**3GPP TSG SA WG3 (Security) Meeting #98e S3-200093-r2**

**e-Meeting, 2 – 6 March 2020** *revision of S3-20xyzw*

|  |
| --- |
| *CR-Form-v12.0* |
| **DRAFT CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **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:***  | [Draft CR] F1 interface set-up procedure |
|  |  |
| ***Source to WG:*** | Samsung, Thales, Nokia, Nokia Shanghai Bell, ZTE |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  NR\_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 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)* |
|  |  |
| ***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:*** | X.2.3.1 (new), X.2.3.2 (new), X.2.3.3 (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:*** | To be implemented on top of baseline draft CR (S3-193808) |
|  |  |
| ***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 X.2.2 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 has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB.

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

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

X.2.2 Security mechanisms for F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU

X.2.3.1 General

The following clause applies to F1 interface between the IAB-node and the IAB-donor.

X.2.3.2 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.

In order to protect the traffic on the F1-U and 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.

In order to protect the traffic on the F1-U and F1-C interface, IPsec ESP and IKEv2 Pre-shared Secret Key (PSK) authentication method shall be supported with confidentiality, integrity and replay protection. IKEv2 Pre-shared Secret Key (PSK) authentication implementation shall be done according to TS 33.310 [5]. The IAB-node and the IAB-donor shall calculates 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 the key MSK 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.

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

NOTE z: If KIAB is used as the PSK for IKEv2 authentication, then 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.

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

NOTE y: If pre-configured PSK and PSK ID is used for IKEv2 authentication (instead of deriving KIAB from KgNB), then the configuration of the PSK(s) at the IAB node and IAB donor for this scenario is out of the scope of the present document.

X.2.3.3 IAB-node migration procedure

Editor's note: Topology adaptation, where the IAB-node migrates from its source parent node to a target parent node is under consideration in RAN WGs. Security aspects of this procedure will be included when RAN WGs have made further progress.

**\*\*\*\* 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. The key 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).

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

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