**3GPP TSG-SA3 Meeting #101-Bis-e *S3-210182***

**e-meeting, 18th - 29th January 2021** Revision of S3-20xxxx

**Source: Intel**

**Title: Updates to solution 18: Removal EN related to identification of serving AMF**

**Document for: Approval**

**Agenda Item: 5.8**

1 Decision/action requested

***It is proposed to approve the updates to the solution in EDGE TR 33.839.***

2 References

*(Reference - in list form - should be made to previous related SA5/3GPP/etc. documents.)*

*(For changes against a draft TS/TR, a pseudo CR - a.k.a. pCR - will be provided using this Tdoc template. In this case, the number, name and version of the draft TS/TR used as base must be provided and the version must be the latest available version of the draft TS/TR.)*

<Examples of references, please delete when you have inserted your actual references:

[1] 3GPP TS 32.500 SON Concepts and Requirements

[2] 3GPP TS 99.999 This example has a very long name, because then we can see how thi References paragraph will handle paragraphs spanning more than one line.

[3] 3GPP TS 99.999 Title of the document

[4] S5-991234, CR 32.999 v10.1.1, Inverting architecture of SON

[5] [S5-100001](http://www.3gpp.com/ftp/TSG_SA/WG5_TM/TSGS5_69/Docs/S5-100001.zip), Agenda, 3GPP SA5#69 Comment>

3 Rationale

pCR Proposes to delete EN related serving AMF.

4 Detailed proposal

**\*\*\*\*START OF 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 23.558: "Architecture for enabling Edge Applications."

[3] 3GPP TR 23.748: "Study on enhancement of support for Edge Computing in the 5G Core network (5GC)".

[4] 3GPP TR 23.758: "Study on application architecture for enabling Edge Applications".

[5] 3GPP TS 23.502: "Procedure for the 5G System; Stage 2".

[6] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[7] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[8] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[9] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

[10] 3GPP TS 33.501: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[11] 3GPP TS 33.187: "Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements".

[12] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[13] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[14] 3GPP TS 23.501: "System Architecture for the 5G System".

[15] 3GPP TS 23.003: "Numbering, addressing and identification".

[16] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

[17] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

[18] IETF RFC 4279 "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[19] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[20] 3GPP TR33.867: "Study on user consent for 3GPP services".

[21] RFC 7858: "Specification for DNS over Transport Layer Security (TLS)".

[22] RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS".

[23] 3GPP TS 33.434: "Security aspects of Service Enabler Architecture Layer (SEAL) for verticals".

[24] IETF RFC 7616: "HTTP Digest Access Authentication".

[25] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

**\*\*\*\*NEXT CHANGES \*\*\***

6.18 Solution #18: Authentication and Authorization Framework for EDGE-4 interfaces using Primary authentication and proxy interface

6.18.1 Introduction

The solution addresses the following key issue:

• Key issue #2: Authentication and Authorization between EEC and ECS

This solution enables authentication and authorization (Proxy AA) with an ECS during registration after primary authentication successful completion. The solution is based on the KAMF generated during the primary authentication.

6.18.2 Solution details



**Figure 6.18.2-1: Authentication and Authorization with the Edge Data Network**

1. The UE performs normal primary authentication and registration to the network. The UE is MEC capable and may indicate this in the MEC capabilities to the AMF during the registration procedure.

2. The UE establishes a PDU Session for IP connectivity. If the UE is MEC capable, then the UE and the AMF derive a key KProxy for authentication with the ECS from the AMF key KAMF. AMF pushes the EEC ID and KProxy to the Proxy AA network function in one of the options. Proxy AA network function maintains a mapping of EEC ID and KProxy.

Note: In case of Option 2, Proxy AA can identify the serving AMF by identifying “Allocated AMF for the registered UE” field in the “UE context in AMF data” as per TS 23.502[5] 5.2.3.3.1.

Editor’s Note: It is ffs on how proxy AA gets UE context.

Editor’s Note: Whether the Kamf can be used to derive the Kecs in case ECS is deployed by the home network is FFS.

Editor's note: It is ffs how this solution works if the EEC ID is not unique across different UEs.

Editor's note: It is ffs how the AMF knows the EEC ID

Editor’s Note: Describe the option as in the figure to solution procedure.

3. The UE sends an Application Registration Request with a MAC-IProxy to the ECS. The MAC-IProxy is computed similarly as, e.g., the SoR-MAC-IAUSF, as defined in Annex A.17 of TS 33.501. The MAC-IProxy is based on the Application Registration Request's payload, which forms the input Application Registration Request Data, and the key KProxy to the KDF..

4. a. The UE is not authenticated at the ECS, and the ECS sends a Verify Request including the Application Registration Request with the MAC-IProxy to the Proxy AA through NEF, which then either verifies by retrieving context it's own stored mapping(step 2 option 1) or it sends a key request to AMF by selecting serving AMF based on UE ID the serving AMF and forwards the message to this AMF.

4. b. The AMF replies with KProxy to Proxy AA, which then stores this in its database. Proxy AA verifies the MAC-IProxy of the Application Registration Request, i.e., it computes with the key KProxy the MAC-I over the Application Registration Request payload the UE and compares the result with the MAC-IProxy included in the message. If both are identical, the message can be authenticated to be sent by the UE.

4. c. Proxy AA Devices KECS from KProxy.

4.d. The Proxy AA sends a Key Response to the ECS, including the result of the authentication and the KECS.

5. Based on the authentication result, the ECS decides whether to accept or to reject the Application Registration Request from the UE. The ECS sends the Application Registration Response message to the UE, including the authentication result, and protects the message with a MAC-IECS based on the received key KECS in a similar way as the UE protected the payload of the message.

6. The UE derives KECS from KProxy and verifies the MAC-IECS. The rest of the procedure will proceed from step 10 of solution 6.7 in 33.839.

6.18.3 Solution Evaluation

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

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