**3GPP TSG-SA3 Meeting #124 draft\_S3-253739-r2**

**Wuhan, China, 13 -17 October 2025 Revision of S3-253422**

**Source: China Telecom, CableLabs, ZTE**

**Title: TEID issue in N9 interface**

**Document for: Approval**

**Agenda item: 5.2.4**

**Spec: 3GPP TR 33.758**

**Version: 0.0.0**

**Work Item: FS\_PLMNNPN\_Ph2**

**Comments**

This contribution proposes KI on TEID issue in N9 interface for SID on security for PLMN hosting a NPN phase 2.

**Proposed Changes**

\* \* \* First Change \* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[x] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)".

[y] Yiming Zhang, et al. “Invade the Walled Garden: Evaluating GTP Security in Cellular Networks”, IEEE Symposium on Security and Privacy (SP), May 2025.

\* \* \* Next Change \* \* \* \*

## 7.X Key Issue #X: TEID issue in N9 interface

### 7.X.1 Key issue details

A UPF can be deployed in the PNI-NPN operational domain and connects to a UPF deployed in the PLMN operational domain via N9 interface. Attackers in PNI-NPN operational domain (e.g., a misbehaving employee in PNI-NPN or an external attacker gaining unauthorized access to the PNI-NPN networks) can obtain the TEID from the UPF deployed in PNI-NPN operational domain.

For example, TS 29.281[x] clause 5.1 states:

*Tunnel Endpoint Identifier (TEID): This field unambiguously identifies a tunnel endpoint in the receiving GTP‑U protocol entity. The receiving end side of a GTP tunnel locally assigns the TEID value the transmitting side has to use. The TEID value shall be assigned* ***in a non-predictable manner****......*

UPFs can select the first TEID in a non-predictable manner (e.g., randomly) but allocate subsequent TEID numbers sequentially.

Furthermore, TS 29.281[x] clause 7.3.1 states:

*When a GTP-U node receives a G-PDU for which no EPS Bearer context, PDP context, PDU Session, MBMS Bearer context, or RAB exists, the GTP-U node shall discard the G-PDU. If the TEID of the incoming G-PDU is different from the value 'all zeros' the GTP-U node shall also return a GTP error indication to the originating node.*

As a TEID without an established context will trigger error codes in the response while a correct TEID will not, allowing an attacker to guess whether a TEID is used effectively.



Figure 7.x-1 Scenario involving N9 interface and having TEID issue

After an attacker in PNI-NPN operational domain1 obtain the TEID assigned by the PLMN UPF to UPF in PNI-NPN operational domain1, the attack can use this information to infer the TEIDs assigned by the PLMN UPF to UPF in PNI-NPN operational domain2, PLMN gNBs, SMF(through N4-u). The attack can further use the TEIDs to hijack subscriber traffic in other GTP tunnels, as described in the research paper "Invade the Walled Garden: Evaluating GTP Security in Cellular Networks"[Y]. More specifically, as illustrated in Figure 7.x-1, the attacker in PNI-NPN operational domain1 can perform the following attacks:

- Attack to other PNI-NPN: The attacker sends a GTP-U PDU message to UPF3 that contain TEID2 (corresponding to the legitimate UPF2→UPF3 GTP-U tunnel)—with the inner packet whose destination IP address is that of a UE which is allowed to access PNI-NPN operational domain2 from PLMN. Since the message matches the PDR corresponding to the legitimate UPF2→UPF3 GTP-U tunnel, UPF3 will forward the messages to the UE according to the related FAR. Similarly, the attacker can send a GTP-U PDU message to UPF3 that contain TEID3 with the inner packet whose source IP address is that of a UE which is allowed to access PNI-NPN operational domain2 from PLMN. UPF3 will forward the messages to UPF2 according to the related FAR. In this way, an attacker in PNI-NPN operational domain1 can send malicious messages to attack UEs which are allowed to access PNI-NPN operational domain2 from PLMN, and also target UPF2 and DN2.

- IP address fraud: The attacker sends a GTP-U PDU message to UPF3 that contain TEID4(corresponding to the legitimate SMF→UPF3 N4-U tunnel)—with the inner packet carrying spoofed IPv6 RA. UPF3 will forward the messages to the UE according to the related FAR. This can cause the UE to adopt the spoofed IPv6 address prefix, ultimately disrupting its connection with the 5GC.

- Bill inflation: The attacker sends a GTP-U PDU message to UPF3 that contain TEID2(corresponding to the legitimate UPF2→UPF3 GTP-U tunnel)—with the inner packet whose source IP address is that of a UE. In this way, the attacker can inflate the victim’s bill by (silently) sending large amounts of traffic.

### 7.X.2 Security threats

Attackers in one PNI-NPN operational domain can forge TEID and infer the TEIDs assigned to PLMN operational domains and other PNI-NPN operational domains and launch further attacks.

### 7.X.3 Potential security requirements

TBD.

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