**3GPP TSG-SA3 Meeting #123 draft-S3-252960-r1**

**Goteborg, Sweden, 25 – 28 August 2025** Revision of S3-252648

**Source: China Telecom, ZTE, China Unicom, China Mobile, CAICT**

**Title: New SID on security for PLMN hosting a NPN phase 2**

**Document for: Approval**

**Agenda Item: 6.1.5**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>   
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study on security for PLMN hosting a NPN phase 2

Acronym: FS\_PLMNNPN\_Ph2

Unique identifier:

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-20

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  |  | X |  |
| No | X | X | X |  |  |
| Don't know |  |  |  |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| X | Study |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | Normative – Other\* |

**\* Other = e.g. testing**

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |  |  |  |
| --- | --- | --- | --- |
| Parent Work / Study Items | | | |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
| 1020039 | Study on security for PLMN hosting a NPN | Antecedent study item |
| 1060067 | Security for PLMN hosting a NPN | Antecedent work item |

# 3 Justification

TR 33.757[1] has studied two scenarios of PLMN hosting a NPN, where the interface between PLMN operational domain and PNI-NPN domain is N4 or SBA interface. In TR 33.757[1], the CP functions deployed in the PNI-NPN operational domain only consider AMF and SMF. However, there are still other deployment use cases and security issues that need to be studied.

1. Protection of N9 interface

A PNI-NPN may deploy a UPF, which connects to an PLMN UPF 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) may use the N9 interface to attack PLMN networks. For example, an attacker from PNI-NPN may be able to use the GTP information (e.g., TEID) obtained from the UPF deployed in PNI-NPN to attack other N9 interfaces, e.g., to hijack subscriber traffic in other GTP tunnels, as described in the research paper "Invade the Walled Garden: Evaluating GTP Security in Cellular Networks".

1. Protection of dedicated CP functions other than AMF, SMF and UDM

In Release 19, the CP functions deployed in the PNI-NPN operational domain only consider AMF and SMF. However, more CP functions (e.g., NWDAF) are likely to be deployed in the PNI-NPN operational domain. It is necessary to study whether additional security measures are needed.

# 4 Objective

Based on the above justification, the following objectives will be studied:

1. Identify key issues and potential security requirements for the scenario of PLMN hosting a NPN where the interfaces between PLMN operational domain and PNI-NPN domain include N9. And develop solutions to address the identified security requirements.

NOTE: This SID will not discuss nor study proxies in the intersection between the PLMN operational domain and PNI-NPN operational domain as already covered in Release 19. Nor will the study cover aspects already specified or standardised in GSMA.

NOTE: It’s assumed that attacks happen from PNI-NPN to PLMN and PLMN to PNI-NPN.

1. Evaluate if security recommendations given in TS 33.501 annex AB apply to the scenario of PLMN hosting a NPN where more CP functions (except AMF, SMF, UDM) are deployed in PNI-NPN domain.

## TU estimates

Total TU estimates for the study phase: 2 TUs (4 meeting cycles)

Total TU estimates for the normative phase: 1 TUs (2 meeting cycles)

Total TU estimates: 3

# 5 Expected Output and Time scale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| New specifications {One line per specification. Create/delete lines as needed} | | | | | |
| Type | TS/TR number | Title | For info  at TSG# | For approval at TSG# | Rapporteur |
| Internal TR | 33.xyz | Study on security for PLMN hosting a NPN phase2 | TSG#111  (Mar 2026) | TSG#112  (Jun 2026) |  |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
|  |  |  |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

None

# 9 Supporting Individual Members

{At least 4 supporting Individual Members are needed. There is an expectation that these companies will provide resources to progress the work. Note that having 4 supporting companies is a necessary but not sufficient condition: the usual TSG approval process by consensus is needed for the WID approval}

|  |
| --- |
| Supporting IM name |
| China Telecom |
| ZTE |
| CableLabs |
| CATT |
| China Unicom |
| China Mobile |
| Samsung |
| Lenovo |
| CAICT |
|  |