**3GPP TSG-CT WG1 Meeting #128-eC1-21xxxx**

**Electronic meeting, 25 February - 5 March 2021 *was* C1-211110**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.502** | **CR** | **0188** | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  |
| *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:***  | Clarification on IKE SA and signalling IPsec SA establishment on untrusted access |
|  |  |
| ***Source to WG:*** | ZTE |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc17-non3GPP |  | ***Date:*** | 2020-02-25 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)* |
|  |  |
| ***Reason for change:*** | According to TS 33.501, it highlights that in the first IKE\_AUTH request message sent by UE: "*...in the IDi the UE shall set the ID type as ID\_KEY-ID in this message and set its value equal to any random number. The UE shall not use its GUTI/SUCI/SUPI as the Id in this step. If the UE is provisioned with the N3IWF root certificate, it shall include the CERTREQ payload within the IKE\_AUTH request message to request N3IWF’s certificate.*"Handling of the procedure above should be clarified in this stage 3 specification.If the UE supports MOBIKE, the UE shall include the MOBIKE\_SUPPORTED notify payload according to TS 23.502. However, it specifies "may" in clause 7.3.2.2.In addition, the second sentence of the NOTE in subclause 7.3.2.1 is confusing. |
|  |  |
| ***Summary of change:*** | Clarify1) the IKE messages following the IKE\_SA\_INIT exchange are encrypted and integrity protected.2) the UE shall include the IDi payload with the ID type set to ID\_KEY\_ID and value set to any random number in the initial IKE\_AUTH request message.3) the UE shall include CERTREQ payload to request N3IWF's certificate if the UE is provisioned with the N3IWF root certificateThe corresponding behavior of N3IWF is described accordingly.4) if the UE supports MOBIKE, the UE shall include the MOBIKE\_SUPPORTED notify payload.Remove the NOTE in subclause 7.3.2.1. |
|  |  |
| ***Consequences if not approved:*** | Unclear and incorrect statement. |
|  |  |
| ***Clauses affected:*** | 7.3.1, 7.3.2.1, 7.3.2.2 |
|  |  |
|  | **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:*** |  |

\* \* \* 1st Change \* \* \* \*

### 7.3.1 General

The purpose of this procedure is to establish a secure connection between the UE and the N3IWF over NWu, which is used to securely exchange the NAS signalling messages between the UE and the AMF via the N3IWF. The UE establishes the secure connection by establishing an IKE SA and first child SA to the N3IWF. The IKE SA and first child SA, called signalling IPsec SA, are created between the UE and the N3IWF after the IKE\_SA\_INIT exchange and after the IKE\_AUTH exchange (see IETF RFC 7296 [6]). The signalling IPsec established is used to transfer NAS signalling traffic. Additional child SAs (user plane IPsec SAs) can be established between the UE and the N3IWF to transfer user-plane traffic (see subclause 7.5).

Upon completion of the N3IWF selection procedure (subclause 7.2) the UE initiates an IKE\_SA\_INIT exchange as specified in IETF RFC 7296 [6]. Upon reception of the IKE\_SA\_INIT response the UE shall inform the upper layers that the access stratum connection is established.

Upon establishment of the access stratum connection, the UE initiates IKE\_AUTH exchange (see IETF RFC 7296 [6]) with EAP-5G encapsulation, as specified in subclause 7.3.2.

The UE encapsulates the initial NAS message and the AN parameters using the EAP-5G procedure as described in subclause 7.3.3. The signalling IPsec SA is established after completion of the EAP-5G procedure and IKE\_AUTH exchange.

\* \* \* 2nd Change \* \* \* \*

#### 7.3.2.1 IKE SA and signalling IPsec SA establishment initiation

The UE proceeds with the establishment of IKE SA and signalling IPsec SA with the selected N3IWF by initiating an IKE\_SA\_INIT exchange according to IETF RFC 7296 [6]. All the IKE messages following the IKE\_SA\_INIT exchange are encrypted and integrity protected using the cryptographic algorithms and keys negotiated in the IKE\_SA\_INIT exchange as specified in IETF RFC 7296 [6].

Upon completion of the IKE\_SA\_INIT exchange, the UE shall initiate an IKE\_AUTH exchange as specified in IETF RFC 7296 [6] to establish an IKE SA and first child SA (signalling IPsec SA). In the initial IKE\_AUTH request message, the UE shall:

- indicate the intention to use EAP by not including the AUTH payload;

- include the IDi payload with the ID type set to ID\_KEY\_ID and value set to any random number; and

- include CERTREQ payload to request N3IWF's certificate if the UE is provisioned with the N3IWF root certificate,

as specified in IETF RFC 7296 [6].

Upon reception of the IKE\_AUTH request message, the N3IWF shall respond with an IKE\_AUTH response message including:

- an EAP-Request/5G-Start packet to inform the UE an EAP-5G session that will be used to convey the initial NAS messages (see the EAP-5G procedure described in subclause 7.3.3);

- the IDr payload with the value set to N3IWF identity; and

- the CERT payload containing the N3IWF's certificate if the CERTREQ payload is included in the IKE\_AUTH request message.

\* \* \* 3rd Change \* \* \* \*

#### 7.3.2.2 IKE SA and signalling IPsec SA establishment accepted by the network

If IKE SA and signalling IPsec SA establishment is accepted by the network, the UE receives from the N3IWF an IKE\_AUTH response message containing an EAP-Success message (as shown in figure 7.3.2-1), which completes the EAP-5G session. No further EAP-5G packets are exchanged.

The UE completes the IKE SA and signalling IPsec SA (first child SA) establishment procedure by initiating an IKE\_AUTH exchange including an AUTH payload computed based on the N3IWF key as described in 3GPP TS 33.501 [5]. In the IKE\_AUTH request message the UE additionally shall include:

- the INTERNAL\_IP4\_ADDRESS attribute, the INTERNAL\_IP6\_ADDRESS attribute, or both, indicating the type of IP address to be used for the IP tunnels, in the CFG\_REQUEST configuration payload. The INTERNAL\_IP4\_ADDRESS attribute shall contain no value and the length field shall be set to 0. The INTERNAL\_IP6\_ADDRESS attribute shall contain no value and the length field shall be set to 0; and

- the MOBIKE\_SUPPORTED notify payload as specified in IETF RFC 4555 [23] if the UE supports IETF RFC 4555 [23].

The N3IWF shall include in the IKE\_AUTH response message containing the AUTH payload:

- a single CFG\_REPLY Configuration Payload including the INTERNAL\_IP4\_ADDRESS attribute with an IPv4 address assigned to the UE, the INTERNAL\_IP6\_ADDRESS attribute with an IPv6 address assigned to the UE, or both;

- the NAS\_IP4\_ADDRESS notify payload with an N3IWF IPv4 address assigned to transport of NAS messages, if the initial IKE\_AUTH request message contained a CFG\_REQUEST configuration payload with the INTERNAL\_IP4\_ADDRESS attribute and NAS messages are to be transmitted using IPv4 based inner IP tunnel;

- the NAS\_IP6\_ADDRESS notify payload with an N3IWF IPv6 address assigned to transport of NAS messages if the initial IKE\_AUTH request message contained a CFG\_REQUEST configuration payload with the INTERNAL\_IP6\_ADDRESS attribute and NAS messages are to be transmitted using IPv6 based inner IP tunnel;

- the NAS\_TCP\_PORT notify payload with an N3IWF TCP port number assigned to transport of NAS messages; and

- the MOBIKE\_SUPPORTED notify payload as specified in IETF RFC 4555 [23], if the initial IKE\_AUTH request message contained a MOBIKE\_SUPPORTED configuration payload with the INTERNAL\_IP4\_ADDRESS attribute.

The UE may support the TIMEOUT\_PERIOD\_FOR\_LIVENESS\_CHECK attribute as specified in 3GPP TS 24.302 [7] subclause 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.

The N3IWF may include the TIMEOUT\_PERIOD\_FOR\_LIVENESS\_CHECK attribute as specified in 3GPP TS 24.302 [7] subclause 8.2.4.2 indicating the timeout period for liveness check in the CFG\_REPLY configuration payload of the IKE\_AUTH response message containing the AUTH payload. Presence of the TIMEOUT\_PERIOD\_FOR\_LIVENESS\_CHECK attribute in the IKE\_AUTH request can be used as input for decision on whether to include the TIMEOUT\_PERIOD\_FOR\_LIVENESS\_CHECK attribute in the IKE\_AUTH response message containing the AUTH payload.

If the TIMEOUT\_PERIOD\_FOR\_LIVENESS\_CHECK attribute as specified in 3GPP TS 24.302 [7] subclause 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 containing the AUTH payload or the UE has a pre-configured or configured timeout period, the UE shall perform the liveness check procedure as described in subclause 7.8.

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

This completes the establishment of the IKE SA and signalling IPsec SA (first child SA) between the UE and the N3IWF. Upon completion of the IKE SA and signalling IPsec SA (first child SA) establishment between the UE and the N3IWF, the UE and the N3IWF shall send further NAS messages over the TCP connection within the signalling IPsec SA (first child SA) (see example in figure 7.3.2.2-1).

An example of an IKE SA and first child SA establishment procedure is shown in figure 7.3.2.2-1.



Figure 7.3.2.2-1: IKE SA and first child SA establishment procedure for UE registration over untrusted non-3GPP access

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