**3GPP TSG-CT WG1 Meeting #138-eC1-22xxxx**

**E-Meeting, 10th – 14th October 2022was C1-225738**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **24.302** | **CR** | **0734** | **rev** | **1** | **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 |  |

|  |
| --- |
|  |
| ***Title:***  |  |
|  |  |
| ***Source to WG:*** | ZTE, Ericsson |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc18-non3GPP |  | ***Date:*** | 2022-10-13 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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 canbe 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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | The IKEv2 authentication and tunnel establishment procedure can be either for a brand new PDN connection establishment or for handover.Therefore, the following paragraph in clause 7.2.2.1 may be interpreted as applicable in both cases of PDN connection establishment and handover case."*If the UE supports N1 mode, the UE shall indicate the PDU session ID in the IKE\_AUTH request message. If N1 mode capability is disabled, the UE may indicate the PDU session ID in the IKE\_AUTH request message.*"However, regardless of the status of UE N1 mode capability, the UE shall not indicate the PDU session ID in the IKE\_AUTH request message (according to 4.11.4.3.7 of 23.502) if:a) the IKEv2 authentication and tunnel establishment for handover the PDN connection from EPS; andb) there is no PDU session ID associated with the PDN connection being transferred from EPS.Hence, clarification needs to be added to reflect the exact case when the PDU session ID is indicated in the IKE\_AUTH request message. |
|  |  |
| ***Summary of change:*** | Clarify during the IKEv2 authentication and tunnel establishment for handover the PDN connection from EPS, if there is no PDU session ID associated with the PDN connection being transferred, the UE cannot indicate the PDU session ID in the IKE\_AUTH request message |
|  |  |
| ***Consequences if not approved:*** | Unclear statement. |
|  |  |
| ***Clauses affected:*** | 7.2.2.1 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\* \* \* First Change \* \* \* \*

#### 7.2.2.1 Tunnel establishment accepted by the network

Once the ePDG has been selected, the UE shall initiate the IPsec tunnel establishment procedure using the IKEv2 protocol as defined in IETF RFC 7296 [28] and 3GPP TS 33.402 [15].

The UE shall send an IKE\_SA\_INIT request message to the selected ePDG in order to setup an IKEv2 security association. Upon receipt of an IKE\_SA\_INIT response, the UE shall send an IKE\_AUTH request message to the ePDG, including:

- The type of IP address (IPv4 address or IPv6 prefix or both) that needs to be configured in an IKEv2 CFG\_REQUEST Configuration Payload. If the UE requests for both IPv4 address and IPv6 prefix, the UE shall send two configuration attributes in the CFG\_REQUEST Configuration Payload: one for the IPv4 address and the other for the IPv6 prefix;

- The "IDr" payload, containing the APN in the Identification Data, for non-emergency session establishment. For emergency session establishment, the UE shall format the "IDr" payload according to clause 7.2.5. The UE shall set the ID Type field of the "IDr" payload to ID\_FQDN as defined in IETF RFC 7296 [28]. The UE indicates a request for the default APN by omitting the "IDr" payload, which is in accordance with IKEv2 protocol as defined in IETF RFC 7296 [28]; and

- The "IDi" payload containing the NAI.

The IKE\_AUTH request message may also contain:

- An indication in a notify payload that MOBIKE is supported by the UE;

- The INTERNAL\_IP6\_DNS or the INTERNAL\_IP4\_DNS attribute in the CFG\_REQUEST Configuration Payload. The UE can obtain zero or more DNS server addressed in the CFG\_REPLY payload within the IKE\_AUTH response message as specified in IETF RFC 7296 [28]; or

- The P\_CSCF\_IP6\_ADDRESS attribute, the P\_CSCF\_IP4\_ADDRESS attribute or both in the CFG\_REQUEST Configuration Payload. The UE can obtain zero or more P-CSCF server addresses in the CFG\_REPLY Configuration Payload within the IKE\_AUTH response message as specified in IETF RFC 7651 [64].

The UE may support the TIMEOUT\_PERIOD\_FOR\_LIVENESS\_CHECK attribute as specified in clause 8.2.4.2. If the UE supports the TIMEOUT\_PERIOD\_FOR\_LIVENESS\_CHECK attribute, the UE shall include the TIMEOUT\_PERIOD\_FOR\_LIVENESS\_CHECK attribute indicating support of receiving timeout period for liveness check in the CFG\_REQUEST configuration payload within the IKE\_AUTH request message. If the TIMEOUT\_PERIOD\_FOR\_LIVENESS\_CHECK attribute as specified in clause 8.2.4.2 indicating the timeout period for the liveness check is included in the CFG\_REPLY configuration payload within the IKE\_AUTH response message or if the UE has a pre-configured timeout period, the UE shall perform the tunnel liveness checks as described in clause 7.2.2A.

NOTE 1: The timeout period for liveness check is pre-configured in the UE in implementation-specific way.

If the UE supports N1 mode and N1 mode capability is enabled, the UE shall indicate the PDU session ID in the IKE\_AUTH request message during the IKEv2 authentication and tunnel establishment for initial attach.

If the UE supports N1 mode and N1 mode capability is disabled, the UE may indicate the PDU session ID in the IKE\_AUTH request message during the IKEv2 authentication and tunnel establishment for initial attach.

If the UE supports N1 mode, regardless whether the N1 mode capability is enabled or disabled, the UE shall indicate the PDU session ID in the IKE\_AUTH request message during the IKEv2 authentication and tunnel establishment for handover of an existing PDN connection from EPS which the PDU session ID is associated with, or for transferring of an existing PDU session from 5GS.

If the UE supports N1 mode, regardless whether the N1 mode capability is enabled or disabled, the UE shall not indicate the PDU session ID in the IKE\_AUTH request message during the IKEv2 authentication and tunnel establishment for handover of a PDN connection which no PDU session ID is associated with.

In order to indicate the PDU session ID in the IKE\_AUTH request message, the UE shall include the N1\_MODE\_CAPABILITY Notify payload as defined in clause 8.2.9.15 in the IKE\_AUTH request message and shall:

- if the UE is establishing a PDN connection not related to any existing PDU session or any existing PDN connection, allocate a PDU session ID which is not currently being used by another PDU session over either 3GPP access or non-3GPP access, set the PDU Session ID field of the N1\_MODE\_CAPABILITY Notify payload to the allocated PDU session ID, and associate the allocated PDU session ID with the PDN connection that is being established;

 if the UE is transferring an existing PDU session from 5GS, set the PDU Session ID field of the N1\_MODE\_CAPABILITY Notify payload to the PDU session ID of the existing PDU session that is being transferred, and associate the PDU session ID with the PDN connection that is being established. If the existing PDU session is a non-emergency PDU session, the UE shall in addition associate the S-NSSAI of the existing PDU session that is being transferred and the related PLMN ID with the PDN connection that is being established; or

- if the UE is transferring an existing PDN connection from EPS and a PDU session ID is associated with the PDN connection that is being transferred, set the PDU Session ID field of the N1\_MODE\_CAPABILITY Notify payload to the PDU session ID associated with the existing PDN connection. If the existing PDN connection is a non-emergency PDN connection and an S-NSSAI and a related PLMN ID are associated with the existing PDN connection, the UE shall in addition associate the S-NSSAI and the related PLMN ID with the PDN connection that is being established.

During the IKEv2 authentication and security association establishment, if the UE supports explicit indication about the supported mobility protocols, it shall provide the indication as described in clause 6.3.

During the IKEv2 authentication and tunnel establishment for initial attach, the UE shall provide an indication about Attach Type, which indicates Initial Attach. To indicate attach due to initial attach, the UE shall include either the INTERNAL\_IP4\_ADDRESS or the INTERNAL\_IP6\_ADDRESS attribute or both in the CFG\_REQUEST Configuration Payload within the IKE\_AUTH request message. The INTERNAL\_IP4\_ADDRESS shall contain no value and the length field shall be set to 0. The INTERNAL\_IP6\_ADDRESS shall contain no value and the length field shall be set to 0.

During the IKEv2 authentication and tunnel establishment for handover, the UE not supporting IP address preservation for NBM shall indicate Initial Attach as described in the previous paragraph.

NOTE 2: The UE cannot handover PDN connection with PDN type "Ethernet" or "non-IP" from E-UTRAN to an ePDG because PDN connections with PDN type "Ethernet" or PDN type "non-IP" are not supported over ePDG.

During the IKEv2 authentication and security association establishment for handover, the UE supporting IP address preservation for NBM, shall provide an indication about Attach Type, which indicates Handover Attach. During the IKEv2 authentication and security association establishment for transfer of an existing PDU session from 5GS, the UE shall provide an indication about Attach Type, which indicates Handover Attach. To indicate attach due to handover, the UE shall include the previously allocated home address information during the IPSec tunnel establishment. Depending on the IP version, the UE shall include either the INTERNAL\_IP4\_ADDRESS or the INTERNAL\_IP6\_ADDRESS attribute or both in the CFG\_REQUEST Configuration Payload within the IKE\_AUTH request message to indicate the home address information which is in accordance with IKEv2 protocol as defined in IETF RFC 7296 [28]. If the previously allocated home address information consists of both an IPv4 address and an IPv6 prefix, then the UE shall include the INTERNAL\_IP4\_ADDRESS attribute and the INTERNAL\_IP6\_ADDRESS attribute in the CFG\_REQUEST configuration payload within the IKE\_AUTH request message. If the previously allocated home address information consists of an IPv4 address only, then the UE shall include the INTERNAL\_IP4\_ADDRESS attribute and shall not include the INTERNAL\_IP6\_ADDRESS attribute in the CFG\_REQUEST configuration payload within the IKE\_AUTH request message. If the previously allocated home address information consists of an IPv6 prefix only, then the UE shall include the INTERNAL\_IP6\_ADDRESS attribute and shall not include the INTERNAL\_IP4\_ADDRESS attribute in the CFG\_REQUEST configuration payload within the IKE\_AUTH request message. The UE shall support IPSec ESP (see IETF RFC 4303 [32]) in order to provide secure tunnels between the UE and the ePDG as specified in 3GPP TS 33.402 [15].

The UE may support multiple authentication exchanges in the IKEv2 protocol as specified in IETF RFC 4739 [49] in order to support authentication and authorization with an external AAA server allowing the UE to support PAP authentication procedure, or CHAP authentication procedure, or both, as described in 3GPP TS 33.402 [15].

If NBM is used and the UE wishes to access an external PDN and therefore needs to perform authentication and authorization with an external AAA server, the UE shall:

- If the IKE\_SA\_INIT response contains a "MULTIPLE\_AUTH\_SUPPORTED" Notify payload, then include a "MULTIPLE\_AUTH\_SUPPORTED" Notify payload in the IKE\_AUTH request as described in IETF RFC 4739 [49] and perform the additional authentication steps as specified in 3GPP TS 33.402 [15]; and

- If the IKE\_SA\_INIT response does not contain a "MULTIPLE\_AUTH\_SUPPORTED" Notify payload, then perform the UE initiated disconnection as defined in clause 7.2.4.1. The subsequent UE action is implementation dependent (e.g. select a new ePDG).

After the successful authentication with the 3GPP AAA server, the UE receives from the ePDG an IKE\_AUTH response message containing a single CFG\_REPLY Configuration Payload including the assigned remote IP address information (IPv4 address or IPv6 prefix) as described in clause 7.4.1. Depending on the used IP mobility management mechanism the following cases can be differentiated:

- If DSMIPv6 is used for IP mobility management, the UE configures a remote IP address based on the IP address information contained in the INTERNAL\_IP4\_ADDRESS or INTERNAL\_IP6\_SUBNET attribute of the CFG\_REPLY Configuration Payload. The UE uses the remote IP address as Care-of-Address to contact the HA.

- If NBM is used for IP mobility management and the UE performs an initial attach, the UE configures a home address based on the address information from the CFG\_REPLY Configuration Payload. Otherwise, if NBM is used and the UE performs a handover attach, the UE continues to use its IP address configured before the handover, if the address information provided in the CFG\_REPLY Configuration Payload does match with the UE's IP address configured before the handover. If the UE's IP address (IPv4 address or IPv6 prefix) does not match with the address information of the CFG\_REPLY Configuration Payload, the UE shall configure a new home address based on the IP address information contained in the INTERNAL\_IP4\_ADDRESS, INTERNAL\_IP6\_SUBNET or INTERNAL\_IP6\_ADDRESS attribute of the CFG\_REPLY Configuration Payload. In the latter case, the IP address preservation is not possible.

NOTE 3: In case of IPv6 address, the UE performs the match only on the IPv6 prefix provided within the CFG\_REPLY Configuration Payload contained in the INTERNAL\_IP6\_SUBNET or INTERNAL\_IP6\_ADDRESS.

If the UE receives a PDN\_TYPE\_IPv4\_ONLY\_ALLOWED Notify payload or a PDN\_TYPE\_IPv6\_ONLY\_ALLOWED Notify payload, then the UE shall not subsequently initiate another UE requested PDN connectivity procedure specific to the non-3GPP access to the same APN to obtain a PDN type different from the one allowed by the network until:

- the UE is switched off;

- the UICC containing the USIM is removed; or

- the network initiated the deactivation of the PDN connectivity to the given APN.

If the UE supports DSMIPv6, the UE may request the HA IP address(es), by including a corresponding CFG\_REQUEST Configuration Payload containing a HOME\_AGENT\_ADDRESS attribute within the IKE\_AUTH request message. The HOME\_AGENT\_ADDRESS attribute content is defined in clause 8.2.4.1. The HA IP address(es) requested in this attribute are for the APN for which the IPsec tunnel with the ePDG is set-up. In the CFG\_REQUEST within the IKE\_AUTH request message, the UE sets respectively the IPv6 address field and the optional IPv4 address field of the HOME\_AGENT\_ADDRESS attribute to 0::0 and to 0.0.0.0. If the UE can not obtain the IP addresses of the HA via IKEv2 signalling, it uses the home agent address discovery as specified in 3GPP TS 24.303 [11].

In case the UE wants to establish multiple PDN connections and if the UE uses DSMIPv6 for mobility management, the UE shall use DNS as defined in 3GPP TS 24.303 [11] to discover the HA IP address(es) for the additional PDN connections after IKEv2 security association was established to the ePDG.

During the IKEv2 authentication and security association establishment, following the UE's initial IKE\_AUTH request message to the ePDG, if the UE subsequently receives an IKE\_AUTH response message from the ePDG containing the EAP-Request/AKA-Challenge, after verifying the received authentication parameters and successfully authenticating the ePDG as specified in 3GPP TS 33.402 [15], the UE shall send a new IKE\_AUTH request message to the ePDG including the EAP-Response/AKA-Challenge. In addition, the UE shall provide the requested mobile device identity if available, as specified in clause 7.2.6.

If the UE supports P-CSCF restoration extension for untrusted WLAN as specified in 3GPP TS 23.380 [66], the UE shall send its capability indication of the support of P-CSCF restoration to the ePDG by including the P-CSCF\_RESELECTION\_SUPPORT Notify payload within an IKE\_AUTH request message. The content of the P-CSCF\_RESELECTION\_SUPPORT Notify payload is described in clause 8.2.9.4.

If:

- the UE supports N1 mode; or

- N1 mode capability is disabled and the UE indicated the PDU session ID in the IKE\_AUTH request message;

and the UE receives the N1\_MODE\_INFORMATION Notify payload as defined in clause 8.2.9.16 in the IKE\_AUTH response message, the UE shall delete the associated S-NSSAI, if any, and (re‑)associate the S-NSSAI in the S-NSSAI Value field of the N1\_MODE\_INFORMATION Notify payload with the PDU session associated with the IKEv2 security association that was established, and if the UE receives the N1\_MODE\_S\_NSSAI\_PLMN\_ID Notify payload as defined in clause 8.2.9.17 in the IKE\_AUTH response message, the UE shall delete the associated PLMN ID, if any, and (re-)associate the PLMN ID that the S-NSSAI relates to in the S-NSSAI PLMN ID field of the N1\_MODE\_S\_NSSAI\_PLMN\_ID Notify payload with the PDU session associated with the IKEv2 security association that was established.

\* \* \* End of Changes \* \* \* \*