**3GPP TSG-SA3 Meeting #116 *S3-242356***

Jeju, South Korea, 20th - 24th May 2024

**Source: Ericsson**

**Title: New solution for key issue #3**

**Document for: Approval**

**Agenda Item: 5.10**

# 1 Decision/action requested

***It is proposed to add the following solution to the TR 33.700-32.***

# 2 References

[1] 3GPP TR 33.700-32 "Study on security aspects of User Identities and Authentication"

# 3 Rationale

This document proposes a solution for key issue #3.

# 4 Detailed proposal

It is proposed to approve the following change to TR 33.700-32 [1].

\*\*\*START OF THE CHANGE\*\*\*

6.Y Solution #Y: Authentication of non-3GPP devices behind a UE or 5G-RG via Server control

6.Y.1 Introduction

This solution addresses the requirements identified in key issue #3 (Authentication and Authorization of one or more non-3GPP devices behind one gateway UE or 5G-RG). This solution is based on storing the device information in a server via a client program that runs in the UE/5G-RG.

6.Y.2 Solution details

Figure 6.Y.2-1 describes the solution architecture. The DIP server is responsible to authenticate the UE/5G-RG subscriber. It is the responsibility of the subscriber to ensure that the device descriptor corresponds to the correct device behind UE/5G-RG. The authentication of the device may happen via the application layer interworking, e.g., between the device and UE/RG locally or between the device and the DIP/AAA server. It is the responsibility of UE/5G-RG subscriber to ensure that the device descriptor is unique. The authentication of the device by the UE/5G-RG can be done locally or via an external AAA server.



Figure 6.Y.2-1: High-level architecture

Editor’s Note: Clarification on which parts of the solution is in scope is FFS.

Editor’s Note: Flow and steps of the procedure are FFS.

6.Y.3 Evaluation

TBD.

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