**3GPP TSG-SA3 Meeting #100bis-e *S3-*** ***202508-r3***

**e-meeting, 12-16 October 2020**

**Source: CableLabs**

**Title: New solution for Key Issue #1**

**Document for: Approval**

**Agenda Item: 2.12**

# 1 Decision/action requested

***It is proposed to approve the proposed solution for TR 33.857.***

# 2 Rationale

This proposal addresses key issue #1 with the advantages of eliminating impact on UE side and minimize impact on core network components.

# 3 Detailed proposal

**\*\*\*\*START OF CHANGES \*\*\***

## 6.Y Solution #Y: EAP authentication between UE and external AAA via AUSF

### 6.Y.1 Introduction

This solution addresses the key issue #1 - Credentials owned by an external entity. It supports the use of any key generating EAP method to authenticate UE by an external entity consisting of a AAA server (AAA-E).

Particular considerations are given to maintain the same key hierarchy as other primary authentication (e.g., EAP-AKA’) when the credentials are owned by an internal entity (i.e., UDM). Such consideration allows to eliminate impact on UE side and minimize impact on core network components.

To maintain the key hierarchy on the UE side, this proposal requires AAA server to be able to derive KSEAF from EMSK according to TS 33.501.

### 6.Y.2 Solution details



1. The UE sends to the SEAF a Registration Request message, including the SUCI which is constructed from the UE SUPI. The SUPI is of the type of NAI in the form of username@realm. The “username” shall be either “anonymous” or omitted if the subscriber identifier privacy is required by SNPN and the public key of the SNPN is not provisioned in the UE.

2. The SEAF sends to the AUSF Nausf\_UEAuthentication\_Authenticate Request message, including the SUCI and the SN-name (the serving network name).

3. The AUSF sends to the UDM the the Nudm\_UEAuthentication\_Get Request, including the SUCI and the SN-name.

4. The UDM de-conceals the SUCI to obtain the SUPI. If the SUCI is not constructed using the null-scheme, the UDM invokes the SIDF located within the UDM to de-conceal the SUCI.

The the “username” portion of the SUPI could be a real username, “anonymous”, or null (i.e., omitted). In any case, the UDM uses the SUPI to determine that the credentials of this UE is owned by an external entity and return the information that is needed by the AUSF to use the AAA-E to authenticate the UE.

Editor Note. Since the EAP method itself may provide subscriber privacy, it is FFS whether such a SUCI calculation using non-null scheme is needed at the UE. If it is needed, the details on SUCI calculation is FFS

5. The UDM sends to the AUSF the Nudm\_UEAuthentication\_Get Response, which also includes the SUPI and any additional information that may assist AUSF to reach AAA-E.

6. The AUSF uses SUPI, any assistant information from the UDM, and/or local information to determine that an AAA server needs to be invoked to authenticate the UE.

The AUSF sends an authentication request to the AAA server. The exact message format of this authentication request depends on the interface overwhich the request is sent. It could be a service based interface if there is an interworking function to external AAA-E, or an AAA interface (e.g., RADIUS or DIAMETER) which may go through an AAA proxy (AAA-P).

Note that SUPI is needed to route the request to the ultimate destination AAA-E since there may be additional AAA proxies in front of the AAA-E. SN-Name is needed to derive KSEAF.

7. An intermediate entity (e.g., AAA-P) forwards the authentication request to the AAA-E.

8. The AAA-E and the UE performs an EAP authentication that is selected by the AAA-E.

9. Upon the successful completion of EAP authentication, the AAA-E dervises KSEAF from EMSK according to 33.501, sends an Access Accept messages to the AAA-P, including EAP Success, SUPI, and KSEAF.

Note that SUPI is needed since the SUPI received by AUSF in step 5 may be anonymous. KSEAF is derived by the AAA-E to maintain the same key hierarchy as the other primary authentication method (e.g., EAP-AKA’). Further, having AAA-E deriving KSEAF and send it the AUSF fully complies with RFC 5295.

10. The AAA-P forwards the Access Accept (or translates it to a service authentication response) to the AUSF, including EAP Success, SUPI, and KSEAF.

11. The AUSF sends to the SEAF an EAP-Success message along with the SUPI and the KSEAF in a Nausf\_UEAuthentication\_Authenticate Response message.

12. The SEAF forwards to the UE the EAP-Success message in an Authentication Result message or a Security Mode Command message.

Upon receiving the EAP-Success message, the UE derives the KAUSF and the KSEAF in the same way as the AUSF according to 3GPP TS 33.501.

By this point, the EAP authentication between the AAA-E and the UE has been successfully completed.

Editor’s Note: The architectural relationship between AUSF and \*-AAA including the derivation of keys is FFS. This includes the transfer of keys/messages in steps 6,7, 9 and 10.

### 6.Y.3 System impact

This solution has impact on UDM, AUSF, and AAA-E.

When UDM receives Nudm\_UEAuthentication\_Get\_Request and obtains a SUPI that is owned by an external entity, it may not be able to and need not to select an authentication method. In addition, the UDM may need to return information back to allow AUSF to use an AAA-E to authenticate the UE.

When AUSF receives Nudm\_UEAuthentication\_Get\_Response, it needs to be able to make decision to use an AAA-E to authenticate the UE.

AAA-E needs to derive KSEAF according to 3GPP TS 33.501.

There is no impact on UE side other than that the UE need to support the EAP method chosen by AAA-E for authentication.

### 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\*\*\***