**3GPP TSG-SA3 Meeting #104e ad-hoc *S3-213362r4***

**e-meeting, 27 - 30 September 2021** Merger of S3-213362 and S3-213573

**Source: Huawei, HiSilicon, Xiaomi**

**Title: update to KI#1 with analysis on broadcasting S-NSSAI group info**

**Document for: Approval**

**Agenda Item: 5.9 FS\_eNS2\_SEC**

# 1 Decision/action requested

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

# 2 References

[1] TR 33.874

# 3 Rationale

This contribution proposes an update to the KI #1 in TR33.874 [1] with some analysis on broadcasting S-NSSAI group information.

# 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

### 5.1.2 Security threats

According to TS 23.501 [1], 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.

A slice group information may or may not ~~contain~~leak sensitive information depending on how the slice group is defined. For example, if a slice group is defined based on the standardized slice type or SST values, there may be no privacy issue ~~is expected~~ as discussed above. *S-NSSAIs with only SST values are valid slice identifiers.*On the other hand, there may be cases that a not well designed ~~if a~~ slice group contains only one SST (used in a S-NSSAI as a valid slice identifier), one S-NSSAI or a few S-NSSAI having the same SD values thus exposing network topologies or being dedicated to special groups of users. In such a case, broadcasting group info may ~~be equivalent to broadcasting S-NSSAI and~~ lead to leak of sensitive information.

According to RAN2, slice grouping information (slice group identity and group mapping info) is assumed to be delivered to UE through NAS signaling which is protected. The group identifier is broadcasted rather than Slice Group itself. The group identifier is defined to identify and protect the slice group.

Therefore, the slice group information for which the slice group identifier is to be broadcasted needs to be defined taking into consideration the leakage of sensitive information~~whether sensitive information is contained~~.

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

~~Sensitive S-NSSAI shall not be broadcasted.~~

~~S-NSSAI group info shall be defined properly without leaking sensitive information through broadcasting.~~

Slice group information needs to be defined taking into consideration the possible leakage of sensitive information due to *the group identifier* being broadcasted.

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