**3GPP TSG-SA3 Meeting #109Adhoc-e *S3-230231***

**Electronic meeting, 16 - 20 January 2023**

**Source: Ericsson, Nokia Shanghai Bell**

**Title: Conclusion for KI#1**

**Document for: Approval**

**Agenda Item: 5.16**

# 1 Decision/action requested

***It is proposed to add the proposed conclusions into the TR 33.858 [2].***

# 2 References

[1] 3GPP TR 23.700-08 Study on enhanced support of Non-Public Networks phase 2

[2] 3GPP TR 33.858 Study on security aspects of enhanced support of Non-Public Networks phase 2

# 3 Rationale

TR 23.700-08 [1] has concluded in clause 8.2 that N3GPP access to SNPN includes the following types of access:

* Untrusted/Trusted N3GPP access including support for onboarding
* NSWO access to SNPN using SNPN credentials

In the current version of the TR 33.858 [2] there are solutions for untrusted and trusted N3GPP access as well as N5CW devices and NSWO. It is thus possible to conclude parts of the KI#1 " Security of non-3GPP access for SNPN".

This document provides a comparison of existing solutions and propose conclusions for the above-mentioned use cases.

# 4 Detailed proposal

\*\*\*BEGIN CHANGES\*\*\*

# 7 Conclusions

## 7.X Conclusions for KI#1 Security of non-3GPP access for SNPN

### 7.X.1 Scope

TR 23.700-08 [2] has concluded in clause 8.2 that N3GPP access to SNPN includes the following types of access:

* Untrusted/Trusted N3GPP access including support for onboarding
* NSWO access to SNPN using SIM or non-SIM based credentials

The case of N5CW devices has not been addressed by TR 23.700-08 [2], but there are solutions for this case proposed in this study.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 7.X.2 Conclusion for Untrusted N3GPP access to SNPN

Solution #1 is selected as basis for normative work for untrusted access to SNPN.

This means that the procedure specified in TS 33.501 [2] clause 7.2.1 will be reused for normative work with the following modifications:

- **Support for all key generating EAP-methods:** Extend the applicable authentication mechanism in step 7 to key-generating EAP authentication methods.

- **Support for onboarding**: Add possibility to send onboarding SUCI in step 5

- **Support for usage of anonymous SUCI**: Add possibility to send anonymous SUCI in step 5 (also affecting steps 6 and 7) if the construction of SUCI as described in clause 6.12 of TS 33.501 [2] cannot be used and if the employed EAP method supports privacy.

Editor's Note: It is FFS if the EAP verification result in step 8 needs to be made mandatory.

Editor’s Note: Further conclusions are FFS.

### 7.X.3 Conclusion for Trusted N3GPP access to SNPN

Solution #2 is selected as basis for normative work with regards to the aspects:

- Support for all key generating EAP-methods

- Support for onboarding

This implies that the procedure specified in TS 33.501 [2] section 7A.2.4 will be reused for normative work with the following modifications:

**- Support for usage of anonymous SUCI**:

- Add possibility to send anonymous SUCI in step 5 (affecting also following steps 5-8) if the construction of SUCI as described in clause 6.12 of TS 33.501 [2] cannot be used and if the employed EAP method supports privacy.

Editor's note: What solution to use to identify KTNGF in step 13 is FFS.

**- Support for all key generating EAP-methods**: Extension of applicable authentication mechanism in step 8 to key-generating EAP authentication methods.

**- Support for onboarding:** Add possibility to send onboarding SUCI in step 5

Editor’s Note: Further conclusions are FFS.

### 7.X.4 Conclusion for N5CW device access to SNPN

Solution #4 is selected as basis for normative work with regards to the aspects:

- Support for all key generating EAP-methods

- Support for usage of anonymous SUCI if the construction of SUCI as described in clause 6.12 of TS 33.501 [2] cannot be used and if the employed EAP method supports privacy.

- Support for SNPN Id (PLMN Id and NID) carried in NAI

Editor’s Note: Conclusions regarding the issue of key derivation for non-NAS capable devices shall be aligned with outcome of study in TR 33.887 and are FFS.

Editor’s Note: Further conclusions are FFS.

### 7.X.5 Conclusion for NSWO support in SNPN

Editor's Note: Conclusions for NSWO for SNPN are FFS.

\*\*\*END CHANGES\*\*\*