**3GPP TSG-SA3 Meeting #116 *S3-242500-r1***

Jeju, South Korea, 20th - 24th May 2024 (revision of S3-241960)

**Source: Huawei, HiSilicon**

**Title: User authentication and authorization**

**Document for: Approval**

**Agenda Item: 5.10**

# 1 Decision/action requested

***Approve the pCR to TR 33.700-32***

# 2 References

None

# 3 Rationale

This contribution proposes a solution to address the key issue #1 in TR 33.700-32.

# 4 Detailed proposal

pCR

\*\*\* Start of 1st CHANGE \*\*\*

## 6.Y Solution #Y: User authentication and authorization

### 6.Y.1 Introduction

This solution addresses the key issue #1.

The solution reuses the NSSAA procedure TS 33.501 [x1] and adapts it to authenticate and authorize a human user using the UE. It allows restriction to user through authorization outcome. By reusing the NSSAA procedure, the following architecture/service requirements (clause 4.2 in TS 23.700-32 [2]/clause 26a in TS 22.101 [x2]) can be satisfied as well:

* The 3GPP system shall support to allow a UE access to a slice based on successful User Identity authentication.
* The 3GPP system shall support to deny a UE access to a slice based on unsuccessful User Identity authentication.

Editor’s note: Whether the requirements apply is FFS

### 6.Y.1 Solution details

Assuming the human user with a user identifier (UID) is using a UE with a 3GPP subscription identified by the UE’s SUPI to access services via the 5GS. Before authentication of the UID, the Primary authentication for the UE needs to be performed. It is also assumed that the networks slice identified by S-NSSAI is supposed to provide the service for the UE and the user.

With reference to the figure 16.2-1 in TS 33.501, the user identity authentication and authorization procedure is described as follows:

1. UE sends a Registration Request.

NOTE: How the user triggers the UE to send the registration request is out of scope.

2. For an initial Registration Request, the AMF shall invoke Primary authentication as described in TS 33.501 [x1]. For a subsequent Registration Request, the Primary authentication may be skipped if the UE has already been authenticated and the AMF has valid security context.

3. The AMF shall determine whether user identifier authentication and authorization (UIAA) procedure is required, based on information stored locally or from UDM. If yes, the AMF triggers the UIAA procedure. The UIAA procedure can be adapted from NSSAA procedure as shown in 16.3 in TS 33.501 [x1] with modification as follows:

NOTE: the step “3-x” is corresponding to the step “x” in clause 16.3 in TS 33.501 [x1]

3-1: The AMF may trigger the start of the NIAA procedure.

Editor’s note: How the AMF knows to perform user authentication is ffs.

3-2: The AMF may request the EAP ID for EAP authentication.

3-3: The UE provides the EAP ID to the AMF. The EAP ID is included in the EAP message which is transparent to the AMF. The UE may provide UID to the AMF as well.

NOTE: UID may be the same or different from EAP ID. The UID format is out of scope of this solution.

3-4: The AMF sends the GPSI, EAP ID and the UID if available to the NSSAAF.

3-5: 5. The NSSAAF forwards the message to the AAA-S directly or through AAA-P if available.

3-6 to 3-11: EAP-messages are exchanged with the UE. One or more than one iterations of these steps may occur.

3-12. EAP authentication completes. The EAP-Success/Failure message is delivered to the NSSAAF/AAA-P along with GPSI and UID. The message may include any restriction information imposed to the UID, e.g. tiers of services/QoS, service duration etc.

3-13. The NSSAAF sends the UIAA result (Success/Failure), GPSI, UID to the AMF.

3-14. The AMF transmits the UIAA result to the UE.

3-15. Based on the UIAA result, the AMF initiates the UE Configuration Update procedure.

Editor’s note: Whether the AMF initiates UE configuration update should be aligned to SA2

### 6.y.3 Evaluation

\*\*\* End of 1st Change\*\*\*

\*\*\* Start of 2nd Change \*\*\*

# 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 23.700-32: "Study on User Identities and Authentication Architecture"

[x1] 3GPP TS 33.501: "Security architecture and procedures for 5G system"

[x2] 3GPP TS 22.101: "Service aspects; Service principles"

…

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

\*\*\* End of 2nd Change\*\*\*