**3GPP TSG-SA3 Meeting #101-e *S3-*** ***202890-r1***

**e-meeting, 9-20 November 2020**

**Source: CableLabs**

**Title: New solution for Key Issue #1 with enhanced security of KAUSF**

**Document for: Approval**

**Agenda Item: 5.12**

# 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 enhancing the security of KAUSF.

# 3 Detailed proposal

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

## 6.Y Solution #Y: EAP authentication between UE and external AAA with enhanced security of KAUSF

### 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).

It proposes a number of options to enhance the security of KAUSF, which may otherwise be derived solely from MSK received from an external AAA over interfaces outside the control of SNPN.

6.Y.2 Solution details

Figure 6.Y.2.1 - Derive KAUSF from MSK and RAND



Figure 6.Y.2.2 - Derive KAUSF from a new key exchange



Figure 6.Y.2.3 - Derive KAUSF from a new EAP authentication

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 sends an Access Accept messages to the AAA-P, including EAP Success, SUPI, and MSK.

Note that SUPI is needed since the SUPI received by AUSF in step 5 may be anonymous.

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

11-12. The AUSF performs additional steps to generate new keying materials to derive KAUSF.

In option 1 (see Figure 6.Y.2.1), the AUSF generates some random data (namely RAND) and derive the KAUSF from both the RAND and the MSK.

In option 2 (see Figure 6.Y.2.2), a new key exchange (e.g., Diffie-Hellman) is executed between the AUSF and the UE to derive new key materials to be used for deriving KAUSF. The MSK received from the AAA-E can be used to authenticate the key exchange.

In option 3 (see Figure 6.Y.2.2), a new EAP authentication is executed between the UE and the AUSF based on the MSK. For example, an EAP-TLS with PSK (preshared key) can be executed to derive a new MSK and a new EMSK. KAUSF is derived from the new EMSK.

13. The AUSF sends to the SEAF an EAP-Success message along with the SUPI and the KSEAF in a Nausf\_UEAuthentication\_Authenticate Response message. In option 1, the RAND is also included.

14. The SEAF forwards to the UE the EAP-Success message in an Authentication Result message or a Security Mode Command message, including ngKSI and ABBA. In option 1, the RAND is also included.

15. Upon receiving the EAP-Success message, the UE derives the KAUSF accordingly based on one of the three options in use.

### 6.Y.3 System impact

This solution has impact on UE, AUSF, and UDM.

When UDM receives Nudm\_UEAuthentication\_Get\_Request and obtains a SUPI that needs to be authenticated by an external entity, the UDM may not be configured with the authentication method thus may not return an authentication method to the AUSF. 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. In addition, the AUSF needs to perform additional steps to enhance the security of KAUSF.

UE need to support the EAP method chosen by AAA-E for authentication. In addition, UE needs to know how to derive KAUSF and perform additional steps to enhance the security of KAUSF.

### 6.Y.4 Evaluation

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

Editor’s Note: The security benefits from the proposed methods are FFS.

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