**3GPP TSG-SA3 Meeting #108e-AdHoc *S3-222904***

**e-meeting, 10 - 14 October 2022**

**Source: Ericsson**

**Title: New solution for KI#1: Use of anonymous SUCI in trusted non-3GPP access for SNPN**

**Document for: Approval**

**Agenda Item: 5.16**

# 1 Decision/action requested

***It is proposed to approve the inclusion of a new solution to the TR 33.858.***

# 2 References

[1] 3GPP TR 33.858: " Study on security aspects of enhanced support of Non-Public Networks phase 2".

[2] [S3-222232](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_108e/Docs/S3-222232.zip)

[3] [S3-222233](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_108e/Docs/S3-222233.zip)

# 3 Rationale

In the last SA3 meeting, a problem was raised related to the use of anonymous SUCI in untrusted and trusted non-3gpp access in SNPNs [2], [3].

When introducing non-3gpp access in SNPN it is assumed that most security procedures can be reused. However, the use of anonymous SUCI is only applicable to SNPNs so there are not yet any procedures specified for this case in relation to non-3GPP access.

This document proposes a solution on how the existing procedures for trusted non-3GPP access can be modified to support anonymous SUCI.

# 4 Detailed proposal

It is proposed to approve the following solution*.*

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.700-08: "Study on enhanced support of Non-Public Networks; Phase 2".

[3] 3GPP TS 22.261: "Service requirements for the 5G system".

[XX] 3GPP TS 33.501: "Security architecture and procedures for 5G system"

[YY] IETF RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)

…

## \*\*\* NEXT CHANGE \*\*\*

## 5.Y Solution #Y: Use of anonymous SUCI in trusted non-3GPP access for SNPN

## 5.Y.1 Introduction

This solution solves Key issue #1 in the case of using anonymous SUCI in trusted non-3GPP access.

When introducing non-3GPP access in SNPN it is assumed that most security procedures can be reused. However, the use of anonymous SUCI is only applicable to SNPNs so there are not yet any procedures specified for this case in relation to non-3GPP access.

In the current procedures for trusted non-3GPP access in clause 7A.2.1 of TS 33.501 [XX], it is specified to use the SUCI/GUTI to map the user to the correct KTNGF in step 13. When using anonymous SUCI, this is not a good solution since an anonymous SUCI is not unique. Instead, another identifier is needed. This solution proposes to use a hash of the key KTNGF as identifier in case anonymous SUCI is used during the authentication towards the SNPN.

This solution defines adaptations of existing procedures needed to support the use of anonymous SUCI in trusted access for SNPN.

### 5.Y.2 Solution details

Procedures in clause 7A.2.1 of TS 33.501 [XX] are reused with the following exception:

-In step 13, if the construction of SUCI as described in clause 6.12 of TS 33.501 cannot be used, then a new type of identifier is used.i The new identifier is proposed to be a hash of the key KTNGF. (potentially using some additional input). It is proposed to send the new identifier using the IDi payload.

It is already specified in section 3.5 of RFC 7296 [YY] that the ID payload used for transport of IDi can be used to transfer a key identifier by setting the ID Type to ID\_KEY\_ID. Support of this ID Type is mandatory. The RFC does not specify how such a key identifier is generated. The proposal here is thus to use a hash of the key KTNGF potentially using some additional input to create a key identifier.

Editor's note: Use of anonymous SUCI in non-3GPP access is FFS

Editor's note: The complexity in the UE to manage two identifiers for the same non-3gpp access is FFS.

### 5.Y.3 System impact

This solution has impact on UE and TNGF.

### 5.Y.4 Evaluation

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