**3GPP TSG-SA3 Meeting #99e *S3-201293***

**E-meeting, 11- 15 May 2020** Revision of S3-20xxxx

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0844** | **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 | **X** | Radio Access Network | **X** | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | F1 interface security set-up procedure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung, Nokia, Nokia Shanghai Bell, ZTE, T-Mobile, Mavenir, CableLabs, Lenovo, Motorola Mobility, Thales | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | IAB | | | | |  | ***Date:*** | | | 20 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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:*** | | Introduce the F1 interface security set-up procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Details of F1 interface security set-up procedure are proposed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Security aspects of IAB are not supported in 5GS. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 9.8.2, M.3.3.1 (new), M.3.3.2 (new), M.3.3.3 (new), Annex A.y (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

**\*\*\*\* START OF CHANGES \*\*\*\***

9.8.2 Security mechanisms for the F1 interface

The F1 interface connects the gNB-CU to the gNB-DU. It consists of the F1-C for control plane and the F1-U for the user plane. The security mechanisms for the F1 interface connecting the IAB-node to the IAB-donor-CU are detailed in clause M.3.3 of this document.

In order to protect the traffic on the F1-U interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

In order to protect the traffic on the F1-C interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

IPsec is mandatory to implement on the gNB-DU and on the gNB-CU. On the gNB-CU side, a SEG may be used to terminate the IPsec tunnel.

In addition to IPsec, for the F1-C interface, DTLS shall be supported as specified in RFC 6083 [58] to provide integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the provisions given in clause 6.2 of TS 33.210 [3].

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect F1 is an operator's decision. In case the gNB or the IAB-node has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB or the IAB-node.

NOTE 3: The security considerations for DTLS over SCTP are documented in RFC 6083 [58].

NOTE 4: The support of DTLS for F1-C, between the IAB-node (gNB-DU) and the IAB-donor-CU, is optional for the IAB-node and the IAB-donor-CU.

**\*\*\*\* NEXT CHANGE \*\*\*\***

## M.3.3 Security mechanisms for F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU (Phase-3)

### M.3.3.1 General

The following clause applies to F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU.

### M.3.3.2 Security mechanisms for the F1 interface

The F1 interface connects the IAB-node (gNB-DU) to the IAB-donor-CU. It consists of the F1-C for control plane and the F1-U for the user plane.

F1 security for IAB is established using the security mechanisms for the F1 interface as specified in clause 9.8.2 of the present document, with IAB node taking the role of gNB-DU and IAB-donor-CU taking the role of gNB-CU.

In addition to the security mechanisms specified in clause 9.8.2 of the present document for the F1 interface, the IKEv2 Pre-shared Secret Key (PSK) authentication shall be supported. When IKEv2 performs a PSK authentication, in the IKE\_AUTH request message, the IAB node shall set the ID type to ID\_KEY-ID and set its value to PSK ID.

NOTE x: The PSK and PSK ID (for IKEv2 PSK authentication) are preconfigured at the IAB node and IAB donor. Pre-configuration of the PSK(s) is out of the scope of the present document.

Additionally, to support a flexible plug and play of IAB-node and IAB-donor without a pre-configuration of the PSK(s), dynamic PSK computation for IKEv2 PSK authentication may also be supported. When dynamic PSK is used, the IAB-node and the IAB-donor shall calculate the PSK (KIAB) as specified in the Annex A.y of this document. The IAB-donor shall uniquely identify the IAB-node’s security context (KgNB) using the IAB-node DU IP address. The IAB-donor shall use KIAB as PSK for IKEv2 between IAB-node and the IAB-donor. KIAB is stored in the IAB-node and in the IAB-donor. This key KIAB and the IPsec SA cryptographic keys are taken into use with the establishment of IPsec Security Association (SA) between the IAB-node and the IAB-donor. KIAB remains valid as long as the IAB-node is connected to the IAB-donor or until the IAB-node is re-authenticated.

NOTE z: KIAB is used as the PSK for IKEv2 authentication, the interface between the IAB-donor-CU and the SEG to provision the key KIAB in the SEG is implementation specific and out of the scope of the present document.

**\*\*\*\* NEXT CHANGE \*\*\*\***

A.y KIAB generation function

This input string is used when the IAB-node and the IAB-donor derive KIAB (PSK) for establishment of secure F1 interface. The following parameters shall be used to form the input S to the KDF:

- FC = 0xaa,

- P0 = IAB-donor-CU IP address

- L0 = length of IAB-donor-CU IP address

- P1 = IAB-node DU IP address

- L1 = length of IAB-node DU IP address

The input key KEY shall be KgNB or S-KgNB. The key KgNB or S-KgNB is in possession of the IAB-UE functionality in the IAB-node and in the IAB-donor-CU, after the IAB-UE setup procedure (Phase-1) or after dual connectivity procedure.

The entire output of the KDF (256 bits) is used as the KIAB.

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