**3GPP TSG-SA3 Meeting #116 *S3-242195-r5***

Jeju, South Korea, 20th - 24th May 2024

**Source: Nokia, Nokia Shanghai Bell**

**Title: Update of KI’s based on comments provided by SA3-LI**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***It is requested to approve the pCR***

# 2 References

# 3 Rationale

This pCR proposes to extend KI#1 and KI#3 to encompass the comments provided by SA3-LI in S3i240294.

# 4 Detailed proposal

**\*\*\*\*** START OF 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".

[2] 3GPP TS 22.261: "Service requirements for the 5G system;Stage 1".

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G system"

[4] 3GPP TS 23.502: "Procedures for the 5G System (5GS)"

[5] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane nodes"

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)"

[7] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)"

[8] 3GPP TS 23.273: " 5G System (5GS) Location Services (LCS); Stage 2"

[9] 3GPP TS 23.501: " System architecture for the 5G System (5GS); Stage 2"

[10] 3GPP TS 29.500: "Technical Realization of Service Based Architecture"

[11] 3GPP TS 33.126: " Lawful Interception requirements"

**\*\*\*\*** NEXT CHANGE **\*\*\*\***

# 6 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 6.1 Key Issue #1: Security for dedicated UPF interacting with PLMN through N4 interface

### 6.1.1 Key issue details

In the scenario where the dedicated UPFs are deployed in NPN customer premise, the compromised UPF might launch signaling attacks towards the SMF in PLMN 5GC network.

If the dedicated UPF is compromised, attackers may utilize compromised dedicated UPF to collect PLMN’s topology, send malformed messages or launch DoS attacks to PLMN etc.

For this scenario, NDS/IP shall be supported to ensure confidentiality, integrity and replay protection as described in clause 9.9 in TS 33.501[3].

However, existing NDS/IP cannot protect PLMN or NPN from attacks from a compromised dedicated UPF or SMF, such as DoS, malformed signaling messages, topology information exposure etc.

### 6.1.2 Security threats

If a dedicated UPF in customer premises, is compromised by an attacker, the following problems may occur:

- The attacker may collect topology information from the PLMN or NPN and use the information to direct further attacks at the PLMN or NPN.

- The attacker may send malformed signaling messages to NFs in operator premises or customer premises to degrade NFs’ ability to process normal signaling messages.

- The attacker may send messages to the NFs in the operator premises or customer premises with wrong NF types according to 3GPP specifications. For example, a comprised dedicated UPF may send messages to the SMF in the operator premises to discover vulnerabilities of the SMF.

- The attacker may launch DoS attacks to flood and disrupt the PLMN or NPN.

### 6.1.3 Potential security requirements

5GS shall support mutual topology information hiding of the PLMN and the NPN customer premises network.

5GS shall support the means to block malformed signaling messages sent from dedicated UPF in the customer premises and compromised SMF in the operator premises.

5GS shall support the means to block messages with wrong NF types sent from dedicated UPF in the customer premises or SMF in the operator premises according to 3GPP specifications.

Editor’s Note: Whether the 5GS should support mitigation of DoS by compromised NF are FFS.

5GS shall support the means to authenticate and authorize the dedicated NFs in the customer premises and operator premises.

The 5G system shall provide the capability for the LI functions in the SMF to communicate with the UPF.

Editor’s Note: The detail of the requirement for LI functions is FFS.

## 6.2 Key Issue #2: Dedicated NFs interacting with PLMN through SBA interface

### 6.2.1 Key issue details

When dedicated UPF and part of CP functions are deployed in the customer premises, the interface between the dedicated NFs in the customer premises and NFs in the operator premises is SBA interface.

If NFs are compromised, attackers may utilize compromised NFs to collect topology, send malformed messages or launch DoS attacks.

For this scenario, SBA security shall be supported to ensure confidentiality, integrity and replay protection as described in clause 13 in TS 33.501[3].

However, existing SBA security cannot protect PLMN nor NPN from attacks from a compromised NFs, such as DoS, malformed signaling messages, topology information exposure etc. via the intersection between the MNO and customer domain.

### 6.2.2 Security threats

If a NF is compromised by an attacker, the following problems may occur:

- The attacker may collect topology information of the PLMN or NPN and use the information to direct further attacks at the PLMN or NPN.

- The attacker may send malformed signaling messages to NFs to degrade NFs’ ability to process normal signaling messages.

- The attacker may send messages to the NFs in the opposite domain with wrong NF types according to 3GPP specifications.

- The attacker may launch DoS attacks to flood and disrupt the availability of NFs in the operator domain and vice versa.

- The attacker may initiate unauthorized service operations. Safeguarding access tokens from an attacker is challenging when it crosses the security/trust boundary between the operator premises and the customer premises.

- A compromised NF in the customer premises may request the NF(s) in a PLMN to consume a service that are not allowed in the customer premises, and vice versa.

### 6.2.3 Potential security requirements

5GS should support mutual topology information hiding of the PLMN and the customer premises network.

5GS should support the means to block malformed signaling messages sent from NFs in the customer premises or operator premises over trust boundary.

5GS should support the means to block messages with wrong NF types sent from NFs in the customer premises or operator premises over the trust boundary according to 3GPP specifications.

Editors Note: Whether the 5GS should support mitigation of DoS by compromised NF are FFS.

5GS should support the means to authenticate and authorize the NFs in the customer premises and operator premises over the trust boundary.

The 5G system shall support a mechanism for secure exchange of DNS queries/answers, when the dedicated NFs are in customer premises.

5GS should support the means to restrict access to services and information exchanged between customer and operator premises and vice versa.

## 6.3 Key issue #3: SUPI privacy issue in PLMN hosting NPN scenario

### 6.3.1 Key issue details

SA1 has captured the scenario for NPN security considerations in clause 8.2 of TS 22.261 [2], which is:

|  |
| --- |
| *The 5G system shall enable a PLMN to host an NPN without compromising the security of that PLMN.**NOTE: Dedicated network entities of NPN can be deployed in customer premises that are outside the control of the PLMN operator.* |

When NPN is hosted by a PLMN, there are two possible deployment scenarios as below:

 - For scenario 1, dedicated UPF is deployed in customer premises, with N4 interface (non-SBA interface) with the operator premises.

- For scenario 2, dedicated UPF and part of CP functions are deployed in customer premises with SBA interface with operator premises.

Considering the primary authentication and authorization procedure specified in the clause in TS 33.501 [3], if a Subscription Permanent Identifier (SUPI) is available in clear text to the NFs in customer premises then it may potentially lead to security threats, privacy breaches, UE location tracking and targeted attacks.

Further, with the evolution of the roaming architectures (Roaming Hub) and Core Network (NPN, Edge computing), distributed CN (multi-site CN), as there is no direct trust relationship between HN and SN/VPLMN/Edge network (i.e., between the different security domains), in this case HN need to consider exposing of permanent and/or sensitive identifiers/ parameter to the NFs in different security domain.

The privacy-sensitive SUPI is the home network operator-provided identifier used exclusively to identify its subscribers and related subscription information to handle the related services.

This key issue is to study how to avoid exposure of the sensitive parameters (specifically, permanent identifiers) to the entities outside the MNO premises (in other security domains).

Another aspect of privacy is the capability to support lawful interception, which applies for NPN, PLMN, and PNINPN networks. The solution addressing KI#3 needs the capability to comply with regional legislation and the related LI identification requirements defined in TS 33.126 [11] clause 6.2.

### 6.3.2 Security Threats

An attacker can compromise NFs in customer premises and can retrieve the SUPI to launch targeted attacks.

An NF can be compromised in customer premises, then a Subscription Permanent Identifier (SUPI) is available to the attacker, it can potentially lead to security threats, like privacy breaches, UE location tracking, mapping of the user to the identifiers, and targeted DoS.

### 6.3.3 Potential security requirements

The 5G system shall support a mechanism to ensure the protection of the sensitive parameters against the risk caused by PLMN hosting NPN and vice versa.

The 5G system shall provide the capability to comply with lawful interception requirements specified in TS 33.126 [11] clause 6.2.

**\*\*\*\*** END OF CHANGE **\*\*\*\***