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

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

**Source: Ericsson, Nokia**

**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 SIM or non-SIM based 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 Solution comparisons and 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 Summary of solutions

The existing solutions are listed in the table below together with the use case they are covering.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Solution #** | **Untrusted N3GPP Access** | **Trusted N3GP Access** | **N5CW** | **NSWO** |
| Solution #1: Authentication mechanism for untrusted non-3GPP Access in SNPN scenarios | X |  |  |  |
| Solution #2: Authentication mechanism for trusted non-3GPP Access in SNPN scenarios |  | X |  |  |
| Solution #3: Use of anonymous SUCI in trusted non-3GPP access for SNPN |  | X |  |  |
| Solution #4: Authentication for devices that do not support 5GC NAS over WLAN access in SNPN scenarios |  |  | X |  |
| Solution #5: Anonymous authentication during connection establishment in trusted non-3GPP network access |  | X |  |  |
| Solution #6: Trusted non-3GPP Access for SNPN |  | X |  |  |
| Solution #7: Untrusted non-3GPP Access for SNPN | X |  |  |  |
| Solution #8: Reusing Existing N3GPP Security for SNPN | X | X | X | X |
| Solution #9: NSWO support in SNPN using any key-generating EAP-method |  |  |  | X |

### 7.X.3 Untrusted N3GPP access to SNPN

#### 7.X.3.1 Comparison of solutions

Solution #1 proposes to reuse existing procedures with added support of SNPN features:

- Support for all key generating EAP-methods

- Support for onboarding

- Support for usage of anonymous SUCI

Solution #7 only covers the aspect of

- Support for usage of anonymous SUCI

Solution #8 proposes to reuse existing procedures without modification.

For trusted N3GPP access, an issue has been identified with the identification of the key KTNGF in the case of using anonymous SUCI. For untrusted N3GPP access there is no similar problem since the same IPSec negotiation is used for the primary authentication and later steps of setting up the IPSec tunnel. Because of this, there is no need for a separate solution of identifying KN3IWF as proposed in Solution #7.

Solution #8 does not take anonymous SUCI into account at all since it is proposing to reuse existing mechanisms. It does not consider support for onboarding.

Solution #1 is the only solution that takes all the SNPN features into account.

#### 7.X.3.2 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)

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

### 7.X.4 Trusted N3GPP access to SNPN

#### 7.X.4.1 Comparison of solutions

Solution #2 proposes to reuse existing procedures with added support of SNPN features:

- Support for all key generating EAP-methods

- Support for onboarding

- Support for usage of anonymous SUCI

Solution #8 proposes to reuse existing procedures without modification, which implies that there would be no support for the features mentioned above.

Solution #3, #5 and #6 are all only covering the aspect of

- Support for usage of anonymous SUCI

The issue of anonymous SUCI is that in the current procedures for trusted N3GPP access in clause 7A.2.1 of TS 33.501 [1], step 13 states:

"the UE shall initiate an IKE\_AUTH exchange and shall include the same UE Id (i.e. SUCI or 5G-GUTI) as in the UE Id provided in step 5."

The purpose of the UE Id is to identify the key for the UE, KTNGF. But if the UE used anonymous SUCI in step 5 it is impossible to identify the KTNGF. The solutions have different proposal for solving the problem of identifying the KTNGF.

Solution#2 requires that the UE has support for generating a SUCI in step 13, although it uses the privacy provided by EAP during primary authentication.

Other solutions present different ways of creating an alternative identifier for the KTNGF:

- Solution#3 proposes to use the hash of the key as identifier

- Solution#5 proposes to use a temporary identifier created by TNGF and sent to UE

- Solution#6 proposes to use the IP address of the UE

Solution #3, #5 and #6 impact the implementation of the UE and TNGF in the sense that they need to use a new type of identifier for KTNGF. Solution #5 has impact also on the protocol since it requires that a new identifier is sent from TNGF to the UE in step 9b.

Solutions #3 and #6 have the least impact on the system. Both solutions have similar impact. However, Solution#6 has some uncertainties how the IP address is allocated for the UE. In step 12 of clause 7A.2.1 of 33.501 states:

” 12. The UE receives IP configuration from the TNAN, e.g. with DHCP.”

In the corresponding figures (Figure 4.12a.2.2-1 in TS 23.502 [7] and Figure 7A.2.1-1 in TS 33.501 [4]) both specifications show an arrow between the UE and TNAP which says “*Local IP configuration*”. Thus, it is the TNAP that allocates the UE’s IP address. Further, the requirements for the interface between TNAP and TNGF called Ta are defined in clause 4.2.8.3.2 of 23.501[6]. That clause states that the entity providing the local IP address is part of TNAN and out of scope of 3GPP.

Hence, depending on the deployment, it may or may not be the TNGF that allocates the IP address of the UE. It may also be some other part of the TNAN, especially the TNAP. Since Solution#6 relies on that the TNGF allocates the UE’s IP address, it means that Solution#6 does not seem to work in all deployments.

With the above uncertainties in mind, it is proposed to select Solution#3 or Solution#5 as basis for normative work with respect to the aspects of anonymous SUCI. For the aspects of onboarding and support all key generating EAP-methods, Solution #2 can be used.

#### 7.X.4.2 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)

Editor's note: What type of identifier to use for 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

### 7.X.5 N5CW device access to SNPN

#### 7.X.5.1 Comparison of solutions

Solution#8 proposes to reuse existing procedures in clause 7A of TS 33.501 [4] which includes N5CW access. However, existing procedures for N5CW are only defined to use EAP-AKA' whereas in SNPN it is possible to use all key-generating EAP-methods.

Solution#4 adds support for all key-generating EAP-methods.

Both solutions want to reuse existing procedures in clause 7A.2.4 of TS 33.501 [4]. It has been pointed out in another study that the procedures in clause 7A.2.4 of TS 33.501 [4] does not work since the non-NAS UE does not have NAS count and cannot derive the key KTWIF.

With the above in mind, only partial conclusions can be made for this use case.

#### 7.X.5.2 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

Editor’s Note: Conclusions regarding the issue of key derivation for non-NAS capable devices shall be aligned with other study items and are FFS.Editor’s Note: Further conclusions for the N5CW device access to SNPN are FFS.

### 7.X.6 NSWO support in SNPN

#### 7.X.6.1 Comparison of solutions

Solution#8 proposes to reuse existing procedure for NSWO. However, existing procedures for NSWO are only defined to use EAP-AKA'.

It has been concluded in clause 8.2 of 3GPP TR 23.700-08 [2] that the NSWO procedure is to be extended to support UE authentication using SNPN credentials (applies both to SIM-based and non-SIM based credentials).

This means that support of all key-generating EAP-methods needs to be specified for NSWO. Solution #9 is the only solution adding this possibility of NSWO support in SNPN. It only takes the case of SNPN having AUSF and UDM (not using Credentials Holder).

#### 7.X.6.2 Conclusion for NSWO support in SNPN

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

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