**3GPP TSG-SA3 Meeting #103-e *draft\_S3-211543-r1***

**e-meeting, 17 -28 May 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | draftCR | **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 changeaffects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | IPUPS can be deployed in UPF(s). Its related assets and threats need to be added to the TR 33.926. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Assets and threats related to IPUPS are added.  A reference to TS 23.501(Release-16) is added.  The “(normative)” of the title Annex L is removed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incomplete specification | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | Annex L,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:*** | |  | | | | | | | | |

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*start of change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

Annex L:   
Aspects specific to the network product class UPF

L.1 Network product class description for the UPF

L.1.1 Introduction

This Annex covers the aspects specific to the UPF network product class.

Note: Operators can deploy UPF(s) supporting the Inter PLMN User Plane Security (IPUPS) functionality at the border of their networkas specified in TS 23.501[Z] clause 5.8.2.14.

L.1.2 Minimum set of functions defining the UPFnetwork product class

As part of the UPF network product, it is expected that the UPF contains UPF application, a set of running processes (typically more than one) executing the software package for the UPF functions and OAM functions that are specific to the UPF network product model. Functionalities specific to the UPF network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.513 [18].

Note:For the purposes of the present Annex, this common set is defined to be the list offunctions contained in clause 6.2.3 in 3GPP TS 23.501 [8].

L.2 Assets and threats specific to the UPF

L.2.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to theUPF to be protected are:

- UPF Application;

- User plane data;

- Session related data, e.g. CN Tunnel information, packet detection rules, network usage, traffic detection information, and etc.;

- Security data, i.e. cryptographic materials for N3, N4 and N9 interfaces

- The interfaces of the UPF to be protected and which are within SECAM scope:

- N3 interface between the UPF and the gNB/ng-eNB

- N4 interface between the UPF and the SMF

- N6 interface between the UPF and the DN

- N9 interface between two UPFs

- Console interface, for local access: local interface on the UPF

- OAM interface, for remote access: interface between the UPF and the OAM system

NOTE 1: The detailed interfaces of the UPF class are described in clause 4 of the present document.

- UPF Software: binary code or executable code

NOTE 2: UPF files may be any file owned by a user (root user as well as non-root users), including user account data andcredentials, log data, configuration data, OS files, UPF application, user plane security mechanism, or cryptographic materials.

L.2.2 Threats related to user plane data transport

***-*** *Threat name:*  No protection or weak protection for user plane data.

***-*** *Threat Category:* Tampering,Information Disclosure.

***-*** *Threat Description:* User traffic is transported between the gNB/ng-eNB and the UPF via N3 interface, or between two UPFs within a PLMN via N9 interface. If the user traffic transported over the interfaces is not confidentiality protected, it can be subject to eavesdropping. Information is leaked to unauthorized parties. If the user traffic is not integrity protected, attackers can tamper with user traffic at will. The receiver of the user traffic obtain false user traffic. If the user traffic is not replay protected, attackers can insert historical legitimate user traffic. This can lead to false network usage reported by the UPF, and consequently resulting in billing fraudulence.

If the protection implemented for the user plane data transported over the N3 interface and the N9 interface within a PLMN uses the wrong security profile, which may contain weak security algorithms or protocol versions known to be vulnerable, the level of the security of the user plane data may be degraded and fail to fulfil the required security.

***-*** *Threatened Asset:* User plane data.

L.2.3 Threats related to signalling data

***-*** *Threat name:*  No protection or weak protection for signalling data over N4 interface

***-*** *Threat Category:* Denial of service, tampering.

***-*** *Threat Description:* SMF controls the user plane path of PDU sessions through N4 interfaces. If the signalling data over N4 interface is not protected e.g. against tampering, the user traffic may be wrongly routed and fail to arrive at the intended recipient. This can create Denial of Service.

To support billing, UPF reports network usage to SMF over N4 interface. Unprotected network usage report can lead to billing fraud.

If the protection implemented for the signalling data over the N4 interface uses the wrong security profile, which may contain weak security algorithms or protocol versions known to be vulnerable, the security level of the signalling data transported over N4 interface may be degraded and fail to fulfil the required security.

***-*** *Threatened Asset:* session related data.

L.2.4 Threats related to TEID

***-*** *Threat name:* Failure to assign unique TEID for a session.

***-*** *Threat Category:* Tampering.

***-*** *Threat Description:* TEID, as part of the CN Tunnel information, is used by the UPF and gNB/ng-eNB for user plane routing. The failure to guarantee the uniqueness of the TEID for a PDU session interrupts the routing of user traffic. It also interrupts charging. If multiple PDU sessions were to share the same TEID at the same time, the counts for the network usage of a single PDU session will be in fact the counts for the network usage of multiple sessions, creating charging errors.

***-*** *Threatened Asset:* session related data.

## L.2.X Threats related to user plane data forwarding

***-*** *Threat name:*  invalid user plane data forwarding.

***-*** *Threat Category:*Tampering,Information Disclosure, Denial of Service.

***-*** *Threat Description:* User plane traffic is transported between UPFs over the N9 interface. If the UPF with IPUPS functionality fails to discard GTP-U packets that do not belong to any active PDU sessions, routing of user plane traffic could be interrupted or Denial of Service attacks to the network could be possible.This threat only applies if the UPF implements the IPUPS functionality.

***-*** *Threatened Asset:* User plane data.

## L.2.Y Threats related to malformed GTP-U messages

- Threat name: Threats of malformed GTP-U messages.

- Threat Category: Denial of service.

- Threat Description: Malicious sender may send malformed GTP-U messages to a victim UPF with IPUPUS functionality. If the malformed GTP-U messages are not filtered, they may consume the processing resource of the victim UPF with IPUPS functionality, and even cause the victim UPFfunctionality to crash, causing denial of service attack.

- Threatened Asset: Sufficient Processing Capacity.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*next change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

# 2 References

[Z] 3GPP TS 23.501: "System Architecture for 5G System; Stage 2" (Release 16)

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*end of change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***