**3GPP TSG-SA3 Meeting #109AdHoc-e *draft\_S3-230144-r1***

Electronic meeting, 16 - 20 January 2023 (revision of S3-yyxxxx)

**Source: Nokia, Nokia Shanghai Bell**

**Title: New SID on 5G security roaming issues**

**Document for: Approval**

**Agenda Item: 5.24**

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 N32 and SEPP hosted scenarios

Acronym: FS\_N32SEPP\_SEC

Unique identifier:

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

Potential target Release: *Rel-19*

# 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 …

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | *Work Task* |
| X | Study Item |

## 2.2 Parent Work Item

N/A

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
|  |  |  |  |
| FS\_eSBA\_SEC | SA3 | 900020 | Study on enhanced security aspects of the 5G Service Based Architecture (eSBA) |

### 2.3 Other related Work Items and dependencies

{List here other Work Items which relate to the proposed one, such as a Work Item in an earlier Release if further enhancing the feature from the previous Release)}

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
|  |  |   |

# 3 Justification

The SBA study TR 33.875 has been the home of two key issues related to N32 security related 5G roaming topics triggered by GSMA liaison statements. The SBA study was already extended to Rel-18 and other topics than those key issues will be finalized.

The two topics related to GSMA discussions are pending on the progress in GSMA and need further elaboration. Those key issues are therefore concluded in TR 33.875 to be further studied in a separate study.

The study will continue work on the following N32 security related 5G roaming topics:

* N32 security in mediated roaming scenarios (was key issue 10 in TR 33.875)

This topic is related to GSMA LS S3-213806.

The GSMA is working on best practice guidance and related specifications for how operators interact with both IPX and roaming hubs. However, the pre-5G architecture of these methods uses the 4G hop-by-hop security paradigm.

In 5G, SEPP communication for roaming relies on end-to-end security by design as specified in TS 33.501, i.e., messages are authenticated and integrity-protected between the SEPP of the visited network and the SEPP of the home network. This creates the need to study in more detail how the migration away from hop-by-hop security can be achieved without loss of the benefits provided by IPX providers and roaming hubs while the 5G security requirements on N32 are met.

* Security in hosted SEPP scenarios (was key issue 12 of TR 33.875)

This topic is related to GSMA LS S3-221737.

In some scenarios, the operator may decide to outsource the operation of its SEPP to an external entity. This scenario is called the “Hosted SEPP” scenario. The Hosted SEPP scenario introduces security requirements which must be fulfilled by N32 and by the connection between PLMN and Hosted SEPP.

The decision of an operator to outsource the operation of a SEPP to an external entity can be independent of whether and which IPX providers are used, and whether and which roaming hub(s) are used. In case an operator uses a Hosted SEPP, the security perimeter of the PLMN as described in TS 33.501, clause 4.2.1, extends to an entity external to the PLMN.

# 4 Objective

The study will focus on security for N32 and SEPP hosted scenarios for 5G roaming raised via liaisons with GSMA.

Identified topics are:

* N32 security in mediated roaming scenarios
* Security in hosted SEPP scenarios

*If further topics are identified, this study will be the home for those as well.*

# 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 |
| TR | 33.XXX | Study on security for N32 and SEPP hosted scenarios | TSG#101 | TSG#103 | Jerichow, AnjaNokiaanja.jerichow(at)nokia.com |
|  |  |  |  |  |  |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| TR 33.875 | Clean up of TR by removing the KIs of concern and related solutions (to be moved to the new study) | TSG#100 |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

Jerichow, Anja (Nokia): anja.jerichow@nokia.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

The result of this study can have impact to CT4 specifications.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Nokia |
| Nokia Shanghai Bell |
| Deutsche Telekom |
| Mavenir |
| Huawei |
| HiSilicon |
| Ericsson |
|  |
|  |
|  |