**3GPP TSG-SA3 Meeting #104-e *S3-212574r1***

**e-meeting, 16 - 27 August 2021** Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: update to KI#1 (NSSAI analysis)**

**Document for: Approval**

**Agenda Item: 5.21 FS\_eNS2\_SEC**

# 1 Decision/action requested

***Include the revision to the KI#1 in TR33.874***

# 2 References

[1]

# 3 Rationale

This contribution proposes an update to the key issue #1. Some analysis on broadcasting S-NSSAI is performed.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF CHANGE \*\*\*

## 5.1 Key Issue #1: privacy issue on broadcasting slice information

### 5.1.1 Key issue details

A gNB may support multiple and different network slices, and on different frequencies in different regions.

In TR 38.832 [6], in order to support fast cell selection and cell reselection for particular network slices, solutions based on broadcasting slice related information are being studied. The broadcast slice related cell info may contain e.g. NSSAI, SST, slice grouping or slice associated information. In this key issue, the following questions are to be addressed:

- Whether broadcasting slice related information in this scenarios will cause any privacy issue

- If yes, mitigation solutions need to be provided

Editor’s Note: as per current TR 33.832 [6], NSSAI is not contained in the broadcast SIB. Whether NSSAI is already excluded from the broadcast SIB or not is to be confirmed by RAN2.

### 5.1.2 Security threats

According to TS 23.501 [2], SST refers to the expected Network Slice behaviour in terms of features and services. An SST could be represented with a standardised SST value or without a standardised SST value. The currently standardized SST values can indicate the slice types of eMBB, URLCC, MIoT and V2X, from which sensitive information of a specific slice can hardly be derived. Hence there is no privacy issue if SST is included in the broadcast SIB.

An S-NSSAI is comprised of a SST and an optional Slice Differentiator (SD), which is to differentiate amongst multiple network slices of the same Slice/Service type. An S-NSSAI may contain privacy-sensitive information, e.g. when dedicated to a group of users may expose the group identity. An S-NSSAI may also contain sensitive information, e.g. network topology that the operator may not want to share with others.

A cell broadcasting sensitive S-NSSAI may become a target of attackers interested in the S-NSSAI information. It is likely for an attacker to further link the S-NSSAI with its UEs/users together with other knowledge/tools, e.g. a frequency band supports only the sensitive S-NSSAI or a few allowing attackers to narrow down the scope. Broadcasting sensitive S-NSSAI should be avoided.

Editor’s Note: In case the S-NSSAI supported by RAN node consists only of an SST field value (without SD field), the privacy implication of broadcasting SST is FFS.

Editor’s Note: the privacy issue of slice grouping and slice associated info is FFS depending on their definition to be made by RAN2.

Editor’s Note: It is FFS whether sensitive S-NSSAI can be broadcasted even if it is protected, as a protected S-NSSAI on its own is enough to link the users to that broadcast even if the actual name of the S-NSAAI is not known.

### 5.1.3 Potential security requirements

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