**3GPP TSG-SA3 Meeting #108e *draft\_S3-221789-r2***

**e-meeting, 22 - 26 August 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **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 |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | User plane security for Non-SBA based interfaces | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2022-08-22 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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 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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | GSMA DESS has sent a LS (S3-221721) to SA3 indicating an inconsistency found in the TS 33.210 and TS 33.501 specifications with regards to user plane security. In current TS 33.501 section 9.9 specifies that NDS/IP shall apply to non-SBA inter-PLMN interfaces (including N9 user plane), whereas TS 33.210 clearly states in 4.3 and B.1 that NDS/IP does not extend to the user plane.  Instead of changing the scope of NDS/IP in TS 33.210, which may impact other specifications with references to it, this CR proposes to rather update the 5G specification TS 33.501 on this specific aspect. The same approach has been followed as for N3, which is a good example of specifying the security mechanisms for a non-SBA user plane interface.  Basically the change consists of removing the reference of NDS/IP in the clauses 9.9 and N.2.2 of TS 33.501, specifying instead explicitly the security mechanisms to protect N9 interface, i.e., mutually authenticated IPsec tunnel, or other protection, e.g., physical protection. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Eliminate the reference of NDS/IP in the clauses 9.9 and N.2.2 of TS 33.501, specifying instead explicitly the security mechanisms to protect non-SBA interfaces internal to the 5GC and between PLMNs, i.e., mutually authenticated IPsec tunnel, or other protection, e.g., physical protection. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | It remains the inconsistency pointed out by GSMA DESS | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 9.9 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \* \* \* \*

## 9.9 Security mechanisms for non-SBA interfaces internal to the 5GC and between PLMNs

Non-SBA interfaces internal to the 5G Core such as N4 and N9 can be used to transport signalling data as well as privacy sensitive material, such as user and subscription data, or other parameters, such as security keys. Therefore, these interfaces shall be confidentiality, integrity, and replay protected.

Roaming interfaces between PLMNs except for N32, shall be confidentiality, integrity, and replay protected. Protection for the N32 interface is specified in clauses 13.1 and 13.2.

For the protection of the above mentioned internal and roaming user plane interfaces, it is required to implement IPsec ESP and IKEv2 certificate-based authentication as specified in sub-clauses 9.1.2 and 9.1.3 of the present document with confidentiality, integrity and replay protection, unless security is provided by other means, e.g. physical security. A SEG may be used to terminate the IPsec tunnels.

Editor’s Note: Whether the use of cryptographic solutions to protect non-SBA interfaces internal to the 5G Core such as N4 and N9, and roaming interfaces between PLMNs except for N32, is an operator’s decision, is FFS.

\* \* \* End of First Change \* \* \* \*

\* \* \* Second Change \* \* \* \*

## N.2.2 Redundant transmission on N3/N9 interfaces

If the user data redundancy is fulfilled by means of two duplicated N3 tunnels, the redundant packets will be transferred between UPF and RAN via two independent N3 tunnels, which are associated with a single PDU Session, over different transport layer path to enhance the reliability of service.



Figure N.2.2-1: Redundant transmission with two N3 tunnels between the UPF and a single NG-RAN node

In order to protect the redundant traffic on the N3 reference point, the current mechanism defined in clause 9.3 of the present document shall be reused. The added path for redundancy shall provide equal level of security compared to single path.

In case two N9 tunnels are involved to fulfil the redundancy for one NG-RAN, the security mechanism defined in clause 9.9 shall be used for protecting the redundant data transferring via two N9 tunnels as described above.

\* \* \* End of Second Change \* \* \* \*