**3GPP TSG-SA3 Meeting #102Bis-e *S3-211004***

**e-meeting, 1 - 5 March 2021** Revision of S3-20xxxx

**Source: Ericsson**

**Title: Solution to KI#2 (Provisioning of credentials) using AKMA**

**Document for: Approval**

**Agenda Item: 2.12**

# 1 Decision/action requested

***It is proposed to add the following solution to the TR in [1]***

# 2 References

[1] 3GPP TR 33.857: "Study on enhanced security support for Non-Public Networks"

# 3 Rationale

This document proposes a new solution to key issue #2 (Provisioning of credentials) for SNPN credentials using AKMA to setup security between the UE and the PS.

# 4 Detailed proposal

\*\*\*\*\*\*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 TS 33.501: "Security architecture and procedures for 5G System"

[3] 3GPP TR 23.700-07: "Study on enhanced support of non-public networks (Release 17)"

[4] 3GPP TS 23.501: "System Architecture for the 5G System"

[5] IETF RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)"

[6] 3GPP TS 23.502: "Procedures for the 5G System (5GS)"

[XX] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)"

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

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

## 6.Y Solution #Y: Credential provisioning using AKMA

### 6.Y.1 Introduction

This solution addresses key issue #2 (Provisioning of credentials) for SNPN credentials. It is assumed that the credentials to be provisioned are certificates.

The core steps of this solution are:

- use solutions for KI#4 to retrieve initial access. The initial access must be authenticated using primary authentication resulting in a KAUSF in the onboarding network.

- use AKMA procedures to setup application layer security between the UE and the provisioning server (PS). Here, PS acts as AF using the AKMA terminology. The Ua\* protocol could for example be TLS with PSK authentication using the KAKMA as PSK.

- Let the UE derive its own key pair and perform certificate enrolment with the PS. This means that the private key of the UE certificate never leaves the UE. Still security is needed between the UE and PS to ensure integrity of the communication. The actual enrolment procedures are out of scope of 3GPP.

In this case it is most likely that the external entity (DCS) is the manufacturer of the device. If the key resulting from the primary authentication between UE and DCS is used to protect the provisioning, the DCS will in the end have access to the SNPN credentials provisioned to the UE.

However, by using AKMA to setup a security relation between UE and PS, although the KAUSF (known to the DCS) is used, another key is established over the Ua\* protocol (TLS in this case). The DCS would need to act as an active attacker to retrieve this key. Also, if we consider the case of the UE deriving its own key pair and doing certificate enrolment towards the PS, it means that the private key never leaves the UE and hence is not available to the external party anyway.

### 6.Y.2 Solution details



Figure 6.Y.2‑1 Procedures for certificate provisioning.

0. Prerequisite: The PS is provisioned with a list of Onboarding SUPIs for the devices owned by the SO-SNPN.

0. Prerequisite: Initial access using primary authentication has been performed resulting in KAUSF in the AUSF of the ON.

1. UE obtains limited connectivity to the Provisioning Server UP session is established between for the UE.

2. AKMA security is setup between the UE and the PS according to procedures in TS 33.535 [XX] using the KAUSF established during initial access as basis. The Ua\* protocol is proposed to be TLS with PSK authentication.

Note: Specification of Ua\* protocols are in scope of AKMA.

Note: How authentication of the UE can be achieved using AKMA is in scope of AKMA.

3. The UE generates it key pair and stores the private key. The UE never exposes the private key to entities outside the UE.

4. The UE performs certificate enrolment towards the PS using an existing enrolment protocol such as EST, ACME or CMPv2.

5. The UE de-registers from the ON.

Editor's note: How the UDM in SO-SNPN gets provisioning data is FFS.

### 6.Y.3 System impact

Editor’s Note: Each solution should clearly list which entities need new functionality and what functionality they need for the provided solution to work.

### 6.Y.4 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

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