**3GPP TSG-SA3 Meeting #101-e *S3-203253***

**e-meeting, 9th - 20th November 2020**

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

|  |
| --- |
|  |
| ***Title:***  | Support for mutual authentication between network entities |
|  |  |
| ***Source to WG:*** | , Verizon, Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 1 |
|  |  |  |  |  |
| ***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:*** | As per TLS RFC, server side of the channel is always authenticated and the client side is optionally authenticated. However, when (D)TLS is used in 5GS for protection of 3GPP defined interfaces, mutual authentication between the entities is required. Only for some interfaces, support for mutual authentication is not mentioned, whereas for other interfaces (particularly for SBI) the support for mutual authentication is explicitly mentioned. This ambiguity needs to be clarified. Therefore, it is clarified that mutual authentication is supported between the entities when using IKEv2 and/or DTLS over N2, Xn, F1 and E1 interfaces. |
|  |  |
| ***Summary of change:*** | Support for mutual authentication is specified when using IKEv2 and/or DTLS. |
|  |  |
| ***Consequences if not approved:*** | Implementation may not support mutual authentication when establishing DTLS and/or IPsec, which leads to disclosure of sensive informations with an unauthenicated entity. |
|  |  |
| ***Clauses affected:*** | 9.2, 9.4, 9.8.2, 9.8.3 |
|  |  |
|  | **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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

9.2 Security mechanisms for the N2 interface

N2 is the reference point between the AMF and the 5G-AN. It is used, among other things, to carry NAS signalling traffic between the UE and the AMF over 3GPP and non-3GPP accesses.

The transport of control plane data over N2 shall be integrity, confidentiality and replay-protected.

In order to protect the N2 reference point, it is required to implement IPsec ESP and IKEv2 certificates-based authentication as specified in sub-clause 9.1.2 of the present document. IPsec is mandatory to implement on the gNB and the ng-eNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

In addition to IPsec, 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].

Mutual authentication shall be supported over the N2 interface between the AMF and the 5G-AN using DTLS and/or IKEv2.

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 N2 is an operator's decision. In case the NG-RAN node (gNB or ng-eNB) has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the NG-RAN node.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*Next Changes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 9.4 Security mechanisms for the Xn interface

Xn is the interface connecting NG-RAN nodes. It consists of Xn-C and Xn-U. Xn-C is used to carry signalling and Xn-U user plane data.

The transport of control plane data and user data over Xn shall be integrity, confidentiality and replay-protected.

In order to protect the traffic on the Xn reference point, it is required to implement IPsec ESP and IKEv2 certificate- based authentication as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection. IPsec shall be supported on the gNB and ng-eNB.

In addition to IPsec, for the Xn-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].

Mutual authentication shall be supported over the Xn interface between the NG-RAN nodes using DTLS and/or IKEv2.

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 Xn is an operator's decision. In case the NG-RAN node (gNB or ng-eNB) has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the NG-RAN node.

QoS related aspects are further described in sub-clause 9.1.3 of the present document.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*Next 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].

Mutual authentication shall be supported over the F1-C interface between the gNB-CU and the gNB-DU using DTLS and/or IKEv2.

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 (with mutual authentication) 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\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

9.8.3 Security mechanisms for the E1 interface

The E1 interface connects the gNB-CU-CP to the gNB-CU-UP. It is only used for the transport of signalling data.

In order to protect the traffic on the E1 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 addition to IPsec, 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].

Mutual authentication shall be supported over the E1interface between the gNB-CU-CP and the gNB-CU-UP using DTLS and/or IKEv2.

IPsec is mandatory to support on the gNB-CU-UP and the gNB-CU-CP. Observe that on both the gNB-CU-CP and the gNB-CU-UP sides, a SEG may be used to terminate the IPsec tunnel.

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 E1 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.

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