 and 6, the SMF+PGW-C contacts the PCF to update the PDN Connection as described in step 5 of Figure 4.3.2.3-1

8. The SMF+PGW-C updates the UE by invoking the PDN GW initiated bearer modification without QoS update procedure (figure 5.4.3-1 of TS 23.401 [13]) initiated by sending an Update Bearer Request message to the SGW. The PCO includes an indication that "UpLink Data is ALLOWED". The UE confirms the update (see clause 5.4.3 of TS 23.401 [13]). If the UE IP address is to be delivered to the UE over user plane (via Router advertisement or DHCP) then the UE IP address is only delivered to the UE after step 8.

9. As in step 6 of of Figure 4.3.2.3-1.

The DN-AAA Server may revoke the authorization for a PDN connection or update DN authorization data for a PDN connection. According to the request from DN-AAA Server, the SMF+PGW-C may release or update the PDN connection.

At any time after the PDN connection establishment, the DN-AAA Server or SMF+PGW-C may initiate Secondary Re-authentication procedure for the PDN connection as described in clause 4.3.2.3. Step 4a to step 4h are performed to transfer the Secondary Re-authentication message between the DN-AAA Server amd the UE. The Secondary Re-authentication procedure may start from step 4a (DN-AAA initiated Secondary Re-authentication procedure) or step 4b (SMF+PGW-C initiated Secondary Re-authentication procedure).

During Secondary Re-authentication, if the SMF+PGW-C receives an indication from the MME that the UE is unreachable then it informs the DN-AAA Server that UE is not reachable for re-authentication. Based on this indication from SMF+PGW-C, the DN-AAA Server may decide to keep the PDN connection or request to release it.

DN-AAA may initiate DN-AAA Re-authorization without performing re-authentication based on local policy. DN-AAA Re-authorization procedure may involve steps 5 and 6 of Figure X.2.1-1 above.

During Secondary Re-authentication/Re-authorization, if the SMF+PGW-c receives DN Authorization Profile Index and/or DN authorized Session AMBR, the SMF+PGW-c reports the received value(s) to the PCF (as described in TS 23.501 [2]) by triggering the Policy Control Request Trigger as described in TS 23.503 [20].

*END OF CHANGES*